Department of Defense

MANUAL

NUMBER 8260.03-M-V1
November 20, 2009

USD(P&R)

SUBJECT: Global Force Management Data Initiative (GFM DI) Implementation: Unique Identification (UID) for GFM

References: See Enclosure 1

1. PURPOSE

a. Manual. Pursuant to DoD Instruction 8260.03 (Reference (a)), the authority in DoD Directive (DoDD) 5124.02 (Reference (b)), and in accordance with DoDD 8320.03 (Reference (c)), this Manual implements policy, assigns responsibilities, and provides procedures and rules for the electronic documentation of force structure data across the Department of Defense.

b. Volume. Volume 1 of this Manual sets forth responsibilities and procedures for the UID of force structure data in software application programs known as GFM organization servers (OSs) and includes:

(1) The generation of force management identifiers (FMIDs) for internal use by OSs.

(2) The integration into force management systems external to the OSs of that subset of FMIDs titled organization unique identifiers (OUIDs).

(3) Acquiring seed values for use as FMID prefixes from the Enterprise-wide Identifier (EwID) Seed Server (ESS), the chosen technical implementation for FMIDs.

2. APPLICABILITY. This Volume applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the “DoD Components”).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy to:

a. Electronically document and maintain currency of authorized force structure in a suite of authoritative data sources (ADSs), known as OSs, in a comprehensive and hierarchical format usable by systems across the Department of Defense as a common reference for data integration in accordance with Reference (a), and to ensure that force structure data is visible, accessible, understandable, and trusted across the Department as required by DoDD 8320.02 (Reference (d)).

b. Uniquely identify all GFM DI data and data relationships within these OSs by means of an FMID, in accordance with Reference (a).

c. Uniquely identify all DoD organizations external to the OSs by means of an OUID, in accordance with Reference (c).

d. Ensure that any tangible personal property or real property chosen by GFM components for inclusion in OSs be uniquely identified as specified in Reference (c) and its implementing DoD Instructions 8320.04 and 4165.14 (References (e) and (f)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. Procedures for implementing and managing the UID of force structure data across the Department of Defense are provided in Enclosure 3. Procedures for acquiring unique identifier seeds for use as FMID prefixes are provided in Appendix A of Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Volume is effective immediately.

Gail H. McGinn
Deputy Under Secretary of Defense (Plans)
Performing the Duties of the
Under Secretary of Defense
(Personnel and Readiness)

Enclosures
1. References
2. Responsibilities
3. UID Procedures for GFM

Glossary

TABLE OF CONTENTS

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 8260.03, "Organizational and Force Structure Construct (OFSC) for Global Force Management (GFM)," August 23, 2006
(b) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008
(c) DoD Directive 8320.03, "Unique Identification (UID) Standards for a Net-Centric Department of Defense," March 23, 2007
(d) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004
(e) DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," June 16, 2008
(f) DoD Instruction 4165.14, "Real Property Inventory and Forecasting," March 31, 2006
(g) Global Force Management Data Initiative Capability Development Document, Increment 1, January 28, 2008[1]
(h) CJCS Manual 3170.01C, "Operation of the Joint Capabilities Integration and Development System," May 1, 2007
(i) U.S. Federal Government Central Contract Registration, "The Central Contractor Registration User's Guide," July 2008[2]
(j) The Business Partner Network Federal Agency Registration Version 4.0 User's Guide for Federal Registrants, December 12, 2003[3]
(k) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009

[1] Copies may be obtained from the Internet at https://www.intelink.gov/wiki/Global_Force_Management_Data_Initiative/CCB
[2] Copies may be obtained from the Internet at http://www.ccr.gov/handbook.aspx
[3] Copies may be obtained by registered users from the Internet at https://www.bpn.gov/far/FARWeb.aspx

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) shall:

a. Require GFM Component OSs comply with the implementation of References (a), (c), (d), and this Volume, in coordination with the Heads of the DoD Components.

b. Within the OSD OSs, implement, maintain, and track via FMIDs all force structure data and relationships under OSD control, with the exception of force structure data under the purview of the Under Secretary of Defense for Intelligence (USD(I)).

c. Establish and maintain the OUID Registry.

d. Require only force structure data authorized under Reference (a) is used for any force structure representation in future human resource domain systems under OSD control as part of the certification process.

e. Coordinate with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the GFM OSs to require the OSs can accept and export unique item identifiers (UIIs) and real property unique identifiers (RPUIDs), as applicable, in their required formats in accordance with References (c), (e), and (f).

2. USD(AT&L). The USD(AT&L), in coordination with USD(P&R) and the Under Secretary of Defense (Comptroller)/DoD Chief Financial Officer, shall:

a. Ensure only force structure data authorized under Reference (a) is used for any force structure representation in other automated systems under USD(AT&L) control.

b. Ensure future data systems will use the OUID as the basis for DoD and non-DoD integrated business transaction management.

3. USD(I). The USD(I) shall:

a. Within the Defense Intelligence Enterprise OSs, implement, maintain, and track, via FMIDs, all force structure data and relationships under USD(I) control.

b. Ensure only force structure data authorized under Reference (a) is used for any force structure representation in future Defense Intelligence Enterprise systems as part of the certification process.

c. Assist the USD(P&R) in the implementation of this Volume.

4. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall:

a. Assist USD(P&R), USD(AT&L), and USD(I) where necessary to ensure OUIDs can be utilized across the Department of Defense with minimal data mediation needs.

b. As required by Reference (d), provide assistance as needed to ensure use of federated enterprise capabilities to publish metadata and to locate, search, and retrieve metadata and data.

5. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments shall:

a. Within the applicable Service OSs, implement, maintain, and track, via FMIDs, all force structure data and relationships under that Service's control.

b. Ensure only force structure data authorized under Reference (a) is used for any force structure representation in future Service systems as part of the certification process.

c. Assist the USD(P&R) in the implementation of this Volume.

6. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff shall:

a. Within the Joint OSs, implement, maintain, and track via FMIDs all force structure data and relationships under Joint Staff control.

b. Ensure only force structure data authorized under Reference (a) is used for any force structure representation in future joint systems as part of the certification process.

c. Assist the USD(P&R) in the implementation of this Volume.

7. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands shall:

a. Ensure only force structure data authorized under Reference (a) is used for any force structure representation in future Joint systems as part of the certification process.

b. Through the Chairman of the Joint Chiefs of Staff, assist the USD(P&R) in the implementation of this Volume.

ENCLOSURE 3

UID PROCEDURES FOR GFM

1. PURPOSE

a. The implementation of FMIDs is directed by Reference (a) to uniquely identify and tag authorized force structure data at all organizational levels of the Department of Defense. Additionally, Reference (c) directs that discrete data across the Department of Defense will use UIDs for the purposes of data discovery, correlation, and information sharing; that a standardized and common vocabulary will be adopted for UID entities; that internationally interoperable data exchange standards are to be used wherever possible; and that authoritative data sources, stewards, and accessibility requirements shall be designated by all DoD Components with UID responsibilities. As required by Reference (d), force structure data must also be visible, accessible, understandable, and trusted to DoD applications outside of the OSs with minimal or no data mediation requirements. The initial seven GFM Components establishing OSs are the OSD, the joint community, the Defense Intelligence Enterprise, the Army, the Navy, the Marine Corps, and the Air Force.

b. To those ends, this Volume establishes a comprehensive plan to manage FMIDs, and the FMIDs subset entitled the OUID, in accordance with the objectives of the GFM DI, to ensure authoritative force structure data is provided electronically in a joint hierarchical way for integration and use in a net-centric environment throughout the Department of Defense.

2. THE ROLE OF FMIDs WITHIN GFM

a. Overview. FMIDs are attributes that contain a unique identifier used to tag data defined within the GFM Extensible Markup Language (XML) Schema Definition (XSD). The GFM XSD provides the information exchange specification for force structure authorization data deemed to be minimally essential by the GFM community of interest, and made accessible to authorized users and applications via the data discovery services of a suite of GFM OSs. Data integration and deconfliction requires that all authorized force structure data be tagged with unambiguous, unique identifiers that comport to a DoD-wide standard for use in all force structure applications. FMIDs serve this function for all data within the GFM XSD, and thus all data exposed by the OSs, including organizations, materiel authorizations, billet authorizations, and relationships and associations between these entities in accordance with the requirements of the GFM DI Capability Development Document (Reference (g)).

b Characteristics. An FMID:

(1) Contains no encoded information about the entity it identifies.

(2) Is a fixed size.

(3) Is exchanged as a single attribute.

(4) Is operationally suitable as defined by CJCS Manual 3170.01C (Reference (h)).

c. Technical Implementation. The EwID is the identifier technology chosen for FMID implementation. EwIDs satisfy the FMID characteristics described in subparagraphs 2.b.(1) through (4) of this enclosure and are obtained from a centrally managed source known as the ESS. EwIDs and the ESS are fully described in Appendix A of this enclosure.

(1) The generalized hierarchy of the information exchange specification provides for the unique identification of all GFM XSD data with a minimal set of entities. The DoD Metadata Registry Uniform Resource Locator (URL) for the GFM XSD is: https://metadata.dod.mil/mdr/viewByNamespace.htm?selectedNamespace=GFMDI. For further guidance on accessing GFM DI artifacts, see the GFM DI Service Registration and Web Service Discovery section of the GFM DI wikipage on the Non-Secure Internet Protocol Router Network (NIPRNET)) Intellipedia, https://www.intelink.gov/wiki/Global_Force_Management_Data_Initiative.

(2) Within the GFM XSD, there are three subcategories of OBJECT ITEM: ORGANIZATION, MATERIEL, and FACILITY. When an OBJECT ITEM possesses the category code pertaining to an ORGANIZATION, then the FMID of that OBJ_ITEM, the OBJ_ITEM_ID, is the OUID for that ORGANIZATION. OUIDs are thus a subset of FMIDs and the GFM OSs are the ADSs for all DoD and National Guard OUIDs.

(3) Although the OBJ_ITEM entity may also be used by OS developers to document materiel or facility instances, this is not mandatory for GFM DI. All data (mandatory and optional) that populates the GFM OSs is tagged internally with FMIDs, but if such optional data is published external to an OS it will include the applicable UIDs for tangible property (UIIs) and real property (RPUIDs), per Reference (c), using an explicitly defined ALIAS within the GFM XSD.

3. FMID MANAGEMENT: GENERATION AND TRACKING

a. The management of FMIDs includes two basic services: generation and tracking.

(1) When an FMID is generated, an EwID seed prefix is acquired from the centrally managed ESS or a subordinate prefix owner and is concatenated with a locally produced suffix by an FMID Generation Service (FGS).

(2) FMID Tracking Services (FTS) provide the ability to track down the source of a data item by its FMID, based upon the tracking feature provided by the EwID technology.

b. There are no stipulations as to how these services are to be coupled with an ADS, only that the services exist and follow the defined protocols.

