RITA Intelligent Transportation Systems Joint Program Office

Core System: Standards Recommendations Report

www.its.dot.gov/index.htm
October 28, 2011

U.S. Department of Transportation
Research and Innovative Technology Administration

Produced by Lockheed Martin
ITS Joint Program Office
Research and Innovative Technology Administration
U.S. Department of Transportation

Notice

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD MM YYYY)	2. REPORT TYPE	3. DATES COVERED
28 10 2011	(Standards Recommendations Report)	N/A

4. TITLE AND SUBTITLE
Core System: Standards Recommendations Report

5a. CONTRACT NUMBER
GS-23F-0150S
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER
5d. PROJECT NUMBER
DTFH61-10-F-00045
5e. TASK NUMBER
3
5f. WORK UNIT NUMBER

6. AUTHOR(S)
Core System Engineering Team

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lockheed Martin
9500 Godwin Drive
Manassas, VA 20110

8. PERFORMING ORGANIZATION REPORT NUMBER
11-USDOTSE-LMDM-00057

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Department of Transportation
Research and Innovative Technology Administration
ITS Joint Program Office
1200 New Jersey Ave., S.E.
Washington D.C. 20590

10. SPONSORING/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

12b. DISTRIBUTION CODE

13. SUPPLEMENTARY NOTES
Standards Recommendations Report for the Core System portion of the *connected vehicle* program

14. ABSTRACT (Maximum 200 words)
This document describes a set of high-level information objects that comprise the critical interfaces for the Core System and should be considered for standardization by the stakeholder community as they pursue the deployment and implementation of the Core System as part of the United States Department of Transportation's (USDOT) next generation integrated transportation system.

15. SUBJECT TERMS
Standards, interfaces, information objects, data, security, core system, connected vehicle, communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	None	27	Walt Fehr
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER (202) 366-0278

CHANGE LOG

Revision	*Change Summary*	*Author*	*Date*
-	Initial Release	Lockheed Martin	10/21/2011
A	Incorporate comments	Lockheed Martin	10/28/2011

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 Identification

This document is the Standards Recommendations Report for the Core System for the United States Department of Transportation's (USDOT) *connected vehicle* program.

1.2 Document Overview

The USDOT initiated this Systems Engineering (SE) project for the Core System as part of the *connected vehicle* program. The purpose of the Standards Recommendations Report is to identify interfaces that should be considered for standardization; either by modifying existing transportation systems standards or by initiating the development of new standards. The interfaces are identified and defined in the Core System: System Requirements Specification (SyRS) and the Core System: System Architecture Document (SAD). In some cases standards may already exist for a similar type of interface. In those cases the existing standards are identified for consideration.
The Core System Standards Recommendation Report consists of the following sections:

- Section 1.0: provides an overview of the document and the Core System
- Section 2.0: lists the reference documents
- Section 3.0: describes the interfaces into and out of the Core System that should be considered for standardization.

1.3 Core System Overview

The USDOT's *connected vehicle* program envisions the combination of the applications, services, and systems necessary to provide the safety, mobility, and environmental benefits through the exchange of data between mobile and fixed transportation users. It consists of the following:

- **Applications** that provide functionality to realize safety, mobility and environmental benefits,
- **Communications** that facilitate data exchange,
- **Core Systems**, which provide the functionality needed to enable data exchange between and among mobile and fixed transportation users, and
- **Support Systems**, including security credentials certificate and registration authorities that allow devices and systems to establish trust relationships.

The Core System's main mission is to enable safety, mobility, and environmental communications-based applications for both mobile and non-mobile users. The scope of the Core System includes those enabling technologies and services that will provide the foundation for application transactions. The Core System works in conjunction with External Support Systems like the Certificate Authority for Dedicated Short Range Communications (DSRC) security, as defined in IEEE Standard 1609.2. The system boundary for the Core System is not defined in terms of devices or agencies or vendors, but by the open, standardized interface specifications that govern the behavior of all interactions between Core System Users.

The Core System supports a distributed, diverse set of applications. These applications use both wireless and wireline communications to provide:

- Wireless communications with and between mobile elements including vehicles (of all types), pedestrians, cyclists, and other transportation users

- Wireless communications between mobile elements and field infrastructure
- Wireless and wireline communications between mobile elements, field infrastructure, and back office/centers

The Federal Communications Commission (FCC) allocated 75 Megahertz (MHz) of spectrum in the 5.9 Gigahertz (GHz) frequency range for the primary purpose of improving transportation safety. In addition to safety of life and public safety applications, the FCC's Final Report and Order also allowed private and non-safety applications to make use of the spectrum on a lower priority basis.

A critical factor driving the conceptual view of the Core System and the entire *connected vehicle* environment is the level of trustworthiness between communicating parties. While the Core System is being planned for anonymity, it is also providing a foundation from which to leverage alternative communications methods for non-safety applications. These alternatives are typically available on the market today and the levels of anonymity and privacy inherent to these systems are typically governed by agreements between communication providers and consumers. So while privacy is not compromised for an individual, what happens between that individual and their communication provider (e.g., 3G service provider) very well may compromise privacy. Some application providers may require personal information in order to function which would require the Application User to opt-in to use that application.

