RITA Intelligent Transportation Systems
Joint Program Office

Core System System Requirements Specification (SyRS)

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

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Report Documentation Page

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE **Core System: System Requirements Specification (SyRS)**	**5a. CONTRACT NUMBER** GS-23F-0150S **5b. GRANT NUMBER** N/A
6. AUTHOR(S) Core System Engineering Team	**5c. PROGRAM ELEMENT NUMBER** N/A **5d. PROJECT NUMBER** DTFH61-10-F-00045 **5e. TASK NUMBER** 3 **5f. WORK UNIT NUMBER** N/A
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Lockheed Martin 9500 Godwin Drive Manassas, VA 20110	**8. PERFORMING ORGANIZATION REPORT NUMBER** 11-USDOTSE-LMDM-00054
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 System Requirements Specification (SyRS) for the Core System portion of the *connected vehicle* program	

14. ABSTRACT (Maximum 200 words)

This document describes the Requirements of the Core System for the United States Department of Transportation's (USDOT) next generation integrated transportation system. It describes the requirements at the system level and at the subsystem level as identified in the Core System ConOps. Each system requirements is traceable to Needs in the ConOps. Requirements are also traceable to functional objects in the Core System System Architecture Document (SAD).

15. SUBJECT TERMS

Connected vehicle, core system, needs, requirements, subsystems, security, credentials, data distribution

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT** None	**18. NUMBER OF PAGES** 162	**19a. NAME OF RESPONSIBLE PERSON** Walt Fehr
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified			**19b. TELEPHONE NUMBER** (202) 366-0278

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39-18

CHANGE LOG

Revision	*Change Summary*	*Author*	*Date*
-	Initial Release	Lockheed Martin	4/18/2011
A	Disposition of both Customer comments and Walkthrough comments incorporated in this revision.	Lockheed Martin	6/13/2011
B	Workshop comments incorporated	Lockheed Martin	7/18/2011
B'	Edits from internal LM review – editorial comments and change to mappings for 2 system requirements.	Lockheed Martin	7/19/2011
C	August 1-3 Walk-through comments have been incorporated in this revision and requirements have been traced to System Needs and System Architecture Objects	Lockheed Martin	9/06/2011
D	Corrected requirements that had reference numbers to Information Objects defined in the System Architecture Document; added table of removed requirements related to DSRC security.	Lockheed Martin	9/15/2011
E	Corrected Performance Reports to Core Certification Authority (CCA) and other feedback from the requirements and architecture walkthroughs.	Lockheed Martin	10/14/2011
F	Corrected the section number for Geo-cast Message Log object and some minor grammatical errors.	Lockheed Martin	10/28/2011

TABLE OF CONTENTS

Section ***Title*** ***Page***

1 Scope ... 1
1.1 Identification ... 1
1.2 Document Overview ... 1
1.3 System Overview ... 2
1.4 Stakeholders ... 10
2 Documents ... 11
2.1 Referenced Documents ... 11
2.2 Resource Documents ... 11
3 Requirements ... 15
3.1 System Requirements ... 15
3.1.1 System Functional Requirements ... 15
3.1.2 System Performance Requirements ... 20
3.1.3 System Interface Requirements ... 20
3.1.4 Non-functional Requirements ... 21
3.1.5 Constraints ... 22
3.2 Subsystem Requirements ... 22
3.2.1 Core2Core Subsystem ... 22
3.2.2 Data Distribution Subsystem ... 27
3.2.3 Misbehavior Management Subsystem ... 32
3.2.4 Network Services Subsystem ... 35
3.2.5 Service Monitor Subsystem ... 37
3.2.6 Time Synchronization Subsystem ... 39
3.2.7 User Permissions Subsystem ... 40
3.2.8 User Trust Management Subsystem ... 44
4 Verification Methods ... 49
4.1 System Requirements Verification ... 49
4.2 Subsystem Requirements Verification ... 51
5 Supporting Documentation ... 54
5.1 Core System Needs ... 54
5.2 State and Modes ... 61
5.3 Internet Based Communications Standards ... 63
5.4 Action Verbs ... 70
5.5 Internal Interfaces ... 73
5.6 DSRC Security Credential Requirements ... 73
6 Traceability Matrices ... 78
6.1 Needs to Requirements Traceability ... 78

6.1.1 Core System Needs to System Requirements Matrix 78
6.1.2 System Requirements to Core System Needs Matrix 81
6.1.3 System to Subsystem Matrix 85
6.1.4 Subsystem to System Matrix 88
6.2 Requirements to Architecture Components 91
6.2.1 Subsystem Requirements to Architecture Traceability.. 91
6.2.2 Architecture to Subsystem Requirements Traceability... 117
6.2.3 System Requirements to Architecture Traceability 137
7 Terminology.. 138
7.1 Glossary... 138
7.2 Abbreviations and Acronyms.. 151
8 Metric/English Conversion Factors 155

LIST OF FIGURES

Figure ***Title*** ***Page***

Figure 1-1. Core System Boundary Diagram 5

Figure 1-2. Core System Context Diagram.......... 6

Figure 1-3. Core System Subsystem Context 7

Figure 5-1: Subsystem State Transitions 61

Figure 5-2: Standby and Operational Modes 62

Figure 5-3: Training Modes 62

LIST OF TABLES

Table ***Title*** ***Page***

Table 4-1. System Requirements Verification Matrix 49

Table 4-2. Subsystem Requirements Verification Matrix 51

Table 5-1. Core System Needs.......... 55

Table 5-2. Network Time Protocol (NTP) Standards 63

Table 5-3. PKI X.509 Standards 63

Table 5-4. Requirements Action Verb Definitions 70

Table 5-5. Internal Subsystem to Subsystem Interfaces 73

Table 5-6. DSRC Security Related Requirements 74

Table 6-1. Core System Needs to System Requirements Traceability Matrix 78

Table 6-2. System Requirements to Core System Needs Traceability 81

Table 6-3. System Requirements (SR) to Subsystem Requirements (SSR) Traceability.......... 85

Table 6-4. Subsystem Requirements (SSR) to System Requirements (SR) Traceability.......... 88

Table 6-5. Subsystem Requirement to Architecture Object Traceability 91

Table 6-6. Architecture View/Object to Subsystem Requirement Traceability 117

Table 6-7. System Requirement to Architecture Object Traceability.......... 137

Table 7-1. Glossary.......... 138

Table 7-2. Abbreviation and Acronym List.......... 151

1 Scope

1.1 Identification

This document is the System Requirements Specification (SyRS) of 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 to define the ConOps, requirements, and architecture for a system that will enable safety, mobility, and environmental applications in an environment where vehicles and personal mobile devices are connected wirelessly, hereafter referred to as the *connected vehicle* environment.

The ConOps is a prerequisite to this document and is recommended reading prior to the SyRS. The ConOps describes the characteristics of the Core System from the system user's viewpoints. The SyRS builds upon those concepts, particularly the User Needs, to document the required functionality, performance, interfaces, and other required characteristics for the Core System.

The structure of this SyRS document is based on Institute of Electrical and Electronics Engineers (IEEE) Standard 1233-1998 IEEE Guide for Developing System Requirements Specifications and Federal Highway Administration's (FHWA) System Engineering Guidebook (SEGB) that adapted IEEE-1233.

The SyRS document consists of the following sections:

- Section 1 provides an overview of the Core System and an introduction to this SyRS document.
- Section 2 lists the documents used as background information or as a source of requirements.
- Section 3 provides the requirements for the Core System. They are organized by the level, either System or one of the 8 subsystems, and then by type of requirement.
    - Section 3.1: System Requirements
        - Section 3.1.1: System Functional Requirements
        - Section 3.1.2: System Performance Requirements
        - Section 3.1.3: System Interface Requirements
        - Section 3.1.4: Non-Functional System Requirements
        - Section 3.1.5: Constraints

- Section 3.2: Subsystem Requirements
    - Section 3.2.1: Core2Core Subsystem Requirements
    - Section 3.2.2: Data Distribution Subsystem Requirements
    - Section 3.2.3: Misbehavior Management Subsystem Requirements
    - Section 3.2.4: Network Services Subsystem Requirements
    - Section 3.2.5: Service Monitor Subsystem Requirements
    - Section 3.2.6: Time Synchronization Subsystem Requirements
    - Section 3.2.7: User Permissions Subsystem Requirements
    - Section 3.2.8: User Trust Management Subsystem Requirements

The subsystem requirements sections each include the functional, performance, interface, and data requirements for that subsystem.

- Section 4 lists the Verification Method of each requirement from Section 3.
- Section 5 provides a listing of Supporting Documentation.
- Section 6 provides the Traceability Matrices tracing each requirement to the User Needs and vice versa.
- Section 7 contains a Glossary of terms and a listing of abbreviations and acronyms.
- Section 8 contains a table of Metric to English measurement conversion factors

The intended audience for this System Requirements Specification (SyRS) includes:

- USDOT
- Transportation managers (including state and local Departments of Transportation (DOTs))
- Vehicle manufacturers and other device manufacturers or software developers
- Information service providers
- Fleet managers
- Commercial vehicle operators and regulators
- Application developers
- Potential Core System acquirers, deployers, operators, and maintainers.

1.3 System Overview

The USDOT's *connected vehicle* program envisions the combination of applications, services and systems necessary to provide 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 in turn provide the foundation for applications. 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. This allowed the VII program and associated research efforts to test the capabilities of 5.9 GHz DSRC for vehicular based safety and mobility applications.

VII considered that some safety and mobility applications would be installed on all participating vehicles. Some safety applications would have been mandated to be installed on participating vehicles. Non-safety or mobility applications would have been installed on an opt-in basis however. The work following VII retains those possibilities that some applications may be mandated for safety while others would be optional.

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, but not necessarily exclusively through anonymous communication. The Core System is planning anonymity into the trusted exchange of data, using the existing privacy principles (VII Privacy Policies Framework version 1.0.2) as guidelines, and balancing privacy against security and safety.

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.

VII was conceived as a nationally deployed and managed system but the current thinking is that the *connected vehicle* system will likely be deployed locally and regionally and it must be able to grow organically to support the changing needs of its user base. Deployments will likely be managed regionally but will need to follow national standards to ensure that the essential capabilities are compatible no matter where the deployments are established.

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 enable commercial applications, but that is not a driving factor, rather a side effect. The primary function of the Core System is the facilitation of communications between users, some of which 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.

The Core System exists in an environment where it facilitates interactions between vehicles, field infrastructure and backoffice users, as illustrated in Figure 1-1 below.

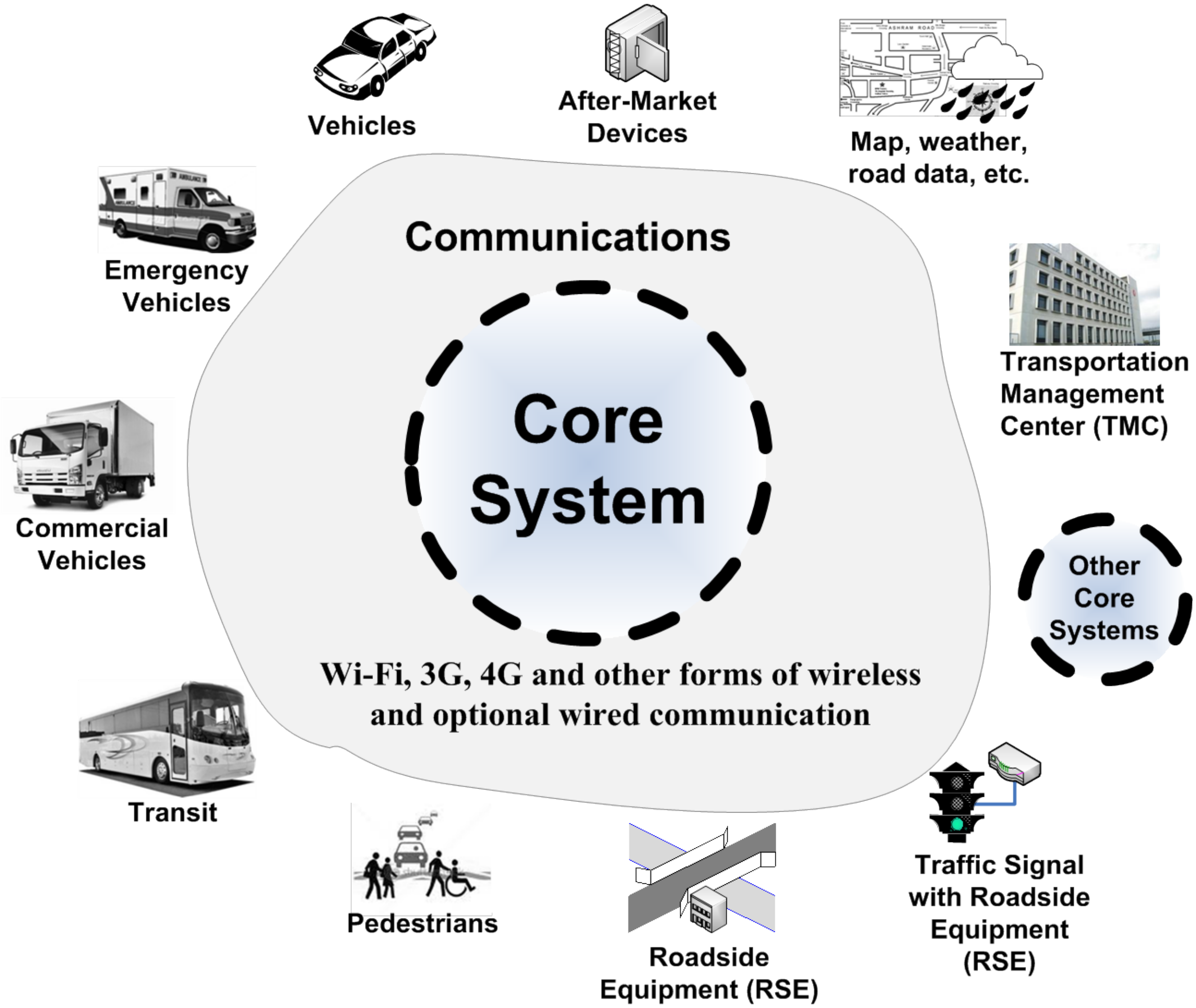

Vehicles
After-Market Devices
Map, weather, road data, etc.
Emergency Vehicles
Communications
Transportation Management Center (TMC)
Core System
Commercial Vehicles
Other Core Systems
Wi-Fi, 3G, 4G and other forms of wireless and optional wired communication
Transit
Traffic Signal with Roadside Equipment (RSE)
Pedestrians
Roadside Equipment (RSE)

Figure 1-1. Core System Boundary Diagram

In Figure 1-1 above, the users, devices, and software applications are outside of the Core System but the Core System is still responsible for facilitating their security which is chiefly done by providing digital certificate-based mechanisms to ensure trust between users. The Core System also provides networking services to facilitate communications, though it does not comprise the communications network. Readers who are familiar with VII should note that the following are not part of the Core System:

- Mobile Users (e.g., vehicle devices, pedestrian smartphones) – any user device.
- Roadside Equipment (RSE) – both public and commercial fixed devices.
- Transportation Management Centers (TMC) and other public or private backoffice or centers

It is also important to note that the Core System is not meant to mandate or change existing transportation equipment, technology or transportation centers. The Core System provides mechanisms for efficiently collecting and distributing transportation data, but does not necessarily replace existing systems, though it is likely that many existing data collection mechanisms will be made obsolete by its data collection and distribution function.

Figure 1-2 below shows the context in which the Core System operates as part of the overall *connected vehicle* environment. The center, field, and mobile systems interact with the Core System as do other Core Systems and external support systems. The center, field, and mobile systems also each other either independently of the Core or, in some cases, enabled by the security services provided by the Core.

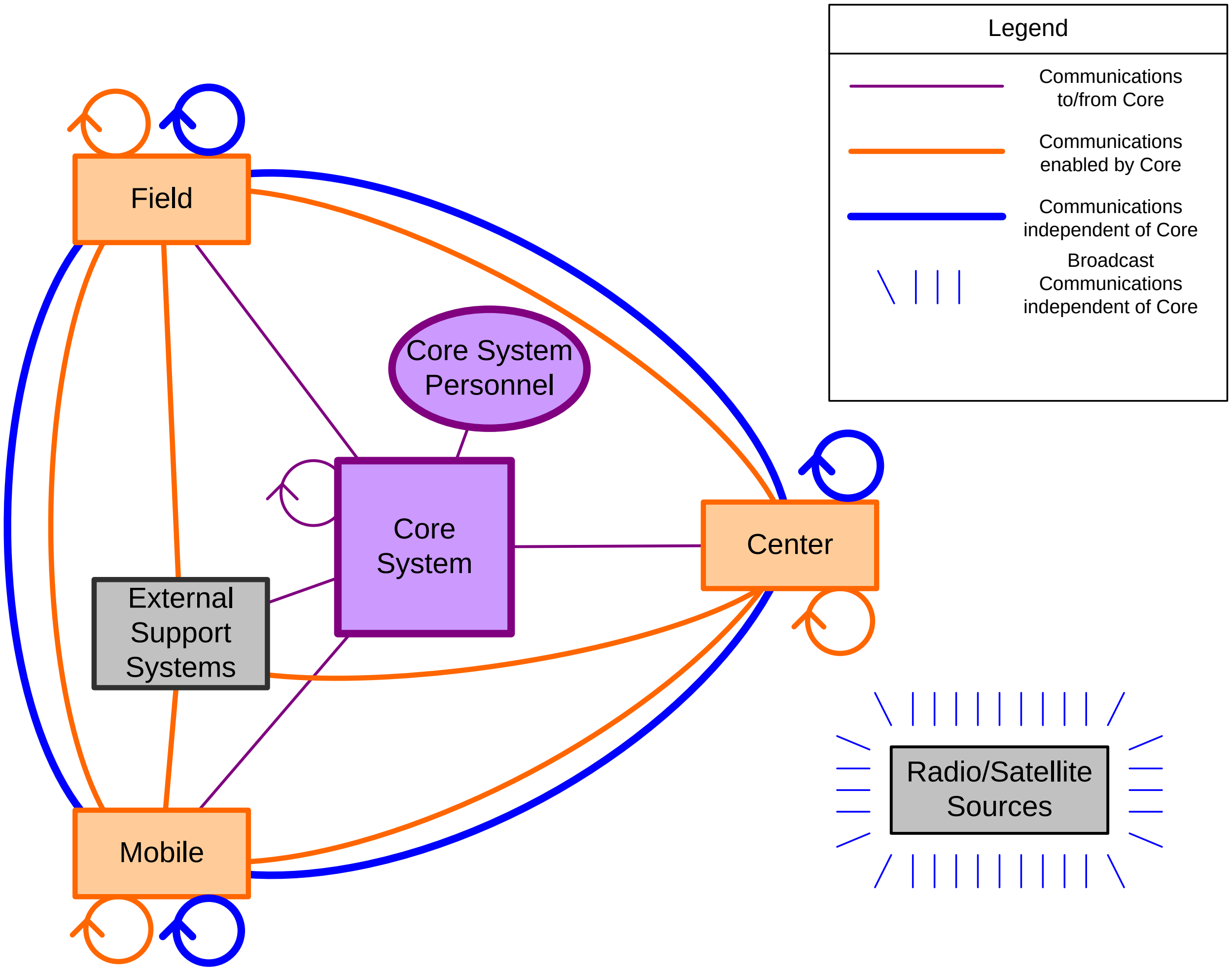

Legend
Communications to/from Core
Communications enabled by Core
Communications independent of Core
Broadcast Communications independent of Core
Field
Core System Personnel
Core System
Center
External Support Systems
Radio/Satellite Sources
Mobile

Figure 1-2. Core System Context Diagram

The diagram shown below in Figure 1-3 illustrates the context in which the Core System operates from the perspective of subsystems it contains and its interaction with the outside. The Core System includes eight subsystems and it interacts with Field, Mobile, and Center Users, other Core Systems, External Support Systems and Core System Operators.