4. FMID GENERATION

a. Generating FMIDs using the EwID technology involves the acquisition of an EwID seed to be used as an FMID prefix as described in Appendix A.

b. FMID generation entails four responsibilities, which are described in section 7 of this enclosure.

c. The prefix is concatenated with a locally produced suffix by an FGS using EwID concatenation as described in Appendix A.

d. The full FMID and the data to which it is tagged are traced by an FTS (see section 5 of this enclosure) via a Web service.

e. FMID generation is completely under the control of the component OS Program Management Offices (PMOs) and may be partitioned and assigned as required. FMID generation may occur in any place or phase as determined by the OS developer. The number of FMID prefixes obtained to accomplish this is left to the discretion of the PMOs, and suffixes may be partitioned if deemed appropriate. These details are hidden from the outside consumer. Whichever approach is chosen by the PMO, it must be supported by the locally implemented tracking service.

5. FMID TRACKING

a. Introduction. It is plausible that data referenced by an FMID may not be included in a data payload that includes the reference. For this reason, an FTS allows the discovery of the data identified by an FMID. This is accomplished by tracking the FMID to its original ADS via a Tracking Service Locator (TSL) that contains either a URL or a Uniform Resource Name (URN).

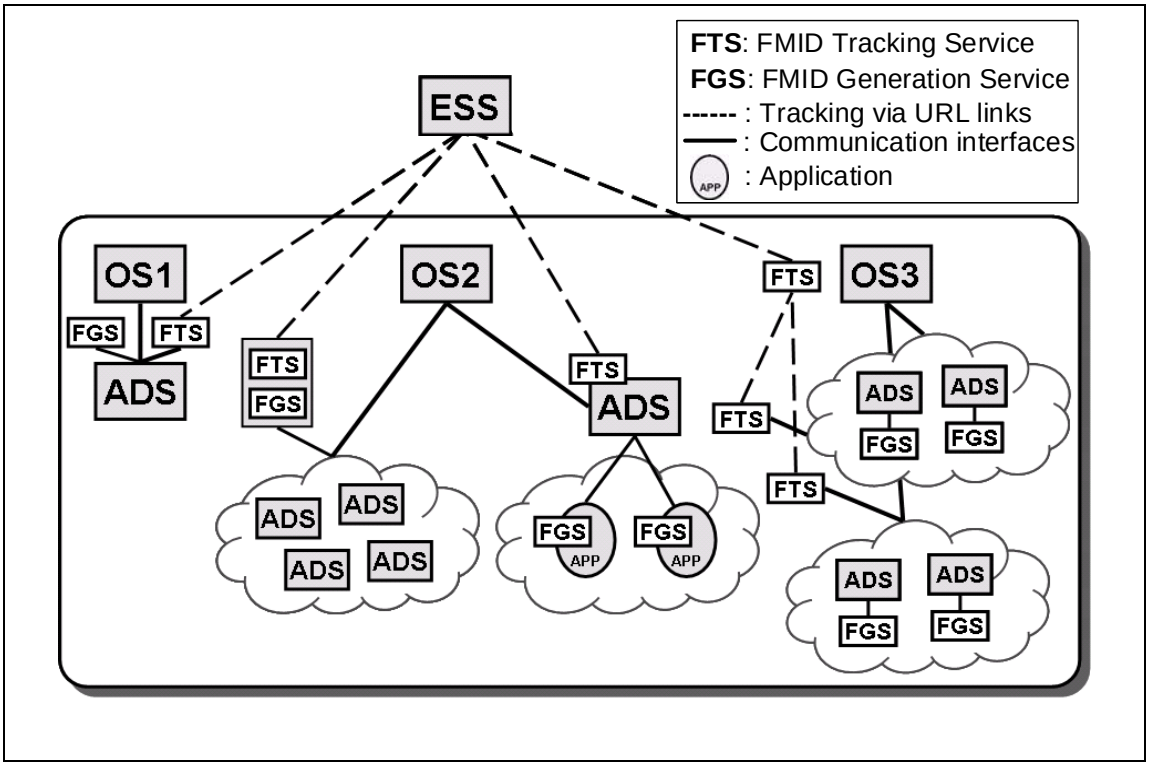
(1) FMID tracking includes FMID prefix tracking as a subset.

(2) An FTS returns information about an FMID upon request. The information may be about the owner of the data, the data itself, or further guidance as to how to locate the ADS (via a URL or URN) called redirection. The information may be resident within the source whose FTS has been interrogated, or it may reside in another source for which

one or more FTS redirections has occurred. This redirection may be hidden from the consumer. FTS design and placement is flexible and is the choice of the component OSs.

(3) Figure 1 illustrates some examples of alternative configurations for FGS and FTS placement for seed distribution. These examples are not complete, but for any chosen arrangement every node in the prefix redirection hierarchy must have its own FGS and FTS for its data source, whether that node is an OS, a subordinate ADS, or an application.

Figure 1. Example of Possible FMID Seed Distribution



b. FMID Tracking Service. FMID tracking can be initiated at any FTS. For external customers, tracking typically begins with a request to the ESS, which will forward the query to the next FTS in the sequence.

(1) An FTS request at the ESS will be forwarded to whatever URL or URN the EwID account holder has placed in the EwID TSL for that account. If no locator exists, only the account holder's submitted point of contact (POC) information will be returned. In the ESS, the tracking feature is invoked manually by the "Find EwID" command on the ESS Web site or the Tracking Service Locator function.

(2) As long as TSLs are provided, an FTS will continue to forward a "Find FMID" request. Eventually, the request arrives at the ADS where the FMID was generated to tag data. At this point, per discretion of the ADS owner, the FMID is identified in one of several ways:

(a) The FMID itself is identified as "Not Valid."

(b) The information identified by the FMID is returned to the requestor as governed by an FTS Web Service Description Language (WSDL).

(c) A refusal message is sent.

(3) This approach provides the FMID user with maximum flexibility in configuring and controlling its tracking service.

c. Tracking FMID Prefixes. The FTS may also provide information about the ownership of an assigned FMID prefix (EwID seed). Recall that FMID prefixes are allocated from the ESS. This information is controlled by the account holder. In the ESS, EwID seed account holder POC data is always returned, to include a TSL that the POC must provide.

d. Tracking FMID Data. All OSs or their subordinate ADSs or applications that incorporate an FTS must provide a lookup facility for querying themselves regarding the specific data that has been tagged by a particular FMID, as well as the TSL referencing any subordinate FTS of a redirected prefix. These FTSs will communicate with each other and the ESS via an FTS WSDL, though the interconnectivity will be transparent to those querying the ESS. Authorized systems querying the ESS will receive an answer from the end user as though the answer came immediately from the ESS itself.

e. ESS to OS Communication. When the ESS processes queries from an authorized requestor, it will either reply that the prefix in question has never been issued, and thus resides unused in the ESS seed pool, or the discovery service will be automatically transferred to the TSL to which the prefix was redirected, as provided in the ESS seed account. The ESS will provide a Web service to exchange data with any authorized system.

6. FMID STATUS DEFINITIONS AND MAINTENANCE

a. Mandatory Tracking. In the ESS, participation in the EwID tracking service is optional to non-GFM consumers. To manage FMIDs for GFM DI, however, participation is required. Once the OSs are established, TSLs will be populated to facilitate tracking of FMIDs. In this context, several status values have been defined.

b. Assigned and Redirected. Assigned prefixes may be used by an FGS to generate complete 64-bit FMIDs, or they may be redirected, or passed down, to a subordinate end user when generation occurs. There is no limit to the number of times that a prefix or FMID may be redirected to subordinate users. For a given prefix, the suffixes may also be partitioned into blocks of values, known as FMID blocks, and those blocks redirected to multiple other servers managing FMIDs. The only limit to which the same seed may

be partitioned is the number of the possible suffixes, which is 4.3 billion. However, every user that redirects a prefix or an FMID block must implement an accompanying FTS that ultimately locates the data to which the FMID has been applied.

c. Active and Inactive. Within an end user's FGS, seeds that are assigned or redirected are considered inactive by default until actually used to generate an FMID.

(1) FMIDs are generated by an FGS by concatenating a 32-bit locally controlled suffix to a 32-bit prefix. To ensure that the FTS will continue to search for an FMID regardless of how many times its prefix has been redirected, an FTS must mark redirected prefixes as active. However, to maximize flexibility, these implementation details are left to the FMID user.

(2) A safe approach is for an FTS to always mark redirected prefixes or redirected FMID blocks as active to ensure the tracking process continues. Using this scheme, only the last FTS, where the FGS is often collocated, would mark an inactive prefix as such. Then, when the prefix is used to generate FMIDs, only the last FTS in the chain has to set the prefix (or FMID block) to active. To implement this FMID management approach, an EwID seed is marked active in the ESS when it has been assigned to an EwID account holder for the purpose of generating FMIDs, regardless of whether it is subsequently used. This will ensure that all FMID tracking queries will be forwarded to the next level (indicated via the TSL) for processing. Alternatively, an FMID prefix is considered to be inactive at the end user level if it has never been used to generate an FMID. Each ancillary server from which the seed has been redirected also marks the seed as active until the final end user in the redirection chain has been reached. At the end user, a seed is considered active once a single FMID has been generated from that seed. The purpose of the designation "active," therefore, is to inform an interrogator of the tracking service either that their tracking query needs to be forwarded to the next level in the chain of redirection or that the last link of that chain has been reached and the seed has been used to generate FMIDs. Whether or not the generated FMIDs have been used to tag data that has since become published, and is thus visible outside of the end user's own system, is not part of the definition of active as it pertains to an FMID prefix.

(3) At an end user's ADS with an accompanying FGS, the "inactive" status of an assigned or redirected FMID prefix is the default nature of that prefix until further action is taken. Depending upon the implementation scheme used, seed activation (upon commencement of FMID generation) could require coordination with the ESS and all subordinate ADSs to which the prefix becomes redirected. It is thus the responsibility of all FMID owners at every link in the prefix redirection chain to ensure that their prefix(s) and their fully linked FMIDs are managed and traceable, and that status and tracking information is responsive to enquiries from authorized requestors.