Within the *connected vehicle* environment the Core System concept distinguishes communications mechanisms from data exchange and from the services needed to facilitate the data exchange. The Core System supports the *connected vehicle* environment by being responsible for providing the services needed to facilitate the data exchanges. The contents of the data exchange are determined by applications unless the data exchange is used as part of the facilitation process between the user and the Core System.

The Core System provides the functionality required to support safety, mobility, and environmental applications. This same functionality may also enable commercial applications but that is not a driving factor for the development of the Core System. The primary function of the Core System is the facilitation of communications between users and some of this communication must also be secure. The Core System may also provide data distribution and network support services depending on the needs of the Core System deployment.

A critical factor driving the conceptual view of the Core System and the entire *connected vehicle* environment is the level of trustworthiness between communicating parties. A complicating factor is the need to maintain the privacy of participants, though not necessarily exclusively through anonymous communication.

For additional information on the Core System, please reference the Core System Concept of Operations (ConOps) document.

2.0 REFERENCED DOCUMENTS

- Core System Concept of Operations (ConOps), Rev E, October 24, 2011
- Core System Requirements Specification (SyRS) Rev F, October 28, 2011
- System Architecture Document (SAD), Rev C, October 14, 2011
- Vehicle Infrastructure Integration (VII) Probe Data Service (PDS) Broker System Design and Interface Design Document
- VII Service Delivery Node (SDN)/Advisory Message Distribution Service (AMDS) Broker System Design and Interface Document
- SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 5272, Certificate Management over Cryptographic Message Syntax (CMS) (CMC)
- IETF RFC 5273, Certificate Management over CMS (CMC): Transport Protocols
- IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- IETF RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification
- IETF RFC 5906, Network Time Protocol Version 4: Autokey Specification
- IETF RFC 5907, Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)
- IETF RFC 5908, Network Time Protocol (NTP) Server Option for Dynamic Host Configuration Protocol over Internet Protocol version 6 (DHCPv6)

3.0 CORE SYSTEM INTERFACE STANDARDS RECOMMENDATIONS

The interfaces into and out of the Core System provide opportunities for information to be shared electronically with other systems.

Standards are fundamental to the establishment of an open systems environment. Standards facilitate deployment of interoperable systems without impeding innovation as technology advances and new approaches evolve.

It is important for the deployment of the Core System and for the support that the Core System provides to the overall *connected vehicle* environment, that those interfaces with other systems (including other Core Systems) be defined based on industry accepted standards.

3.1 Core System Top Level Functional View

The diagram below shows the top level interfaces for the Core System. Interfaces are described in the SAD by the Information Objects they carry. Information Objects are descriptions of data along with the necessary structure and syntax to allow their interpretation and use. An Information Object may also have associated metadata – data about the data. The Information Views may define the relationships among Information Objects, rules for their use and transformation, and policies on access. In the figure, objects which have a bold outline are to be secured in some way. Objects with a white background originate from outside of the Core System while the other objects are color-coded to match the subsystem which generates the output. Objects that have italicized text are those that require an acknowledgement from the recipient.