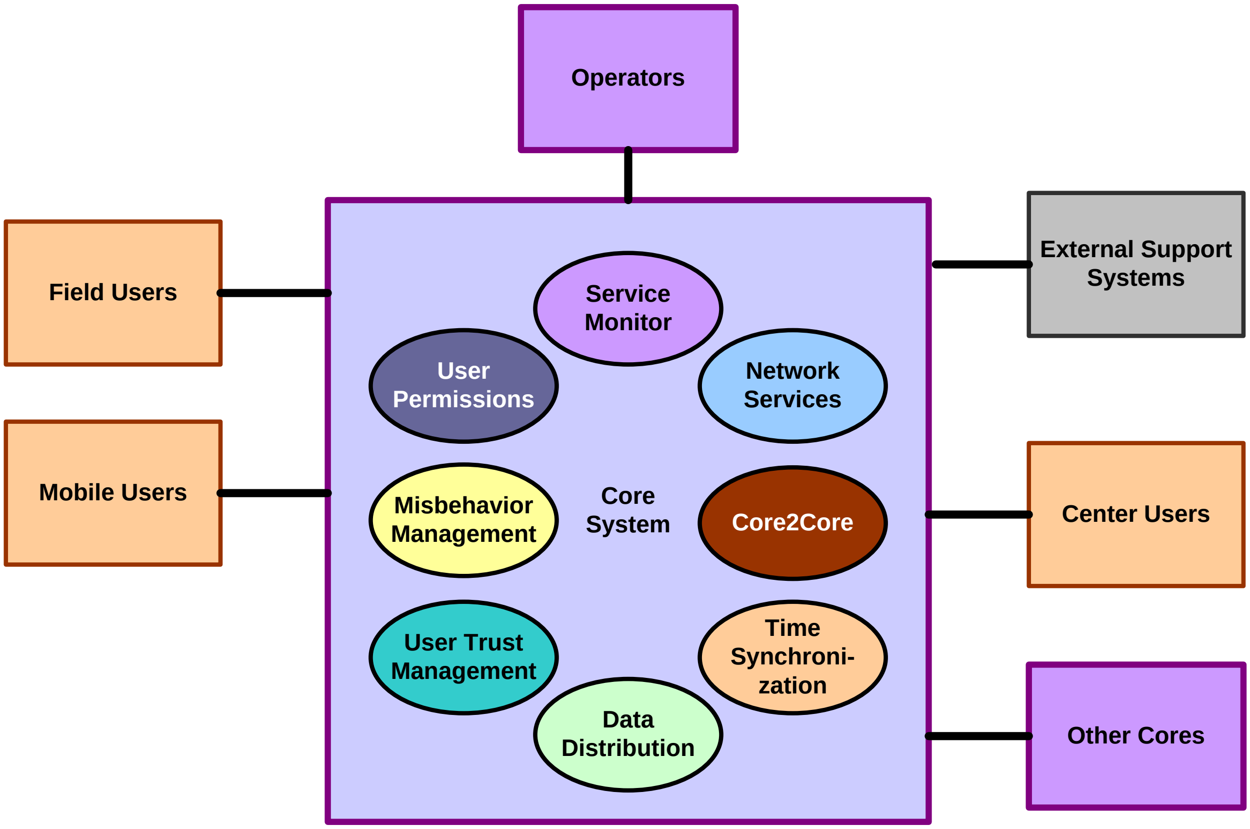


Figure 1-3. Core System Subsystem Context

The following provides a description of each of the subsystems of the Core System arranged alphabetically. A subsystem is defined as an integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses. See INCOSE Systems Engineering Handbook v3.1, The Hierarchy within a System, Appendix E-1 for a discussion of subsystems. The requirements have been organized around this set of subsystems.

Core2Core Subsystem: The Core2Core Subsystem interfaces with other Core Systems, declaring its jurisdictional scope, offered services, and services it desires from other Cores. The Core2Core subsystem will maintain a knowledge base of data and services available among other Cores. In this way the Core System can act as a System User to another Core System, providing proxy services that it does not offer but another Core does. Additionally, Core2Core is responsible for compatibility between Cores, ensuring that one Core does not encroach on the scope of another Core, and similarly accepting error messages from Mobile Users that might indicate a cross-jurisdictional compatibility or scope coverage issue. Interfaces between Cores will be formalized in interfaces specifications. Conflicts and discrepancies between Cores will have to be resolved by agreements between the organizations responsible for the respective Cores.

Data Distribution Subsystem: The Data Distribution Subsystem maintains a directory of System Users that want data and facilitates the delivery of that data to those users. It supports multiple distribution mechanisms, including:

- Source-to-Points: The data provider communicates data directly to data consumers. In this case no data is sent to the Core System, however the Core is involved to check System User Permissions and to provide addressing services through those subsystems
- Publish-Subscribe: The data provider communicates data to the Data Distribution subsystem, which forwards it to all users that are subscribed to receive the data.

Data Distribution allows data consumers to specify (and change the specification of) data they wish to receive using criteria including:

- Data type
- Data quality characteristics
- Data format requirements
- Geographic area
- Sampling rate
- Minimum and maximum frequency of data forwarding

Data Distribution maintains a registry of which data consumers get what data according to the criteria defined above. Data Distribution Publish-Subscribe does not store or buffer data beyond that which is necessary to complete publish-subscribe actions. If a given data consumer is unable to receive data that it has subscribed to because of a communications or other system failure, the data in question may be lost. The degree to which data distribution buffering accommodates connectivity failures will be up to the Core System deployment. Some Cores may offer “temporary storage” in this fashion.

Data Distribution repackages data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

Data Distribution will also maintain source-to-points information. With this option, the data consumer will connect directly to the data provider with the address supplied by the Data Distribution subsystem. When connected, the data provider sends the data directly to each consumer bypassing the Core System.

Data Distribution does not share or exchange data with other Core Systems. System Users that want data from multiple Cores need to subscribe to each Core.

Misbehavior Management Subsystem: The Misbehavior Management Subsystem analyzes messages sent to the Core System to identify users operating outside of their assigned permissions. It works with the User Permissions subsystem to identify suspicious requests and to maintain a record of specifically identifiable users that:

1. Provide false or misleading data
2. Operate in such a fashion as to impede other users
3. Operate outside of their authorized scope

Because most end users will rarely interface with the Core System, Misbehavior Management will also accept reports of misbehaving users from other users. Center, Mobile, and Field users can send misbehavior reports that reference credentials attached to messages and note the type of misbehavior in question. Misbehavior Management will record such reports and according to a set of Core System Personnel-controlled rules will determine when to revoke credentials from such reported misbehaving users. For anonymous users revocation is more complex and may result instead in a lack of credential renewal. Large numbers of failed renewals could have a significant effect on operations; system requirements and design activities will need to ensure that renewal failures do not adversely affect system performance or user experience.

Network Services Subsystem: The Network Services Subsystem provides information to System Users and Core System services that enable communication between those users and services. The Network Services subsystem will provide the information necessary for users to communicate with other users that have given permission to be communicated with. Network Services will also provide the information necessary to enable users to communicate with a group of users by maintaining information regarding available communications methods, addresses, and performance characteristics for geo-cast communications.

Network Services will also provide management for Communications Layer resources. It will enable decisions about which communications medium to use when more than one is available. This includes identifying available communications methods current performance characteristics and applicable user permission levels. Permission requirements will be coordinated with the User Permissions subsystem.

Service Monitor Subsystem: The Service Monitor Subsystem monitors the status of Core System services, interfaces, and communications networks connected to the Core. It informs System Users of the availability and status of its services.

Service Monitor also monitors the integrity of internal Core System components and supporting software, and mitigates against vulnerabilities. This includes periodic verification of the authenticity of Core service software and supporting software. This also includes monitoring for vulnerabilities including but not limited to virus protection, network port monitoring, and monitoring for patches to third party components. Should a vulnerability be detected or a component of the Core found to have lost integrity, Service Monitor takes steps to mitigate against damage and performance degradation.

The Service Monitor Subsystem ensures the physical security of Core System services by monitoring the environmental conditions that Core components operate in (e.g. temperature and humidity) as well as the condition of its power system. It takes steps to mitigate against system failures in the event that environmental conditions exceed operating thresholds. Actions could include the activation of environmental or backup power systems and/or the modification of Core service operations, as well as Core System Personnel (Core System staff) notification.

Service Monitor also monitors the performance of all services and interfaces and makes performance metrics available to Core System Personnel (Core System staff).

Time Synchronization Subsystem: The Time Synchronization Subsystem uses a time base available to all System Users and makes this time available to all Core System services which use this time base whenever a time reference is required.

User Permissions Subsystem: The User Permissions Subsystem provides tools allowing System Users to verify whether a given user, identified by digital certificate-based credentials, is authorized to request or perform the action requested in the message payload. It also maintains the status of users, whether they have a specific account, their allowed behaviors with defined permissions (publish, subscribe, actions allowed to request, and administration etc.), or if they belong to an anonymous group. User Permissions provides the tools for Core System Personnel to: create new users and groups, modify existing users and groups, and modify permissions associated with users and groups.

User Trust Management Subsystem: The User Trust Management Subsystem manages access rules and credentials in the form of X.509 digital certificates for all System Users and Core System components that require and are entitled to them. It creates and distributes cryptographic keys to qualifying System Users. It works with User Permissions to determine whether a given user applying for credentials or keys is entitled to them. It also manages the revocation of credentials and the distribution of Certificate Revocation Lists (CRLs) of disallowed credentials to interested System Users.

The provision, distribution, and management of IEEE 1609.2 based digital certificates (both identity and anonymous certificates) that are primarily used by Mobile and Field Users using 5.9GHz Dedicated Short Range Communications (DSRC) will be handled by an External Support System to be defined. The User Trust Management Subsystem will maintain a relationship with this ESS, and provide information about how to contact this ESS to interested System Users. User Trust Management will forward requests for IEEE 1609.2 certificate revocation for misbehaving System Users from Misbehavior Management to this ESS.

1.4 Stakeholders

The term “stakeholder” may be somewhat overused but generally refers to any individual or organization that is affected by the activities of a business process or, in this case, a system being developed. They may have a direct or indirect interest in the activity and their level of participation may vary. The term here includes public agencies, private organizations or the traveling public (end users) with a vested interest, or a "stake" in one or more aspect of the *connected vehicle* environment and this Core System. Core System stakeholders span the breadth of the transportation environment including:

- Transportation Users, e.g., private vehicle drivers, public safety vehicle operators, commercial vehicle operators, passengers, cyclists and pedestrians
- Transportation Operators, e.g. traffic managers, transit managers, fleet managers, toll operators, road maintenance and construction
- Public Safety organizations, e.g. incident and emergency management, including fire, police and medical support
- Information Service Providers, e.g. data and information providers for transportation-related data, including traffic, weather and convenience applications
- Environmental Managers, including emissions and air quality monitors
- Original Equipment vehicle Manufacturers (OEMs)
- In-vehicle device manufacturers
- Communications Providers, including cellular network operators
- Federal regulatory and research agencies under the umbrella of USDOT
- Core System owners.

2 Documents

This section identifies all needed standards, policies, laws, concept of operations, concept exploration documents and other reference material that supports the requirements.

This section is divided into two portions. The first section lists the documents that are explicitly referenced as part of this document. The second section lists the documents or other resources that were used for background information and as a source for potential requirements during the development of this SyRS though there may not be a direct reference.

2.1 Referenced Documents

- Core System Concept of Operations (ConOps), Rev E, October 24, 2011
- Core System System Architecture Document (SAD), Rev C, October 14, 2011
- IEEE Std. 1233 – IEEE Guide for Developing System Requirements Specifications, 22 Dec 1998
- IEEE 1609.2 Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, June 2006. Note: This standard defines three types of end entities, or potential certificate holders: Identified, Identified Not Localized, and WAVE Service Announcement (WSA) Signer. It says that future versions of this standard will also define end entities of type Anonymous.
- IEEE 1609.4 Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operations, Oct 2006
- IEEE Std. 446-1995, Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications, Approved 12 December 1995; Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, NY 10017.
- INCOSE Systems Engineering Handbook version 3.1, August 2007.
- Telecommunications Industry Association (TIA) Standard for Telecommunications Infrastructure Standard for Data Centers, ANSI/TIA-942-2005, approved on April 12, 2005; published by TIA Standards and Technology Dept., 2500 Wilson Blvd, Arlington, VA 22201.
- Vehicle Infrastructure Integration (VII) USDOT Day-1 Use Case Descriptions, v1.0, May 2006
- Vehicle Infrastructure Integration Consortium (VIIC) Standards Recommendations, VIIC Document SYS090-05, May 23, 2010
- VII Concept of Operations (ConOps), BAH, v1.2, September-06
- VII National System Requirements (NSR), BAH, v1.3.1, April-08
- VII Privacy Policies Framework, Version 1.0.2, February 16, 2007

2.2 Resource Documents

- A Provisional Technical Architecture for the VII, PB Farradyne, July 2004
- A Summary of European Cooperative Vehicle Systems Research Projects, Jun-09
- Achieving the Vision: Policy White Paper, 4/30/2010
- An Initial Assessment of the Ability of 4G Cellular Technology to Support Active Safety Applications, Final Draft, 11/18/2009

- Architecture Specification for the Vehicle and Certificate Authority Certificate Management Subsystems, VIIC
- CAMP Security Final Report, Draft, 8/31/2010
- CEN TC278-WG16_ISO TC204-WG18_2nd Meeting-Sept-2010_ Agenda, 7/24/2010
- Certificate Authority (CA) Subsystem Specification, BAH, v1.1, February-07
- Certificate Management Concept of Operation, VIIC, SEC 110-01
- Cooperative Intersection Collision Avoidance System for Violations (CICAS-V) for Avoidance of Violation-Based Intersection Crashes Paper, Michael Maile and Luca Delgrossi, March 2009
- Data Element Dictionary, BAH, v1.0, February-07
- EC Standardization Mandate M/453 Preliminary work plan for ETSI TC ITS, 7/27/2010
- Enterprise Network Operations Center (ENOC) Subsystem Specification, BAH, v1.1
- ETSI Intelligent Transport Systems (ITS) Security Services and Architecture, ETSI TS 102 731, v1.1.1, 9/21/2010
- European ITS Framework Architecture, v4.0, 2009
- European ITS Communication Architecture, v3.0, 2010
- Final Report: VII POC Executive Summary – Infrastructure (Volume 1B), BAH
- Final Report: VII POC Executive Summary – Vehicles (Volume 1A), VIIC
- Final Report: VII POC Results and Findings – Infrastructure (Volume 3B), BAH
- Final Report: VII POC Results and Findings – Vehicles (Volume 3A), VIIC
- Final Report: VII POC Technical Description – Infrastructure (Volume 2B), BAH, 5-15-09 Final
- Final Report: VII POC Technical Description – Vehicles (Volume 2A), VIIC, volume 2
- Functional and Performance Requirements for the VII POC OBE Subsystem, VIIC
- IEEE P1609 Working Group Meeting Notice and Draft Agenda, 7/14/2010
- IEEE 1609.1 Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager, Oct 2006
- IEEE 1609.3 Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, Apr 2007
- IEEE 802.11p-2010, 15 July 2010
- IEEE Standard 802.16: A Technical Overview, C80216-02_05, 6/4/2002
- IEEE Standard for Software Configuration Management Plans, 12 Aug 2010
- IEEE Std. 1028-1997 – IEEE Standard for Software Reviews, 9 December 1997
- IEEE Std. 1220-2005 – IEEE Standard for Application and Management of Systems Engineering Process, 9 September 2005
- Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994
- Infrastructure Lexicon, BAH, v1.1, February-07
- Intelligent Transport Systems (ITS) Communications Architecture, ETSI EN 302 665 V1.1.1 (2010-09), European Telecommunications Standards Institute 2010.
- Internet Official Protocol Standards, RFC 5000, Internet Engineering Task Force (IETF) May 2008

- Internet Protocol Defense Advanced Research Projects Agency (DARPA) Internet Program Protocol Specification, RFC 791, Internet Engineering Task Force (IETF), Sept 1981.
- ITS Standards Development Organizations Membership Overlap Analysis, Jan-10
- ITS Strategic Research Plan, 2010-2014: Executive Summary, US DOT, 3/29/2010
- Joint CEN and ETSI Response to Mandate M/453 – EC Comments, 7/27/2010
- M/453 Co-operative Systems Progress Report, 7/27/2010
- Mileage-based User Fee Technology Study, 8/7/2009
- Network Subsystem Specification Addendum, BAH, v1.0.1a, March-07
- Network Subsystem Specification, BAH, v1.1, April-07
- OBE Communications Manager Subsystem Requirements Specification, VIIC, ENA 110-02
- OBE Subsystem Design Description, VIIC, SYS 112-02 (OBE), SYS 112-01
- OBE to RSE Interface Requirements Specification, VIIC, SYS 120-04
- POC OBE Subsystem Functional and Performance Requirements, VIIC, SYS 110-02
- POC Probe Data Collection Vehicle Application Requirements, VIIC, APP 220-01
- POC Trippath Generation Application Requirements, VIIC, APP 220-04
- Policy Roadmap for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Safety, Draft: 05/19/2010
- Potential Haul-In Aftermarket Device Suppliers, 6/11/2010
- Requirements for Internet Hosts – Application and Support, RFC 1123, Internet Engineering Task Force (IETF), Oct 1989
- Requirements for Internet Hosts – Communications Layers, RFC 1122, Internet Engineering Task Force (IETF), Oct 1989
- Risk Management Plan for the Deployment of IVI Collision Avoidance Safety Systems, Draft, Ver 1, 11/4/2004
- RSE Procurement Analysis, BAH, v1.0, June-06,
- Roadway Geometry and Inventory Trade Study for Applications, 7/1/2010
- RSE Software Requirements Specification (SRS), BAH, v2.0, July-07
- RSE Subsystem Specification, BAH, v1.2
- SAE J2735 - Dedicated Short Range Communications (DSRC) Message Set Dictionary, v2, Nov 2009
- SAE J2735 Standard: Applying the Systems Engineering Process, 6/30/2010
- Service Delivery Node (SDN) Subsystem Specification, version 1.1, February 2007
- Standardization Mandate
- Transit Crosscutting Application Development and Implementation Program Plan and Roadmap (2010-2014), 3.1, Jul-10
- US Code Section 36 CFR Part 1194 - Electronic and Information Technology Accessibility Standards (36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended), Dec. 21, 2000
- USDOT Federal Highway Administration (FHWA) and California Department of Transportation (CalTRANS) Systems Engineering Guidebook, version 3, Dec 2, 2009.
- Vehicle Safety Communications – Applications (VSC-A) Project: Crash Scenarios and Safety Applications, Michael Maile, May 2, 2007

- Vehicle Safety Communications in the United States Paper, Michael Shulman and Richard Deering, March 2007
- Vehicle Segment Certificate Management Concept of Operations, VIIC, SEC 110_01
- Vehicle Segment Security Plan (Security ConOps), SEC 100-10, Jan 2007
- Vehicle-Vehicle and Vehicle-Infrastructure Communications based Safety Applications, Michael Maile, February 2010
- VII Architecture and Functional Requirements, PB Farradyne, VII Architecture version 1.1 2005_07_20
- VII Communications Analysis Report, BAH, v3.0, July-06
- VII System Discussion, 7/8/2010
- VII USDOT Day-1 Use Case Descriptions, BAH, Combined Final v1.0, May-06
- X-072 Interface Requirements Specification, SYS 120-02

3 Requirements

This section of the document lists the Core System Requirements. The requirements are organized first by level, i.e. system vs. subsystem. The System level requirements then are divided into the following types:

1) Functional — The Functional requirements specify actionable behaviors of the Core System. “What the system shall do”.
2) Performance — The Performance requirements specify quantifiable characteristics of Core System operations.
3) Interface — The Interface requirements define the Core System external interfaces to non-Core Systems (the outside world).
4) Non-Functional — The Non-Functional requirements define the characteristics of the overall operation of the system such as reliability, maintainability, safety, and environmental [e.g. temperature] requirements.
5) Constraints — The Constraints requirements pertain to how the Core System will be built and deployed.

The subsystem requirements that follow are based on the subsystems identified in the Core System ConOps and are then divided into the following types:

1) Functional — The Functional requirements specify actionable behaviors of the subsystems.
2) Performance — The Performance requirements specify quantifiable characteristics of the operations of that subsystem.
3) Interface — The Interface requirements define the external interfaces to non-Core Systems (the outside world).

Section 5.4 on page 70 defines the action verbs that are used in the requirements.

Many of the functional requirements are specifying activities that involve objects from the Core System Architecture. Where an object is being sent, received, or processed it is referenced by using its document section number per the current (14 October 2011) version of the System Architecture Document (SAD), e.g. “4.5.1.3.1.2 C2C Misbehavior Report”. To better understand the contents of those objects the reader should review the SAD.

3.1 System Requirements

This section provides the high-level requirements for the Core System, i.e. “What the system shall do”. They are organized by the types of requirements and are related to the Needs identified in the ConOps.