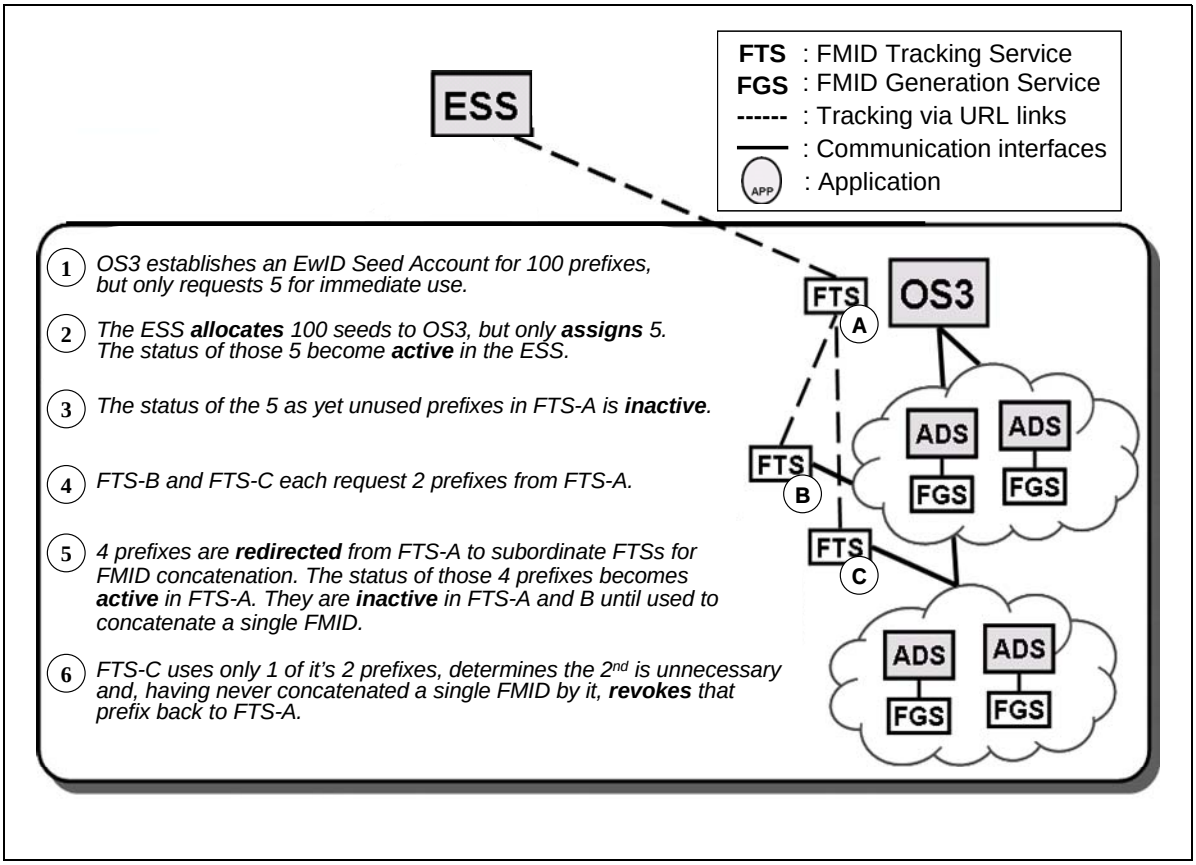
d. Prefix Revocation. It is possible that an end user acquires more prefixes than it ultimately requires. A prefix that has never been concatenated to generate a single FMID may be returned to the source from which it was immediately obtained for redirection

elsewhere, to include redirection to a more senior server. Such a prefix is said to have been revoked.

(1) Note that this is not the prefix's status, however, which remains inactive at each new end-user level to which the prefix is revoked, even back to the ESS itself. Seed status at any new end user level would only change to active through an end user's generation of an FMID using that prefix.

(2) Therefore, a prefix once activated by an end user in the generation of an FMID may never be returned to inactive status. A prefix once activated by an end user may never be revoked. However, a prefix once labeled as active within an intermediary server may return to inactive status if the prefix is revoked from a server subordinate to it. Figure 2 illustrates the use of FMID distribution terminology.

Figure 2. Definitions for FMID Seed Distribution



e. FMID Persistence. Whenever data is formatted in accordance with the GFM XSD, it is tagged with an FMID that remains with that data perpetually. FMIDs are never reassigned from one entity to another. Even when data becomes obsolete, the FMID tagged to that data is retained to enable the work of discovery services inside of historical archives.

7. OS RESPONSIBILITIES

a. OS Coordination with the ESS. Every OS must subscribe to the ESS.

(1) ESS subscribers must agree to four criteria, three of which reiterate current requirements for holders of ESS user accounts, while the fourth is FMID-specific. Users:

(a) Ensure contact information remains accurate, including the currency of the TSL. The ESS TSL provides the initial location to begin the search for the ADS that has responsibility for an assigned FMID.

(b) Produce concatenated FMIDs of 64-bit length, using only the prefixes received from the ESS.

(c) Maintain a mechanism to ensure FMIDs are never duplicated, to include an emergency backup scheme in case FMID generation and tracking become interrupted.

(d) Will be able to exchange FMIDs per the GFM XSD.

(2) Programmatic communication beyond the OS TSL level is handled internally by the OS PMO, though this is transparent to those querying the ESS.

(3) Internal OS communication must be sufficient to reliably track prefix redirection and FMID generation for the OS to respond to data queries from any authorized system, whether requested directly or through the conduit of the ESS.

b. Intra OS Communication. In support of the expanded services of the FTS, each OS shall generate FMIDs for all data items identified within the GFM XSD. An OS will generate FMIDs utilizing only those prefixes tracked by the FTS.

(1) It is the responsibility of the OS PMO to ensure FMID suffixes are not duplicated by any FGS that populates the OS.

(2) This vigilance requires the presence of an internal tracking service for every OS that:

(a) Ensures intercommunication with all FGSs subordinate to the OS.

(b) Ensures the uniqueness of each FMID it generates.

(c) Provides POC information about all FTSs and FGSs.

(d) Provides a lookup service to search for locally generated data by its FMID in support of the expanded services of the FTS.

(3) Internal OS data exchange will be conducted in accordance with the WSDL approved by the GFM DI Configuration Control Board.

c. Extra OS Communication. All data exchanged from OSs with consumers shall retain its originally assigned FMID.

(1) The sending OSs shall include an identification tag to enable the identification of the OS and, if applicable, the originating ADS that populated the OS.

(2) The OSs will provide Web services to exchange data with any authorized external system in accordance with the WSDL approved by the GFM DI Configuration Control Board.

8. FMIDs ACROSS SECURITY DOMAINS

a. The FMID design characteristic, being unintelligent, does not include any information as to classification of the entity or relationship to which it is tagged. However, an FMID shares the classification of the data object it tags and should be handled accordingly. OSs will generate FMIDs for unclassified NIPRNET and classified environments (SECRET Internet Protocol Router Network (SIPRNET) or higher domains). Beginning with the unclassified security domain, OS data will be replicated to OSs in the next higher security domain (e.g., NIPRNET to SIPRNET) via a cross domain solution (CDS) that supports the FTS.

b. Data should always be originally created in the domain commensurate with its classification, and all attributes assigned to that data should share that classification, to include the FMID. As one progresses up, or across, the security domains, OSs will contain an ever increasing overall representation of DoD organization data in a consistent manner. Therefore, unclassified data shall always be created on the NIPRNET for replication to higher security domains, where the original FMID is retained. This means that unclassified data will always be tagged with FMIDs derived from the unclassified ESS, and integrated on higher security domains with classified data.

c. The GFM XSD partitions data into sufficiently small elements that, once integrated on a higher domain, all unclassified data need not be marked classified commensurate with that higher domain. A “system high” security policy, if applicable, will consider all data classified commensurate with the domain on which it resides, regardless of data origin. FMIDs used to tag Secret data are to be considered Secret and share the same metadata security label as the data itself.

d. OSs will have to create data in their resident security domain, thus requiring an ESS at each domain. The ESS CDS will include the capability to track EwIDs assigned to higher domains, though not what they identify, and those that have been imported to the current domain from a lower domain. The actual tracking of what FMIDs identify is accomplished by the ESS at each domain. An FGS can obtain EwID seeds from the ESS

at that security domain and operate in the identical manner as it does at the lower domain. FMIDs generated at a higher security domain will not be passed to the lower domain without being scrutinized as would any data crossing to a lower security domain. FMID pedigree and security metadata information will be transmitted with the data element for tracking purposes.

e. If universal description, discovery, and integration (UDDI) services are provided on the utilized networks, then every TSL will use a URN. A URN can span many networks and be mapped to different URLs in each network UDDI registry.

9. OUID CONCEPT OF OPERATIONS (CONOPS)

a. In GFM DI, the vernacular of military organization is mapped to the terms used for a graph. The nodes are called organizational elements (OEs). OEs are aggregation points based upon leadership. Every internal OE must have a designated leader.

b. As discussed in section 2 of this enclosure, the generalized hierarchy of the information exchange specification provides for the unique identification of all GFM XSD data with a minimal set of entities. When the attribute OBJ_ITEM_ID possesses the category code pertaining to the subtype ORGANIZATION, that FMID also serves as the OUID for that OE.

c. All DoD and National Guard OUIDs originate in the OSs as the OBJ_ITEM_ID, whereas non-DoD organizations that are part of the force structure, such as State governments or coalition partners, will be entered or interfaced via the OSD that will transmit the data to the OUID Registry. The OUID Registry will be initially populated only with organizations of the category code for unit and will expand when required to support the other organization subtypes.

d. The OUID Registry serves as a central repository and tracking service that supports integration of OUIDs from DoD and extra-DoD sources, as well as supporting cross-referencing with extant organization identifiers and names in use by legacy systems. Embedded non-DoD organizations that already have widely-used legacy identifiers will be documented in the OSD OS and will be assigned an OUID, but the legacy identifiers will still be readily available for use in DoD consumer systems.

e. Each OUID represents only one OE. The OUID will be used in system interfaces and reporting across the DoD warfighting mission areas, not to supersede but to complement existing accepted international interoperable data exchange standards for globally unique identification of organizations. The OUID will be integrated into all new systems that share organizational information. While each organization will have only one OUID, the OUID Registry will have the capability to support a series of crosswalks between the OUID and the legacy organization identifiers, which will be maintained by those legacy systems to support OUID use by those systems on interfaces and in reporting.

f. The OUID does not replace existing international interoperable data exchange standards, but compliments them to facilitate their use across the Department of Defense. It will not replace identifiers used to support existing policies, agreements, and practices external to the Department of Defense (e.g., Treasury Code or Data Universal Numbering System (DUNS)) or internal to the Department of Defense (e.g., Unit Identification Code (UIC), Personnel Accounting Symbol (PAS), or Reporting Unit Code (RUC)).

g. For non-DoD organizations with financial relationships to the Department of Defense, there are two ADSs to be used:

(1) The ADS for current and potential government vendors doing business with the Department of Defense is the Central Contractor Registry (CCR) maintained by Defense Logistics Agency. The primary identifier used by the CCR is the DUNS. All DoD vendors are also required to have a Commercial and Government Entity code. The CCR also contains the vendor's Tax Identification Number. Each of these identifiers is used based on their existing international and national accepted usage according to The Central Contractor Registration User's Guide (Reference (i)).

(2) The ADS for Federal trading partners for intragovernmental transactions such as fiduciary, exchange, and non-expenditure transfers, is the Federal Registry (FedReg), which is part of the Business Partner Network. The primary identifier used by the FedReg is the DUNS. The FedReg also contains the Treasury Index Agency Code, Agency Location Code, and Disbursing Office Symbol. Each of these identifiers will continue to be used based on their national and international applicability according to The Business Partner Network Federal Agency Registration Version 4.0 User's Guide for Federal Registrants (Reference (j)).

h. Vendor and trading partner organizations are not part of the authorized force structure. Only contractor or outsourced capabilities are stored in the OSs. Therefore, the identifiers contained within the CCR and FedReg could be stored in the OSs for those associated non-DoD organizations that require identification in the force structure. Associated non-military organizations that are neither in the CCR or the FedReg, nor have an ADS, could be entered in the OSD OS. The OSD OS would then feed the OUID Registry. If an ADS is identifiable, that ADS could feed the OUID Registry directly, once permissions are established. One example would be coalition partner organizations from a North Atlantic Treaty Organization system.

10. OUID PROPERTIES AND RULES

a. Properties. An OUID will have the following properties:

(1) An OUID is from the set of FMIDs that identify OEs for DoD organizations (see section 2 of this enclosure). Only those FMIDs generated in the organization table element of an OS are OUIDs.

