



# SYMMETRY WHITE PAPER

## Identity Management Middleware (IMM)

A Symmetry Brief

26 Oct 2015





# Identity Management Middleware (IMM) Symmetry White Paper

Together AMAG Technology has worked with development partner Hawkeye Technologies to develop the Identity Management Middleware (IMM) Client. This white paper reviews how the IMM software product interacts with a defined identity management interface to allow the real-time validation of DOD credentials. The IMM Client comes in a version supporting the Joint Gatekeeper Service (JGS) as well as a version supporting Interoperability Layer Services (IoLS). The IMM Client can be used as a real-time identity validation system for installation entry, or it can be used as a front-end registration process for the Symmetry Security Management System.

## Background

The US Department of Defence (DOD) utilizes a massive database called the Defence Enrolment Eligibility Reporting System (DEERS). This database includes the identity information for all Defence Identity document cardholders including Common Access Card (CAC), Dependent Teslin Card, Retiree Teslin Card, etc. The DEERS database is only directly accessible through the Real-Time Automated Personnel Identification System (RAPIDS) workstations; however, DOD has made web services available to allow authorized and vetted providers to access specific information from DEERS. The Interface Web Services (IWS) allow limited access to information stored in DEERS.

The US Navy commissioned an identity management solution that would interface with IWS that would help them provide faster response time and additional functionality throughout the Navy enterprise. This was originally called Enterprise Network Application Database, and Logistical Enabler (ENABLER), but with additional functionality and support for all DOD divisions needed, it became the Joint Gatekeeper Service (JGS). JGS currently expands on the functionality available through IWS by caching identity information at the JGS server and maintaining a registered local population list for each account that interacts with JGS. The registered population can then be updated locally with a single web service call. JGS also offers many other convenience features.

The DOD recognized the benefits of JGS, but also wanted to expand the ability to interface with multiple authoritative databases such as the Federal PKI Bridge to allow PKI validation of PIV and PIV-I credentials. DOD also wanted to add support for a Continuous Information Management Engine which would collect debarment information from such authoritative sources as the Terrorist Watch List, National Criminal Information Center (NCIC), and more. In order to provide this functionality under a DOD managed program, the Defense Manpower Data Center (DMDC), who maintain the DEERS

database, developed the Interoperability Layer Services (IoLS). IoLS is available to select, vetted and authorized vendors.

## Identity Management Middleware

Together AMAG and Hawkeye Technologies have developed the Identity Management Middleware (IMM) Client. This software product interacts with a defined identity management interface and allows the real-time validation of DOD credentials. As noted previously the IMM Client comes in a version supporting JGS as well as a version supporting IoLS. The IMM Client can be used as a real-time identity validation system for installation entry, or it can be used as a front-end registration for the Symmetry Security Management System. The figure below shows the IMM Client interface.