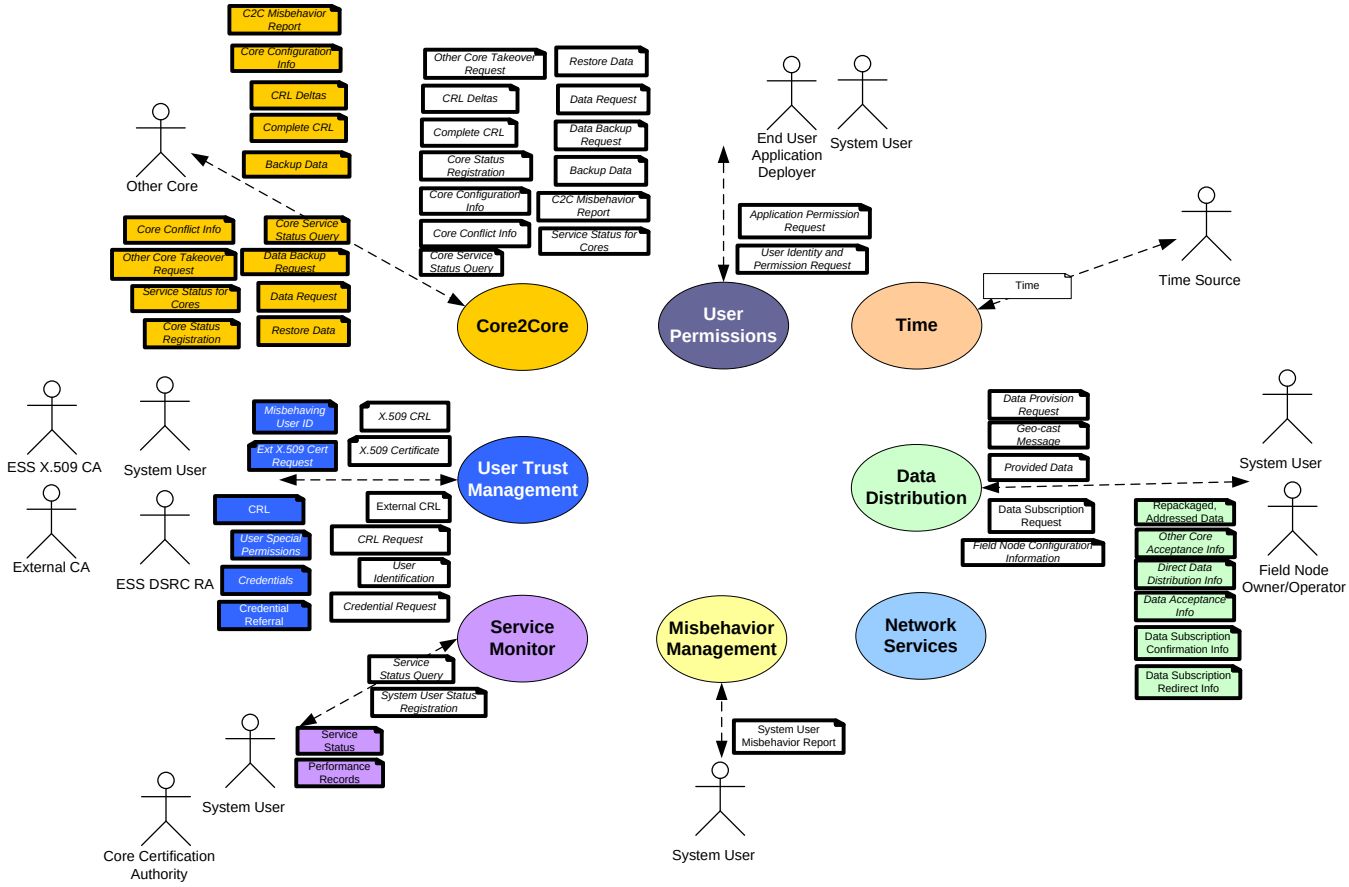

Figure 3-1. Core System Functional View – Top Level Interfaces

These external system interfaces represent the opportunities to standardize the interfaces that would be implemented between disparate systems. The human machine interface between the Core System and its operators is not depicted above and is not a candidate for standardization.

3.2 Core System External Interface Information Objects

The interfaces can also be represented in an Information View as a set of Information Objects that are organized by the subsystems that generate or receive them. The figure below shows the Core System Information View that organizes External Information Objects (see section 3.6 of the SAD for a description of the notations in the figure). These are the same objects shown in the functional view above but are shown with a different organization.