3.1.1 System Functional Requirements

3.1.1.1 Core to Core Requirements

3.1.1.1.1 A Core System shall transmit the 4.5.1.3.1.7 Core Status Registration to other Core Systems.

3.1.1.1.2 A Core System shall accept 4.5.1.3.1.7 Core Status Registration from other Core Systems.

3.1.1.1.3 A Core System shall use the contents of the 4.5.1.3.1.7 Core Status Registration to update the contents in the 4.2.4.3.22 Service Status Distribution Catalog.

3.1.1.1.4 A Core System shall transmit its 4.5.1.3.1.2 C2C Misbehavior Report to other Core Systems.

3.1.1.1.5 A Core System shall accept 4.5.1.3.1.2 C2C Misbehavior Report from other Core Systems.

3.1.1.1.6 A Core System shall use the contents of the 4.5.1.3.1.2 C2C Misbehavior Report to update the 4.5.2.3.3.10 Suspicious Data contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.1.1.1.7 A Core System shall transmit its 4.5.1.3.1.6 Core Service Status Query to other Core Systems.

3.1.1.1.8 A Core System shall accept the 4.5.1.3.1.6 Core Service Status Query from other Core Systems.

3.1.1.1.9 A Core System shall transmit the 4.5.1.3.1.4 Service Status for Cores response to another Core System upon request.

3.1.1.1.10 A Core System shall accept the 4.5.1.3.1.4 Service Status for Cores from other Core Systems.

3.1.1.1.11 A Core System shall transmit the 4.5.1.3.1.3 Complete CRL to other Core Systems.

3.1.1.1.12 A Core System shall accept the 4.5.1.3.1.3 Complete CRL from other Core Systems.

3.1.1.1.13 A Core System shall use the contents of the 4.5.1.3.1.3 Complete CRL to update the contents in the 4.2.6.3.6 CRL Storage.

3.1.1.1.14 A Core System shall transmit the 4.5.1.3.1.8 CRL Deltas to other Core Systems.

3.1.1.1.15 A Core System shall accept the 4.5.1.3.1.8 CRL Deltas from other Core Systems.

3.1.1.1.16 A Core System shall use the contents of the 4.5.1.3.1.8 CRL Deltas to update the contents in the 4.2.6.3.6 CRL Storage.

3.1.1.1.17 A Core System shall transmit the 4.5.1.3.1.4 Core Configuration Info to other Core Systems.

3.1.1.1.18 A Core System shall accept the 4.5.1.3.1.4 Core Configuration Info from other Core Systems.

3.1.1.1.19 A Core System shall transmit the 4.5.1.3.1.5 Core Conflict Info to other Core Systems.

3.1.1.1.20 A Core System shall accept the 4.5.1.3.1.5 Core Conflict Info from other Core Systems.

3.1.1.1.21 A Core System shall transmit the 4.5.1.3.1.9 Data Backup Request to other Core Systems.

3.1.1.1.22 A Core System shall accept the 4.5.1.3.1.9 Data Backup Request from other Core Systems.

3.1.1.1.23 A Core System shall use the contents of the 4.5.1.3.1.9 Data Backup Request to update the contents in the 4.2.10.3.19 Other Core Data Backups.

3.1.1.1.24 A Core System shall transmit the 4.5.1.3.1.10 Data Request to other Core Systems.

3.1.1.1.25 A Core System shall accept the 4.5.1.3.1.10 Data Request from other Core Systems.

3.1.1.1.26 A Core System shall transmit the 4.5.1.3.1.1 Backup Data to other Core Systems.

3.1.1.1.27 A Core System shall accept the 4.5.1.3.1.1 Backup Data from other Core Systems.

3.1.1.1.28 A Core System shall use the contents of the 4.5.1.3.1.1 Backup Data to update the 4.5.2.3.1.3 Data to be Backed Up contents in the 4.2.10.2.3 Backup Other Core Data.

3.1.1.1.29 A Core System shall transmit the 4.5.1.3.1.12 Restore Data to other Core Systems.

3.1.1.1.30 A Core System shall accept the 4.5.1.3.1.12 Restore Data from other Core Systems.

3.1.1.1.31 A Core System shall use the contents of the 4.5.1.3.1.12 Restore Data to update the contents of the 4.2.10.3.10 Generic Core Data Store.

3.1.1.1.32 A Core System shall transmit the 4.5.1.3.1.11 Other Core Takeover Request to other Core Systems.

3.1.1.1.33 A Core System shall accept the 4.5.1.3.1.11 Other Core Takeover Request from other Core Systems.

3.1.1.2 Data Distribution Requirements

3.1.1.2.1 A Core System shall receive the 4.5.1.3.2.5 Data Subscription Request from Data Subscribers.

3.1.1.2.2 A Core System shall send the 4.5.1.3.2.3 Data Subscription Confirmation Info response to a Data Subscriber upon request.

3.1.1.2.3 A Core System shall use the contents of the 4.5.1.3.2.5 Data Subscription Request to update the contents in the 4.2.2.3.6 Data Subscription Catalog.

3.1.1.2.4 A Core System shall accept the 4.5.1.3.2.2 Data Provision Request from a Data Provider.

3.1.1.2.5 A Core System shall transmit the 4.5.1.3.2.1 Data Acceptance Info response to a Data Provider upon request.

3.1.1.2.6 A Core System shall use the contents of the 4.5.1.3.2.2 Data Provision Request to update the contents in the 4.2.2.3.5 Data Acceptance Catalog.

3.1.1.2.7 A Core System shall accept the 4.5.1.3.2.8 Geo-Cast Message from System Users.

3.1.1.2.8 A Core System shall use the contents of the 4.5.1.3.2.8 Geo-Cast Message to update the contents in the 4.2.2.3.8 Geo-cast Message Log.

3.1.1.2.9 A Core System shall accept the 4.5.1.3.2.7 Field Node Configuration Information request from System Users.

3.1.1.2.10 A Core System shall use the contents of the 4.5.1.3.2.7 Field Node Configuration Information to update the contents in the 4.2.2.3.7 Geo-cast Device Catalog.

3.1.1.2.11 A Core System shall send the 4.5.1.3.2.11 Repackaged, Addressed Data to a Data Subscribers upon request.

3.1.1.3 Misbehavior Requirements

3.1.1.3.1 A Core System shall receive 4.5.1.3.3.1 System User Misbehavior Report from System Users.

3.1.1.3.2 A Core System shall use the contents of the 4.5.1.3.3.1 System User Misbehavior Report to update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.1.1.3.3 A Core System shall identify misbehaving System Users.

3.1.1.3.4 A Core System shall enable a privileged System Operator to configure misbehavior correlation processing.

3.1.1.3.5 A Core System shall maintain misbehavior information in the 4.2.2.3.11 Misbehavior Reports Log.

3.1.1.4 Networking Requirements

3.1.1.4.1 A Core System shall receive the 4.5.1.3.4.1 Data In from System Users (i.e., as any combination of Digitally Signed, Secure and Acknowledgement message).

3.1.1.4.2 A Core System shall send the 4.5.1.3.4.2 Data Out to System Users (i.e., as any combination of Digitally Signed, Secure and Acknowledgement message).

3.1.1.4.3 A Core System shall support IPv6 for non-DSRC Users.

3.1.1.4.4 A Core System shall route messages between networks for those System Users that are connected via a private network.

3.1.1.4.5 A Core System shall install intrusion detection software to identify suspicious network traffic.

3.1.1.4.6 A Core System shall use the contents of the Intrusion Alert to update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.1.1.4.7 A Core System shall manage system performance monitoring of itself.

3.1.1.5 System Monitoring Requirements

3.1.1.5.1 A Core System shall accept the 4.5.1.3.5.4 System User Status Registration from System Users.

3.1.1.5.2 A Core System shall accept the 4.5.1.3.5.3 Service Status Query from System Users.

3.1.1.5.3 A Core System shall transmit the 4.5.1.3.5.2 Service Status response to a System User upon request.

3.1.1.5.4 A Core System shall transmit the 4.5.1.3.5.1 Performance Records to the Core Certification Authority (CCA).

3.1.1.5.5 A Core System shall accept requests from a privileged System Operator to transition a Core System's state.

3.1.1.5.6 A Core System shall accept requests from a privileged System Operator to transition a Core Systems mode.

3.1.1.5.7 A Core System shall maintain its state in the 4.2.5.3.4 Event Log.

3.1.1.5.8 A Core System shall maintain its mode in the 4.2.5.3.4 Event Log.

3.1.1.5.9 A Core System shall manage its software configuration.

3.1.1.5.10 A Core System shall manage its hardware configuration.

3.1.1.5.11 A Core System shall manage its transitions between states.

3.1.1.5.12 A Core System's service coverage area shall be configurable.

3.1.1.5.13 A Core System shall provide message distribution based on its geographical location to System Users.

3.1.1.6 Time Requirements

3.1.1.6.1 A Core System shall receive the 4.5.1.3.6.1 Time message from an external reference time source.

3.1.1.7 User Permission requirements

3.1.1.7.1 A Core System shall accept the 4.5.1.3.7.2 User Identity and Permission Request from System Users.

3.1.1.7.2 A Core System shall use the contents of the 4.5.1.3.7.2 User Identity and Permission Request to update the contents in the 4.2.3.3.14 User Permission Registry.

3.1.1.7.3 A Core System shall transmit the User Permission Confirmation response to the System User.

3.1.1.7.4 A Core System shall accept the 4.5.1.3.7.1 Application Permission Request from System Users.

3.1.1.7.5 A Core System shall transmit the Application Permission Confirmation response to the System User.

3.1.1.7.6 A Core System shall use the contents of the 4.5.1.3.7.1 Application Permission Request to update the contents in the 4.2.6.3.15 User Permission Registry.

3.1.1.8 User Trust Requirements

3.1.1.8.1 A Core System shall transmit the 4.5.1.3.8.10 User Special Permissions to the External Support System (ESS) DSRC Registration Authority (RA).

3.1.1.8.2 A Core System shall accept the 4.5.1.3.8.9 User Identification from External Support System (ESS) DSRC Registration Authority (RA).

3.1.1.8.3 A Core System shall accept the 4.5.1.3.8.1 Credential Request from System Users.

3.1.1.8.4 A Core System shall transmit the 4.5.1.3.8.3 Credentials to a System User upon request.

3.1.1.8.5 A Core System shall use the contents of the 4.5.1.3.8.1 Credential Request (for a DSRC Certificate) to update the contents in the 4.2.6.3.3 Application Permission Registry.

3.1.1.8.6 A Core System shall use the contents of the 4.5.1.3.8.1 Credential Request to update the contents in the 4.2.6.3.16 User Trust Management Configuration.

3.1.1.8.7 A Core System shall transmit the 4.5.1.3.8.6 Ext X.509 Cert Request to the External Support System (ESS) X.509 Certificate Authority (CA).

3.1.1.8.8 A Core System shall accept the 4.5.1.3.8.11 X.509 Certificate from External Support System (ESS) X.509 Certificate Authority (CA).

3.1.1.8.9 A Core System shall accept 4.5.2.3.6.6 Remotely Encrypted Message from a System User.

3.1.1.8.10 A Core System shall transmit a Locally Encrypted Message to System Users when the message is from a Core System.

3.1.1.8.11 A Core System shall accept the 4.5.1.3.8.12 X.509 CRL from External Support System (ESS) X.509 Certificate Authority (CA).

3.1.1.8.12 A Core System shall use the contents of the 4.5.1.3.8.12 X.509 CRL to update the contents in the 4.2.7.3.26 User Trust Management Configuration.

3.1.1.8.13 A Core System shall send the 4.5.1.3.8.4 CRL message to System Users.

3.1.1.8.14 A Core System shall validate messages from System Users.

3.1.2 System Performance Requirements

3.1.2.1 A Core System shall be available (i.e., able to provide all of its listed services while operating in Normal Mode in the Operational State) 99.5% of the time.

3.1.3 System Interface Requirements

3.1.3.1 A Core System shall communicate with other Core Systems.

3.1.3.2 A Core System shall communicate to System Users.

3.1.3.3 A Core System shall communicate with an external time source to receive time.

3.1.3.4 A Core System shall communicate to a privileged System Operator.

3.1.3.5 A Core System shall connect to the Internet.

3.1.3.6 A Core System shall connect to private networks.

3.1.3.7 A Core System shall connect to the Core Certification Authority (CCA).

3.1.4 Non-functional Requirements

3.1.4.1 Physical Security

3.1.4.1.1 Access Control shall be provided in crucial areas such as the computer rooms, entrance rooms, electrical and mechanical areas, as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.

3.1.4.2 Environmental Features

3.1.4.2.1 The equipment hosting the Core System shall operate when exposed to a relative humidity from 40% to 55%, as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.

3.1.4.2.2 The facility hosting the Core System nodes shall operate in ambient temperatures from 20° C (68° F) to 25° C (77° F), as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.

3.1.4.2.3 The facility hosting the Core System nodes shall operate up to a maximum Dew Point of 21° C (69.8° F), as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.

3.1.4.2.4 The facility hosting the Core System nodes shall maintain the temperature so that it does not vary by more than 5° C (9° F) per hour, as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.

3.1.4.2.5 The facility hosting the Core System nodes shall include heat and smoke detectors that meet or exceed all local fire code regulations.

3.1.4.3 Backup Power

3.1.4.3.1 The facility hosting the Core System nodes shall include supplemental power (e.g., generator or Uninterruptible Power Supply (UPS)) as specified in the IEEE Std 446 Recommended Practice for Emergency and Standby Power System for Industrial and Commercial Applications.

3.1.4.3.2 The Core System's equipment shall be installed in electrically grounded network equipment racks, as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.

3.1.4.4 Maintainability

3.1.4.4.1 A Core System's Mean Time To Repair (MTTR) for each Core Service shall not exceed 3.0 hours [TBR].

3.1.4.4.2 A Core System Mean Time Between Failures (MTBF) shall be greater than 597 hours (24.8 days) [TBR].

3.1.5 Constraints

3.1.5.1 A Core System shall conform to the privacy principles as defined in the VII Privacy Policies Framework regarding the use of personal information.

3.2 Subsystem Requirements

This section provides the requirements for each of the subsystems within the Core System as described in the ConOps and are divided by the type of requirements: functional and interface.

3.2.1 Core2Core Subsystem

The Core2Core Subsystem interfaces with other Core Systems, declaring its jurisdictional scope, offered services, and services it desires from other Cores. The Core2Core subsystem will maintain a knowledge base of data and services available among other Cores. In this way the Core System can act as a System User to another Core System, providing proxy services that it does not offer but another Core does. Additionally, Core2Core is responsible for compatibility between Cores, ensuring that one Core does not encroach on the scope of another Core, and similarly accepting error messages from Mobile Users that might indicate a cross-jurisdictional compatibility or scope coverage issue. Interfaces between Cores will be formalized in interfaces specifications. Conflicts and discrepancies between Cores will have to be resolved by agreements between the organizations responsible for the respective Cores.

3.2.1.1 Functional Requirements

3.2.1.1.1 The Core2Core Subsystem shall transmit the 4.5.1.3.1.7 Core Status Registration to other Core Systems.

3.2.1.1.2 The Core2Core Subsystem shall accept 4.5.1.3.1.7 Core Status Registration from other Core Systems.

3.2.1.1.3 Upon accepting a 4.5.1.3.1.7 Core Status Registration from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.4 Upon accepting a valid 4.5.1.3.1.7 Core Status Registration from other Core Systems, the Core2Core Subsystem shall use its contents to update the contents in the 4.2.4.3.22 Service Status Distribution Catalog.

3.2.1.1.5 Upon accepting a valid 4.5.1.3.1.7 Core Status Registration from other Core Systems, the Core2Core Subsystem shall send the 4.5.2.3.5.1 Core ID, function to the User Permissions Subsystem.

3.2.1.1.6 If a 4.5.1.3.1.7 Core Status Registration from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.4.3.22 Service Status Distribution Catalog.

3.2.1.1.7 The Core2Core Subsystem shall transmit its 4.5.1.3.1.2 C2C Misbehavior Report to other Core Systems.

3.2.1.1.8 The Core2Core Subsystem shall accept 4.5.1.3.1.2 C2C Misbehavior Report from other Core Systems.

3.2.1.1.9 Upon accepting a 4.5.1.3.1.2 C2C Misbehavior Report from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.10 Upon accepting a valid 4.5.1.3.1.2 C2C Misbehavior Report from other Core Systems, the Core2Core Subsystem shall use its contents to update the 4.5.2.3.3.10 Suspicious Data contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.1.1.11 If a 4.5.1.3.1.2 C2C Misbehavior Report from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.2.3.11 Misbehavior Reports Log.

3.2.1.1.12 The Core2Core Subsystem shall transmit its 4.5.1.3.1.6 Core Service Status Query to other Core Systems.

3.2.1.1.13 The Core2Core Subsystem shall accept the 4.5.1.3.1.6 Core Service Status Query from other Core Systems.

3.2.1.1.14 Upon accepting a 4.5.1.3.1.6 Core Service Status Query from other Core Systems, a Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.15 Upon accepting a valid 4.5.1.3.1.6 Core Service Status Query from a Core System, the Core2Core Subsystem shall transmit its 4.5.1.3.1.4 Service Status for Cores response to that Core System.

3.2.1.1.16 The Core2Core Subsystem shall accept the 4.5.1.3.1.4 Service Status for Cores from other Core Systems.

3.2.1.1.17 The Core2Core Subsystem shall send the 4.5.2.3.5.2 Operator ID, function to the User Permissions Subsystem.

3.2.1.1.18 The Core2Core Subsystem shall transmit the 4.5.1.3.1.3 Complete CRL to other Core Systems.

3.2.1.1.19 The Core2Core Subsystem shall accept the 4.5.1.3.1.3 Complete CRL from other Core Systems.

3.2.1.1.20 Upon accepting a 4.5.1.3.1.3 Complete CRL from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.21 Upon accepting a valid 4.5.1.3.1.3 Complete CRL from other Core Systems, the Core2Core Subsystem shall use its contents to update the contents in the 4.2.6.3.6 CRL Storage.

3.2.1.1.22 If a 4.5.1.3.1.3 Complete CRL from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.6.3.6 CRL Storage.

3.2.1.1.23 The Core2Core Subsystem shall transmit the 4.5.1.3.1.8 CRL Deltas to other Core Systems.

3.2.1.1.24 The Core2Core Subsystem shall accept the 4.5.1.3.1.8 CRL Deltas from other Core Systems.

3.2.1.1.25 Upon accepting a 4.5.1.3.1.8 CRL Deltas from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.26 Upon accepting a valid 4.5.1.3.1.8 CRL Deltas from other Core Systems, the Core2Core Subsystem shall use its contents to update the contents in the 4.2.6.3.6 CRL Storage.

3.2.1.1.27 If a 4.5.1.3.1.8 CRL Deltas from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.6.3.6 CRL Storage.

3.2.1.1.28 The Core2Core Subsystem shall accept the 4.5.2.3.1.2 Config Info for Other Cores from other Core subsystems.

3.2.1.1.29 The Core2Core Subsystem shall transmit the 4.5.2.3.1.2 Config Info for Other Cores from other Core subsystems.

3.2.1.1.30 The Core2Core Subsystem shall accept the 4.5.2.3.1.7 Detailed Service Status from the Service Monitor Subsystem.

3.2.1.1.31 The Core2Core Subsystem shall transmit the 4.5.2.3.1.1 Core Config Info to other Core Systems.

3.2.1.1.32 The Core2Core Subsystem shall accept the 4.5.2.3.1.1 Core Config Info from other Core Systems.

3.2.1.1.33 The Core2Core Subsystem shall transmit the 4.5.1.3.1.4 Core Configuration Info to other Core Systems for services offered in its covered area.

3.2.1.1.34 The Core2Core Subsystem shall accept the 4.5.1.3.1.4 Core Configuration Info from other Core Systems.

3.2.1.1.35 The Core2Core Subsystem shall transmit the 4.5.1.3.1.5 Core Conflict Info to other Core Systems for boundary or coverage area issues.

3.2.1.1.36 The Core2Core Subsystem shall accept the 4.5.1.3.1.5 Core Conflict Info from other Core Systems.

3.2.1.1.37 The Core2Core Subsystem shall transmit the 4.5.1.3.1.10 Data Request to other Core Systems.

3.2.1.1.38 The Core2Core Subsystem shall accept the 4.5.1.3.1.10 Data Request from other Core Systems.

3.2.1.1.39 The Core2Core Subsystem shall transmit the 4.5.1.3.1.9 Data Backup Request to other Core Systems.

3.2.1.1.40 The Core2Core Subsystem shall accept the 4.5.1.3.1.9 Data Backup Request from other Core Systems.

3.2.1.1.41 Upon accepting a 4.5.1.3.1.9 Data Backup Request from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.42 Upon accepting a valid 4.5.1.3.1.9 Data Backup Request from other Core Systems, the Core2Core Subsystem shall use its contents to update the contents in the 4.2.10.3.19 Other Core Data Backups.

