

Vehicle Infrastructure Integration (VII)

Enterprise Network Operations Center (ENOC) to Managed Entity (ME) [Managed Entity] Software Interface Requirements Specification



**U.S. Department of Transportation
Federal Highway
Administration**

February 26, 2007
Version 1.1

Booz | Allen | Hamilton

This report is confidential and intended solely for the use and information of the company to whom it is addressed.

Acceptance / Approval Page

// // _____ Reviewed by _____
David Cline Date
Quality Assurance

// // _____ Reviewed by _____
Mark Lawrence Date
Deputy Project Manager

// // _____ Approved by _____
Craig Pickering Date
Project Manager

// // _____ Approved by _____
Bill Jones Date
US Department of Transportation

DOCUMENT CHANGE HISTORY

Date	Author	Description
11/20/2006	Booz Allen Hamilton	Released v. 1.0
02/12/2006	Booz Allen Hamilton	<ul style="list-style-type: none">- Lexicon removed and incorporated in “VII Infrastructure Lexicon 1.0 Document”.- Data Element Dictionary and incorporated in “VII Data Element Dictionary 1.0” Document.- All diagrams updated to reflect Managed Entity (to include: RSE, SDN, Administrative Users, etc.) so that the reader can better follow the message flow between the ENOC and the ME, the only line that would exist is this line.- ASU9 wording changed.- ASU19 deleted, redundant.- ASU25, ASU26, ASU27, and ASU28 added.- Appendix B: Version column added, versions updated.- Added clarifying text to Section 1.1.

Table of Contents

1. INTRODUCTION	1
1.1 SCOPE.....	1
1.2 DOCUMENT OVERVIEW	1
1.3 DOCUMENT CONVENTIONS.....	1
1.3.1 Message and Interface Naming.....	1
2. INTERFACE DESCRIPTION	3
2.1 SECURITY AUTHENTICATION.....	3
2.1.1 Interface: Security.Authenticate	3
2.2 SECURITY AUTHORIZATION.....	3
2.2.1 Interface: Security.Authorize	3
2.3 SECURITY ENTITY LIFECYCLE MANAGEMENT.....	4
2.3.1 Interface: Security.ManageEntityLifecycle	4
2.4 SECURITY SYNCHRONIZATION.....	5
2.4.1 Interface: Security.Synchronize.....	5
3. INTERFACE REQUIREMENTS	6
3.1 SECURITY AUTHENTICATION.....	6
3.1.1 Interface: Security.Authenticate	6
3.2 SECURITY AUTHORIZATION.....	6
3.2.1 Interface: Security.Authorize.....	6
3.3 SECURITY ENTITY LIFECYCLE MANAGEMENT.....	6
3.3.1 Interface: Security.ManageEntityLifecycle	6
3.4 SECURITY SYNCHRONIZATION.....	6
3.4.1 Interface: Security.Synchronize	6
APPENDIX A: ASSUMPTIONS AND DEPENDENCIES	A-1
ASSUMPTIONS	A-1
DEPENDENCIES.....	A-2
APPENDIX B: REFERENCE DOCUMENTS	B-1
APPENDIX C: NATIONAL SYSTEM REQUIREMENTS TRACEABILITY	C-1

1. INTRODUCTION

This Software Interface Requirements Specification (IRS) is based on guidance and information provided by the United States Department of Transportation (USDOT), subsequent meetings and discussions, and agreed upon assumptions by the USDOT and VIIC. Every effort has been made to ensure the content and approach in developing this document reflect available guidance from the USDOT and accurately reflect the overall scope and intent of VII's objectives.

1.1 SCOPE

This document, the Vehicle Infrastructure Integration (VII) Enterprise Network Operations Center (ENOC) to Managed Entity Interface Requirements Specification, addresses the top-level software interface requirements for the I-13 interfaces as specified in the VII National System Requirements. This specification is one of a series of technical documents detailing the SDN Subsystem and defining the technical characteristics of the VII System. The main focus of this document is the Proof of Concept (POC) system functionality, which will subsequently be implemented in the National System. For further background on the VII System's projected operations, refer to the *VII National System Requirements* (Reference 1) and the *VII Concept of Operations* (Reference 17).