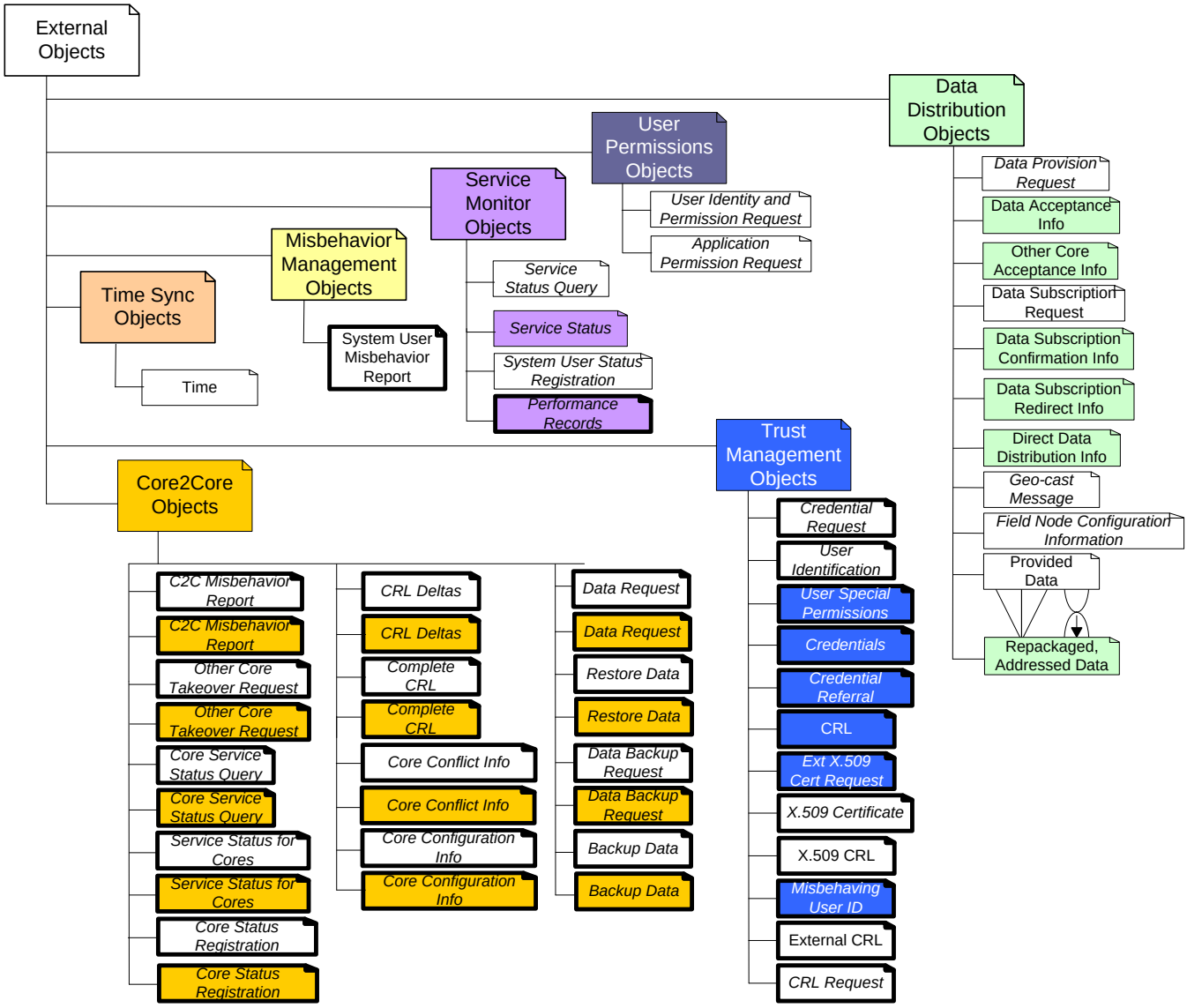

Figure 3-2. Information View – Top Level External Objects

The object descriptions are included in section 3.4 beginning on page 16.

3.3 Information Objects Standardization Candidates

Some of the information objects identified above are already standardized or are the subject of other development efforts. Others require new development efforts.

The new standards activities can be grouped by the type of interface over which these information objects would travel as shown in the table below. In many cases, the information objects may be defined as messages or message sets going between systems over these interfaces. Standards Development Organizations (SDOs) may decide to group or bundle the data differently as they develop the standards.

The tables below show the Information Objects numbered as they are in section 4.5 of the SAD and grouped by the type of interface. The following types of interfaces are defined:

- Core-to-Core: The interfaces between peer Core Systems over fixed-point (likely wired) communications infrastructure using Internet Protocols v6 (IPv6) and most likely secured as discussed in the SAD. See Table 3-1.
- Core-to-ESS: Core Systems will have an interface with External Support Systems that provide certificates and to exchange other security/trust related information. This interface type will also likely be over fixed, wired communications infrastructure using Internet Protocols v6 (IPv6) and most likely secured as discussed in the SAD. See Table 3-2.
- Core-to-System Users: System Users (applications) may be located in a Center, in the Field, or in a Mobile device. These interfaces share the fact that the communications with the Core System will be based on standardized Internet Protocols, i.e. IPv6. The structure of the message content should be consistent regardless of the type of interface used. See Table 3-3.
- Core-to-Other Support: These include the interfaces to a standard Time Source, the application developers, and the Core Certification Authority (CCA). See Table 3-4.

For each object the tables list any applicable standards activities or whether a new activity is recommended. The right most column shows any other applicable references or notes.

Table 3-1. Core to Core Interface and Applicable Standards

Information Object	Applicable Standard	Other Notes
4.5.1.3.1.1 Backup Data	New standard for Core-to-Core interface is recommended.	A protocol like File Transfer Protocol might be used to transfer the data but other more secure and efficient means should be investigated.
4.5.1.3.1.2 C2C Misbehavior Report	New standard for Core-to-Core interface is recommended.	The message content is different than the Misbehavior Report objects to and from System users (object ID 4.5.1.3.3.1). This report may include additional information about the misbehavior that may be part of the Intrusion Protection System component of the Core System.
4.5.1.3.1.3 Complete CRL	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.

Information Object	Applicable Standard	Other Notes
4.5.1.3.1.4 CRL Deltas	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.
4.5.1.3.1.5 Core Configuration Info	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.6 Core Conflict Info	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.7 Core Service Status Query	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.8 Core Status Registration	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.9 Data Backup Request	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.10 Data Request	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.11 Other Core Takeover Request	New standard for Core-to-Core interface is recommended.	
4.5.1.3.1.12 Restore Data	New standard for Core-to-Core interface is recommended.	A protocol like File Transfer Protocol might be used to transfer the data but other more secure and efficient means should be investigated.
4.5.1.3.1.13 Service Status for Cores	New standard for Core-to-Core interface is recommended.	