3.2.1.1.43 If a 4.5.1.3.1.9 Data Backup Request from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.10.3.19 Other Core Data Backups.

3.2.1.1.44 The Core2Core Subsystem shall receive the 4.5.2.3.1.3 Data to be Backed Up from other Core subsystems.

3.2.1.1.45 The Core2Core Subsystem shall transmit the 4.5.1.3.1.1 Backup Data to other Core Systems.

3.2.1.1.46 The Core2Core Subsystem shall accept the 4.5.1.3.1.1 Backup Data from other Core Systems.

3.2.1.1.47 Upon accepting a 4.5.1.3.1.1 Backup Data from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.48 Upon accepting a valid Backup Data from other Core Systems, the Core2Core Subsystem shall use its contents to update the 4.5.2.3.1.3 Data to be Backed Up contents in the 4.2.10.3.3 Backup Other Core Data.

3.2.1.1.49 If a 4.5.1.3.1.1 Backup Data from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.10.3.3 Backup Other Core Data.

3.2.1.1.50 The Core2Core Subsystem shall transmit the 4.5.1.3.1.11 Other Core Takeover Request to other Core Systems.

3.2.1.1.51 The Core2Core Subsystem shall accept the 4.5.1.3.1.11 Other Core Takeover Request from other Core Systems.

3.2.1.1.52 The Core2Core Subsystem shall transmit the 4.5.1.3.1.12 Restore Data to other Core Systems.

3.2.1.1.53 The Core2Core Subsystem shall accept the 4.5.1.3.1.12 Restore Data from other Core Systems.

3.2.1.1.54 Upon accepting a 4.5.1.3.1.12 Restore Data from other Core Systems, the Core2Core Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.1.1.55 Upon accepting a valid 4.5.1.3.1.12 Restore Data from other Core Systems, the Core2Core Subsystem shall use its contents to update the contents of the 4.2.10.3.10 Generic Core Data Store.

3.2.1.1.56 If a 4.5.1.3.1.12 Restore Data from other Core Systems contains a data item that the Core2Core Subsystem determines as invalid, the Core2Core Subsystem shall exclude that data item from its update of the 4.2.10.3.10 Generic Core Data Store.

3.2.1.1.57 The Core2Core Subsystem shall receive the 4.5.2.3.1.4 Core Distribution List from the Service Monitor Subsystem.

3.2.1.1.58 The Core2Core Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.1.1.59 The Core2Core Subsystem shall receive the Locally Encrypted Message from the User Trust Subsystem.

3.2.1.1.60 The Core2Core Subsystem shall establish persistent secure transmission connections to other Core Systems when continuous exchange of messaging (e.g., 4.5.1.3.1.1 Backup Data and 4.5.1.3.1.6 Core Service Status Query) occurs between Core Systems.

3.2.1.1.61 The Core2Core Subsystem shall establish session-oriented communication connections to other Core Systems when message exchanges occur intermittently (e.g., 4.5.1.3.1.7 Core Status Registration) between Core Systems.

3.2.1.1.66 Time Requirements

3.2.1.1.66.1 The Core2Core Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.1.1.67 State/Mode/Status Requirements

3.2.1.1.67.1 The Core2Core Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.1.1.67.2 The Core2Core Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.1.1.67.3 The Core2Core Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.1.1.67.4 The Core2Core Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.1.2 External Interface Requirements

3.2.1.2.1 The Core2Core Subsystem shall enable a privileged System Operator to update the contents of the C2C Configuration data store.

3.2.1.2.2 The Core2Core Subsystem shall enable a privileged System Operator to update the contents of the 4.2.3.3.11 Other Core Configs data store.

3.2.1.2.3 The Core2Core Subsystem shall enable other Core Systems to communicate with it.

3.2.1.2.4 The Core2Core Subsystem shall enable a privileged System Operator to update the contents of the Configure Core2Core.

3.2.2 Data Distribution Subsystem

The Data Distribution Subsystem maintains a directory of System Users that want data and facilitates the delivery of that data to those users. It supports multiple distribution mechanisms, including:

- Source-to-Points: The data provider communicates data directly to data consumers. In this case no data is sent to the Core System, however the Core is involved to check System User Permissions and to provide addressing services through those subsystems
- Publish-Subscribe: The data provider communicates data to the Data Distribution subsystem, which forwards it to all users that are subscribed to receive the data.

Data Distribution allows data consumers to specify (and change the specification of) data they wish to receive using criteria including:

- Data type
- Data quality characteristics
- Data format requirements
- Geographic area
- Sampling rate
- Minimum and maximum frequency of data forwarding

Data Distribution maintains a registry of which data consumers get what data according to the criteria defined above. Data Distribution Publish-Subscribe does not store or buffer data beyond that which is necessary to complete publish-subscribe actions. If a given data consumer is unable to receive data that it has subscribed to because of a communications or other system failure, the data in question may be lost. The degree to which data distribution buffering accommodates connectivity failures will be up to the Core System deployment. Some Cores may offer “temporary storage” in this fashion.

Data Distribution repackages data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

Data Distribution will also maintain source-to-points information. With this option, the data consumer will connect directly to the data provider with the address supplied by the Data Distribution subsystem. When connected, the data provider sends the data directly to each consumer bypassing the Core System.

Data Distribution does not share or exchange data with other Core Systems. System Users that want data from multiple Cores need to subscribe to each Core.

3.2.2.1 Functional Requirements

3.2.2.1.1 Data Subscription Processing

3.2.2.1.1.1 The Data Distribution Subsystem shall receive the 4.5.1.3.2.5 Data Subscription Request from Data Subscribers.

3.2.2.1.1.2 Upon receiving a 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber, the Data Distribution Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.2.1.1.3 Upon receiving a valid 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber, the Data Distribution Subsystem shall send the 4.5.1.3.2.3 Data Subscription Confirmation Info response to that Data Subscriber.

3.2.2.1.1.4 Upon receiving a valid 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber, the Data Distribution Subsystem shall use its contents to update the contents in the 4.2.2.3.6 Data Subscription Catalog.

3.2.2.1.1.5 Upon receiving a 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber that does not meet the acceptance criteria, the Data Distribution Subsystem shall send the 4.5.1.3.2.4 Data Subscription Redirect Info response to that Data Subscriber.

3.2.2.1.1.6 Upon receiving a 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber for Source-to-Point Data Distribution (i.e., data provider communicates data directly to data consumer) that the Core determines as invalid, the Data Distribution Subsystem shall send the 4.5.1.3.2.6 Direct Data Distribution Info response to that Data Subscriber.

3.2.2.1.1.7 If a 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber contains a data item that the Data Distribution Subsystem determines as invalid, the Data Distribution Subsystem shall exclude that data item from its update of the 4.2.2.3.6 Data Subscription Catalog.

3.2.2.1.2 Data Provision Processing

3.2.2.1.2.1 The Data Distribution Subsystem shall accept the 4.5.1.3.2.2 Data Provision Request from a Data Provider.

3.2.2.1.2.2 Upon accepting a 4.5.1.3.2.2 Data Provision Request from a Data Provider, the Data Distribution Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.2.1.2.3 Upon accepting a valid 4.5.1.3.2.2 Data Provision Request from a Data Provider, the Data Distribution Subsystem shall transmit the 4.5.1.3.2.1 Data Acceptance Info response to that Data Provider.

3.2.2.1.2.4 Upon accepting a valid 4.5.1.3.2.2 Data Provision Request from a Data Provider, the Data Distribution Subsystem shall use its contents to update the contents in the 4.2.2.3.5 Data Acceptance Catalog.

3.2.2.1.2.5 Upon accepting a 4.5.1.3.2.2 Data Provision Request from a Data Provider that does not meet the acceptance criteria, the Data Distribution Subsystem shall transmit the 4.5.1.3.2.9 Other Core Acceptance Info response to that Data Provider.

3.2.2.1.2.6 If a 4.5.1.3.2.2 Data Provision Request from a Data Provider contains a data item that the Data Distribution Subsystem determines as invalid, the Data Distribution Subsystem shall exclude that data item from its update of the 4.2.2.3.5 Data Acceptance Catalog.

3.2.2.1.2.7 The Data Distribution Subsystem shall accept the 4.5.1.3.2.7 Field Node Configuration Information request from System Users.

3.2.2.1.2.8 Upon accepting a 4.5.1.3.2.7 Field Node Configuration Information request from a System User, the Data Distribution Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.2.1.2.9 Upon receiving 4.5.1.3.2.10 Provided Data from System Users, the Data Distribution Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.2.1.2.10 Upon accepting a 4.5.1.3.2.10 Provided Data from a System User, the Data Distribution Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.2.1.2.11 Upon receiving valid 4.5.1.3.2.10 Provided Data from a System User that require repackaging, the Data Distribution Subsystem shall send the 4.5.1.3.2.11 Repackaged, Addressed Data to Data Subscribers.

3.2.2.1.2.12 The Data Distribution Subsystem shall send the 4.5.2.3.5.2 Operator ID, function to the User Permissions Subsystem.

3.2.2.1.2.13 The Data Distribution Subsystem shall send the 4.5.2.3.5.4 Provider ID, function to the User Permissions Subsystem.

3.2.2.1.2.14 The Data Distribution Subsystem shall send a 4.5.2.3.1.1 Core Config Info to the Core2Core Subsystem.

3.2.2.1.2.15 The Data Distribution Subsystem shall send a 4.5.2.3.1.2 Config Info for Other Cores to the Core2Core Subsystem.

3.2.2.1.2.16 The Data Distribution Subsystem shall send a 4.5.2.3.1.3 Data to be Backed Up to the Core2Core Subsystem.

3.2.2.1.2.17 The Data Distribution Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.2.1.2.18 The Data Distribution Subsystem shall receive the 4.5.2.3.7.1 Restore Data from the Core2Core Subsystem.

3.2.2.1.2.19 The Data Distribution Subsystem shall receive the Locally Encrypted Message from the User Trust Subsystem.

3.2.2.1.2.20 The Data Distribution Subsystem shall send the 4.5.2.3.3.10 Suspicious Data to the Misbehavior Management Subsystem (for System User misbehavior) to update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.2.1.2.21 The Data Distribution Subsystem shall send the Suspicious Data Provision Request to the Misbehavior Management Subsystem (for Data Provider misbehavior) to update the contents in the 4.2.4.3.15 Misbehavior Reports Log.

3.2.2.1.2.22 The Data Distribution Subsystem shall send the Suspicious Data Subscription Request to the Misbehavior Management Subsystem (for Data Subscriber misbehavior) to update the contents in the 4.2.4.3.15 Misbehavior Reports Log.

3.2.2.1.3 Data Repackaging/Aggregation

3.2.2.1.3.1 The Data Distribution Subsystem shall aggregate provisional data (i.e., Aggregated Data) by repackaging relevant information to be transmitted to a Data Subscriber.

3.2.2.1.3.2 The Data Distribution Subsystem shall provide parsing of provisional data (i.e., Aggregated Data) by repackaging a subset of data to be transmitted to a Data Subscriber.

3.2.2.1.3.3 The Data Distribution Subsystem shall provide sampling of provisional data (i.e., Aggregated Data) by repackaging a sample set of data to be transmitted to a Data Subscriber.

3.2.2.1.4 Geocasting Service (GCS)

3.2.2.1.4.1 The Data Distribution Subsystem shall accept the 4.5.1.3.2.8 Geo-Cast Message from System Users.

3.2.2.1.4.2 Upon accepting a 4.5.1.3.2.8 Geo-Cast Message from a System User, the Data Distribution Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.2.1.4.3 Upon accepting a valid 4.5.1.3.2.8 Geo-Cast Message from a System User, the Data Distribution Subsystem shall use its contents to update the contents in the 4.2.2.3.8 Geo-cast Message Log.

3.2.2.1.4.4 If a 4.5.1.3.2.8 Geo-Cast Message from a System User contains a data item that the Data Distribution Subsystem determines as invalid, the Data Distribution Subsystem shall exclude that data item from its update of the 4.2.2.3.8 Geo-cast Message Log.

3.2.2.1.4.5 The Data Distribution Subsystem shall receive the 4.5.2.3.2.1 Geo-cast Info Changes from the Misbehavior Management Subsystem using its contents to update the contents in the 4.2.2.3.7 Geo-cast Device Catalog.

3.2.2.1.4.6 Upon accepting a valid 4.5.1.3.2.7 Field Node Configuration Information request from a System User, the Data Distribution Subsystem shall use its contents to update the 4.5.2.3.2.1 Geo-cast Info Changes contents in the 4.2.2.3.7 Geo-cast Device Catalog.

3.2.2.1.4.7 If a 4.5.1.3.2.7 Field Node Configuration Information request from a System User contains a data item that the Data Distribution Subsystem determines as invalid, the Data Distribution Subsystem shall exclude that data item from its update of the 4.2.2.3.7 Geo-cast Device Catalog.

3.2.2.1.4.8 The Data Distribution Subsystem shall send the 4.5.2.3.3.12 Suspicious Geo-Cast to the Misbehavior Management Subsystem (for System User Geo-cast misbehavior) using its contents to update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.2.1.5 Time Requirements

3.2.2.1.5.1 The Data Distribution Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.2.1.6 State/Mode/Status Requirements

3.2.2.1.6.1 The Data Distribution Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.2.1.6.2 The Data Distribution Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.2.1.6.3 The Data Distribution Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.2.1.6.4 The Data Distribution Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.2.1.6.5 When in Restricted Mode, the Data Distribution Subsystem shall prioritize the 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber.

3.2.2.1.6.6 When in Restricted Mode, the Data Distribution Subsystem shall prioritize the 4.5.1.3.2.2 Data Provision Request from a Data Provider.

3.2.2.1.6.7 When operating in Maintenance Mode, the Data Distribution Subsystem shall not accept the 4.5.1.3.2.8 Geo-Cast Message from System Users.

3.2.2.1.6.8 When operating in Maintenance Mode, the Data Distribution Subsystem shall not accept the 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber.

3.2.2.1.6.9 When operating in Standby State, the Data Distribution Subsystem shall not accept the 4.5.1.3.2.2 Data Provision Request from a Data Provider.

3.2.2.1.6.10 When operating in Standby State, the Data Distribution Subsystem shall not accept the 4.5.1.3.2.5 Data Subscription Request from a Data Subscriber.

3.2.2.2 External Interface Requirements

3.2.2.2.1 The Data Distribution Subsystem shall enable a privileged System Operator to update the contents of the Data Distribution Configuration data store.

3.2.2.2.2 The Data Distribution Subsystem shall enable a privileged System Operator to update the contents of the Configure Data Distribution.

3.2.3 Misbehavior Management Subsystem

The Misbehavior Management Subsystem analyzes messages sent to the Core System to identify users operating outside of their assigned permissions. It works with the User Permissions subsystem to identify suspicious requests and to maintain a record of specifically identifiable users that:

1. Provide false or misleading data
2. Operate in such a fashion as to impede other users
3. Operate outside of their authorized scope

Because most end users will rarely interface with the Core System, Misbehavior Management will also accept reports of misbehaving users from other users. Center, Mobile, and Field users can send misbehavior reports that reference credentials attached to messages and note the type of misbehavior in question. Misbehavior Management will record such reports and according to a set of Core System Personnel-controlled rules will determine when to revoke credentials from such reported misbehaving users. For anonymous users revocation is more complex and may result instead in a lack of credential renewal. Large numbers of failed renewals could have a significant effect on operations; system requirements and design activities will need to ensure that renewal failures do not adversely affect system performance or user experience.

3.2.3.1 Functional Requirements

3.2.3.1.1 The Misbehavior Management Subsystem shall receive 4.5.1.3.3.1 System User Misbehavior Report from System Users.

3.2.3.1.2 Upon receiving a 4.5.1.3.3.1 System User Misbehavior Report from a System User, the Misbehavior Management Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.3.1.3 Upon receiving a valid 4.5.1.3.3.1 System User Misbehavior Report from a System User, the Misbehavior Management Subsystem shall use its contents to update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.3.1.4 If a 4.5.1.3.3.1 System User Misbehavior Report from a System User contains a data item that the Misbehavior Management Subsystem determines as invalid, the Misbehavior Management Subsystem shall exclude that data item from its update of the 4.2.2.3.11 Misbehavior Reports Log.

3.2.3.1.5 The Misbehavior Management Subsystem shall send the 4.5.2.3.5.2 Operator ID, function to the User Permissions Subsystem.

3.2.3.1.6 The Misbehavior Management Subsystem shall send the 4.5.2.3.5.6 System User ID, function to the User Permissions Subsystem.

3.2.3.1.7 The Misbehavior Management Subsystem shall send the 4.5.2.3.5.7 System User ID, Revoke function to the User Permissions Subsystem.

3.2.3.1.8 The Misbehavior Management Subsystem shall send the 4.5.2.3.5.3 Operator ID, Revoke function to the User Permissions Subsystem.

3.2.3.1.9 The Misbehavior Management Subsystem shall send a 4.5.2.3.1.1 Core Config Info to the Core2Core Subsystem.

3.2.3.1.10 The Misbehavior Management Subsystem shall send a 4.5.2.3.1.2 Config Info for Other Cores to the Core2Core Subsystem.

3.2.3.1.11 The Misbehavior Management Subsystem shall send a 4.5.2.3.1.3 Data to be Backed Up to the Core2Core Subsystem.

3.2.3.1.12 The Misbehavior Management Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.3.1.12.1 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.9 Suspicious Application Request from the User Permissions Subsystem.

3.2.3.1.12.2 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.13 Suspicious Permission Request from the User Permission Subsystem.

3.2.3.1.12.3 Upon receiving a valid misbehavior Report from the User Permission Subsystem, the Misbehavior Management Subsystem shall update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.3.1.13 The Misbehavior Management Subsystem shall send a 4.5.2.3.2.1 Geo-cast Info Changes to the Data Distribution Subsystem when identifying a misbehaving Geo-cast device.

3.2.3.1.14 The Misbehavior Management Subsystem shall receive a 4.5.2.3.7.1 Restore Data from the Core2Core Subsystem.

3.2.3.1.15 The Misbehavior Management Subsystem shall receive a 4.5.2.3.3.10 Suspicious Data from the Data Distribution Subsystem.

3.2.3.1.16 The Misbehavior Management Subsystem shall receive a 4.5.2.3.3.12 Suspicious Geo-Cast from the Data Distribution Subsystem.

3.2.3.1.17 The Misbehavior Management Subsystem shall receive a 4.5.2.3.3.4 Intrusion Alert from the Network Services Subsystem.

3.2.3.1.18 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.8 SUID, Function Permission response from the User Permissions Subsystem.

3.2.3.1.19 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.3 Internal Misbehavior Report from the User Permissions Subsystem identifying misbehavior information (e.g., misbehaving user, type of misbehavior).

3.2.3.1.20 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.5 Operator Permissions response from the User Permissions Subsystem.

3.2.3.1.21 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.14 System User Permissions response from the User Permissions Subsystem.

3.2.3.1.22 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.1 Authenticity Error Message from the User Trust Subsystem.

3.2.3.1.23 The Misbehavior Management Subsystem shall receive the 4.5.2.3.3.2 Decryption Error Message from the User Trust Subsystem.

3.2.3.1.24 The Misbehavior Management Subsystem shall record unauthorized operator access attempts to Core Services in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.3.1.25 Time Requirements

3.2.3.1.25.1 The Misbehavior Management Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.3.1.26 State/Mode/Status Requirements

3.2.3.1.26.1 The Misbehavior Management Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.3.1.26.2 The Misbehavior Management Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.3.1.26.3 The Misbehavior Management Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.3.1.26.4 The Misbehavior Management Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.3.2 External Interface Requirements

3.2.3.2.1 The Misbehavior Management Subsystem shall enable a privileged System Operator to update the contents of the Misbehavior Management Configuration data store.

3.2.3.2.2 The Misbehavior Management Subsystem shall enable a privileged System Operator to update the contents of the Configure Misbehavior Management.