(2) An organization can have only one OUID. Since the OUID uniquely identifies a specific OE that serves as an aggregation point of other force structure data, it is indirectly referenced by many attributes (from the GFM XSD) that are contained in the OS, such as the formal name, derived names, and nicknames. This enables the cross-referencing of disparate naming conventions and aliases for the same organization. For example, the same OUID could tag the various methods of referencing the First Infantry Division: 1st Inf Div, 1st ID, 1ID, and The Big Red One. Additionally, broader alias information (i.e., other ways systems reference those units) will exist in the OUID Registry. There will be a check to ensure that:

(a) An OUID is assigned to only one organization.

(b) An organization has not been assigned more than one OUID at any one time.

(c) An OUID is not reused.

b. Rules. The complete set of attributes for an OE are not isolated to the single GFM XSD OBJ_ITEM element, but rather are grouped into logical sub-entities, each with their own FMID. The GFM XSD has been specifically designed so that changes to an OE occur in entities other than the OBJ-ITEM to minimize changes to an OE's OUID. This design tenet is referred to as OUID Retention and is a key feature of the GFM XSD induced by the fact that external systems will associate their data with the OUID.

(1) OUID Retention

(a) A consequence of the GFM DI concept of OEs is that a unit is defined by its parts, and not, as traditionally has been the case, as a single entity such as a UIC. A UIC represents, in tree graph terminology, the set of the parent OE and all of its descendant OEs, each identified by an OUID, and the links to them. Therefore, a change in a parent OE's OUID does not imply changes in any OUID of the descendant OEs if their inherent attributes have not changed.

(b) The Organization Start Date and Organization Termination Date-Time-Group (DTG) will identify when an organization is active. The move from one fiscal year (FY) to the next does not necessitate a change in OUID, since an OE may span many years and that duration could be set into the far future. Changing an existing termination DTG attribute for an OE does not necessitate a new OUID. For example, if an OE had been previously slated to expire at the end of the current FY and the DTG was thus changed to extend it, then a new OUID is not required.

(c) When an OE's termination DTG has passed, the OUID and associated organization information will be retained for historical purposes. An archival process and time interval will be defined based on the hardware configuration, storage capacity,

and response times where the archived data will be available for access, but with a longer request and response time than for the OUID Registry.

(d) As the attributes of an organization authorization change (e.g., due to reflagging or a formal name change such as CENTAF to AFCENT), the OS PMO must determine if the altered OE requires a new OUID. When an OUID change occurs in the force structure documented in the OSs, updates will be provided via a publisher-subscriber process to which the OSs will publish and OUID consumers, including the OUID Registry, will subscribe.

(2) Joint Billet OUID Management

(a) Billets are OEs and billet OUIDs are to be managed by the ADS for that billet's authorization, with the ADS defined as the OS that manages or processes the majority of that billet's activity.

(b) The Joint OS is the ADS for Service Billets under CJCS authority.

(c) The OSD OS is the ADS for Service Billets under OSD authority.

(d) The Defense Intelligence Enterprise OS is the ADS for Service billets within Defense Intelligence entities that are external to Service organizations (e.g., the Combat Support Agencies).

11. THE OUID REGISTRY

a. The OUID Registry supports the GFM process by integrating OUIDs from the DoD OSs with organizational identifiers about non-DoD government and non-government organizations. It also provides the means for DoD systems to map their current identifiers to the proper organization.

b. The OUID Registry is an integrated repository for OUID information and serves as a gateway for obtaining and managing OUID information. It will:

(1) Maintain the OUID for DoD organization data obtained from Service, joint, Defense Intelligence Enterprise, and OSD-level OSs and other ADSs.

(2) Maintain the OUID for identified non-DoD organization and non-contractor data that is a part of the force structure, such as foreign government organizations or foreign military alliances. The OSD OS will be the ADS, unless another ADS is identified. These organizations can be manually entered into the OSD OS.

(3) Allow identified ADSs to update the registry with alias identifiers and/or names.

(4) Provide the means to include organization attributes when, and only when, the attribute is required to identify an organization in an ADS or to "lookup" an OUID.

(5) Only include identifiers commonly used in multiple systems, as determined by the OUID Registry ADS Panel (see section 12 of this enclosure). If an identifier is internal to only one system, it will not be included in the registry. If necessary, the specific system can maintain its own internal identifier mapping to the OUID.

(6) Provide the means of granting permission to create and update registry information, including alias information, for each ADS.

(7) Provide the means of obtaining and maintaining required POC information for each ADS.

(8) Conduct reviews via the Registry ADS Panel to evaluate the requests for a system to become an ADS for either the organization and/or alias information.

c. The OUID provides a single identifier type for all DoD organizations that can be mapped to any alias identifiers via the OUID Registry, regardless of any variances in the type of the alternate identifiers.

d. The OUID Registry will validate the OUIDs on a periodic basis (e.g., monthly), determined by validation processing time, resources, and frequency of error detection. The validation could be broken up with a subset on each weekend of a month. There will be a check to validate that:

(1) A suffix does not overrun a prefix.

(2) The prefix is registered to an FGS.

(3) The OUID is unique.

(4) A new prefix is "active."

(5) An OUID and Organization Name pair are correct with the ADS. If there have not been any changes to the organization information in the prior 3 months, then the ADS will be queried for the OUID, Organization Name, and start and termination dates to verify the organization information is correct.

e. The OUID Registry will have the capability for an ADS to link an alias organization identifier to an OUID.

(1) If an alias is used by more than one system, the crosswalk between the OUID and alias should be maintained in the OUID Registry by the ADS that assigned or is responsible for that alias within the Department of Defense.

(2) The OUID Registry alias capability will also allow an alias name to be mapped to an OUID from an identified authorized ADS, if the alias name is used outside the ADS.

(3) If there are any issues with the existing alias organization identifiers, such as multiple identifiers of the same type assigned to one organization or one identifier assigned to multiple organizations, these issues will be reflected in the crosswalk between the OUID and the alias identifier. A query using an alias with issues could result in a response with more than one organization.

f. A POC will be identified for each ADS for the organization data and alias data.

(1) Periodically (e.g., every 6 or 12 months), the POC information will be verified. If the POC information is invalid, permissions for the account will be locked or inactivated until current POC information is provided.

(2) If there have not been any updates to the organization information for a pre-defined period (e.g., 6 months or 12 months), there will be a prompt to the POC to validate the information.

g. The OUID Registry will not contain any of the organization relationship or structure information, unless that information is embedded in the construct of a set of aliases. The OUID can be used for accessing GFM OS data to obtain additional organization data, and organization relationships and structure. In addition, an OUID can be used to provide the capability to access additional relationships managed outside of the OSs through other business enterprise systems (e.g., financial relationships maintained by the systems supporting the Standard Financial Information Structure (SFIS)).

h. When an OS is queried by the OUID Registry about an OUID, it will provide all alias names and identifiers contained in the OS for the identical FMID. This includes organization formal names, organization nicknames, abbreviations, or identifiers (e.g., UIC or PAS).

i. A user or system can request the following OUID Registry information:

(1) An OUID based on an Alias Identifier.

(2) An OUID based on an Organization Name.

(3) An Alias Identifier based on an OUID.

(4) An Organization Name based on an OUID.

(5) An ADS for an OUID based on an OUID.

(6) An ADS for an Alias Identifier based on an OUID.

(7) An ADS for an Organization Name based on an OUID.

(8) A POC for ADS based on System UID.

j. In case the input request returns multiple results, a set of data attributes (e.g., start and termination dates) will be returned to allow the user or system to distinguish the correct one.

12. OUID OPERATION AND MAINTENANCE OVERVIEW

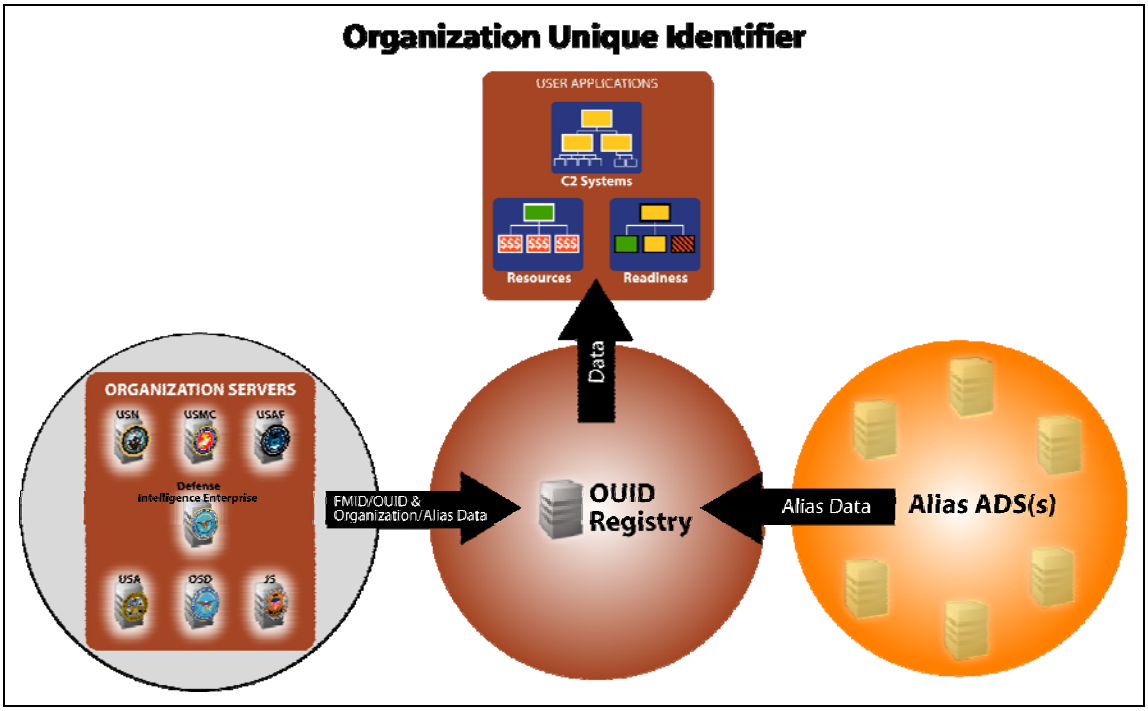
a. OUID Registry Processes

(1) Initial Registration and OUID Generation. There will be a close relationship between the OSs and the OUID Registry for DoD organizations, as depicted in Figure 3. When an OS creates a new organization, the data for the organization must be made available in GFM XSD format and tagged with an FMID (OBJ_ITEM_ID) within the appropriate OS. This FMID will be the OUID for that organization. Upon generation of the FMID, it and the related organizational data will be provided to the OUID Registry on a subscription basis.

(a) If no ADS exists for an organization, the data will be manually entered and maintained in the OSD OS and transmitted to the OUID Registry, by a user with the appropriate permissions and access.

(b) All new systems will store and use OUIDs when exchanging DoD organization information. A legacy system is not required to store the OUID internally, but the system will need to use the OUID on information exchanges. For example, legacy systems that assign equipment or personnel to force structure, or utilize SFIS data, will use the OUID when sharing this data outside its family of systems (e.g., operational command and control systems). One option is for the ADS to map its internal identifiers to the OUIDs in the interface translation layer. Another option is to use the OUID Registry crosswalk to look up the OUID and an alias.