The table below lists the information objects that pertain to the interface with the External Support Systems pertaining to trust credentials. Many of these objects are based on concepts that have already been well defined and standardized by the Internet Engineering Task Force (IETF) through their Request for Comments (RFC) document process. Some objects identified here are unique to the interface between a Core System and an External Support System (ESS) in the *connected vehicle* environment.

Table 3-2. Core to External Support System (ESS) Interface and Applicable Standards

Information Object	Applicable Standard	Other Notes
4.5.1.3.8.1 Credential Request	Existing standards are available for this object, see: RFC 4211: Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	Other RFCs pertaining to certificate management may apply as well.
4.5.1.3.8.2 Credential Referral	New standard for Core-to-ESS interface is recommended.	New concept for Core Systems that will need to be standardized.
4.5.1.3.8.3 Credentials	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to the definition of digital certificates and their management.
4.5.1.3.8.4 CRL	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.
4.5.1.3.8.5 CRL Request	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.

Information Object	Applicable Standard	Other Notes
4.5.1.3.8.6 Ext X.509 Cert Request	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.
4.5.1.3.8.7 External CRL	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.
4.5.1.3.8.8 Misbehaving User ID	New standard for Core-to-ESS interface is recommended.	New concept for Core Systems and will need to be standardized, may be able to leverage the definition of some content from IETF RFCs.
4.5.1.3.8.9 User Identification	New standard for Core-to-ESS interface is recommended.	
4.5.1.3.8.10 User Special Permissions	New standard for Core-to-ESS interface is recommended.	
4.5.1.3.8.11 X.509 Certificate	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.

Information Object	Applicable Standard	Other Notes
4.5.1.3.8.12 X.509 CRL	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.

The table below lists the information objects that pertain to the interface with the System Users pertaining to data distribution, misbehavior reporting, system status monitoring, user permissions, and user trust management. Some of these objects can start with previous work from the VII program to define publish/subscribe interfaces and with the SAE J2735 message standard for the DSRC communications. The security or trust management related objects are based on concepts that have already been well defined and standardized by the Internet Engineering Task Force (IETF) through their Request for Comments (RFC) document process.

Table 3-3. Core to System User Interface and Applicable Standards

Information Object	Applicable Standard	Other Notes
4.5.1.3.2.1 Data Acceptance Info	New standard for Core-to-System User interface is recommended.	
4.5.1.3.2.2 Data Provision Request	New standard for Core-to-System User interface is recommended.	
4.5.1.3.2.3 Data Subscription Confirmation Info	New standard for Core-to-System User interface is recommended.	VII Probe Data Service (PDS) Broker System Design and Interface Design Document should be reviewed for content and formatting.
4.5.1.3.2.4 Data Subscription Redirect Info	New standard for Core-to-System User interface is recommended.	
4.5.1.3.2.5 Data Subscription Request	New standard for Core-to-System User interface is recommended.	VII Probe Data Service (PDS) Broker System Design and Interface Design Document should be reviewed for content and formatting.
4.5.1.3.2.6 Direct Data Distribution Info	New standard for Core-to-System User interface is recommended.	
4.5.1.3.2.7 Field Node Configuration Information	New standard for Core-to-System User interface is recommended.	
4.5.1.3.2.8 Geo-Cast Message	New standard for Core-to-System User interface is recommended.	VII SDN/AMDS Broker System Design and Interface Document

Information Object	Applicable Standard	Other Notes
4.5.1.3.2.9 Other Core Acceptance Info	New standard for Core-to-System User interface is recommended.	
4.5.1.3.2.10 Provided Data	Existing standards are available for this object, see: SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary.	SAE J2735 focused on Vehicle-provided data so it applies for data provided from Mobile Users. New standard for Core-to-System User interface is recommended for Field and Center-provided data.
4.5.1.3.2.11 Repackaged, Addressed Data	New standard for Core-to-System User interface is recommended.	Content may also be based on SAE J2735 for probe data and advisory message content.
4.5.1.3.3.1 System User Misbehavior Report	New standard for Core-to-System User interface is recommended. Possible addition of a misbehavior report msg to SAE J2735.	
4.5.1.3.5.2 Service Status	New standard for Core-to-System User interface is recommended.	
4.5.1.3.5.3 Service Status Query	New standard for Core-to-System User interface is recommended.	
4.5.1.3.5.4 System User Status Registration	New standard for Core-to-System User interface is recommended.	
4.5.1.3.7.2 User Identity and Permission Request	New standard for Core-to-System User interface is recommended.	
4.5.1.3.8.1 Credential Request	Existing standards are available for this object, see: RFC 4211: Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	Other RFCs pertaining to certificate management may apply as well.
4.5.1.3.8.2 Credential Referral	User Trust Management Interface Std is recommended.	New concept for Core Systems that will need to be standardized.
4.5.1.3.8.3 Credentials	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to the definition of digital certificates and their management.