3.2.4 Network Services Subsystem

The Network Services Subsystem provides information to System Users and Core System services that enable communication between those users and services. The Network Services subsystem will provide the information necessary for users to communicate with other users that have given permission to be communicated with. Network Services will also provide management for Communications Layer resources. It will enable decisions about which communications medium to use when more than one is available. This includes identifying available communications methods current performance characteristics and applicable user permission levels. Permission requirements will be coordinated with the User Permissions subsystem.

3.2.4.1 Functional Requirements

3.2.4.1.1 The Network Services Subsystem shall receive the 4.5.1.3.4.1 Data In from System Users (i.e., as any combination of Digitally Signed, Secure and Acknowledgement message).

3.2.4.1.2 The Network Services Subsystem shall send the 4.5.1.3.4.2 Data Out to System Users (i.e., as any combination of Digitally Signed, Secure and Acknowledgement message).

3.2.4.1.3 The Network Services Subsystem shall send a 4.5.2.3.1.1 Core Config Info to the Core2Core Subsystem.

3.2.4.1.4 The Network Services Subsystem shall send a 4.5.2.3.1.2 Config Info for Other Cores to the Core2Core Subsystem.

3.2.4.1.5 The Network Services Subsystem shall send a 4.5.2.3.1.3 Data to be Backed Up to the Core2Core Subsystem.

3.2.4.1.6 The Network Service Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.4.1.7 The Network Services Subsystem shall receive the Locally Encrypted Message from the User Trust Subsystem.

3.2.4.1.8 The Network Services Subsystem shall send a 4.5.2.3.4.2 Service Control Node Performance to the Service Monitor Subsystem.

3.2.4.1.9 The Network Services Subsystem shall send the 4.5.2.3.5.2 Operator ID, function to the User Permissions Subsystem.

3.2.4.1.10 The Network Services Subsystem shall route messages between networks for those System Users that are connected via a private network.

3.2.4.1.11 The Network Services Subsystem shall support IPv6 for non-DSRC Users.

3.2.4.1.12 Intrusion Detection Software

3.2.4.1.12.1 The Network Services Subsystem shall install intrusion detection software to identify suspicious network traffic.

3.2.4.1.12.2 The Network Service Subsystem shall send the Intrusion Alert to the Misbehavior Management Subsystem using its contents to update the contents in the 4.2.2.3.11 Misbehavior Reports Log.

3.2.4.1.13 Time Requirements

3.2.4.1.13.1 The Network Services Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.4.1.14 State/Mode/Status Requirements

3.2.4.1.14.1 The Network Services Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.4.1.14.2 The Network Services Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.4.1.14.3 The Network Services Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.4.1.14.4 The Network Services Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.4.2 External Interface Requirements

3.2.4.2.1 The Network Services Subsystem shall enable a privileged System Operator to update the contents of the Network Configuration data store.

3.2.4.2.2 The Network Services Subsystem shall connect to the Internet to enable System Users to communicate to the Core System.

3.2.4.2.3 The Network Services Subsystem shall connect to private networks to enable System Users to communicate to the Core System.

3.2.4.2.4 The Network Services Subsystem shall enable a privileged System Operator to update the contents of the Configure Network Services.

3.2.5 Service Monitor Subsystem

The Service Monitor Subsystem monitors the status of Core System services, interfaces, and communications networks connected to the Core. It informs System Users of the availability and status of its services.

Service Monitor also monitors the integrity of internal Core System components and supporting software, and mitigates against vulnerabilities. This includes periodic verification of the authenticity of Core service software and supporting software. This also includes monitoring for vulnerabilities including but not limited to virus protection, network port monitoring, and monitoring for patches to third party components. Should a vulnerability be detected or a component of the Core found to have lost integrity, Service Monitor takes steps to mitigate against damage and performance degradation.

The Service Monitor Subsystem ensures the physical security of Core System services by monitoring the environmental conditions that Core components operate in (e.g. temperature and humidity) as well as the condition of its power system. It takes steps to mitigate against system failures in the event that environmental conditions exceed operating thresholds. Actions could include the activation of environmental or backup power systems and/or the modification of Core service operations, as well as Core System Personnel (Core System staff) notification.

Service Monitor also monitors the performance of all services and interfaces and makes performance metrics available to Core System Personnel (Core System staff).

3.2.5.1 Functional Requirements

3.2.5.1.1 Core System Subsystem Status Processing

3.2.5.1.1.1 The Service Monitor Subsystem shall accept the 4.5.1.3.5.4 System User Status Registration from System Users.

3.2.5.1.1.2 The Service Monitor Subsystem shall accept the 4.5.1.3.5.3 Service Status Query from System Users.

3.2.5.1.1.3 Upon accepting a 4.5.1.3.5.3 Service Status Query from a System User, the Service Monitor Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.5.1.1.4 Upon accepting a valid 4.5.1.3.5.3 Service Status Query from a System User, the Service Monitor Subsystem shall transmit the 4.5.1.3.5.2 Service Status response to that System User.

3.2.5.1.1.5 The Service Monitor Subsystem shall transmit the 4.5.1.3.5.1 Performance Records to the Core Certification Authority (CCA).

3.2.5.1.1.6 The Service Monitor Subsystem shall use the contents of the 4.2.4.3.22 Service Status Distribution Catalog to determine which System Users (including other Core Systems) are registered with this Core System.

3.2.5.1.1.7 The Service Monitor Subsystem shall send a 4.5.2.3.1.4 Core Distribution List to the Core2Core Subsystem for all registered Core Systems.

3.2.5.1.1.8 The Service Monitor Subsystem shall send a 4.5.2.3.1.1 Core Config Info to the Core2Core Subsystem for services offered by this Core System.

3.2.5.1.1.9 The Service Monitor Subsystem shall send a 4.5.2.3.1.2 Config Info for Other Cores to the Core2Core Subsystem.

3.2.5.1.1.10 The Service Monitor Subsystem shall send a 4.5.2.3.1.3 Data to be Backed Up to the Core2Core Subsystem.

3.2.5.1.1.11 The Service Monitor Subsystem shall send a 4.5.2.3.1.7 Detailed Service Status to the Core2Core Subsystem.

3.2.5.1.1.12 The Service Monitor Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.5.1.1.13 The Service Monitor Subsystem shall receive the 4.5.1.3.1.7 Core Status Registration from the Core2Core Subsystem.

3.2.5.1.1.14 The Service Monitor Subsystem shall receive the 4.5.2.3.7.1 Restore Data from the Core2Core Subsystem.

3.2.5.1.1.15 The Service Monitor Subsystem shall receive the 4.5.2.3.4.2 Service Control Node Performance from the Network Services Subsystem.

3.2.5.1.1.16 The Service Monitor Subsystem shall receive the Locally Encrypted Message from the User Trust Subsystem.

3.2.5.1.2 Time Requirements

3.2.5.1.2.1 The Service Monitor Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.5.1.3 State/Mode/Status Requirements

3.2.5.1.3.1 The Service Monitor Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.5.1.3.2 The Service Monitor Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.5.1.3.3 The Service Monitor Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.5.1.3.4 The Service Monitor Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.5.1.3.5 The Service Monitor Subsystem shall update the Core System's Health and Safety Status to the 4.2.5.2.8 System State and Performance Log.

3.2.5.1.3.6 The Service Monitor Subsystem shall update the Core System's performance, monitoring and configuration changes to the 4.2.5.2.8 System State and Performance Log.

3.2.5.2 External Interface Requirements

3.2.5.2.1 The Service Monitor Subsystem shall enable a privileged System Operator to update the contents of the Service Monitor Configuration data store.

3.2.5.2.2 The Service Monitor Subsystem shall enable a privileged System Operator to update the contents of the Configure Service.

3.2.5.2.3 The Service Monitor shall connect to the Core Certification Authority (CCA) to accept performance records from the Core System.

3.2.6 Time Synchronization Subsystem

The Time Synchronization Subsystem uses a time base available to all System Users and makes this time available to all Core System services which use this time base whenever a time reference is required.

3.2.6.1 Functional Requirements

3.2.6.1.1 The Time Synchronization Subsystem shall receive the 4.5.1.3.6.1 Time message from an external reference time source.

3.2.6.1.2 Upon accepting the 4.5.1.3.6.1 Time message from an external reference time source, the Time Synchronization Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.6.1.3 Upon receiving a valid 4.5.1.3.6.1 Time message from an external time source, the Time Synchronization Subsystem shall send the 4.5.2.3.7.2 Time Local Form to its Core subsystems within 10ms (TBR).

3.2.6.1.4 The 4.5.2.3.7.2 Time Local Form shall not drift (lagging or leading in time) from the external time source standard time reference by more than [TBR] 1 second per year.

3.2.6.1.5 The Time Synchronization Subsystem shall receive the 4.5.2.3.7.1 Restore Data from the Core2Core Subsystem.

3.2.6.1.6 The Time Synchronization Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.6.1.7 The Time Synchronization Subsystem shall receive the Locally Encrypted Message from the User Trust Subsystem.

3.2.6.1.8 The Time Synchronization Subsystem shall send the 4.5.2.3.5.2 Operator ID, function to the User Permissions Subsystem.

3.2.6.1.9 The Time Synchronization Subsystem shall provide Coordinated Universal Time (UTC) to all Core System subsystems.

3.2.6.1.10 State/Mode/Status Requirements

3.2.6.1.10.1 The Time Synchronization Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.6.1.10.2 The Time Synchronization Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.6.1.10.3 The Time Synchronization Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.6.1.10.4 The Time Synchronization Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.6.2 External Interface Requirements

3.2.6.2.1 The Time Synchronization Subsystem shall establish an interface to the National Institute of Standards and Technology (NIST).

3.2.6.2.2 The Time Synchronization Subsystem shall enable a privileged System Operator to update the contents of the TS Configuration data store.

3.2.6.2.3 The Time Synchronization Subsystem shall enable a privileged System Operator to update the contents of the Configure Time Synchronization.

3.2.7 User Permissions Subsystem

The User Permissions Subsystem provides tools allowing System Users to verify whether a given user, identified by digital certificate-based credentials, is authorized to request or perform the action requested in the message payload. It also maintains the status of users, whether they have a specific account, their allowed behaviors with defined permissions (publish, subscribe, actions allowed to request, and administration etc.), or if they belong to an anonymous group. User Permissions provides the tools for Core System Personnel to: create new users and groups, modify existing users and groups, and modify permissions associated with users and groups.

3.2.7.1 Functional Requirements

3.2.7.1.1 The User Permissions Subsystem shall accept the 4.5.1.3.7.2 User Identity and Permission Request from System Users.

3.2.7.1.2 Upon accepting the 4.5.1.3.7.2 User Identity and Permission Request from a System User, the User Permissions Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.7.1.3 Upon accepting a valid 4.5.1.3.7.2 User Identity and Permission Request from a System User, the User Permissions Subsystem shall use its contents to update the contents in the 4.2.3.3.14 User Permission Registry.

3.2.7.1.3.1 If 4.5.1.3.7.2 User Identity and Permission Request does not meet the acceptance criteria then the User Permissions Subsystem shall send a 4.5.2.3.3.13 Suspicious Permission Request to the Misbehavior Management Subsystem.

3.2.7.1.4 Upon accepting a valid 4.5.1.3.7.2 User Identity and Permission Request from a System User, the User Permissions Subsystem shall transmit the User Permission Confirmation response to that System User.

3.2.7.1.5 The User Permissions Subsystem shall accept the 4.5.1.3.7.1 Application Permission Request from System Users.

3.2.7.1.6 Upon accepting the 4.5.1.3.7.1 Application Permission Request from a System User, the User Permissions Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.7.1.7 Upon accepting a valid 4.5.1.3.7.1 Application Permission Request, the User Permissions Subsystem shall transmit the Application Permission Confirmation response to that System User.

3.2.7.1.8 Upon accepting a valid 4.5.1.3.7.1 Application Permission Request from a System User, the User Permissions Subsystem shall use its contents to update the contents in the 4.2.6.3.15 User Permission Registry.

3.2.7.1.8.1 If 4.5.1.3.7.1 Application Permission Request does not meet the acceptance criteria then the User Permissions Subsystem shall send a 4.5.2.3.3.9 Suspicious Application Request to the Misbehavior Management Subsystem.

3.2.7.1.9 If a 4.5.1.3.7.1 Application Permission Request from a System User contains a data item that the User Permissions Subsystem determines as invalid, the User Permissions Subsystem shall exclude that data item from its update of the 4.2.6.3.15 User Permission Registry.

3.2.7.1.10 The User Permissions Subsystem shall receive the 4.5.2.3.5.1 Core ID, function from other Core subsystems to verify other Core Systems permission to a given function.

3.2.7.1.11 The User Permissions Subsystem shall receive the 4.5.2.3.7.1 Restore Data from the Core2Core Subsystem.

3.2.7.1.12 The User Permissions Subsystem shall receive the 4.5.2.3.5.1 Core ID, function from other Core subsystems to verify other Core System's permission to a given function.

3.2.7.1.13 The User Permissions Subsystem shall receive the 4.5.2.3.5.2 Operator ID, function from other Core subsystems to verify an operator's permission to a given function.

3.2.7.1.14 Upon receiving a 4.5.2.3.5.2 Operator ID, function from other Core subsystems, the User Permissions Subsystem shall send the 4.5.2.3.7.3 Permission response to that Core subsystem.

3.2.7.1.15 The User Permissions Subsystem shall receive the 4.5.2.3.5.4 Provider ID, function from the Data Distribution Subsystem to verify data provider's permission to a given function.

3.2.7.1.16 Upon receiving a 4.5.2.3.5.4 Provider ID, function from other Core subsystems, the User Permissions Subsystem shall send the 4.5.2.3.7.3 Permission response to that Core subsystem.

3.2.7.1.17 The User Permissions Subsystem shall receive the 4.5.2.3.5.7 System User ID, Revoke function from the Misbehavior Management Subsystem to revoke a System User's permission to a given function.

3.2.7.1.18 The User Permissions Subsystem shall receive the 4.5.2.3.5.3 Operator ID, Revoke function from the Misbehavior Management Subsystem to revoke an operator's permission to a given function.

3.2.7.1.19 The User Permissions Subsystem shall receive the 4.5.2.3.5.10 Permission Change Request from the User Trust Management Subsystem to modify a System User's permission.

3.2.7.1.20 The User Permissions Subsystem shall receive the 4.5.2.3.5.9 Certificate Owner ID from the User Trust Management Subsystem to verify a System User's permission to request a DSRC Identity certificate.

3.2.7.1.21 Upon receiving a 4.5.2.3.5.9 Certificate Owner ID from the User Trust Management Subsystem, the User Permissions Subsystem shall send the Cert Permission response to the User Trust Management Subsystem.

3.2.7.1.22 The User Permissions Subsystem shall receive the 4.5.2.3.5.8 Cert Owner, App query from the User Trust Management Subsystem to verify an application's permissions.

3.2.7.1.23 Upon receiving a 4.5.2.3.5.8 Cert Owner, App query from the User Trust Management Subsystem, the User Permissions Subsystem shall send the 4.5.2.3.6.1 App Permissions response to the User Trust Management Subsystem.

3.2.7.1.24 The User Permissions Subsystem shall send a 4.5.2.3.1.1 Core Config Info to the Core2Core Subsystem.

3.2.7.1.25 The User Permissions Subsystem shall send a 4.5.2.3.1.2 Config Info for Other Cores to the Core2Core Subsystem.

3.2.7.1.26 The User Permissions Subsystem shall send a 4.5.2.3.1.3 Data to be Backed Up to the Core2Core Subsystem.

3.2.7.1.27 The User Permissions Subsystem shall receive the 4.5.2.3.5.6 System User ID, function from the Misbehaving Management Subsystem to verify data provider's permission to a given function.

3.2.7.1.28 Upon receiving a 4.5.2.3.5.6 System User ID, function from the Misbehaving Management Subsystem, the User Permissions Subsystem shall send the 4.5.2.3.3.8 SUID, Function Permission response.

3.2.7.1.29 The User Permissions Subsystem shall send the 4.5.2.3.3.3 Internal Misbehavior Report to the Misbehavior Management Subsystem identifying misbehavior information (e.g., misbehaving user, type of misbehavior).

3.2.7.1.30 The User Permissions Subsystem shall send the 4.5.2.3.3.5 Operator Permissions response to the Misbehavior Management Subsystem.

3.2.7.1.31 The User Permissions Subsystem shall send the 4.5.2.3.3.14 System User Permissions response to the Misbehavior Management Subsystem.

3.2.7.1.32 The User Permissions Subsystem shall receive the Locally Encrypted Message from the User Trust Subsystem.

3.2.7.1.33 The User Permissions Subsystem shall send the Scope Query to the User Trust Subsystem requesting the operational scope of its User Trust Management Subsystem.

3.2.7.1.34 The User Permissions Subsystem shall receive the 4.5.2.3.5.11 User ID, Apps from the User Trust Subsystem.

3.2.7.1.35 Time Requirements

3.2.7.1.35.1 The User Permissions Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.7.1.36 State/Mode/Status Requirements

3.2.7.1.36.1 The User Permissions Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.7.1.36.2 The User Permissions Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.7.1.36.3 The User Permissions Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.7.1.36.4 The User Permissions Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.7.2 External Interface Requirements

3.2.7.2.1 The User Permissions Subsystem shall enable a privileged System Operator to update the contents of the User Permission Configuration data store.

3.2.7.2.2 The User Permissions Subsystem shall enable a privileged System Operator to update the contents of the Configure User Permissions.

3.2.8 User Trust Management Subsystem

The User Trust Management Subsystem manages access rules and credentials in the form of X.509 digital certificates for all System Users and Core System components that require and are entitled to them. It creates and distributes cryptographic keys to qualifying System Users. It works with User Permissions to determine whether a given user applying for credentials or keys is entitled to them. It also manages the revocation of credentials and the distribution of Certificate Revocation Lists (CRLs) of disallowed credentials to interested System Users. The provision, distribution, and management of IEEE 1609.2 based digital certificates (both identity and anonymous certificates) that are primarily used by Mobile and Field Users using 5.9GHz Dedicated Short Range Communications (DSRC) will be handled by an External Support System (ESS) to be defined. The User Trust Management Subsystem will maintain a relationship with this ESS, and provide information about how to contact this ESS to interested System Users. User Trust Management will forward requests for IEEE 1609.2 certificate revocation for misbehaving System Users from Misbehavior Management to this ESS.

3.2.8.1 Functional Requirements

3.2.8.1.1 Message Authentication and Confidentiality

3.2.8.1.1.1 The User Trust Management Subsystem shall verify signed messages received from System Users.

3.2.8.1.1.2 The User Trust Management Subsystem shall sign messages it sends to System Users.

3.2.8.1.1.3 The User Trust Subsystem shall receive the 4.5.2.3.6.7 Special App Permissions from the User Permissions Subsystem.

3.2.8.1.1.4 The User Trust Subsystem shall transmit the 4.5.1.3.8.10 User Special Permissions to the External Support System (ESS) DSRC Registration Authority (RA).

3.2.8.1.2 Credentialing Functions

3.2.8.1.2.1 The User Trust Subsystem shall accept the 4.5.1.3.8.1 Credential Request from System Users.

3.2.8.1.2.2 Upon accepting the 4.5.1.3.8.1 Credential Request from a System User, the User Trust Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.8.1.2.3 Upon accepting a valid 4.5.1.3.8.1 Credential Request from a System User, the User Trust Subsystem shall transmit the 4.5.1.3.8.3 Credentials to that System User.

3.2.8.1.2.4 Upon accepting a valid 4.5.1.3.8.1 Credential Request (for a DSRC Certificate) from a System User, the User Trust Subsystem shall use its contents to update the contents in the 4.2.6.3.3 Application Permission Registry.

3.2.8.1.2.5 If a 4.5.1.3.8.1 Credential Request (for a DSRC Certificate) from a System User contains a data item that the User Trust Subsystem determines as invalid, the User Trust Subsystem shall exclude that data item from its update of the 4.2.6.3.3 Application Permission Registry.

3.2.8.1.2.6 Upon accepting a valid 4.5.1.3.8.1 Credential Request from a System User, the User Trust Subsystem shall use its contents to update the contents in the 4.2.6.3.16 User Trust Management Configuration.

3.2.8.1.2.7 If a 4.5.1.3.8.1 Credential Request from a System User contains a data item that the User Trust Subsystem determines as invalid, the User Trust Subsystem shall exclude that data item from its update of the 4.2.6.3.16 User Trust Management Configuration.

3.2.8.1.2.8 Upon accepting the 4.5.1.3.8.1 Credential Request from a System User that does not meet the acceptance criteria, the User Trust Subsystem shall transmit the 4.5.1.3.8.2 Credential Referral response indicating non-approval for that System User.