1.2 DOCUMENT OVERVIEW

This IRS captures the complete system requirements for *ENOC to Managed Entity Interface* as part of the *Vehicle Infrastructure Integration (VII)* project.

The remaining IRS sections are organized as follows:

- **Section 2. Interface Description:** Describes the interfaces between the ENOC Subsystem and Managed Entities, in the order of the services they support.
- **Section 3. Interface Requirements:** Lists the requirements for the interfaces between the ENOC Subsystem and Managed Entities.
- **Appendix A. Assumptions and Dependencies:** Provides a list of the assumptions and dependencies upon which the requirements rest.
- **Appendix B. Reference Documents:** Lists documents related to the ENOC Subsystem and Managed Entities.
- **Appendix C. National System Requirements Traceability:** Traces requirements from this document to their parent requirements in the National System Requirements.

1.3 DOCUMENT CONVENTIONS

1.3.1 Message and Interface Naming

The VII System includes many services and components, all of which must communicate with one another. For clarity in discussion, this section provides a convention for describing how these communications occur. The term "unit," as used in this discussion, may refer to a system, subsystem, service, component, or any other entity in the VII System.

Every instance of communication between two units is referred to as a *message*; for example, a subscription request is one type of message, and the response is another. The grouping of all messages that two units send each other in performing a task is called the *interface* between those units. Two units might have multiple interfaces between them depending on the tasks they perform.

An interface's name is composed of the unit to which the interface belongs, followed by a period, followed by the task performed by the messages traversing that interface. For example, the Lookup Information interface, which belongs to the Information Lookup Service (ILS), is called **ILS.LookupInformation**. Messages that use an interface are specified with the interface name, followed by the message name in brackets. For instance, the

message used to request information in a geographic area is called **ILS.LookupInformation[GeospatialRequest]**, and the response is **ILS.LookupInformation[GeospatialResponse]**.

2. INTERFACE DESCRIPTION

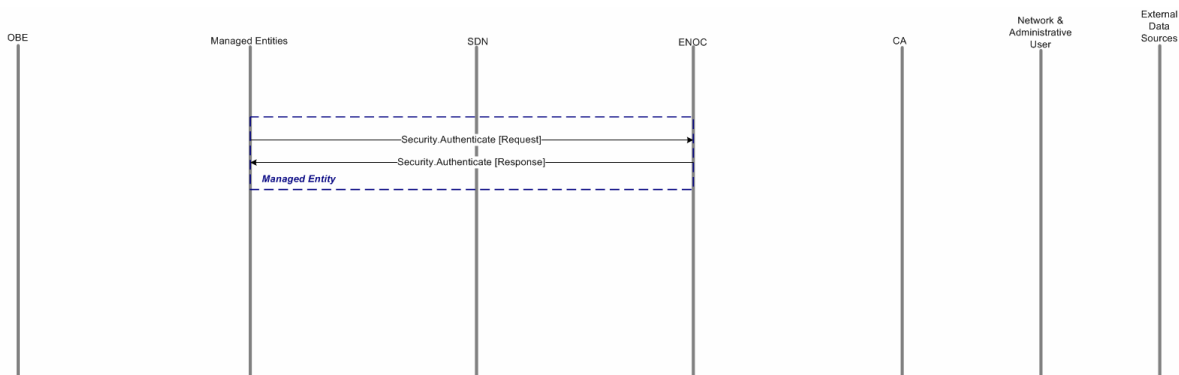
2.1 SECURITY AUTHENTICATION

2.1.1 Interface: Security.Authenticate

This process provides the authentication service to internal and external VII entities. The ENOC Subsystem accepts a request for authentication in the form of a credential. In most cases, the authentication token used throughout this network will be either IEEE 1609.2 or X.509 certificates. To authenticate the certificate-holding entity, entities are required to authenticate to the ENOC Subsystem, which will ensure the token's validity. The ENOC Subsystem will return a message indicating the entity's authentication status.