Information Object	Applicable Standard	Other Notes
4.5.1.3.8.4 CRL	Existing standards are available for this object, see: RFC 5272: Certificate Management over CMS RFC 5273: Certificate Management over CMS (CM); Transport Protocols RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Many other relevant RFCs, those named are most related to CRLs and CRL management.

The table below lists the information objects that pertain to the interface with the other external systems with which the Core System will interface: Core Certification Authority (CCA) will monitor system performance relative to the established goals. The Core System will maintain an interface with an external time source. The Core System will also provide an interface for potential *connected vehicle* application developers to request permissions for their applications to access Core System services. The time related objects are based on concepts that have already been well defined and standardized by the Internet Engineering Task Force (IETF) through their Request for Comments (RFC) document process.

Table 3-4. Core to Other Support System Interfaces and Applicable Standards

Information Object	Applicable Standard	Other Notes
4.5.1.3.5.1 Performance Records	New standard for Core-to-CCA interface is recommended.	
4.5.1.3.6.1 Time	Existing standards are available for this object, see: RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification RFC 5906: Network Time Protocol Version 4: Autokey Specification RFC 5907: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4) RFC 5908: Network Time Protocol (NTP) Server Option for DHCPv6	
4.5.1.3.7.1 Applications Permission Request	New standard for interface to potential application developers is recommended.	

3.4 Information Objects for New Standards Activities

The following listing of objects is taken from the Information View – Top Level External Objects of the SAD. This listing provides details of the objects in the tables above that are exchanged, sent, and received over the Core System's external interfaces and that should be potentially be standardized. They are numbered based on the way they are numbered in section 4.5 of the SAD for easier reference. Descriptions of the objects that are already standardized can be found in the SAD.

4.5.1.3.1.1 Backup Data
Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Cores that have established relationships for backup and takeover.
Description: This is data extracted from a Core data store. Contents depend on the contents of that data store. Format is dependent on the receiving Core's formatting specification.

4.5.1.3.1.2 C2C Misbehavior Report
Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Cores that have established relationships for exchange of misbehavior information. In practice, this will probably be limited to Cores that share geographic boundaries or have overlapping service areas.
Description: This includes the certificate ID associated with misbehavior, the type of misbehavior, time of the misbehavior, time of the misbehavior detection, certificate ID of the misbehavior report generator, and if available the identity of the misbehaving entity.

4.5.1.3.1.4 Core Configuration Info
Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with all other Cores that have a boundary or coverage area in common with or have a backup/takeover relationship with the Core System.
Description: This is a description of the services offered by the Core reporting the configuration info. Includes the area over which the service is offered, to whom the service is offered and a measure of the maximum expected performance of the Core's provision of those services (e.g., Data Distribution: max 500 subscribers and total data output < 10 Mb/s).

4.5.1.3.1.5 Core Conflict Info
Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with all other Cores that have a boundary or coverage area in common with the Core System.

Description: This is a description of the conflict in service provision between the two Cores. It includes the services that are in conflict and a description of the nature of the conflict, including area and System User types affected.

4.5.1.3.1.6 Core Service Status Query

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Core Systems that have a need to understand the status of services of one another. In practice this is likely limited to Cores that share geographic boundaries or have overlapping service areas.
Description: This requests the status of the targeted Core's services.

4.5.1.3.1.7 Core Status Registration

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Core Systems that have a need to understand the status of services of one another. In practice this is likely limited to Cores that share geographic boundaries or have overlapping service areas.
Description: This requests that the targeted Core provide the sending Core with status information on a periodic basis. The message includes the requestor's IP address, the services for which it requires status, the detail level of information to be provided and desired update frequency.

4.5.1.3.1.9 Data Backup Request

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Cores that have established relationships for backup and takeover.
Description: This is the request sent to a Core that has a backup relationship with the sending Core. It includes the following characteristics of the data the Core wishes to back up: type of data store (e.g. Data Subscription Catalog), size of data to be backed up, desired backup start time, required backup completion time, length of time data must be backed up, projected restoration time (if any).

4.5.1.3.1.10 Data Request

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Cores that have established relationships for backup and takeover.
Description: This is the request sent to a Core that has previously backed up data. It includes the data store the Core wishes to restore, the time it needs the restore to start, the time it needs the restore to complete by.

4.5.1.3.1.11 Other Core Takeover Request

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed
Notes: Exchanged with Cores that have established relationships for service takeover. In practice, this will probably be limited to Cores that share geographic boundaries or have overlapping service areas.
Description: This includes the service, coverage area, start and expected end time and expected performance load that the Core wants the destination Core to provide service for.

4.5.1.3.1.12 Restore Data

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Cores that have established relationships for backup and takeover.
Description: This is formerly backed up data. The contents depend on the contents of that data store. Format is dependent on the sending Core's formatting specification.

4.5.1.3.1.13 Service Status for Cores

Directionality: Input and Output
Source/Destination: Other Core
Attributes: Digitally Signed and Secure, Acknowledgement required
Notes: Exchanged with Core Systems that have a need to understand the status of services of one another. In practice this is likely limited to Cores that share geographic boundaries or have overlapping service areas.
Description: This describes the status of all of the Core's services. For each service it includes the following data: state, mode, time of last mode transition, previous mode, projected time until next mode transition (if known), % load of maximum.