3.2.8.1.2.9 The User Trust Subsystem shall transmit the 4.5.1.3.8.6 Ext X.509 Cert Request to the External Support System (ESS) X.509 Certificate Authority (CA).

3.2.8.1.2.10 The User Trust Subsystem shall accept the 4.5.1.3.8.11 X.509 Certificate from External Support System (ESS) X.509 Certificate Authority (CA).

3.2.8.1.2.11 The User Trust Subsystem shall accept the 4.5.1.3.8.9 User Identification from External Support System (ESS) DSRC Registration Authority (RA).

3.2.8.1.2.12 Upon accepting the 4.5.1.3.8.9 User Identification from External Support System (ESS) DSRC Registration Authority (RA), the User Trust Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.8.1.2.13 Upon accepting a valid 4.5.1.3.8.9 User Identification from External Support System (ESS) DSRC Registration Authority (RA), the User Trust Subsystem shall use the 4.5.2.3.5.11 User ID, Apps contents to update the contents in the 4.2.3.3.14 User Permission Registry.

3.2.8.1.2.14 If a 4.5.1.3.8.9 User Identification from External Support System (ESS) DSRC Registration Authority (RA) contains a data item that the User Trust Subsystem determines as invalid, the User Trust Subsystem shall exclude that data item from its update of the 4.2.3.3.14 User Permission Registry.

3.2.8.1.3 Certificate Revocation List (CRL) Functions

3.2.8.1.3.1 The User Trust Subsystem shall accept the 4.5.1.3.8.12 X.509 CRL from External Support System (ESS) X.509 Certificate Authority (CA).

3.2.8.1.3.2 Upon accepting the 4.5.1.3.8.12 X.509 CRL from External Support System (ESS) X.509 Certificate Authority (CA), the User Trust Subsystem shall ensure that its contents meet the acceptance criteria for all of its data objects.

3.2.8.1.3.3 Upon accepting a valid 4.5.1.3.8.12 X.509 CRL from External Support System (ESS) X.509 Certificate Authority (CA), the User Trust Subsystem shall use its contents to update the contents in the 4.2.7.3.26 User Trust Management Configuration.

3.2.8.1.3.4 If a 4.5.1.3.8.12 X.509 CRL from External Support System (ESS) X.509 Certificate Authority (CA) contains a data item that the User Trust Subsystem determines as invalid, the User Trust Subsystem shall exclude that data item from its update of the 4.2.7.3.26 User Trust Management Configuration.

3.2.8.1.3.5 The User Trust Subsystem shall send the 4.5.1.3.8.4 CRL message to System Users.

3.2.8.1.3.6 The User Trust Subsystem shall transmit the 4.5.2.3.6.3 Complete CRL to the Core2Core Subsystem.

3.2.8.1.3.7 The User Trust Subsystem shall accept the 4.5.2.3.6.3 Complete CRL to the Core2Core Subsystem.

3.2.8.1.3.8 The User Trust Subsystem shall transmit the 4.5.2.3.1.6 CRL Deltas to the Core2Core Subsystem.

3.2.8.1.3.9 The User Trust Subsystem shall accept the 4.5.2.3.1.6 CRL Deltas from the Core2Core Subsystem.

3.2.8.1.4 Encryption/Decryption Functions

3.2.8.1.4.1 The User Trust Management Subsystem shall transmit a Locally Encrypted Message to System Users when the message is from a Core System.

3.2.8.1.4.2 The User Trust Management Subsystem shall transmit a Locally Encrypted Message to other Core Systems when that Core System interface is non-persistent. (Note: message exchanges between Core Systems on a persistent interface are not encrypted).

3.2.8.1.4.3 The User Trust Management Subsystem shall accept 4.5.2.3.6.6 Remotely Encrypted Message from other Core subsystems.

3.2.8.1.4.4 The User Trust Management Subsystem shall accept 4.5.2.3.6.6 Remotely Encrypted Message from a System User.

3.2.8.1.4.5 Upon accepting the 4.5.2.3.6.6 Remotely Encrypted Message from a System User, the User Trust Subsystem shall ensure that its contents meet the acceptance criteria as a Decrypted Message.

3.2.8.1.4.6 If a 4.5.2.3.6.6 Remotely Encrypted Message from a System User contains a data item that the User Trust Subsystem determines as invalid, the User Trust Subsystem shall send a 4.5.2.3.3.2 Decryption Error Message to the Misbehavior Management Subsystem.

3.2.8.1.4.7 If a 4.5.2.3.6.6 Remotely Encrypted Message from a System User is a message that the User Trust Subsystem determines as an authenticity verification failure, the User Trust Subsystem shall send the 4.5.2.3.3.1 Authenticity Error Message to the Misbehavior Management Subsystem.

3.2.8.1.4.8 If a 4.5.2.3.6.6 Remotely Encrypted Message from a System User is a message that the User Trust Subsystem determines as a decryption failure, the User Trust Subsystem shall send the 4.5.2.3.3.2 Decryption Error Message to the Misbehavior Management Subsystem.

3.2.8.1.5 Other Functions

3.2.8.1.5.1 The User Trust Subsystem shall send a Locally Encrypted Message to other Core subsystems.

3.2.8.1.5.2 The User Trust Subsystem shall receive the Scope Query from the User Permissions Subsystem shall send the Scope Query requesting the operational scope of its User Trust Management Subsystem.

3.2.8.1.5.3 The User Trust Subsystem shall send the 4.5.2.3.5.2 Operator ID, function to the User Permissions Subsystem.

3.2.8.1.5.4 The User Trust Subsystem shall send the 4.5.2.3.5.10 Permission Change Request to the User Permissions Subsystem.

3.2.8.1.5.5 The User Trust Subsystem shall send the 4.5.2.3.5.9 Certificate Owner ID to the User Permissions Subsystem.

3.2.8.1.5.6 The User Trust Subsystem shall send the 4.5.2.3.5.8 Cert Owner, App to the User Permissions Subsystem.

3.2.8.1.5.7 The User Trust Subsystem shall receive the 4.5.2.3.7.1 Restore Data from the Core2Core Subsystem.

3.2.8.1.5.8 The User Trust Subsystem shall receive the 4.5.2.3.6.5 Misbehaving User ID from the Misbehaving Management Subsystem.

3.2.8.1.5.9 The User Trust Subsystem shall receive the 4.5.2.3.6.1 App Permissions from the User Permissions Subsystem.

3.2.8.1.5.10 The User Trust Subsystem shall receive the 4.5.2.3.7.3 Permission response from the User Permissions Subsystem.

3.2.8.1.5.11 The User Trust Subsystem shall send a 4.5.2.3.1.1 Core Config Info to the Core2Core Subsystem.

3.2.8.1.5.12 The User Trust Subsystem shall send a 4.5.2.3.1.2 Config Info for Other Cores to the Core2Core Subsystem.

3.2.8.1.5.13 The User Trust Subsystem shall send a 4.5.2.3.1.3 Data to be Backed Up to the Core2Core Subsystem.

3.2.8.1.5.14 Upon receiving a Scope Query from the User Permissions Subsystem, the User Trust Subsystem shall send the 4.5.2.3.3.7 Scope response to the User Permissions Subsystem.

3.2.8.1.6 Time Requirements

3.2.8.1.6.1 The User Trust Management Subsystem shall receive the 4.5.2.3.7.2 Time Local Form from the Time Synchronization Subsystem.

3.2.8.1.7 State/Mode/Status Requirements

3.2.8.1.7.1 The User Trust Management Subsystem shall accept an Operational Changes message from a privilege System Operator.

3.2.8.1.7.2 The User Trust Management Subsystem shall update its State Changes to the 4.2.5.3.4 Event Log.

3.2.8.1.7.3 The User Trust Management Subsystem shall update its Actions to the 4.2.5.3.4 Event Log.

3.2.8.1.7.4 The User Trust Management Subsystem shall update its Anomalies to the 4.2.5.3.4 Event Log.

3.2.8.1.7.5 When operating in Maintenance Mode, the User Trust Management Subsystem shall not accept the 4.5.1.3.8.1 Credential Request from System Users.

3.2.8.1.7.6 When operating in Standby State, the User Trust Management Subsystem shall not accept not accept the 4.5.1.3.8.1 Credential Request from System Users.

3.2.8.2 External Interface Requirements

3.2.8.2.1 The User Trust Management Subsystem shall enable a privileged System Operator to update the contents of the User Trust Management Configuration data store.

3.2.8.2.2 The User Trust Management Subsystem shall enable a privileged System Operator to update the contents of the Configure User Trust Management.

4 Verification Methods

This section contains two tables extracted from the Requirements Database. Table 4-1 lists the system requirements and its verification method. Table 4-2 lists the subsystem requirements and their verification methods. For each requirement, one of the following methods of verification will be listed:

- **Demonstration (D)** is a requirement that the system can demonstrate without external test equipment.
- **Test (T)** is a requirement that requires some external piece of test equipment (e.g. logic analyzer, and/or volt meter).
- **Analyze (A)** is a requirement that is met indirectly through a logical conclusion or mathematical analysis of a result. For example, Algorithms for congestion: the designer may need to show that the requirement is met through the analysis of count and occupancy calculations in software or firmware.
- **Inspection (I)** is verification through a visual comparison. For example, quality of welding may be done through a visual comparison against an in-house standard.

4.1 System Requirements Verification

The table below lists the verification methods (VMs) for the system-level requirements (SR IDs).

Table 4-1. System Requirements Verification Matrix

SR ID	VM
3.1.1.1.1	T
3.1.1.1.2	T
3.1.1.1.3	T
3.1.1.1.4	T
3.1.1.1.5	T
3.1.1.1.6	T
3.1.1.1.7	T
3.1.1.1.8	T
3.1.1.1.9	T
3.1.1.1.10	T
3.1.1.1.11	T
3.1.1.1.12	T
3.1.1.1.13	T
3.1.1.1.14	T
3.1.1.1.15	T
3.1.1.1.16	T
3.1.1.1.17	T
3.1.1.1.18	T
3.1.1.1.19	T
3.1.1.1.20	T
3.1.1.1.21	T
3.1.1.1.22	T
3.1.1.1.23	T
3.1.1.1.24	T
3.1.1.1.25	T
3.1.1.1.26	T
3.1.1.1.27	T
3.1.1.1.28	T
3.1.1.1.29	T
3.1.1.1.30	T
3.1.1.1.31	T
3.1.1.1.32	T
3.1.1.1.33	T
3.1.1.2.1	T
3.1.1.2.2	T
3.1.1.2.3	T
3.1.1.2.4	T
3.1.1.2.5	T
3.1.1.2.6	T
3.1.1.2.7	T
3.1.1.2.8	T
3.1.1.2.9	T

SR ID	VM
3.1.1.2.10	T
3.1.1.2.11	T
3.1.1.3.1	T
3.1.1.3.2	T
3.1.1.3.3	D
3.1.1.3.4	D
3.1.1.3.5	D
3.1.1.4.1	T
3.1.1.4.2	T
3.1.1.4.3	D
3.1.1.4.4	D
3.1.1.4.5	T
3.1.1.4.6	T
3.1.1.4.7	T
3.1.1.5.1	T
3.1.1.5.2	T
3.1.1.5.3	T
3.1.1.5.4	T
3.1.1.5.5	T
3.1.1.5.6	T
3.1.1.5.7	T
3.1.1.5.8	T
3.1.1.5.9	D
3.1.1.5.10	D
3.1.1.5.11	D
3.1.1.5.12	D
3.1.1.5.13	D
3.1.1.6.1	T
3.1.1.7.1	T
3.1.1.7.2	T
3.1.1.7.3	T
3.1.1.7.4	T
3.1.1.7.5	T
3.1.1.7.6	T
3.1.1.8.1	T
3.1.1.8.2	T
3.1.1.8.3	T
3.1.1.8.4	T
3.1.1.8.5	T
3.1.1.8.6	T
3.1.1.8.7	T
3.1.1.8.8	T
3.1.1.8.9	T
3.1.1.8.10	T
3.1.1.8.11	T
3.1.1.8.12	T
3.1.1.8.13	T
3.1.1.8.14	T

SR ID	VM
3.1.2.1	T
3.1.3.1	T
3.1.3.2	T
3.1.3.3	T
3.1.3.4	T
3.1.3.5	T
3.1.3.6	T
3.1.3.7	T
3.1.4.1.1	D
3.1.4.2.1	T
3.1.4.2.2	T
3.1.4.2.3	T
3.1.4.2.4	T
3.1.4.2.5	I
3.1.4.3.1	D
3.1.4.3.2	I
3.1.4.4.1	A
3.1.4.4.2	A
3.1.5.1	I

4.2 Subsystem Requirements Verification

The table below lists the verification methods (VMs) for the subsystem-level requirements (SSR IDs).

Table 4-2. Subsystem Requirements Verification Matrix

SSR ID	VM
3.2.1.1.1	T
3.2.1.1.2	T
3.2.1.1.3	T
3.2.1.1.4	T
3.2.1.1.5	T
3.2.1.1.6	T
3.2.1.1.7	T
3.2.1.1.8	T
3.2.1.1.9	T
3.2.1.1.10	T
3.2.1.1.11	T
3.2.1.1.12	T
3.2.1.1.13	T
3.2.1.1.14	T
3.2.1.1.15	T
3.2.1.1.16	T
3.2.1.1.17	T
3.2.1.1.18	T
3.2.1.1.19	T
3.2.1.1.20	T
3.2.1.1.21	T
3.2.1.1.22	T
3.2.1.1.23	T
3.2.1.1.24	T
3.2.1.1.25	T
3.2.1.1.26	T
3.2.1.1.27	T
3.2.1.1.28	T
3.2.1.1.29	T
3.2.1.1.30	T
3.2.1.1.31	T
3.2.1.1.32	T
3.2.1.1.33	T
3.2.1.1.34	T
3.2.1.1.35	T
3.2.1.1.36	T
3.2.1.1.37	T
3.2.1.1.38	T
3.2.1.1.39	T
3.2.1.1.40	T
3.2.1.1.41	T
3.2.1.1.42	T
3.2.1.1.43	T
3.2.1.1.44	T
3.2.1.1.45	T
3.2.1.1.46	T
3.2.1.1.47	T
3.2.1.1.48	T
3.2.1.1.49	T
3.2.1.1.50	T
3.2.1.1.51	T
3.2.1.1.52	T
3.2.1.1.53	T
3.2.1.1.54	T
3.2.1.1.55	T
3.2.1.1.56	T
3.2.1.1.57	T
3.2.1.1.58	T
3.2.1.1.59	T
3.2.1.1.60	T
3.2.1.1.61	T
3.2.1.1.66.1	T
3.2.1.1.67.1	T
3.2.1.1.67.2	T
3.2.1.1.67.3	T
3.2.1.1.67.4	T
3.2.1.2.1	D
3.2.1.2.2	D
3.2.1.2.3	D
3.2.1.2.4	D
3.2.2.1.1.1	T
3.2.2.1.1.2	T
3.2.2.1.1.3	T
3.2.2.1.1.4	T
3.2.2.1.1.5	T
3.2.2.1.1.6	T
3.2.2.1.1.7	T
3.2.2.1.2.1	T
3.2.2.1.2.2	T
3.2.2.1.2.3	T
3.2.2.1.2.4	T
3.2.2.1.2.5	T
3.2.2.1.2.6	T
3.2.2.1.2.7	T
3.2.2.1.2.8	T
3.2.2.1.2.9	T
3.2.2.1.2.10	T
3.2.2.1.2.11	T
3.2.2.1.2.12	T
3.2.2.1.2.13	T
3.2.2.1.2.14	T
3.2.2.1.2.15	T
3.2.2.1.2.16	T
3.2.2.1.2.17	T
3.2.2.1.2.18	T
3.2.2.1.2.19	T
3.2.2.1.2.20	T
3.2.2.1.2.21	T
3.2.2.1.2.22	T
3.2.2.1.3.1	D
3.2.2.1.3.2	T
3.2.2.1.3.3	T

SSR ID	VM
3.2.2.1.4.1	T
3.2.2.1.4.2	T
3.2.2.1.4.3	T
3.2.2.1.4.4	T
3.2.2.1.4.5	T
3.2.2.1.4.6	T
3.2.2.1.4.7	T
3.2.2.1.4.8	T
3.2.2.1.5.1	D
3.2.2.1.6.1	T
3.2.2.1.6.2	T
3.2.2.1.6.3	T
3.2.2.1.6.4	T
3.2.2.1.6.5	T
3.2.2.1.6.6	T
3.2.2.1.6.7	T
3.2.2.1.6.8	T
3.2.2.1.6.9	T
3.2.2.1.6.10	T
3.2.2.2.1	D
3.2.2.2.2	D
3.2.3.1.1	T
3.2.3.1.2	T
3.2.3.1.3	T
3.2.3.1.4	T
3.2.3.1.5	T
3.2.3.1.6	T
3.2.3.1.7	T
3.2.3.1.8	T
3.2.3.1.9	T
3.2.3.1.10	T
3.2.3.1.11	T
3.2.3.1.12	T
3.2.3.1.12.1	T
3.2.3.1.12.2	T
3.2.3.1.12.3	T
3.2.3.1.13	T
3.2.3.1.14	T
3.2.3.1.15	T
3.2.3.1.16	T

SSR ID	VM
3.2.3.1.17	T
3.2.3.1.18	T
3.2.3.1.19	T
3.2.3.1.20	T
3.2.3.1.21	T
3.2.3.1.22	T
3.2.3.1.23	T
3.2.3.1.24	T
3.2.3.1.25.1	T
3.2.3.1.26.1	T
3.2.3.1.26.2	T
3.2.3.1.26.3	T
3.2.3.1.26.4	T
3.2.3.2.1	D
3.2.3.2.2	D
3.2.4.1.1	T
3.2.4.1.2	T
3.2.4.1.3	T
3.2.4.1.4	T
3.2.4.1.5	T
3.2.4.1.6	T
3.2.4.1.7	T
3.2.4.1.8	T
3.2.4.1.9	T
3.2.4.1.10	T
3.2.4.1.11	D
3.2.4.1.12.1	D
3.2.4.1.12.2	T
3.2.4.1.13.1	T
3.2.4.1.14.1	T
3.2.4.1.14.2	T
3.2.4.1.14.3	T
3.2.4.1.14.4	T
3.2.4.2.1	D
3.2.4.2.2	D
3.2.4.2.3	D
3.2.4.2.4	D
3.2.5.1.1.1	T
3.2.5.1.1.2	T
3.2.5.1.1.3	T

SSR ID	VM
3.2.5.1.1.4	T
3.2.5.1.1.5	T
3.2.5.1.1.6	T
3.2.5.1.1.7	T
3.2.5.1.1.8	T
3.2.5.1.1.9	T
3.2.5.1.1.10	T
3.2.5.1.1.11	T
3.2.5.1.1.12	T
3.2.5.1.1.13	T
3.2.5.1.1.14	T
3.2.5.1.1.15	T
3.2.5.1.1.16	T
3.2.5.1.2.1	D
3.2.5.1.3.1	T
3.2.5.1.3.2	T
3.2.5.1.3.3	T
3.2.5.1.3.4	T
3.2.5.1.3.5	T
3.2.5.1.3.6	T
3.2.5.2.1	D
3.2.5.2.2	D
3.2.5.2.3	D
3.2.6.1.1	T
3.2.6.1.2	T
3.2.6.1.3	T
3.2.6.1.4	T
3.2.6.1.5	T
3.2.6.1.6	T
3.2.6.1.7	T
3.2.6.1.8	T
3.2.6.1.9	T
3.2.6.1.10.1	T
3.2.6.1.10.2	T
3.2.6.1.10.3	T
3.2.6.1.10.4	T
3.2.6.2.1	D
3.2.6.2.2	D
3.2.6.2.3	D
3.2.7.1.1	T

SSR ID	VM
3.2.7.1.2	T
3.2.7.1.3	T
3.2.7.1.3.1	T
3.2.7.1.4	T
3.2.7.1.5	T
3.2.7.1.6	T
3.2.7.1.7	T
3.2.7.1.8	T
3.2.7.1.8.1	T
3.2.7.1.9	T
3.2.7.1.10	T
3.2.7.1.11	T
3.2.7.1.12	T
3.2.7.1.13	T
3.2.7.1.14	T
3.2.7.1.15	T
3.2.7.1.16	T
3.2.7.1.17	T
3.2.7.1.18	T
3.2.7.1.19	T
3.2.7.1.20	T
3.2.7.1.21	T
3.2.7.1.22	T
3.2.7.1.23	T
3.2.7.1.24	T
3.2.7.1.25	T
3.2.7.1.26	T
3.2.7.1.27	T
3.2.7.1.28	T
3.2.7.1.29	T
3.2.7.1.30	T
3.2.7.1.31	T
3.2.7.1.32	T
3.2.7.1.33	T
3.2.7.1.34	T
3.2.7.1.35.1	T
3.2.7.1.36.1	T
3.2.7.1.36.2	T
3.2.7.1.36.3	T
3.2.7.1.36.4	T
3.2.7.2.1	D
3.2.7.2.2	D
3.2.8.1.1.1	T
3.2.8.1.1.2	T
3.2.8.1.1.3	T
3.2.8.1.1.4	T
3.2.8.1.2.1	T
3.2.8.1.2.2	T
3.2.8.1.2.3	T
3.2.8.1.2.4	T
3.2.8.1.2.5	T
3.2.8.1.2.6	T
3.2.8.1.2.7	T
3.2.8.1.2.8	T
3.2.8.1.2.9	T
3.2.8.1.2.10	T
3.2.8.1.2.11	T
3.2.8.1.2.12	T
3.2.8.1.2.13	T
3.2.8.1.2.14	T
3.2.8.1.3.1	T
3.2.8.1.3.2	T
3.2.8.1.3.3	T
3.2.8.1.3.4	T
3.2.8.1.3.5	T
3.2.8.1.3.6	T
3.2.8.1.3.7	T
3.2.8.1.3.8	T
3.2.8.1.3.9	T
3.2.8.1.4.1	D
3.2.8.1.4.2	D
3.2.8.1.4.3	T
3.2.8.1.4.4	T
3.2.8.1.4.5	T
3.2.8.1.4.6	T
3.2.8.1.4.7	T
3.2.8.1.4.8	T
3.2.8.1.5.1	T
3.2.8.1.5.2	T
3.2.8.1.5.3	T
3.2.8.1.5.4	T
3.2.8.1.5.5	T
3.2.8.1.5.6	T
3.2.8.1.5.7	T
3.2.8.1.5.8	T
3.2.8.1.5.9	T
3.2.8.1.5.10	T
3.2.8.1.5.11	T
3.2.8.1.5.12	T
3.2.8.1.5.13	T
3.2.8.1.5.14	T
3.2.8.1.6.1	T
3.2.8.1.7.1	T
3.2.8.1.7.2	T
3.2.8.1.7.3	T
3.2.8.1.7.4	T
3.2.8.1.7.5	T
3.2.8.1.7.6	T
3.2.8.2.1	D
3.2.8.2.2	D

5 Supporting Documentation

This section provides references or other information that may add to the understanding of the Requirements without going elsewhere. This section contains the Core System Needs, Internet Based Communication Standards, and Action Verb definitions.