- **Type:** Synchronous
- **Message Frequency:** Frequent
- **Network Interface:** Backbone

Figure 2-1: Security Authentication Interface Messages



2.2 SECURITY AUTHORIZATION

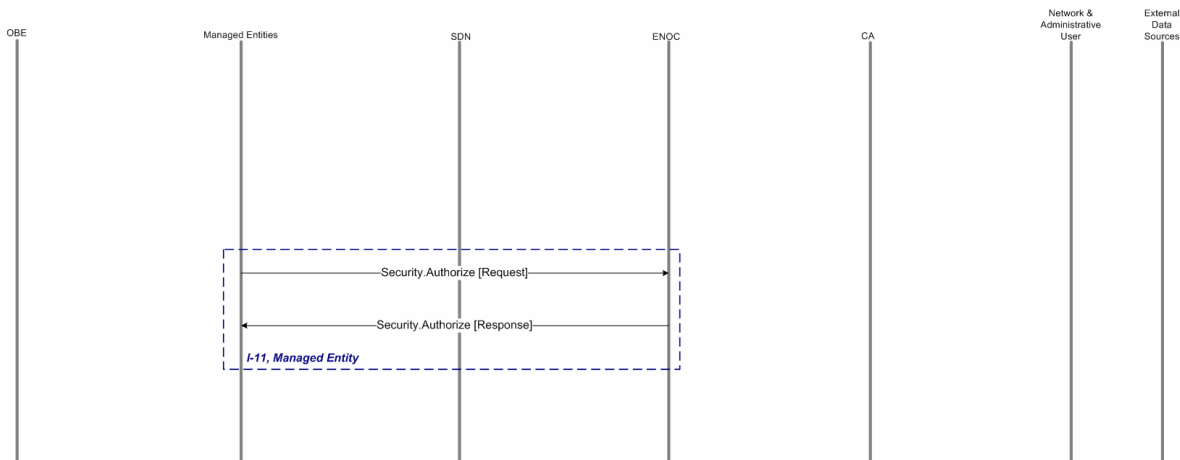
2.2.1 Interface: Security.Authorize

This interface provides the ability for the ENOC Subsystem to authorize roadside equipment (RSE), entities, network users, and service delivery nodes (SDN) across the VII network.

- **Type:** Synchronous
- **Message Frequency:** Frequent
- **Network Interface:** Backbone

Various components can call this process to determine access rights and authorization of entities requesting information or services throughout the network. The authorization decisions are based on defined policy stored in the ENOC Subsystem.

Figure 2-2: Security Authorization Interface Messages



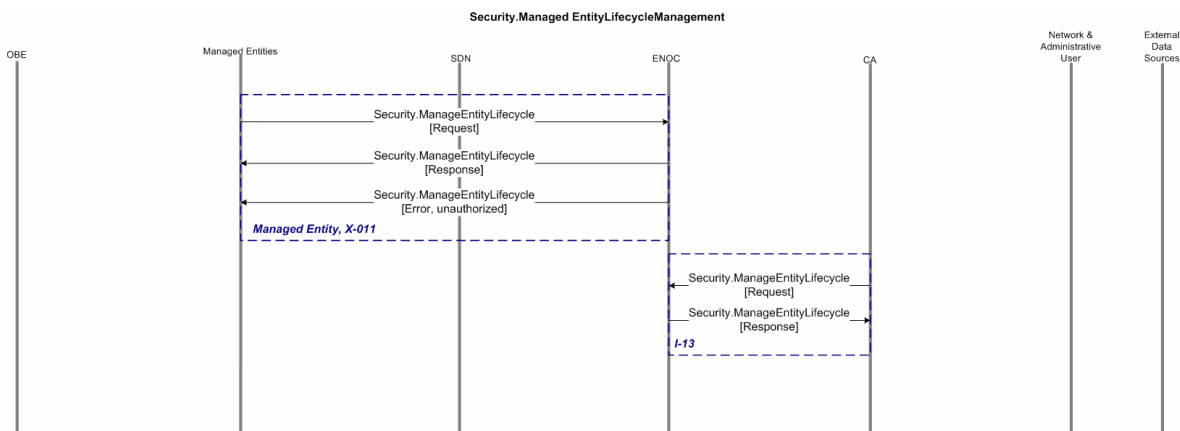
2.3 SECURITY ENTITY LIFECYCLE MANAGEMENT