4.5.1.3.2.1 Data Acceptance Info

Directionality: Output
Source/Destination: System User
Attributes: Digitally Signed
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or by geometric area specified by polygon using lat/long coordinates as vertices. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This is the response to the Data Provision Request. Indicates the service area over which the data in the Data Provision Request is accepted. This message may also be provided if a System User provides data that the Core does not accept.

4.5.1.3.2.2 Data Provision Request

Directionality: Input
Source/Destination: System User
Attributes: Digitally Signed, Acknowledgement Required
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This includes the type of data to be provided, source type and area over which the System User will provide data. For Mobile Users this is limited to SAE J2735 message types. For Field and Center Users this may include messages in SAE J2735, but may include other messages.

4.5.1.3.2.3 Data Subscription Confirmation Info

Directionality: Output
Source/Destination: System User
Attributes: Digitally Signed
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This is a response to the Data Subscription Request, describing the exact parameters of the System User's subscription.
Applicable Standard: New Data Distribution Interface Std is recommended. VII Probe Data Service (PDS) Broker System Design and Interface Design Document may provide foundation.

4.5.1.3.2.4 Data Subscription Redirect Info

Directionality: Output
Source/Destination: System User
Attributes: Digitally Signed
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This is a response to the Data Subscription Request, rejecting the subscription. If the Core knows of another Core that may be able to satisfy the subscription, this message includes the IP address of that Core.

4.5.1.3.2.5 Data Subscription Request

Directionality: Input
Source/Destination: System User
Attributes: Digitally Signed

Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This is the request to subscribe to data; includes the System User's Core account name and authorization and the following:

- Data the System User wishes to subscribe to (SAE J2735 messages if Mobile)
- Maximum data acceptance rate
- Aggregation time for the data (e.g., 1 hour would result in only 1 message per hour, with the message content the aggregation of the data elements over that one hour period)
- Sampling rate for the data (e.g., 1 in every 10 samples)
- Desired start time for subscription
- Desired end time for subscription

4.5.1.3.2.6 Direct Data Distribution Info

Directionality: Output
Source/Destination: System User
Attributes: Digitally Signed
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This is data describing 3rd parties that accept data that the Core does not accept. Includes the IP address and format expectations of the 3rd party.

4.5.1.3.2.7 Field Node Configuration Information

Directionality: Input
Source/Destination: System User
Attributes: Digitally Signed, Acknowledgement required
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users. Use of geo-cast messaging may be limited; criteria for establishing those limits must be defined.
Description: This specifies the location, IP address, communications range, bandwidth and constraints for use of Field Node Infrastructure. Constraints on the use of the Field Node may be imposed by the Field Node Owner/Operator, and also need to be specified here.

4.5.1.3.2.8 Geo-Cast Message

Directionality: Input
Source/Destination: System User

Attributes: Digitally Signed, Acknowledgement required
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users. Use of geo-cast messaging may be limited; criteria for establishing those limits must be defined.
Description: This is a message that the System User wishes to distribute over a specific area, either once or repeatedly over a period of time. The message includes the content to be distributed and information describing the desired distribution area and time over which the distribution should be made.

4.5.1.3.2.9 Other Core Acceptance Info

Directionality: Output
Source/Destination: System User
Attributes: Digitally Signed
Notes: Specification of coverage areas need to be standardized, so that System Users and Cores all have a common frame of reference for when dealing with data acceptance information. For example, coverage areas could be organized by county, or a fraction of lat/long coordinates. Similarly, Cores must operate with the same concepts of System User types (e.g., Transit Vehicles) so that they may properly coordinate activities that are limited to certain types of System Users.
Description: This is the response to the Data Provision Request, sent when the Core does not accept the data the System User wishes to provide. It indicates the IP Address of another Core that services the area referenced in the Data Provision Request.

4.5.1.3.2.10 Provided Data

Directionality: Input
Source/Destination: System User
Attributes: Digitally Signed
Notes: Data from Mobile Users restricted to what is permitted by SAE J2735.
Description: This is data received from System User Data Providers intended for the publish/subscribe engine. Format of the data received from System Users is described by SAE J2735. Message formats for Field and Center Users are TBD.

4.5.1.3.2.11 Repackaged, Addressed Data

Directionality: Output
Source/Destination: System Users
Attributes: Digitally Signed
Notes: If the Core does not perform sampling, aggregation or selection of specific data fields, then there is no transformation or aggregation relationship with the incoming Data.
Description: This is data repackaged to match a specific subscriber's subscription criteria. This is data that was originally provided by other System Users (Data, above) that has been selected based on subscription criteria. If the subscription includes aggregation or sampling then the data will be aggregated or sampled as appropriate. If the subscription requested selection of specific data fields of incoming Data messages, then only those fields would be included.