5.1 Core System Needs

The following table contains a copy of the Core System Needs from the Core System Concept of Operations document. These Core System Needs are the basis for the requirements in this document. Section 6 on page 78 includes the traceability from these needs to the requirements and vice versa.

Table 5-1. Core System Needs

ID	Core System Need	Description / Rationale	Priority	Subsystem (s)
1	Data Protection	The Core System needs to protect data it handles from unauthorized access. This is required to support applications that exchange sensitive information, such as personally identifying or financial information, which if intercepted could compromise the privacy or financial records of the user.	Essential	User Trust Management
2	Core Trust	The Core System needs to establish trust with its System Users. Such trust relationships are necessary so that the Core System can be assured that System Users are who they say they are, and therefore trust the source.	Essential	User Trust Management
3	System User Trust	The Core System needs to facilitate trust between System Users. Such trust relationships are necessary so that System Users can be assured that other System Users "are who they say they are," and therefore trust the source and data they receive from other System Users.	Essential	User Trust Management
4	Core Trust Revocation	The Core System needs to revoke the trust relationship it has with its System Users when necessary. A trusted System User may operate in a fashion that indicates it should no longer be trusted, in which case the Core System must have a way of revoking that trust.	Essential	Misbehavior Management, User Trust Management
5	System User Trust Revocation	The Core System needs to facilitate the revocation of the trust relationships between System Users when necessary. A trusted System User may operate in a fashion that indicates it should no longer be trusted, in which case the Core System must have a way of facilitating revocation of trust between System Users.	Essential	Misbehavior Management, User Trust Management
6	Authorization Management	The Core System needs to manage authorization mechanisms to define roles, responsibilities and permissions for System Users. This enables the Core System to establish operational environments where different System Users may have different capabilities in terms of accessing Core services and interacting with one another. For instance, some Mobile elements may be authorized to request signal priority, or some Centers may be permitted to use the geographic broadcast service, while those without those permissions would not.	Essential	User Permission

ID	Core System Need	Description / Rationale	Priority	Subsystem (s)
7	Authorization Verification	The Core System needs to verify that System Users and Core Operations Personnel are authorized to perform an attempted operation. This enables the Core System to restrict operations to those users are permitted to use those operations. For example, geo-broadcast may be restricted to transportation or public safety agencies, so other users may be prohibited from performing geo-broadcast.	Essential	User Permission
8	Misbehavior Management	The Core System needs to identify System Users acting as bad actors. Bad actors are not necessarily malicious; they could be malfunctioning devices that may interfere with other System Users, Communications Layer systems or the Core System. Identifying bad actors enables subsequent action to protect the integrity of all users sharing the transportation environment.	Desirable	Misbehavior Management
9	Time Base	The Core System needs to operate on a common time base. Coordination of time between the internal systems that operate the Core System prevents internal synchronization errors and enables time-sensitive interactions with System Users.	Essential	Time Synchronization
10	Data Request	The Core System needs to provide a mechanism for data consumers to request data that is produced by data providers. This is a single request for a subscription to a certain type of data, and subsequent modification of the request to change data types or subscription parameters. Parameters include data frequency, type and location of where the data was generated. This enables the distribution of anonymously-provided data to interested data consumers, without requiring them to enter into a relationship with data providers. Request formats need to provide data consumers with the ability to differentiate and receive only the types of data they requested. For example this includes data type, geographic range, frequency and sampling rate. This request method supports a wide variety of user needs, from planners requesting all traffic data all the time, to traveler information services requesting a subset of traffic data, to weather information services only interested in windshield wiper status for vehicles in a specific area.	Desirable	Data Distribution

ID	Core System Need	Description / Rationale	Priority	Subsystem (s)
11	Data Provision	The Core System needs to supply information to data providers enabling them to transmit data to interested data consumers. At a minimum, data characteristics need to include type, frequency and location where data was generated, so that users that have requested data (see need data request) can differentiate between available data. This need enables data providers to direct the data they create to data consumers, and serves as the provider-side corollary to the data request need. This supports a variety of applications, including those focused on the center provision of data to users. It also serves as the answer to the System User's question of "I have data, how do I provide it and to whom?"	Desirable	Data Distribution
12	Data Forward	The Core System needs to provide a mechanism to distribute data that is produced by a System User acting as a data provider and requested by another System User. The Core System needs to provide this distribution mechanism, rather than relying on individual provider-consumer relationships, because multiple consumers may want access to the same data. By having the Core System distribute the data, System Users are relieved of the need to transmit the data multiple times. Also, some data that may be critical to the proper functioning of mandatory applications, such as data supporting geo-location of users (position corrections), time base data and roadway geometry data, all of which likely comes from a single source and needs to be distributed to large numbers of System Users. Additionally, System Users may interact over resource-constrained communication links, so Core-provided data redistribution reduces the potential load on those links.	Desirable	Data Distribution
13	Network Connectivity	The Core System needs to connect to the Internet. This allows the Core to provide services to any System User capable of connecting to the Internet.	Desirable	Network Services

ID	Core System Need	Description / Rationale	Priority	Subsystem (s)
14	Geographic Broadcast	The Core System needs to provide the information necessary for System Users who wish to communicate with a group of System Users in a specific area to do so. This capability enables System Users to target those in a specific area for information they wish to distribute without having to send individual messages to each recipient. Examples of applications that might use this include Amber Alerts, traffic information, and air quality alerts.	Desirable	Data Distribution, Network Services
15	Core System Service Status	The Core System needs to be able to accept and maintain the status of Core System services and provide accurate status information to System Users. Additionally, System Users may not be able to access a Core System service (because of their location for example) and would want to know where and when they could expect access to the Service.	Desirable	Service Monitor
16	System Integrity Protection	The Core System needs to protect the integrity of the Core System. This includes defense against the loss of integrity from a deliberate attack, software bug, environmental or hardware failure, as well as mitigation strategies to facilitate a predictable return to normal operations. Protection and controlled restoration of normal operations ensures that System Users have a high confidence in the security of the information they entrust to the Core System.	Essential	Service Monitor
17	System Availability	The Core System needs to be available for System Users to access Core System Services. This ensures that System Users have a high confidence in the performance of the Core System, and can rely on its services to accomplish their objectives.	Essential	Service Monitor
18	System Operational Performance Monitoring	The Core System needs to monitor its performance. This includes the status of interfaces, services, and metrics for the number of requests and the resolution of those requests. Monitoring the performance of Core System services and interfaces is necessary to understand when the system is operating properly, and to gauge when the system may be nearing capacity so that action may be taken to prevent the system from failing to provide services, e.g. maximum number of transactions/second, or internal communication bandwidth.	Essential	Service Monitor

ID	Core System Need	Description / Rationale	Priority	Subsystem (s)
19	Core System Independence	The Core System needs to be able to be independently deployed and operated providing Core System services to all System Users within its jurisdictional scope. This ensures that one entity's Core System deployment is not contingent on or dependent on another for basic functionality.	Essential	Core2Core, Service Monitor, User Permission, User Trust Management
20	Core System Interoperability	The Core System needs to provide services in such a way that if a mobile user moves into an area of another Core System their interface to the Core System still operates. This helps manage user expectations and helps ensure that when a mobile user subscribes to a service or installs an application the user experience is consistent across multiple Core Systems.	Essential	Core2Core, Data Distribution, Misbehavior Management, Network Services, Service Monitor, Time Synchronization, User Trust Management
21	Core System Interdependence	The Core System needs to operate in coordination with other Core Systems. This ensures that Core services deliver information that is consistent with information delivered by other Core systems, which will help avoid inconsistencies and incompatibilities between Cores and between Mobile users interacting with multiple Cores.	Essential	Core2Core, Data Distribution, Misbehavior Management, Network Services, Time Synchronization, User Trust Management
22	Core System Data Protection	The Core System needs to protect data it maintains from unauthorized access. This ensures that information held by the Core, which may include sensitive information about System Users, is accessed only by authorized users.	Essential	Service Monitor, User Trust Management
23	Anonymity Preservation	The Core System needs to preserve the anonymity of anonymous System Users that use its services. This ensures that System Users communicating with the Core who wish to remain anonymous will not have their anonymity breached as a result of communicating with the Core.	Essential	User Trust Management
24	Private Network Connectivity	The Core System needs to connect to a private network. This allows the Core to provide services to any System User that provides a private network connection to the Core, which contributes to meeting the Deployability goal. It also allows Cores to establish dedicated connections between them, which contributes to the Cores collectively meeting goals of scalability, maintainability and reliability.	Essential	Network Services

ID	Core System Need	Description / Rationale	Priority	Subsystem (s)
25	Private Network Routing	The Core System needs to route communications between other Cores and System Users, when one or both of the parties involved in the communication is connected to the Core by a private network. This enables System Users connected by private network to interact with Center-based applications, and also facilitates backup operations between Cores.	Essential	Network Services

5.2 State and Modes

The states and modes of operation of the Core System are described in this section. This description is consistent with the description included in the System Architecture Document, Functional View – Top Level. Other subsystem states may be defined as needed in later phases of development. Depending on local policies and procedures, a particular Core System may deviate from these states. For example, a training state may not be supported at all.

Subsystems may be in one of four states, as illustrated in Figure 5-1:

- Installation
- Operational
- Standby
- Training

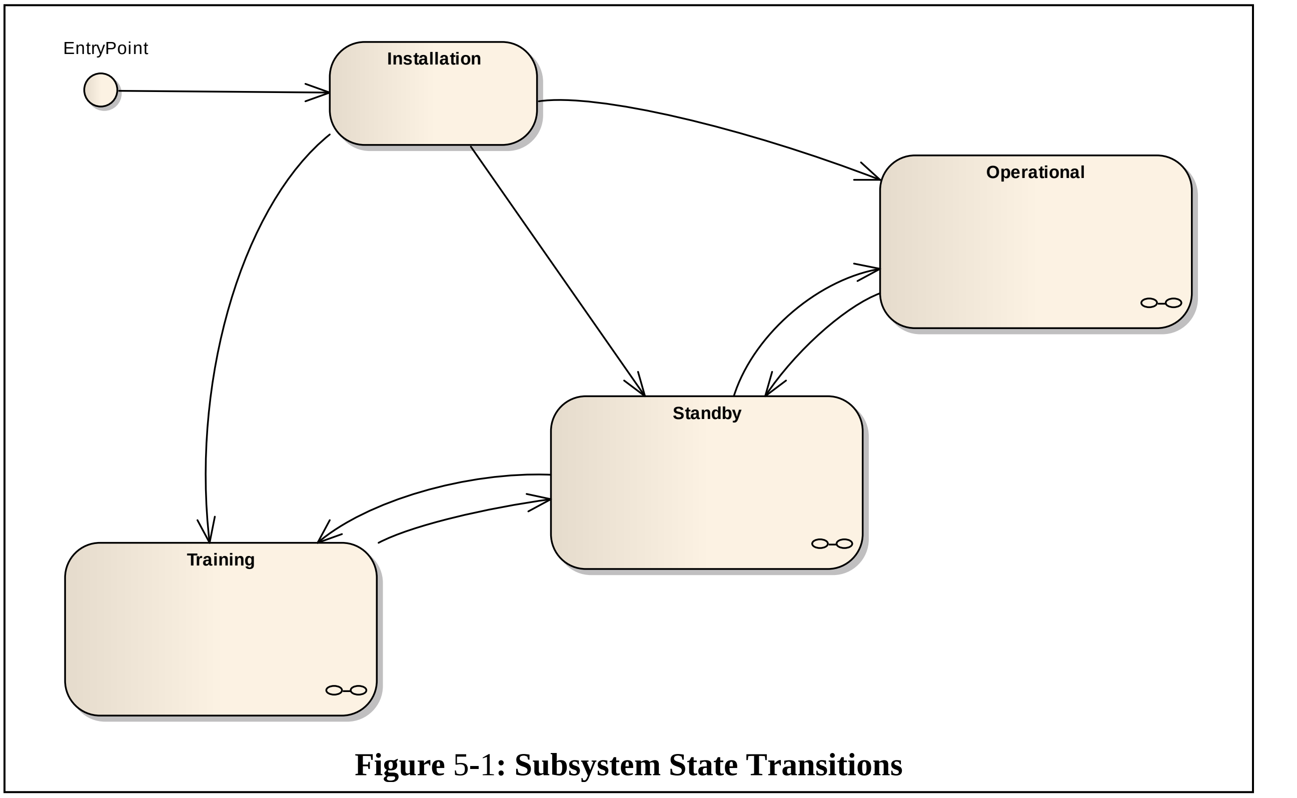


Figure 5-1**: Subsystem State Transitions**

A description of each of the states follows.

- Installation: This state includes all pre-operational activities necessary to plan, develop, install and verify the procedures and system configurations used to support the Core System.
- Operational: This state includes all activities during the normal conduct of operations.

- Standby: The Core System or subsystem operating in a Standby state will be providing backup to one or more other Cores or other Core subsystems. From the standby state the Core or subsystem may take over the functions of another Core or subsystem if required.
- Training: The Core System will be placed in a Training state when it is used for imparting training on the Core features. Certain features like real-time display of log messages and debug messages may be enabled in the Training state which may not otherwise be accessible under normal conditions.

While within the Standby and Operational states, each subsystem may be in one of five modes, as illustrated in Figure 5-2:

Normal mode: In the normal mode, there is little or no functional or performance impacts on the ability of the subsystem to provide its services.

Degraded mode: In the degraded mode, the subsystem is impaired to a significant extent: its ability to provide services is greatly reduced or eliminated completely. Also, Service Monitor's ability to manage the subsystem may be impaired.

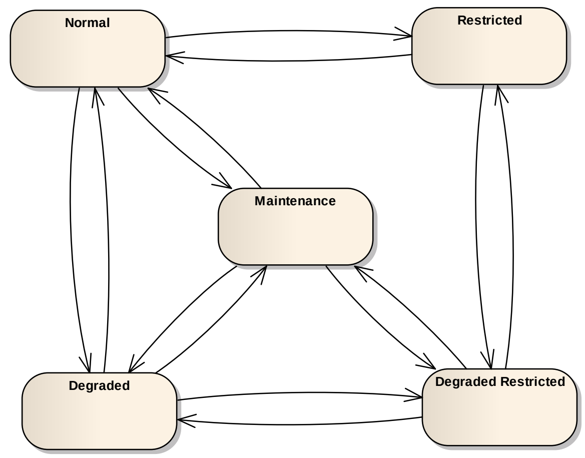


Figure 5-2: Standby and Operational Modes

Restricted mode: In the restricted mode, the subsystem is capable of performing as expected; however certain services or features are disabled to support a specific event such as an evacuation. The restriction is determined by operators/entities outside of the system and subsequently implemented by the system in response to an authorized operation (command) from the external entity. This may also be implemented via a policy-based management system whereby policies (as specified by an authorized external entity) are automatically implemented by the Core System in response to detection of events, behaviors or performance thresholds. In a restricted mode, the Core System could curtail the use of particular subsystems to privileged users, such first responders and other emergency personnel.

Degraded/Restricted Mode: If during the course of operating in a restricted mode there is a loss of functionality, or if while in degraded mode there is a need to enter restricted mode, the subsystem may enter the degraded/restricted mode. This mode is a combination of the restricted and degraded modes, where subsystem services are offered only to particular users, but performance is degraded.

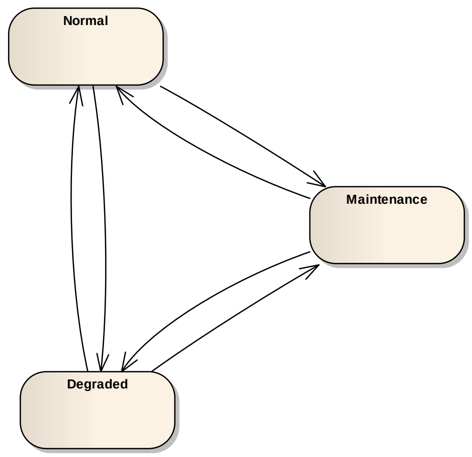


Figure 5-3: Training Modes

Maintenance Mode: Core Personnel may place a subsystem in maintenance mode to replace an impaired component or upgrade a component. Depending on the nature of maintenance planned, the impact on the subsystem's ability to provide services may be impacted. Also, its ability to manage itself and provide visibility into how it is performing may be impacted.

While in the Training state, each subsystem may be in one of three modes, as illustrated in Figure 5-3. Definitions of these modes are the same as those defined above under Standby and Operational.

5.3 Internet Based Communications Standards

The section contains a listing of Internet Engineering Task Force (IETF) Request for Comments (RFCs). These standards define how internet communications systems are implemented. The Core System implementations will need to be aware of the developments in this industry to ensure interoperable communications with external systems.

These tables provide the document number, title, date of the current publication, its development status and an indication of whether filing disclosures about Intellectual Property Rights (IPR).