Figure 3. OUID Registry and ADSs



(c) The OUID registry will have the capability to allow an approved ADS to map its organization identifier to the OUID and to have this mapping available for other systems to use. If that identifier is widely used in other legacy systems, it should be linked as an alias to the OUID within the OUID Registry, providing other legacy systems access to this mapping. An OUID Registry ADS Panel will review requests from a system POC for that system to become an organization and alias ADS. The panel will review the interface mechanism, and identify and resolve possible conflicts with existing ADSs. Once approved as an ADS, the system administrator will grant the appropriate permissions to the ADS.

(d) When an organization is de-activated, disestablished, disbanded, or closed, the organization termination date needs to reflect this action. Organizations will not be physically deleted from the OUID Registry for historical purposes. The original OUID will be used if an organization is re-activated, unless policy directs that a new OUID be generated. The method to archive historical data and the method to access this data will be based on the hardware configuration, storage capacity, and response times.

(e) There will be an automated method to verify that the FMID prefix is valid in the FGS. Based on performance, this check could either run periodically or in real time.

(f) Once an organization is entered in the OUID Registry, an approved ADS for an alias will have permission to create an alias for that organization. The alias can be a name or an identifier. The alias identifiers will include alias start and termination dates, source system information, and source system POC information.

(2) Registry Maintenance and Change of Organization Information. An organization ADS is required to keep the organizational data in the OUID Registry current. Updates to the OUID Registry of organization data from the OSs will be provided on a subscription basis. The method for updates from other ADSs will be defined based on that system's data access rules and procedures. If the data is available using a "publish and subscribe" implementation, the organization data will be provided to the OUID Registry when it is changed or deleted. If the system does not have a "publish and subscribe" capability, interface agreements will be developed for changes or deletions to the organization data. There will be a standardized data interface capability available to address this need.

(a) Since an organization's aliases may come from different ADSs, the updates to alias information must only come from an alias's ADS. For example, if the OUID Registry has both the UIC and the Operating Agency Code (OAC), Operating Budget Account Number (OBAN), and Responsibility Center/Cost Center (RCCC) for an organization, only the ADS for UIC would be able to update the UIC information, and only the ADS for OAC, OBAN, and RCCC would be able to update the OAC, OBAN, and RCCC information.

(b) Like an OUID, an alias will have start and termination dates. These dates support changes to aliases or alias-types (e.g., when the Marine Corps changes from Monitored Command Code (MCC) and RUC to UIC).

(c) The POC of an ADS for an alias type will need to request alias creation, modification, and deletion permissions for that system. The OUID Registry ADS Panel will evaluate the request for approval or denial. The OUID Registry administrator will monitor the maintenance of the alias and access history of the alias to determine how and if the alias is used.

(d) The deletion will be a logical deletion, implemented only by setting the alias termination date. The type of organizations available to the ADS to update will be determined based on the request. For example, the ADS might only be responsible for the aliases of Marine Corps organizations and therefore limited to only Marine Corps organizations in the OUID Registry.

(3) Inactivation of an Organization in the Registry. A full history will be maintained by the OUID Registry that will allow time-based queries to view and report historical information. The history will include the old values, the date the value changed, and who changed the values. All OUID Registry sets of data will have start and termination dates to support time-based viewing and reporting of data. Within the OUID Registry, a deletion is a logical delete based on setting a termination date, which means that the data is not physically deleted from the database. The organization termination date will be used to indicate if an organization is activated or deactivated. An archival process and time interval will be defined based on the hardware configuration, storage

capacity, and response times. The archived data will be available for access but with a longer request and response time.

(a) The initial load of the OUID will not include prior organization historical data. When an organization is populated in the OUID Registry, it may have an organization termination date, such as for temporary organizations. The OUID Registry will store all valid data that an ADS provides.

(b) The capability to perform a physical delete will be limited to the system administrator. The system administrator will only use the delete capability on rare occasions to back out OUID Registry error conditions such as the partial processing of an ADS transaction because of a power failure.

b. OUID Registry Roles and Permissions. The OUID Registry will include the rules necessary to assign access and permissions that define who is allowed to create, read, update, and delete organization data.

(1) A roles and access list, which is submitted, maintained, and approved by DoD Component designated organization(s) and/or personnel, will be established and maintained to support this process.

(2) The ADS for an organization will be required to provide the OUID Registry with up-to-date organization information. There will be procedures to validate the organization information. If the information has not changed in a pre-defined period of time (e.g., yearly), the ADS or the POC of the ADS will be prompted to verify that the information is correct and current.

c. OUID Registry Configuration Management. The configuration management process will be used to add attributes, code values, and validation rules to the OUID Registry as needed. Any changes to the OUID Registry will be coordinated with the ADS, as appropriate, to keep the efforts coordinated.

d. OUID Registry Backup and Recovery. The OUID Registry backup and recovery requirements will be defined and the appropriate procedures will be implemented by the developer. As part of the recovery process, any additional steps to re-retrieve organization data from the set of ADSs will need to be included. Redundant OUID Registry instances could be used to ensure availability.

13. OUID IMPLEMENTATION OVERVIEW

a. The OUID provides the means for the Department of Defense to migrate to the use of one organization identifier across the DoD enterprise for information discovery and sharing in the net-centric environment as part of a service-oriented architecture in the Global Information Grid.

b. Note that the OUID will not supersede, but rather complement, existing accepted international interoperable data exchange standards for globally unique identification of organizations.

(1) New System Implementation. All new systems requiring force structure data will be developed with the capability to use OUIDs within that system and to use it when interfacing organization information.

(a) The implementation of the use of OUIDs across the DoD enterprise will be in accordance with the system processes as outlined in applicable DoD and Component directives and system technical direction. The OUID Registry provides the means to implement the use of OUIDs with the least amount of impact on current and future systems.

(b) If the rules for generating and maintaining the OUID are followed, then an OUID will identify only one organization uniquely across the DoD enterprise. This will provide the means to access the different types of organizational data stored in different ADSs with the same identifier without maintaining look-up, crosswalk, or conversion tables.

(c) Current policies, practices, and agreements with organizations outside of the Department of Defense may still require the use of other organization identifiers (e.g., UIC, PAS, or RUC) in addition to the OUID, some of which will be included in the OSs. The OUID Registry provides a mapping capability to other organization identifiers, as needed. If a system does not share data across the DoD enterprise but only communicates within a stand-alone family of systems using existing accepted international interoperable data exchange standards for globally unique identification of organizations, then the OUID may not be needed.

(2) Legacy System Implementation. Legacy systems can fully implement the OUID as the single organization identifier within their system. They may also look up the OUID based on organization aliases and use the OUID when interfacing organization information. The objective is to minimize the impact on legacy systems by providing the most efficient means of incorporating the use of OUIDs into these systems. If there is a requirement to allow the ADS to link existing organization identifiers (e.g., UIC, PAS, or RUC) to the OUID, then the look-up process will allow legacy systems to use the OUID on interfaces by providing a crosswalk between the organization identifier used in the system and the OUID. If an organization identifier is or could be used by more than one system, that identifier should be mapped and maintained in the OUID Registry by the ADS for the identifier. If only one of the systems uses that organization identifier (e.g., an internal identifier), then the mapping does not need to be maintained by the OUID Registry, but can be maintained locally by that system.

(3) General System Implementation. The OUID Registry will utilize the DoD Metadata registry for the OUID data element definitions and attributes and the XML schema to identify and understand the organizational data. XML is a general-purpose

markup language for creating special-purpose markup languages, capable of describing many different types of data.

(a) Legacy systems will use the DoD data and XML registries, OUID Registry catalogs, and OUID Registry search services in conjunction with OUID Registry security levels and access control levels to access organizational data stored in the OUID Registry.

(b) If a system receives OUIDs from systems other than the OUID Registry, periodic checks should be performed to ensure these OUIDs are valid in the OUID Registry. If possible, a system should know the pedigree of the OUID and the source of the OUID to ensure that the system has current OUIDs and to aid in conflict resolution.

14. OUID TRACKING

a. Since the OUID is a subset of FMIDs, the FTS will be used to identify the source of the data. The ESS EwID TSL (see Appendix 1 of this enclosure) can identify who registered an FMID prefix (or EwID seed) and allows a URL or URN to be provided to reach the system that generated the FMID. The TSL will re-direct a query to the system for information about the FMID prefix. If a tracking URL is not provided by an account holder, then a user can query the ESS for the POC information.

b. When the ADS for an alias organization identifier requests access to the OUID Registry, the request or interface agreement will include a system identifier, TSL, and POC information. This information will be used to track an alias identifier from the OUID Registry back to the ADS.

Appendixes

1. ESS CONOPS
2. OUID Structure

APPENDIX 1 TO ENCLOSURE 3

ESS CONOPS

1. PURPOSE. The EwID is the technological schema chosen by the Department of Defense to implement the use of FMIDs across the DoD enterprise to uniquely identify force structure data via the GFM XSD. This appendix describes EwID properties, implementation, and tracking from the centrally managed ESS.

2. PROPERTIES OF UNIQUE IDENTIFIERS

a. In any system of information sources, a critical feature is the ability to link together disparate pieces of data and information via relationships. One way to facilitate this task is to provide a common technique for identifying the pieces so that they can be conveniently referenced. Arbitrary linking of data can be accomplished by standardizing one field across disparate data sources. This is the objective of unique identifiers. If data can be identified using a common scheme, then one can spontaneously reference and relate arbitrary pieces of information with minimal prior coordination.

b. There are four preferred properties associated with unique identifiers. The first two are general and the second two are specific.

(1) No Embedded Intelligence. It is an accepted practice in computer science and the construction of data sources (DSs) that an identifier should be used with no intelligence embedded within it. Usually, this will be the primary identifier for the data. This property makes the identifier invariant to future changes to the data itself. In other words, one should not create identifiers with embedded meaning because, sooner or later, the requirements for the meaning may change, thus requiring massive adjustments to the identifier management scheme. Therefore, no information about the data being tagged should be gleaned from the identifier.

(2) Be a Fixed Size. To facilitate ease of implementation for software developers, the identifier should be a fixed size common to the computing hardware. Often, within in computing systems, these are a number of bytes (8 bits) that are a power of two (e.g., 1, 2, 4, 8, 16 …). As computing machines become more sophisticated, this number often increases (e.g., in 2005, state-of-the-art processors can handle 64-bit (8 byte) instructions; consequently, it is desirable for the operating system software to handle this size data).

(3) Actual Size. To implement a unique identifier, a size must be selected. There are several factors to be considered in selecting a size beyond being convenient for the computer hardware. Preeminent among these is the size of the required (and future required) address space that dictates how many entities can be uniquely tagged.

(a) The size of an EwID is 64 bits.