2.3.1 Interface: Security.ManageEntityLifecycle

The entity lifecycle management process will provide security management capabilities at the SDN. The manage process may provide the service for internal Network Operators to be provisioned, deprovisioned, updated, and revoked. The ENOC Subsystem will control the registration or deregistration of constituent Network Users. Authorization policies surrounding access control are stored locally for the SDN and managed within the SDN Subsystem. Through the manage process, Administrative Users may request changes in service offerings within Administrative Users’ jurisdictions. With this, a logical grouping of RSEs within their jurisdiction will be defined in a repository.

- **Type:** Synchronous
- **Message Frequency:** Frequent
- **Network Interface:** Backbone

Figure 2-3: Entity Lifecycle Management Interface Messages



2.4 SECURITY SYNCHRONIZATION

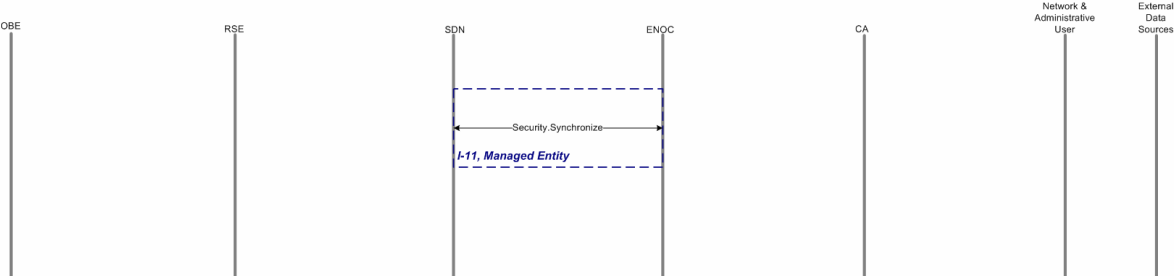
2.4.1 Interface: Security.Synchronize

Synching with the SDN data:

- **Type:** Synchronous
- **Message Frequency:** Frequent
- **Network Interface:** Backbone

The security synchronization interface will pass data between the ENOC Subsystem and the SDN Subsystem. A local instance of the data will reside at the SDN Subsystem and will be maintained on a regularly scheduled basis to remain consistent with the ENOC Subsystem. The synchronized data will include identity data to be used for authentication, authorization, and entity lifecycle management purposes. It is expected that synchronization will occur between ENOC Subsystems as well.

Figure 2-4: Security Synchronization Interface Messages



3. INTERFACE REQUIREMENTS

3.1 SECURITY AUTHENTICATION

3.1.1 Interface: Security.Authenticate

REQ #	REQUIREMENT	POC	NATIONAL
IRS476	The ENOC to Managed Entity interface shall have the ability to use a Certificate Revocation List (CRL) per RFC 3280.	Yes	Yes
IRS477	The ENOC to Managed Entity interface shall have the ability to use an Online Certificate Status Protocol (OCSP) transaction for valid certificate verification.	No	Yes
IRS480	The ENOC to Managed Entity interface shall support the response of accessing a Certificate Revocation List (CRL) per RFC 3280.	Yes	Yes
IRS481	The ENOC to Managed Entity interface shall support the response of an Online Certificate Status Protocol (OCSP) transaction for valid certificate verification.	No	Yes