4.5.1.3.3.1 System User Misbehavior Report

Directionality: Input
Source/Destination: System Users
Attributes: Digitally Signed
Notes: System Users will have to be characterized for reliability and believability in order to use misbehavior reports they provide.
Description: This is data describing misbehaving users. It Includes the certificate ID associated with misbehavior, the type of misbehavior, time of the misbehavior, time of the misbehavior detection, certificate ID of the misbehavior report generator, and if available the identity of the misbehaving entity.

4.5.1.3.5.1 Performance Records

Directionality: Output
Source/Destination: Core Certification Authority
Attributes: Digitally Signed, Secure, Acknowledgement Required
Notes: Makeup and operations of the Core Certification Authority may impact the information desired in this message.
Description: This is detailed information describing the long-term performance of Core services, provided to the Core Certification Authority. It includes of a record of availability for each system service since the last reporting period, performance loading records for services, and conflicts reported between this Core and other Cores.

4.5.1.3.5.2 Service Status

Directionality: Output
Source/Destination: System Users
Attributes: Digitally signed, optionally Acknowledgement Required
Notes: None.
Description: This is the status of the Core's subsystems. This may be limited to specific subsystems if in response to a query. For each service, this message indicates the current state and mode and if there is a known time for that state or mode to change.

4.5.1.3.5.3 Service Status Query

Directionality: Input
Source/Destination: System Users
Attributes: Digitally Signed, Acknowledgement Required
Notes: None.
Description: This is the request from System Users for Core service status information. Includes a listing of the services the System User desires status information about.

4.5.1.3.5.4 System User Status Registration

Directionality: Input
Source/Destination: System User

Attributes: Digitally Signed, Acknowledgement Required
Notes: None.
Description: This is a request from a System User to register for periodic reports of the Core's service status. It includes the System User's IP Address and desired update frequency

4.5.1.3.7.1 Application Permission Request

Directionality: Input
Source/Destination: End User Application Developer
Attributes: Digitally Signed and Acknowledgement Required
Notes: Dependent on the Core's support for field applications.
Description: This is a submission of application permissions that must be managed using IEEE 1609.2 certificates. It includes the identification of the application, developer, version, and certificate permission information according to the formats in IEEE 1609.2.

4.5.1.3.7.2 User Identity and Permission Request

Directionality: Input and Output
Source/Destination: System User
Attributes: Digitally Signed and Acknowledgement Required
Notes: Dependent on the Core's support for field applications. Since the identity credentials include Personally Identifiable Information (PII), this message could impact the privacy of System Users.
Description: This is a submission of identity credentials and a request for permissions to use the Core System services. Optionally includes a request for application services managed by certificates distributed by the Core.

4.5.1.3.8.1 Credential Request

Directionality: Input
Source/Destination: System User
Attributes: Digitally Signed and Acknowledgement Required
Notes: Signed using the System User's currently valid digital certificate. If they have no such certificate, they must have a long term "base, low permissions" certificate that enables this request.
Description: This is request for credentials. It includes the System User's identity and the period of time the user needs the new certificate to be valid for.

4.5.1.3.8.2 Credential Referral

Directionality: Output
Source/Destination: System User
Attributes: Digitally Signed and Acknowledgement Required
Notes: None.
Description: This message is provided in response to a credential request that the Core cannot satisfy. It contains the IP address of another Core or ESS that provides the type of credentials the System User is requesting.

4.5.1.3.8.8 Misbehaving User ID

Directionality: Output
Source/Destination: External Support System X.509 CA or External Support System DSRC CA.
Attributes: Digitally Signed, Secure and Acknowledgement Required
Notes: Standardized types of misbehavior will have to be defined. Interfaces to the ESS CAs will have to be defined. Feasibility of obtaining revocation from ESS X.509 CA is TBD.
Description: This contains the ID and type of misbehavior the System User has committed. Depending on the method of identification, the contents could include a user ID, a certificate ID or a pseudo-ID.

4.5.1.3.8.9 User Identification

Directionality: Input
Source/Destination: ESS DSRC Registration Authority
Attributes: Digitally Signed and Acknowledgement Required
Notes: Establishment of standard System User classes must be done in order to use the acquire permissions for classes of users without requiring identity. Since the message includes PII, this message could impact the privacy of System Users.
Description: This is a request for special permissions for a System User from the ESS DSRC RA. It includes an identification of the System User or the class that the System User is part of that the RA wishes to acquire permissions for.

4.5.1.3.8.10 User Special Permissions

Directionality: Output
Source/Destination: ESS DSRC Registration Authority
Attributes: Digitally Signed and Acknowledgement Required
Notes: Establishment of standard System User classes must be done in order to use the acquire permissions for classes of users without requiring identity. Since the identity referenced by this message could be PII, this message could impact the privacy of System Users.
Description: This is the response to the ESS DSRC RA. It includes an identification of the special permissions the user is entitled to.