(b) The difference between the internal storage of this data structure and how it may be presented is often misunderstood. There is no intrinsic meaning to the 64 bits that comprise an EwID other than it is a unique sequence of bits. An EwID may be presented in many ways, normally based upon the application that contains it. Common presentation types are character strings and decimal integers. A common way to represent a sequence of bits is called hexadecimal (or hex) notation. In hex notation, 16 characters are used to represent the 16 unique patterns of four bits. Therefore, the 16 characters 0-9 and A-F are used to denote the 16 combinations of four bits: 0000 through 1111. This allows a 64-bit EwID to be represented by 16 hexadecimal characters; it is a coincidence that hexadecimal notation also contains 16 characters. Hex notation is favored over decimal, integer representations because it is the least ambiguous of any notation, thus causing fewer translation errors. When decimal notation is used it shall be interpreted as an unsigned integer, meaning that the lowest decimal value is 0 (represented by 64 zero bits) while the highest value is 18 billion-billion (represented by 64 one bits). A common mistake is to call an unsigned 64-bit value a 20 digit value. Although it takes 20 digits to contain the decimal number of 18 billion-billion, a 20 digit number can be as large as 20 nines, or 99 billion-billion. Therefore, if a 20 digit, unsigned number is used to contain an EwID, it must be restricted to the value 18 billion-billion or less.

(4) Allocation Scheme. Unique identifiers must be allocated and distributed among the users. Allocation strategies can be categorized as centralized or decentralized. In a centralized scheme, part of the unique identifier is controlled by an external authority. This requires that a site external to the user be visited to obtain part of the unique identifier, and it is this centrally managed portion of the identifier that ensures uniqueness across the enterprise. In a decentralized scheme, the unique identifier is created completely locally. This strategy requires a scheme that, with a very low probability, will allow two independent users to generate a duplicate value. The probability must be so low that the values can be considered universally unique. A decentralized scheme has the major advantage that the user is independent from any centralized service that may slow down the allocation process; however, the cost is a larger identifier size and a more complex generation scheme.

3. PROPERTIES OF DATA SOURCE KEYS AND IDENTIFIERS

a. Within data sources, different techniques may be used to accomplish the task of identification. The technical details depend on the type of database, or model, used. The two most common are the relational and object-oriented model that identify items using primary keys (PK) and object identifiers, respectively. A major accomplishment toward interoperability would be the acceptance of a common identification scheme that spans both of these data storage technologies.

b. In the relational model, data is stored in tables with attributes (i.e., columns), and the rows of a table may represent an entity or a relationship between entities. Every row of a table must be uniquely identifiable. A candidate key is a set of attributes that accomplishes this task. There may be several candidate keys for the rows of a table. One of these is selected as the PK for the table. A consequence of this approach is that a PK may be composed of several attributes. Further, these attributes may be imported from other tables (called foreign keys) that may contain codes or symbols that provide insight into the properties of the item they identify. This means that the structure of the PK may be different for every table.

c. To alleviate some of these problems, the concept of surrogate keys (SKs) was introduced in the computer science profession in 1979 and expanded in subsequent decades. An SK is a PK that is composed of a single attribute with no intelligence encoded into it. These constraints mean that the SK cannot be composed of parts imported from another table and that the value of the SK provides no insight about the item it identifies. It is these characteristics that led to the first two properties of unique identifiers listed in section 2 of this appendix (i.e., no embedded intelligence and a fixed size).

d. However, an SK only needs to be unique within a single table. The same SK may exist in numerous tables (e.g., a common approach is to number rows from 1 to N in every table as it occurs with the automatic indexing feature found in many databases). Enterprise keys (EKs), introduced in 2000, expanded this concept across all tables of the enterprise. Therefore, if the enterprise were the Department of Defense, then every unique row of every table of every database in the Department would be uniquely identified via an EK. This is a powerful property when the challenging task of integration is pursued. Further, if the enterprise can accept a standard size for the EK, the problem of building applications is significantly simplified for the application builder that uses the data.

4. IMPLEMENTATION OF AN EWID SYSTEM

a. EwID is the general form of an EK from the relational database community. Analogous to an EK, an EwID is an SK that is unique across the whole enterprise. It is a universal SK. For example, if the enterprise is the Department of Defense, then no two data items may have the same EwID within the Department unless they represent the exact same object. To facilitate interoperability, the format of an EwID must be technologically independent. It must be usable by relational databases, object databases, formatted flat files, or any other formatted source of data. This is an important characteristic for integrating disparate data systems.

b. EwIDs are functionally identical to the Universally Unique Identifier (UUID) standard that is recognized by the International Organization for Standardization. UUIDs, called Globally Unique Identifiers by the Microsoft Corporation™, are 128 bits long and are implemented using a decentralized allocation strategy (i.e., they require no

central registration process). However, EwIDs were developed for a different environment.

(1) First, EwIDs provide a convenient, automated tracking service to locate the source or the data identified by an EwID. This is required to facilitate reference data that is obtained or derived from a variety of diverse sources. It is permissible for this type of data to be referred to by only its identifier since the data associated with the identifier is normally already resident in the local data stores. However, this may not always be true and situations may occur in which an EwID is received without the data it identifies, and without that data having been previously obtained, provided, or received. For this situation, the tracking service allows users to quickly locate and obtain the missing information (with permission of the data owner).

(2) Second, EwIDs must be usable over limited bandwidth communications systems such as those found in the tactical wireless environment. For this reason, they are half the size at 64 bits in length, which was determined to be the smallest usable size to achieve unique identification.

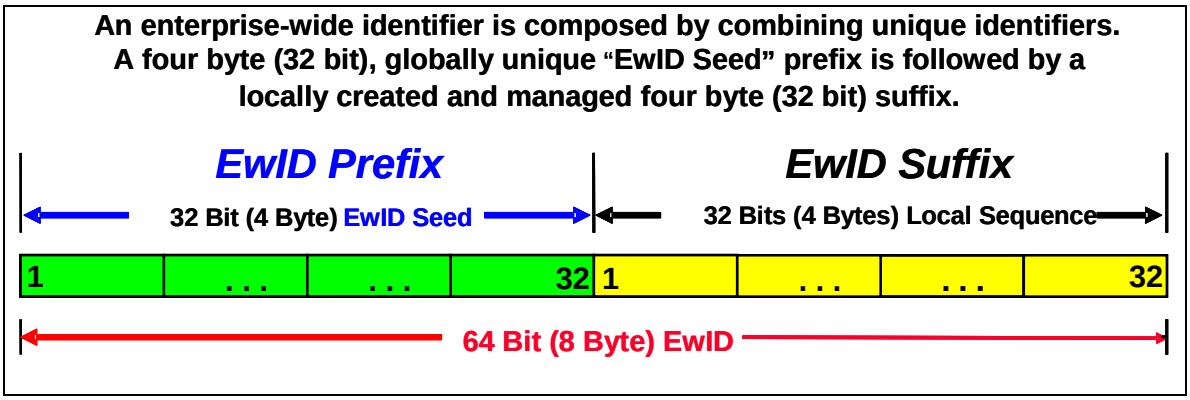
(3) Third, they must be retrofitted and usable by a wide variety of older, legacy systems. For this reason, simplicity of implementation was considered a major characteristic. EwIDs can be implemented completely independent of any operating system interactions, allowing them to be embedded in the application software if necessary.

5. EWID STRUCTURE AND ALLOCATION STRATEGY

a. When a data source creates data, it must obtain an EwID to identify that data. The EwID is a persistent label that remains attached to data for its lifetime. Because the data has an EwID, no matter where it propagates within the enterprise, its EwID is guaranteed never to collide with any other EwIDs already resident in any database. The phrase "within the enterprise" refers to other data sources that are also using the EwID scheme.

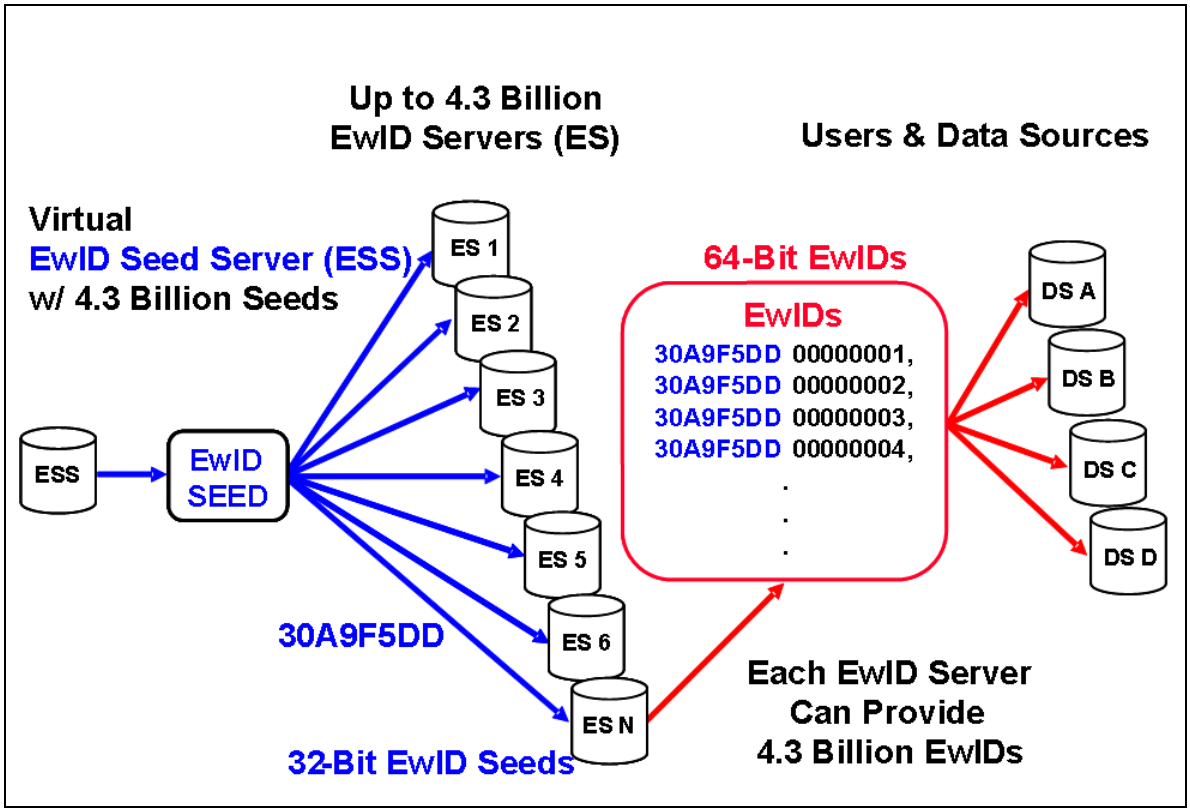
b. A primary challenge in creating an EwID system is developing an approach to guarantee that EwIDs are unique, while ensuring that they can be readily obtained and cause no performance degradation. A common method for producing globally unique values is by concatenating two smaller values. EwID implementation uses a centralized, registration-based allocation scheme to accommodate an efficient tracking service and to fully exploit the smaller 64 bit size by eliminating waste (i.e., allowing all combinations of 64 bits to be used). The centralized source is called an EwID Seed Server (ESS), and provides 32-bit prefixes ("seeds") that are unique to all the members of the enterprise. Prefixes are assigned to a user's EwID server (ES) where a globally unique 64-bit EwID is generated by concatenating a locally managed suffix to the prefix. Figure 4 illustrates this approach. This provides a flexible seed allocation scheme while permitting system managers as much control and freedom as possible.