3.2 SECURITY AUTHORIZATION

3.2.1 Interface: Security.Authorize

REQ #	REQUIREMENT	POC	NATIONAL
IRS488	The ENOC to Managed Entity interface shall support the XACML specification for Fine-grained authorization polices.	Yes	Yes

3.3 SECURITY ENTITY LIFECYCLE MANAGEMENT

3.3.1 Interface: Security.ManageEntityLifecycle

REQ #	REQUIREMENT	POC	NATIONAL
IRS473	The ENOC to Managed Entity interface shall use IETF RFC X.509-compliant message parameters.	Yes	Yes

3.4 SECURITY SYNCHRONIZATION

3.4.1 Interface: Security.Synchronize

REQ #	REQUIREMENT	POC	NATIONAL
IRS464	The ENOC to Managed Entity interface shall support multiple managed resource reconciliations.	No	Yes
IRS465	The ENOC to Managed Entity interface shall support multiple authoritative resource reconciliation.	No	Yes
IRS467	The ENOC to Managed Entity interface shall support data synchronization.	No	Yes

APPENDIX A: ASSUMPTIONS AND DEPENDENCIES

ASSUMPTIONS

ASSUMPTION ID	ASSUMPTION TEXT
ASU3	The Proof of Concept will have no more than 100 concurrently connected RSE Subsystems for each SDN Subsystem
ASU4	The Proof of Concept will have no more than three (3) concurrently connected SDN Subsystems.
ASU5	An RSE Subsystem will collect and aggregate no more than 375 Probe Data Messages per second. This assumes (5 vehicles / lane / sec) * (10 lanes) * (30 Probe Data Snapshots / vehicle) / (4 Probe Data Snapshots / Probe Data Message)
ASU6	The Proof of Concept will have no more than one (1) ENOC Subsystem.
ASU9	The ENOC will consist of the Management Service and the Security Service
ASU10	The ENOC subsystem shall use network management protocols which comply with recognized internetworking management standards
ASU11	The ENOC subsystem shall use recognized internetworking management standards for fault, configuration, accounting and performance management
ASU12	The ENOC subsystem shall use non standard network management protocols if necessary to manage specific managed network elements
ASU13	The ENOC subsystem shall be a platform comprised of multiple sub-components which together complete the requirements of the ENOC subsystem
ASU14	The ENOC subsystem shall capture and process configuring orders for all types of service and managed network elements
ASU15	ENOC operators will be able to access standard process documentation for handling reported incidents and requests for service
ASU16	ENOC operators will be trained to follow standard process for handling reported incidents and requests for service
ASU17	Roadside Equipment (RSEs) will support two types of digital certificates: IEEE 1609.2 for wireless communication and X.509v3 for network communication requirements.
ASU18	CA to SDN, CA to ENOC, RSE to SDN, and SDN to ENOC communication will use X.509 v3 compliant certificates for certificate-based activities.
ASU20	The VII wireless infrastructure (OBE, RSE) will use IEEE 1609.2 compliant certificates for certificate-based activities.
ASU21	Bridging of X.509 and IEEE 1609.2 Certificate Authorities will not be required.
ASU22	The VII CA Subsystem shall consist of two separate CA certificate systems: the X.509 CA, and the IEEE 1609.2 compliant CA.
ASU23	VII Infrastructure systems and devices will use X.509 certificates for digital signatures, encryption, and identification.
ASU25	All connections internal to the SDN and the NAP shall use Ethernet.
ASU26	A separate document will be created to specify requirements regarding electrical power supply, surge protection, physical space, humidity control, temperature control and similar environmental factors for the supporting facilities.
ASU27	The VII POC Environment shall have no more than 50 Network and/or Administrative Users.
ASU28	RSE Backhaul traffic flowing to and from RSE Backhaul Gateways will be aggregated by service providers.