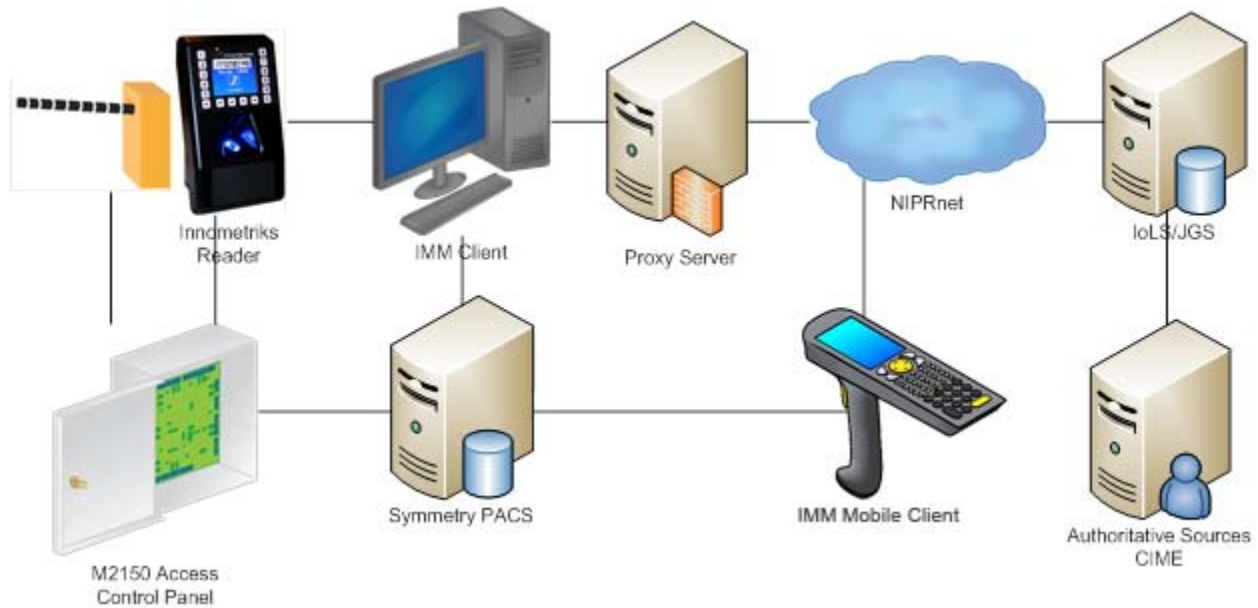


In this case shown, a credential was scanned and submitted to IoLS. The response from IoLS indicated that the credential was assigned to “Tony Stark” (this was a test identity and personal details and biographic information are fictional), the individual has a Warrant for Arrest associated with their identity and therefore their credential has been revoked (is no longer a trusted agent of the DOD). The large red ‘X’ indicates this individual should not be allowed on base (they may be registered in the local physical access control system, PACS, to track the event, but automatic access will not be granted). The green fingerprint icon indicates that a fingerprint template (ANSI 378 format) has been downloaded from IoLS and can be used along with the photograph to validate Tony Stark’s identity (two-factor authentication). Additional details returned by IoLS about Tony Stark and the security alert are available by clicking on the “Members” button.

When used as a registration client to Symmetry, IoLS is checked on each card presentation. Biometric data can be authenticated as well. Once validated, the credential information including biographic information can be imported in the local Symmetry PACS. Symmetry will log every access of the cardholder through the system. The IMM Client used as a registration client can be configured to retrieve updates of the registered local population from IoLS on a regular basis (e.g. nightly). Therefore, if a cardholder is revoked or otherwise identified by the Continuous Information Management Engine (CIME), this information will be captured in an update cycle and invalidate the credential locally. The IMM Client imports alarm information into Symmetry to track all of these updates and registrations.

When used as a Gate Entry Credential Validation system, IMM Client can be configured to check for the existence of the credential in the local PACS before reaching out to IoLS for validation. The local PACS provides a much faster response to the operator. IMM Client is so tightly integrated with Symmetry that if the Force Protection Condition (FPCON) level is elevated in Symmetry, this can impact the way that IMM Client operates (i.e. at FPCON Delta the base will operate stand-alone and will not communicate over NIPRnet).

The following figure depicts a typical installation.



As a vehicle approaches the gate entrance they present their DOD credential to the biometric-enabled card reader. The card reader sends this credential information to the IMM Client. The IMM Client checks Symmetry for the existence of the credential. If available locally, information is displayed for the guard, the card reader sends the credential information to Symmetry which will raise the gate arm automatically if the credential is valid and the FPCON doesn't prevent entry. If not available locally, the IMM Client will query the local IoLS Proxy for the credential information. The IoLS Proxy does not cache Personally Identifiable Information. Rather the proxy consolidates requests from multiple local IMM



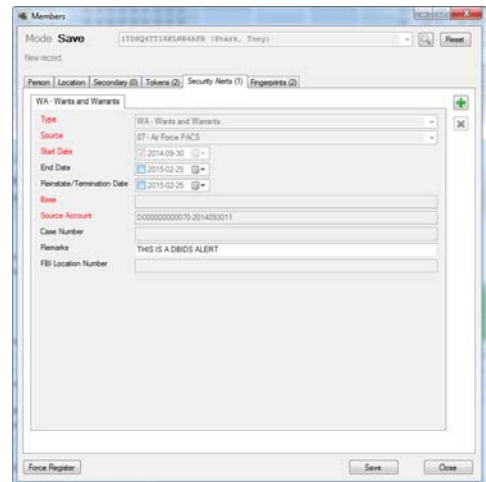
Clients and relays them to IoLS. Interoperability Layer Services (IoLS) responds with information about the credential and individual. IMM Client parses the information and presents it to the guarding officer while importing the information into Symmetry. The card reader sends the credential information to Symmetry which will raise the gate arm if the card information is valid and the FPCON doesn't prevent entry. This automatic registration of credentials used at the gate is a very powerful function of the IMM Client.

The IMM Mobile Client can also be used as a registration client at the Pass and ID office (aka Visitor Control Center). A DOD credential can be scanned by a mobile handheld barcode reader (IMM Mobile) and the information be sent to IoLS in a similar manner as described above with the end result being the import of the credential information into the Symmetry PACS.

Additionally, Hawkeye Technologies offers Hawkeye Mobile Online and Hawkeye Mobile ID products that run on a MIL-STD ruggedized handheld computer for mobile entry operations. These products scan the DOD credential and interact with the local Symmetry PACS to present cardholder name, picture and additional personal data to the Sentry to determine access eligibility.



In any of the above configurations, the IMM client can display additional information about the reason for failed validation of the credential. As depicted in the image above, the card for "Tony Stark" was revoked. Upon further review, the reason for the revocation seems to be that Wants or Warrants have been issued against this person – not the specific card that was used! Therefore, a powerful feature of the IMM Client is that it vets the submitted credential AND the person assigned to the credential.



Additional information on the installation of the software can be found in the embedded documentation here:



AMAG IMM Client - Quickstart.docx

For more information contact AMAG Technology, [www.amag.com](http://www.amag.com), Ryan Kaltenbaugh, Director of Government Sales, [ryan.kaltenbaugh@amag.com](mailto:ryan.kaltenbaugh@amag.com).