Figure 4. EwID Composition



c. Figure 5 illustrates the EwID allocation architecture and distinguishes the roles of an ESS, an EwID seed, an ES, and an EwID. It includes three levels of operation: an ESS (on the left), ESs 1 through N (in the middle), and EwID users (on the right) tagging data within data sources (DS). EwID users (often a database) request an EwID from an ES. Because of the sizes address space of the prefix and suffix, an ESS can parcel out 4.3 billion EwID seeds, each capable of supporting 4.3 billion suffixes for a total allocation of 18 billion-billion EwIDs. 4.3 billion is equal to 2^{32}, which is the number of combination possible from a sequence of 32 bits, each bit being either a 1 or a 0.

Figure 5. The EwID Server Architecture



d. In summary, an EwID is a 64-bit value used to uniquely identify a piece of data or object. EwIDs are obtained from EwID servers (ES, not an ESS) that create them by appending a locally controlled 32-bit suffix to a 32-bit prefix. The prefix is an EwID seed that is obtained via an ESS on which one must have an account. An ES can produce nearly 4.3 billion EwIDs because of the size of the locally controlled suffix.

6. OBTAINING EWID SEEDS

a. To obtain EwID seeds, users must obtain an ESS user account. Obtaining a user account is simple, is open to anyone who wishes to apply, and is accomplished via the ESS Web site at https://ess.arl.army.mil/. When users apply, they must first agree to maintain POC information by keeping it current; guarantee that any ES established produces 64-bit EwIDs using a bona-fide EwID seed as a prefix that was obtained from an ESS; and guarantee that the ES includes a mechanism to prevent duplicate EwIDs. This implies that the ES must have some type of backup scheme to prevent re-use in the event of a power loss or major malfunction.

b. Users select a unique user name to allow them to log on to the ESS and provide official contact information. All contact information can be updated, but changing the organization and e-mail address requires the concurrence of an ESS account administrator in order to maintain control of ESS usage. The “Region” and “Province” fields are to facilitate international users. New fields can be easily added as required.

c. Once the request is submitted, an e-mail is sent to the registered e-mail address requesting validation. Requestors login to the ESS Web site and enter the code sent in the e-mail. Once this is accomplished, an e-mail is sent to the ESS administrators notifying them that an account request is pending from a validated source. An ESS administrator may then approve the account.

d. Once approved, a requestor becomes an ESS subscriber and may request EwID seed accounts. For many people, one seed account is sufficient; however, a person may require several seed accounts because he or she is handling several end-users or may have security considerations. To create an EwID seed account, a subscriber logs in to the ESS and goes to the “New Account” page. An EwID seed account does not have to have a globally unique name since it is associated with an ESS user account; ESS users can select any name.

7. USAGE LEVEL

a. There are four usage levels available for an EwID seed account: normal (1 EwID seed), moderate (10 EwID seeds), heavy (100 EwID seeds), and special (> 100 EwID seeds). The objective is to provide the EwID seed user with as many seeds as they require, but no more. For this reason, users are encouraged to be frugal and may increase

their usage level at a later time without creating a new account. Since one EwID seed supports the creation of 4.3 billion EwIDs, one EwID seed may be enough.

b. One reason for requiring more than one EwID seed is database performance (i.e., independence from an external ES). The use of EwIDs must not cause any database performance degradation or system management problems. If a set of data sources is tightly coupled over a high bandwidth communications environment, then a single ES (established with a single EwID seed) may be adequate to serve many systems without degradation. However, if one has many distributed systems that are widely dispersed, then an EwID seed may be required for each system. This is the expected situation for battle command systems and is the environment for which this implementation is based. If a project manager is building 12,000 tactical systems, then 12,000 EwID seeds may be required. If every person has a wearable computer, then every one of those systems may require a separate EwID seed. The data source dispersion problem may be solved in different ways, depending upon estimated requirements.

(1) If every system is likely to create 4.3 billion pieces of data, then a separate EwID seed (an EwID prefix) may be used for each system. This equates to solving the problem at the ESS level.

(2) The alternative is for the system manager to solve the problem at the ES level by breaking the locally controlled, EwID suffix into blocks. For example, the 4.3 billion EwID suffixes could be broken into 100 EwID blocks of 43 million each and dispersed into 100 distributed systems. As a system nears the end of its block of EwIDs, the manager obtains a new EwID seed and creates another set of blocks to be distributed. It is this flexibility that is afforded by the properties of surrogate keys (i.e., no embedded intelligence) that makes managing EwIDs so simple.

c. Just as with ESS user accounts, an ESS administrator approves and enables individual EwID seed accounts. Once approved, the ESS user may obtain EwID seeds up to the maximum number authorized for the EwID seed account without communicating with an ESS administrator. When users log on to the ESS, they are placed in their ESS User Area (i.e., homepage) that lists all of their accounts, their status, the number of EwID seeds remaining, and the number of EwID seeds obtained. A user can acquire a list of their EwID seeds by selecting the “List” text. The ESS guarantees that no other ESS subscriber has been assigned this seed, and therefore, no EwID created using it will ever collide with any EwID created by another ESS subscriber.

d. The enterprise of ESS subscribers is not constrained by Service, governmental, or national boundaries. For two organizations to implement EwIDs, all that is required is an agreement by the parties to get ESS accounts and abide by the rules in paragraph 6.a. of this enclosure. Further, although there are significant advantages for database maintenance when using EwIDs as primary keys, all the interoperability advantages are obtained when they are used as alternate keys. Thus, EwIDs can be implemented without modifying the existing primary key system in a legacy database.

8. EWID TRACKING AND TSLs

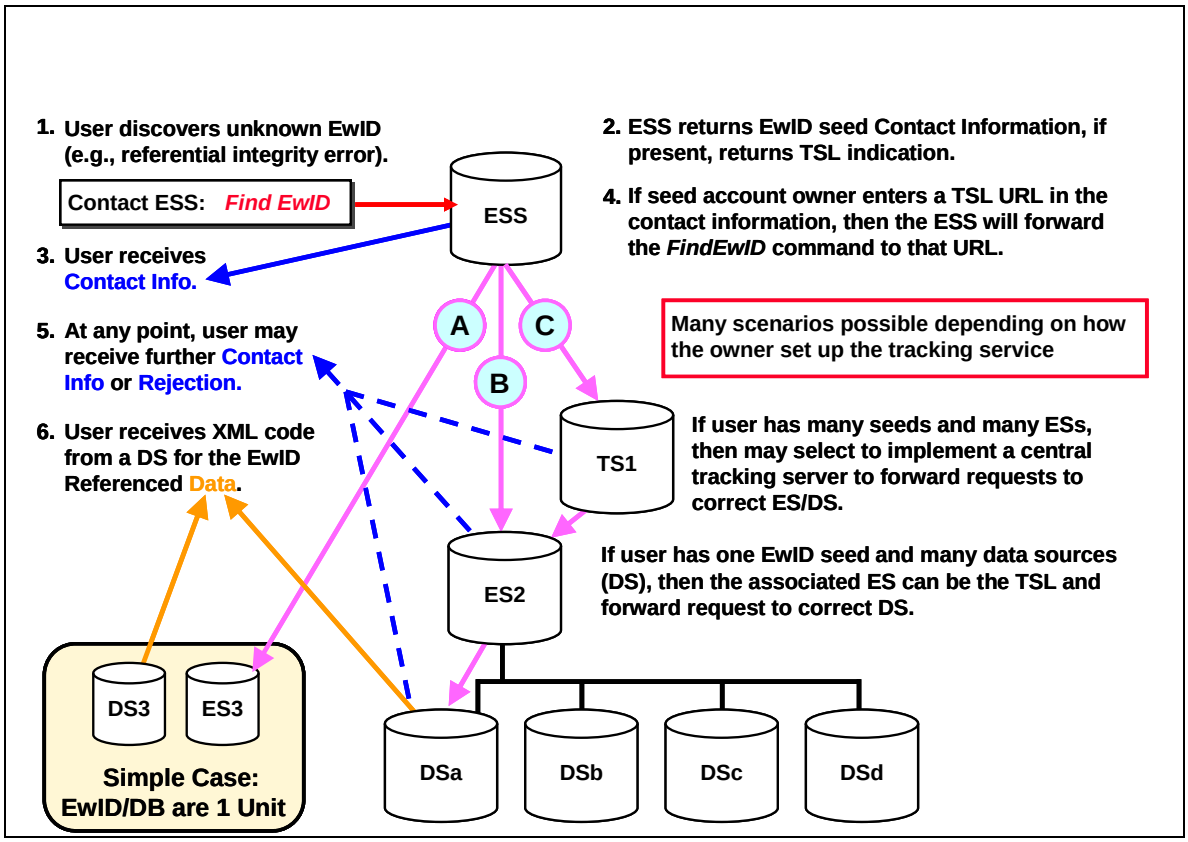
a. A key requirement of the ESS is to be able to track down the data identified via the EwIDs created from the EwID seeds it provides. However, since EwIDs have no embedded intelligence, it is pragmatically impossible to track down data provided only the EwID. To facilitate a solution to this problem, an EwID tracking system will be provided beginning at the ESS.

b. Although an EwID has no embedded intelligence, meaning that no information about the data tagged can be gleaned from the EwID value, one can discover the owner of the EwID seed by contacting the ESS. Current ESS policy is that the contact information associated with an ESS user account is available to all subscribers. This feature is executed using the "Find EwID" option. The database will provide the name and contact information of the EwID seed account owner, and the inquirer may contact the EwID seed owner about the data item tagged with that EwID. Any information provided is at the EwID seed owner's discretion.

c. EwID searches are conducted by automated services of the EwID TSL. For each EwID seed account (not user account), a URL or URN may be entered to indicate that the ESS user has implemented a tracking system for some or all of the EwID seeds it has obtained. When UDDI services are provided, a URN is preferable because it will be mapped to a URL by that service. This allows the system to automatically forward the "Find EwID" command, along with the inquirer's identity, to the source of the data tagged by the EwID, whether that source is the seed account owner or a subordinate ADS, The process will continue until the data source is discovered. At this point a "Get_Data(EwID)" or similar command is issued to the data source, and the resulting data is sent to the requestor in the form of an XML document. This requires that a mechanism be developed to convert the "Find EwID" command into a local command that executes a query in the native data source query language and converts the result into XML code, using the GFM XSD, to be returned to the requestor. In other words, a tracking service ultimately interacts with the source of the data, but this may occur after several redirections as designed by the data owner (see Figure 2).

d. A recursive EwID tracking system is illustrated in Figure 6. This example shows several different levels of complexity that are based upon the implementation decisions of the system manager. The line marked with an 'A' shows the simplest level that occurs when an ES (labeled "ES3") is embedded in a data source. The user's TSL allows the ESS to redirect the "Find EwID" request directly to the source of the data. If the user is tracking the listed EwID, then the ES executes a Get_Data(EwID) command to the DS, which in turn generates the XML code that is returned to the requestor. Alternatively, the DS could intercept the Find EwID command and execute this process. The former is the most likely scenario because the single EwID seed with a single independent database is expected to be the most common situation. Under this condition, the data that is tagged with the requested EwID is discovered with only a single redirection by the ESS of the Find EwID operation.