DEPENDENCIES

DEPENDENCY ID	DEPENDENCY
DEP1	Probe Data Service (PDS) performance requirements are dependent upon the structure and size of the SAE J2735 Probe Data Message.
DEP2	Advisory Message Distribution Service (AMDS) performance requirements are dependent upon network transport availability.
DEP3	The implementation of ENOC management services is dependent on the establishment of network connectivity between the ENOC and the managed network elements.
DEP4	The implementation of ENOC security services is dependent on the establishment of network connectivity between the ENOC and the managed security elements
DEP5	A Network management agent is running in each managed network element and network connectivity exists between the managed network element and the ENOC
DEP6	The ENOC has connectivity to the managed network elements
DEP7	Connectivity with the ENOC Subsystem.
DEP8	The existence of a VII CA certificate repository.
DEP9	Hardware Security Modules (HSMs) capable of supporting required certificate assurance levels.
DEP10	A VII CA Certificate Practice Statement (CPS) describing the practices and standards to which the CA shall be managed.
DEP11	The VII System will support Lightweight Directory Access Protocol (LDAP) Version 3.0.
DEP12	The VII System will support Secure Lightweight Directory Access Protocol (LDAPS).
DEP13	The VII System will support Hypertext Transfer Protocol (HTTP).
DEP14	The VII System will support Secure Hypertext Transfer Protocol (HTTPS).

APPENDIX B: REFERENCE DOCUMENTS

REF #	REFERENCE	VERSION
1	VII National System Requirements	Version 1.2.1
2	Road Side Equipment (RSE) Subsystem Specification	Draft 1.0
3	Enterprise Network Operations Center (ENOC) Subsystem Specification	Version 1.1
4	Certificate Authority (CA) Subsystem Specification	Version 1.1
5	ENOC to Administrative User Subsystem Software IRS [X-011]	Version 1.1
6	Network User to SDN Subsystem Software IRS [X-031, X-032, X-033]	Version 1.1
7	ENOC to Managed Entity Subsystem Software IRS	Version 1.0
8	ENOC to Managed Network Element Software IRS	Version 1.0
9	Reference Maps – TBD	TBD
10	Navstar GPS Space Segment/Navigation User Interfaces, ICD GPS 200	Revision C
11	SDN to RSE Subsystem Software IRS [I-06]	Version 1.1
12	ENOC to CA Subsystem Software IRS [I-13]	Version 1.1
13	ENOC to SDN Subsystem Software IRS [I-11]	Version 1.1
14	<i>Service Provider Management Systems to SDN Subsystem IRS [X-061] Not in scope for POC</i>	Not in Scope
15	VII USDOT Day-1 Use Case Descriptions (May 2006)	Version 1.0
16	Network Subsystem Specification	Version 1.0
17	VII Concept of Operations	Draft 1.2
18	VII Systems Security Plan	Version 2.1
19	SDN Subsystem Specification (SSS)	Version 1.1
20	Internet Engineering Task Force (IETF) Request for Comments (RFC) 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols	© 1999
21	Internet Engineering Task Force (IETF) RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	© 2004
22	VII Infrastructure Lexicon	Version 1.0
23	Draft SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary	Rev. 15
24	POC Additions & Exceptions to the POC Version of SAE J2735	APP190-02
25	VII x.509 Certificate Authority Certificate Practice Statement (CPS)	TBD

APPENDIX C: NATIONAL SYSTEM REQUIREMENTS TRACEABILITY

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
IRS455	VF SEC 07
IRS456	VF SEC 07
IRS457	VF SEC 07
IRS458	VF SEC 07
IRS459	VF SEC 07
IRS460	VF SEC 07
IRS464	VF SEC 06
IRS465	VF SEC 06
IRS488	VF SEC 01