Figure 6. A Recursive EwID Tracking System



e. The line marked with a 'B' illustrates a slightly more complex level in which the ES manager has decided to implement EwID suffix blocking. Because only the user (not the ESS) has any knowledge of the blocking (or any allocation) scheme, a "Find EwID" request must first be directed to the ES or other designated server for further redirection. In this case, the ES (labeled "ES2") forwards the "Find EwID" command to the correct DS (e.g., DSa). Alternatively, it could forward a "Get_Data(EwID)" command to the appropriate DS and handle the results of the query by converting it into XML code and returning it to the requestor.

f. The line marked with a 'C' illustrates the most complex level. In this case, a user has an EwID seed account with multiple EwID seeds, each with its own ES. When this occurs, the user must have an intermediate tracking service established to forward the "Find EwID" command to the correct ES. (This is because of the decision to associate the TSL with an EwID seed account, and not with the individual EwID seeds.) It does not matter if a user has a normal, moderate, heavy, or special EwID seed account; each account may be associated with only a single TSL. By having a single TSL per EwID seed account, the burden of effort is divided equitably between the ESS and the user's local systems.

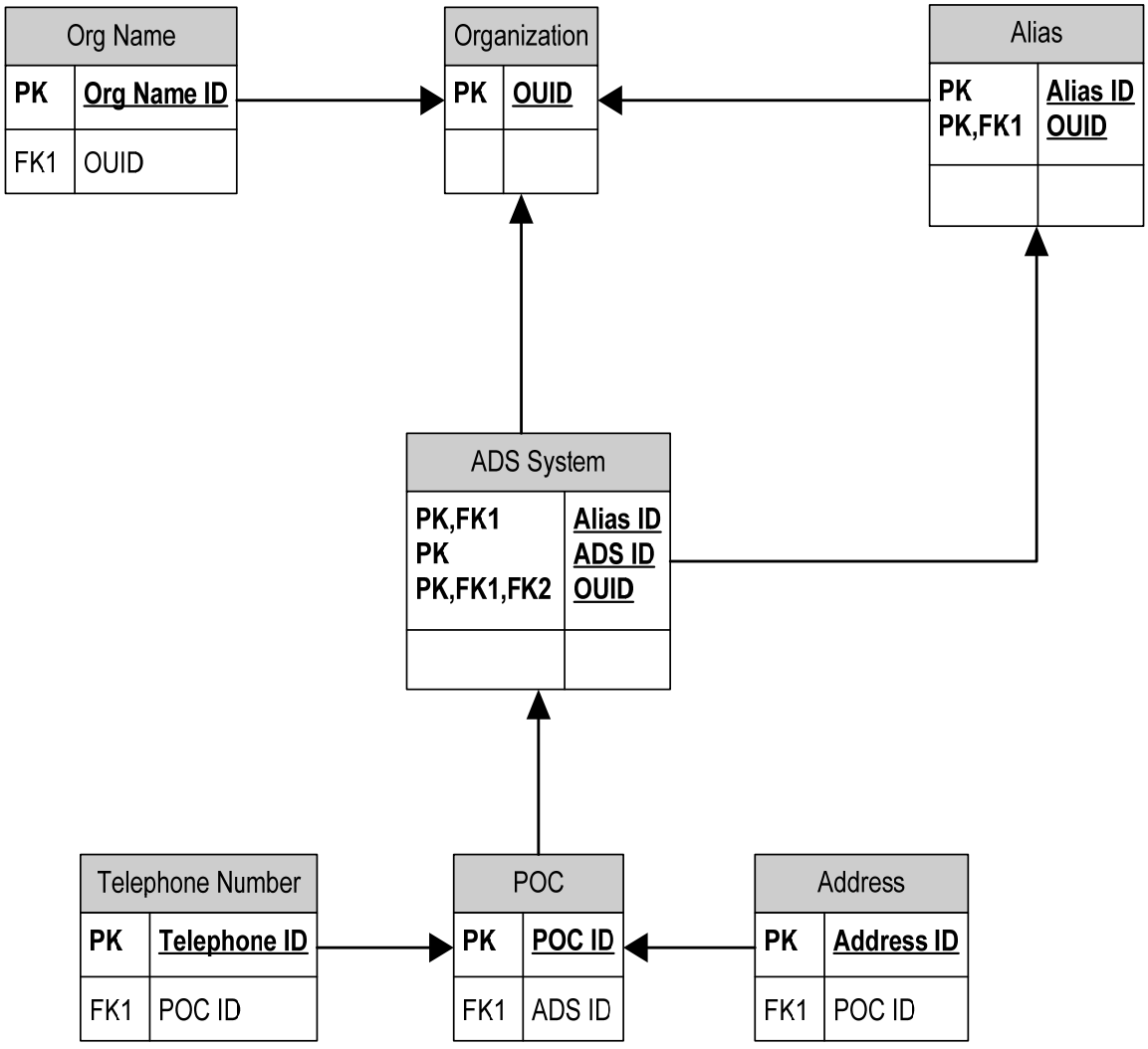
g. Finally, there is a user settable parameter to indicate the activation state of an allocated EwID seed. This is a toggled value that a user can set for each EwID. There

are several reasons for this field, the most prominent being the time lapse between the acquisition of an EwID seed and the establishment of an ES that uses that seed. When a user executes the "Get EwID" command, the EwID status is set to "inactive." Once an ES is established and is activated, the user can toggle this field to indicate that the EwID seed is now in use. Currently, this parameter is used only as an indicator (e.g., to display the status). A user can toggle this variable without any effect on the ESS. For example, a user may change the state to "inactive" to indicate that an ES is no longer active or operational. This does not automatically imply that the tracking services for the ES are switched off, but only that it is no longer available for dispensing EwIDs.

APPENDIX 2 TO ENCLOSURE 3

OUID STRUCTURE

Figure 7. OUID Structure



GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ADS	authoritative data source
CCR	Centralized Contractor Registry
CDS	cross domain solution
CONOPS	concept of operations
DS	data source
DTG	date-time-group
DUNS	Data Universal Numbering System
EK	enterprise key
ES	EwID Servers
ESS	EwID Seed Server
EwID	Enterprise-wide Identifier
FedReg	Federal Agency Registration
FGS	FMID Generation Service
FMID	Force Management Identifier
FTS	FMID Tracking System
FY	fiscal year
GFM	Global Force Management
GFM DI	Global Force Management Data Initiative
GFM XSD	Global Force Management XML Schema Definition
IP	internet protocol
IUID	Item Unique Identification
MCC	Monitored Command Code
NIPRNET	Non-Secure Internet Protocol Router Network
OAC	Operating Agency Code
OBAN	Operating Budget Account Number
OE	organizational element
OFSC	Organizational and Force Structure Construct
OS	organization server
OUID	organization unique identifier
PAS	Personnel Accounting Symbol
PK	primary key

PMO	Program Management Office
POC	point of contact
RCCC	Responsibility Center/Cost Center
RPUID	Real Property Unique Identifier
RUC	Reporting Unit Code
SFIS	Standard Financial Information Structure
SIPRNET	SECRET Internet Protocol Router Network
SK	surrogate key
TSL	Tracking Service Locator
UDDI	Universal Description, Discovery, and Integration
UIC	Unit Identification Code
UID	Unique Identification
UII	Unique Item Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
UUID	Universally Unique Identifier
WSDL	Web Service Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Volume.

active. The status of an EwID seed (FMID prefix value) that denotes it has been assigned from the ESS and either concatenated to generate a 64-bit FMID or redirected to a subsidiary system to which a query must be forwarded. This status is used to manage the FMID tracking process at FMID Tracking Servers. Whether or not generated FMIDs have been used to tag data for publication is not part of the term "active" when applied to an EwID.

ADS. Defined in Reference (c).

allocation. The number of EwID seeds that a EwID seed account holder has been authorized to obtain. The number of EwID seeds allocated does not reserve specific EwID seed values for future use, but does guarantee that the number of seeds allocated will be available when requested. EwID seed values are specified only when seeds are assigned.

assigned. A 32-bit EwID seed of a specific value that has been provided to an ESS subscriber for generation of a full 64-bit FMID, or for redirection to a subordinate end user.

authorization data. Defined in Reference (a).

billet organization. Defined in Reference (a).

crew organization. Defined in Reference (a).

ES. The device that concatenates a locally managed suffix to an EwID seed obtained from the ESS to create an identifier that is unique to all the members of the enterprise.

ESS. The authoritative source of EwID seeds, on which EwID seed users, or their intermediaries, must have an account. The ESS Web site is https://ess.arl.army.mil/.

ESS user account. A formal relationship that allows one to login to the ESS and utilize its functions, to include the creation of EwID seed accounts.

EwID. A scheme to generate unique identifiers that includes a centralized and decentralized component. A prefix is provided by a centralized source to ensure enterprise-wide uniqueness, and a locally controlled suffix extends the procedure to distributed users. An EwID conveys no information about the entity it identifies, is a fixed, 64-bit size, and is exchanged as a single attribute. Previously termed an Enterprise Identifier or EID, the name was changed to avoid confusion with an Item Unique Identifier data field with the same acronym that is used to tag tangible items, such as equipment.

EwID seed account. An account that allows users to obtain and manage EwID seeds, and set up tracking links. EwID seeds are managed based upon the properties of the EwID account through which they were allocated. The account properties include a specified maximum EwID seed allocation amount that may be increased at a later time. There are four usage levels for an EwID seed account: normal (1 EwID seed), moderate (10 EwID seeds), heavy (100 EwID seeds), and special (>100 EwID seeds). EwID seeds are not assigned upon the creation of an account, but upon a subsequent user request for them.

FMID. The set of identifiers and indexes used to identify data within the GFM XSD. FMIDs convey no information about the entity they identify, are a fixed size, and are exchanged as a single attribute.

force structure. Defined in Reference (a).

generation. The act of concatenating a 32-bit prefix (seed) provided from a centrally managed source with a locally managed 32-bit suffix to create a full 64-bit FMID.

Global Information Grid. Defined in DoD Directive 8000.01 (Reference (k)).

inactive. The status of an assigned FMID prefix value that that has never been used to generate an FMID. This status is used to manage the FMID tracking process at FMID Tracking Servers. An inactive seed may be revoked back to the source from which it was immediately obtained.

joint community. All departments or agencies of a government that are concerned with activities, operations, organizations, etc., in which elements of two or more Military Departments participate.

OFSC. Defined in Reference (a).

operational suitability. Defined in Reference (h).

OS. The term "server" is used in its original meaning as a software application program that accepts connections based upon a request/response paradigm. In this usage, it does not mean a physical computer system.

OUID. The means of uniquely distinguishing one DoD organizational element from another, allowing DoD systems to identify an organization individually across the DoD enterprise.

redirect. The act of delegating responsibility for an FMID prefix to a subordinate server. The ultimate user of a redirected seed will thus not be identified in the ESS as the EwID account holder of that seed. The end user must therefore be identified through sequences of tracking services of every server through which the seed was redirected.

revoke. In FMID management, the act of removing an FMID prefix that has never been used from the list of EwID seeds assigned to a user to be given back to the server from which it was originally received. This removes the seed from that end user's EwID or FMID seed account.

tracking. The act of returning information about a given FMID. This can be POC data, a TSL, the data tagged by it, etc. In the ESS, it is invoked by the "Find" command or the TSL function.

unassigned. Any of the 4.3 billion possible EwID seed values that have never been assigned by the ESS to any EwID account holder. For the purposes of FMID management, the term is only used to describe seed values at the level of the ESS itself. The status of an assigned seed value is described as "active" or "inactive."

UID. Defined in Reference (c).

WSDL. An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.