Table 5-2. Network Time Protocol (NTP) Standards

Document	Title	Date	Status
RFC 5905 (draft-ietf-ntp-ntpv4-proto)	Network Time Protocol Version 4: Protocol and Algorithms Specification	2010-06	RFC 5905 (Proposed Standard) Errata
RFC 5906 (draft-ietf-ntp-autokey)	Network Time Protocol Version 4: Autokey Specification	2010-06	RFC 5906 (Informational)
RFC 5907 (draft-ietf-ntp-ntpv4-mib)	Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)	2010-06	RFC 5907 (Proposed Standard) Errata
RFC 5908 (draft-ietf-ntp-dhcpv6-ntp-opt)	Network Time Protocol (NTP) Server Option for DHCPv6	2010-06	RFC 5908 (Proposed Standard)

Source: http://datatracker.ietf.org/wg/ntp/

Table 5-3. PKI X.509 Standards

Document	Title	Date	Status	Ipr
Active Internet-Drafts				
draft-ietf-pkix-certimage-11	Internet X.509 Public Key Infrastructure - Certificate Image	2011-02-15	RFC Ed Queue (for 55 days) RFC Editor State: RFC-EDITOR	
draft-ietf-pkix-eai-addresses-00	Internationalized Email Addresses in X.509 certificates	2011-03-07	I-D Exists	

Document	Title	Date	Status	Ipr
draft-ietf-pkix-ocspagility-10	Online Certificate Status Protocol Algorithm Agility	2011-03-11	RFC Ed Queue (for 27 days) RFC Editor State: EDIT	
draft-ietf-pkix-pubkey-caps-02	S/MIME Capabilities for Public Key Definitions	2011-04-06 new	I-D Exists	
draft-ietf-pkix-rfc2560bis-03	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	2011-04-05 new	I-D Exists	
draft-ietf-pkix-rfc5272-bis-03	Certificate Management over CMS (CMC) Updates	2011-04-06 new	I-D Exists	
draft-ietf-pkix-rfc5280-clarifications-02	Clarifications to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2011-03-28	I-D Exists	
RFC 2459 (draft-ietf-pkix-ipki-part1)	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	1999-01	RFC 2459 (Proposed Standard) Obsoleted by RFC 3280 Errata	
RFC 2510 (draft-ietf-pkix-ipki3cmp)	Internet X.509 Public Key Infrastructure Certificate Management Protocols	1999-03	RFC 2510 (Proposed Standard) Obsoleted by RFC 4210	
RFC 2511 (draft-ietf-pkix-crmf)	Internet X.509 Certificate Request Message Format	1999-03	RFC 2511 (Proposed Standard) Obsoleted by RFC 4211	
RFC 2527 (draft-ietf-pkix-ipki-part4)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	1999-03	RFC 2527 (Informational) Obsoleted by RFC 3647 Errata	
RFC 2528 (draft-ietf-pkix-ipki-kea)	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	1999-03	RFC 2528 (Informational)	
RFC 2559 (draft-ietf-pkix-ipki2opp)	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	1999-04	RFC 2559 (Historic) Obsoleted by RFC 3494	

Document	Title	Date	Status	Ipr
RFC 2560 (draft-ietf-pkix-ocsp)	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	1999-06	RFC 2560 (Proposed Standard) Errata	
RFC 2585 (draft-ietf-pkix-opp-ftp-http)	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	1999-05	RFC 2585 (Proposed Standard) Errata	
RFC 2587 (draft-ietf-pkix-ldapv2-schema)	Internet X.509 Public Key Infrastructure LDAPv2 Schema	1999-06	RFC 2587 (Proposed Standard) Obsoleted by RFC 4523	
RFC 2797 (draft-ietf-pkix-cmc)	Certificate Management Messages over CMS	2000-04	RFC 2797 (Proposed Standard) Obsoleted by RFC 5272	
RFC 2875 (draft-ietf-pkix-dhpop)	Diffie-Hellman Proof-of-Possession Algorithms	2000-07	RFC 2875 (Proposed Standard)	
RFC 3029 (draft-ietf-pkix-dcs)	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	2001-02	RFC 3029 (Experimental)	
RFC 3039 (draft-ietf-pkix-qc)	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	2001-01	RFC 3039 (Proposed Standard) Obsoleted by RFC 3739	
RFC 3161 (draft-ietf-pkix-time-stamp)	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	2001-08	RFC 3161 (Proposed Standard) Updated by RFC 5816 Errata	
RFC 3279 (draft-ietf-pkix-ipki-pkalgs)	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2002-04	RFC 3279 (Proposed Standard) Updated by RFC 4055, RFC 4491, RFC 5480, RFC 5758 Errata	

Document	Title	Date	Status	Ipr
RFC 3280 (draft-ietf-pkix-new-part1)	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2002-04	RFC 3280 (Proposed Standard) Obsoleted by RFC 5280 Updated by RFC 4325, RFC 4630 Errata	1
RFC 3281 (draft-ietf-pkix-ac509prof)	An Internet Attribute Certificate Profile for Authorization	2002-04	RFC 3281 (Proposed Standard) Obsoleted by RFC 5755 Errata	
RFC 3379 (draft-ietf-pkix-dpv-dpd-req)	Delegated Path Validation and Delegated Path Discovery Protocol Requirements	2002-09	RFC 3379 (Informational)	
RFC 3628 (draft-ietf-pkix-pr-tsa)	Policy Requirements for Time-Stamping Authorities (TSAs)	2003-11	RFC 3628 (Informational)	
RFC 3647 (draft-ietf-pkix-ipki-new-rfc2527)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	2003-11	RFC 3647 (Informational) Errata	
RFC 3709 (draft-ietf-pkix-logotypes)	Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates	2004-02	RFC 3709 (Proposed Standard) Errata	
RFC 3739 (draft-ietf-pkix-sonof3039)	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	2004-03	RFC 3739 (Proposed Standard)	
RFC 3770 (draft-ietf-pkix-wlan-extns)	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	2004-05	RFC 3770 (Proposed Standard) Obsoleted by RFC 4334 Errata	
RFC 3779 (draft-ietf-pkix-x509-ipaddr-as-extn)	X.509 Extensions for IP Addresses and AS Identifiers	2004-06	RFC 3779 (Proposed Standard) Errata	
RFC 3820 (draft-ietf-pkix-proxy)	Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	2004-06	RFC 3820 (Proposed Standard)	
RFC 3874 (draft-ietf-pkix-sha224)	A 224-bit One-way Hash Function: SHA-224	2004-09	RFC 3874 (Informational)	

Document	Title	Date	Status	Ipr
RFC 4043 (draft-ietf-pkix-pi)	Internet X.509 Public Key Infrastructure Permanent Identifier	2005-05	RFC 4043 (Proposed Standard) Errata	
RFC 4055 (draft-ietf-pkix-rsa-pkalgs)	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2005-06	RFC 4055 (Proposed Standard) Updated by RFC 5756 Errata	
RFC 4059 (draft-ietf-pkix-warranty-extn)	Internet X.509 Public Key Infrastructure Warranty Certificate Extension	2005-05	RFC 4059 (Informational)	
RFC 4158 (draft-ietf-pkix-certpathbuild)	Internet X.509 Public Key Infrastructure: Certification Path Building	2005-09	RFC 4158 (Informational)	
RFC 4210 (draft-ietf-pkix-rfc2510bis)	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)	2005-09	RFC 4210 (Proposed Standard) Errata	
RFC 4211 (draft-ietf-pkix-rfc2511bis)	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	2005-09	RFC 4211 (Proposed Standard) Errata	
RFC 4325 (draft-ietf-pkix-crlaia)	Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension	2005-12	RFC 4325 (Proposed Standard) Obsoleted by RFC 5280	
RFC 4334 (draft-ietf-pkix-rfc3770bis)	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	2006-02	RFC 4334 (Proposed Standard) Errata	
RFC 4386 (draft-ietf-pkix-pkixrep)	Internet X.509 Public Key Infrastructure Repository Locator Service	2006-02	RFC 4386 (Experimental)	
RFC 4387 (draft-ietf-pkix-certstore-http)	Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP	2006-02	RFC 4387 (Proposed Standard)	
RFC 4476 (draft-ietf-pkix-acpolicies-extn)	Attribute Certificate (AC) Policies Extension	2006-05	RFC 4476 (Proposed Standard)	

Document	Title	Date	Status	Ipr
RFC 4491 (draft-ietf-pkix-gost-cppk)	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile	2006-05	RFC 4491 (Proposed Standard) Errata	
RFC 4630 (draft-ietf-pkix-cert-utf8)	Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2006-08	RFC 4630 (Proposed Standard) Obsoleted by RFC 5280	
RFC 4683 (draft-ietf-pkix-sim)	Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)	2006-10	RFC 4683 (Proposed Standard) Errata	
RFC 4985 (draft-ietf-pkix-srvsan)	Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name	2007-08	RFC 4985 (Proposed Standard) Errata	
RFC 5019 (draft-ietf-pkix-lightweight-ocsp-profile)	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments	2007-09	RFC 5019 (Proposed Standard)	
RFC 5055 (draft-ietf-pkix-scvp)	Server-Based Certificate Validation Protocol (SCVP)	2007-12	RFC 5055 (Proposed Standard)	2
RFC 5272 (draft-ietf-pkix-2797-bis)	Certificate Management over CMS (CMC)	2008-06	RFC 5272 (Proposed Standard) Errata	
RFC 5273 (draft-ietf-pkix-cmc-trans)	Certificate Management over CMS (CMC): Transport Protocols	2008-06	RFC 5273 (Proposed Standard)	
RFC 5274 (draft-ietf-pkix-cmc-compl)	Certificate Management Messages over CMS (CMC): Compliance Requirements	2008-06	RFC 5274 (Proposed Standard)	
RFC 5280 (draft-ietf-pkix-rfc3280bis)	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2008-05	RFC 5280 (Proposed Standard) Errata	
RFC 5480 (draft-ietf-pkix-ecc-subpubkeyinfo)	Elliptic Curve Cryptography Subject Public Key Information	2009-03	RFC 5480 (Proposed Standard) Errata	
RFC 5636 (draft-ietf-pkix-tac)	Traceable Anonymous Certificate	2009-08	RFC 5636 (Experimental)	
RFC 5697 (draft-ietf-pkix-other-certs)	Other Certificates Extension	2009-11	RFC 5697 (Experimental)	

Document	Title	Date	Status	Ipr
RFC 5755 (draft-ietf-pkix-3281update)	An Internet Attribute Certificate Profile for Authorization	2010-01	RFC 5755 (Proposed Standard)	
RFC 5756 (draft-ietf-pkix-rfc4055-update)	Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters	2010-01	RFC 5756 (Proposed Standard) Errata	
RFC 5758 (draft-ietf-pkix-sha2-dsa-ecdsa)	Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA	2010-01	RFC 5758 (Proposed Standard) Errata	
RFC 5816 (draft-ietf-pkix-rfc3161-update)	ESSCertIDv2 Update for RFC 3161	2010-04	RFC 5816 (Proposed Standard)	
RFC 5877 (draft-ietf-pkix-attr-cert-mime-type)	The application/pkix-attr-cert Media Type for Attribute Certificates	2010-05	RFC 5877 (Informational) Errata	
RFC 5912 (draft-ietf-pkix-new-asn1)	New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)	2010-06	RFC 5912 (Informational) Errata	
RFC 5913 (draft-ietf-pkix-authorityclearanceconstraints)	Clearance Attribute and Authority Clearance Constraints Certificate Extension	2010-06	RFC 5913 (Proposed Standard)	
RFC 5914 (draft-ietf-pkix-ta-format)	Trust Anchor Format	2010-06	RFC 5914 (Proposed Standard) Errata	
RFC 5934 (draft-ietf-pkix-tamp)	Trust Anchor Management Protocol (TAMP)	2010-08	RFC 5934 (Proposed Standard) Errata	
RFC 6024 (draft-ietf-pkix-ta-mgmt-reqs)	Trust Anchor Management Requirements	2010-10	RFC 6024 (Informational)	
RFC 6025 (draft-ietf-pkix-asn1-translation)	ASN.1 Translation	2010-10	RFC 6025 (Informational)	
Active Internet-Drafts				
draft-chen-pkix-securityinfo-00	X.509 Extension with Security Information	2010-10-15 expires soon	I-D Exists	
draft-moreau-pkix-aixcm-00	Auto Issued X.509 Certificate Mechanism (AIXCM)	2008-08-06	I-D Exists RFC Editor State: ISR-AUTH	
draft-patterson-pkix-attribute-signing-eku-00	attributeSigning extendedKeyUsage value	2011-03-28	I-D Exists	

Source: http://datatracker.ietf.org/wg/pkix/

IPR Note 1:

draft-ietf-pkix-new-part1, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile":

2001-05-30	ID # 38	"IBM's patent statement pertaining to PKIX, specifically certificateHold for Non-Repudiation"

IPR note 2:

draft-ietf-pkix-scvp, "Server-based Certificate Validation Protocol (SCVP)":

2005-03-25	ID # 563	"CoreStreet, Ltd.'s statement about IPR claimed in draft-ietf-pkix-scvp-18"
2005-06-16	ID # 589	"CoreStreet, Ltd. Statement about IPR claimed in IETF's draft Simple Certificate Validation Protocol - draft-ietf-pkix-scvp-18"

5.4 Action Verbs

The following table lists the action verbs used in the requirements along with a definition.

Table 5-4. Requirements Action Verb Definitions

Verb	Definition
accept	to obtain valid data into the service/system sent from a valid source and sending an acknowledgement response message to the originator
aggregate	To combine data elements of similar format into a single data element that is a statistical representation of the original elements.
conform	refers to the alignment of the system to an external standard - interface, workmanship, operating, etc.
communicate	the activity of exchanging information, data or messages to a recipient
connect	to link to another entity by means of a communication circuit
determine	to find out or calculate
display	to present information to a system operator, typically through a graphical user interface or command line prompt
drift	to vary or deviate from a set standard reference
enable	to make other actions possible by supplying prerequisite information or resources required for the task or activity to take place
establish	to begin or create something that will follow a prescribed set of rules governing the behavior such as an interface between entities.

Verb	Definition
ensure	to make safe, certain; or to guarantee an outcome or condition.
exceed	to go over a prescribed threshold or parameter
exclude	to keep out from a group; to omit
identify	to extract information from a message or an activity/process that matches certain criteria
include	to create a message or report that contains certain elements that could be from multiple sources; or to have or regard or treat as part of a whole
install	to set up for use or service
maintain	to keep or retain possession of; to preserve or hold intact or within a certain set of parameters
manage	to work upon or try to alter for a purpose - involving collecting information and acting on it based on predefined sets of thresholds or criteria
operate	describes the conditions in which the Core System is performing its services and functions
prioritize	to evaluate a group of tasks and ranking them in their order of importance or urgency
protect	to carry out certain procedures and setup predefined safeguards in order to maintain the status or integrity of an entity
process	a series of actions, changes, or functions bringing about a result
provide	to make available, present, or furnish information or data (e.g., certificates, service coverage area, list of services) to a recipient
receive	to obtain valid data into the service/system sent from a valid source, but sending no acknowledgement response to the originator
Record	to add information into a set of data (database, log, files) to be organized with other data
report	to create an output either to a System User or a System Operator that is organized to include one or more data elements that could be combined from multiple sources and may be arranged in a prescribed format
request	to send a message to another entity to cause that other entity to reply with data that is called out in the 'request' message
route	the process of determining the communication link path for moving a packet of data from a source to a destination
send	to dispatch, by a means of communication, data from one entity to another without the expectation of receiving an acknowledgement response from that entity

Verb	Definition
sign	to apply a digital certificate, or electronic "identification card" that establishes the credentials of the sender of an electronic message
store	to place or leave in a location (e.g., computer memory, disk, database) for preservation or later use or disposal
support	to implement an interface or service in agreement with or in accordance with an external standard definition or established protocol
synchronize	to occur or operate at the same time or rate
transition	to change from one state or mode to another
transmit	to dispatch, by a means of communication, data from one entity to another with the expectation of receiving an acknowledgement response from that entity
update	to modify or change the existing data or information to new data or information
use	to apply or utilize, such as data in a message
validate	to authenticate, sanction or provide authoritative approval
vary	to change in value, either up or down (positively or negatively)
verify	to confirm or substantiate the truth, accuracy, or reality of something - credentials, identity, configuration

5.5 Internal Interfaces

The following table shows the internal interfaces between subsystems within the Core System. The column on the left represents the subsystems that will be sending data to the subsystems represented by the columns to the right.

Table 5-5. Internal Subsystem to Subsystem Interfaces

	Receiving Subsystems							
Sending Subsystems	CC	DD	MM	NS	SM	TS	UP	UTM
Core2Core (CC)		y	y	y	y		y	y
Data Distribution (DD)	y		y	y	y		y	y
Misbehavior Management (MM)	y				y		y	y
Network Services (NS)	y	y	y		y		y	y
Service Monitor (SM)	y	y	y	y		y	y	y
Time Synchronization (TS)	y	y	y	y	y		y	y
User Permissions (UP)	y	y	y	y	y			y
User Trust Management (UTM)	y	y	y	y	y		y	

5.6 DSRC Security Credential Requirements

The following table contains a listing of requirements from earlier versions of this SyRS that dealt with the creation, distribution, and management of security credentials supporting DSRC, i.e. those based on IEEE Standard 1609.2. The implication would have been that one of the Core System services would have been to play the role of a Certificate Authority (CA) to generate the digital certificates required for mobile users and field users to communicate using 5.9 GHz DSRC. While the Core System no longer supports this aspect of trust management they are provided here as reference and as a companion to the discussion in the Core System SAD that deals with the unselected alternative architecture views related to DSRC security.

The requirements were written at both the System and Subsystem level. The subsystems were affected were Core2Core and User Trust Management.

Table 5-6. DSRC Security Related Requirements

Requirement ID	DSRC Security Related Requirements
3.1.1	*Core System Functional Requirements*
3.1.1.41	The Core System shall manage IEEE 1609.2 Certificate Authority functions for System Users.
3.1.1.44	The Core System shall provide an interface to an authorized System Operator to manage IEEE 1609.2 Certificate Authority functions.
3.1.1.45	The Core System shall provide an interface to an authorized System Operator to manage Certificate Authority (CA) locations.
3.1.1.46	The Core System shall manage 1609.2 Certificates to System Users.
3.1.1.47	When misbehaved system users have been identified, a Core System shall add an entry for that System User to the IEEE 1609.2 Certificate Revocation List (CRL).
3.1.2	*Core System Performance Requirements*
3.1.2.15	The Core System shall process up to [TBD] 1609.2 Certificate Requests per second from System Users.
3.1.2.17	The Core System shall generate 1609.2 Certificate Revocation Lists (CRL) periodically at [TBD] rate.
3.1.3	*Core System Interface Requirements*
3.1.3.8	A Core System shall support a communication interface over which a Core System can provide System Users with IEEE 1609.2 Certificates.
3.1.7	*Constraints*
3.1.7.2	The IEEE 1609.x family of standards (including 1609.1, 1609.2, 1609.3 and 1609.4) shall serve as the interface standards for 5.9GHz DSRC.
3.2.1	*Core2Core Subsystem Functional Requirements*
3.2.1.1.1.13	The Core2Core Subsystem shall send the complete IEEE 1609.2 certificate revocation list (CRL) to other Core Systems.
3.2.1.1.1.14	The Core2Core Subsystem shall send delta updates of current IEEE 1609.2 certificate revocation list (CRL) to other Core Systems.
3.2.8.1	*User Trust Management Subsystem Functional Requirements*
3.2.8.1.2	*IEEE 1609.2 Certificate Authority Functions*
3.2.8.1.2.1	The User Trust Management Subsystem shall accept certificate request messages for IEEE 1609.2 Anonymous certificates from the System Users.
3.2.8.1.2.2	The User Trust Management Subsystem shall receive certificate request messages for IEEE 1609.2 Anonymous Certificates from System Users.
3.2.8.1.2.3	The User Trust Management Subsystem shall support issuance of IEEE 1609.2 Anonymous certificates to System Users as defined in IEEE 1609.2 specification.
3.2.8.1.2.4	The User Trust Management Subsystem shall support issuance of IEEE 1609.2 Identity certificates to System Users as defined in IEEE 1609.2 specification.

Requirement ID	DSRC Security Related Requirements
3.2.8.1.2.5	The User Trust Management Subsystem shall support IEEE 1609.2 Certificate Authority functions to System Users as defined in IEEE 1609.2 specification.
3.2.8.1.2.6	The User Trust Management Subsystem shall accept certificate request messages from Core System subsystems for IEEE 1609.2 Identify Certificates.
3.2.8.1.2.7	If the Certificate Request validation is successful, the User Trust Management Subsystem shall respond with a IEEE 1609.2 certificate response message including a signed IEEE 1609.2 Identity Certificate to the requesting entity.
3.2.8.1.2.8	If the Certificate Request validation fails, the User Trust Management Subsystem shall respond with a IEEE 1609.2 certificate response message with a failure status to the requesting entity.
3.2.8.1.2.9	The User Trust Management Subsystem shall create System User IEEE 1609.2 Identity Certificates based on command from the Operator.
3.2.8.1.2.10	The User Trust Management Subsystem shall create System User IEEE 1609.2 Identity Certificates based on input from the User Permissions Subsystem.
3.2.8.1.2.11	The User Trust Management Subsystem shall create System User IEEE 1609.2 Anonymous Certificates based on command from the Operator.
3.2.8.1.2.12	The User Trust Management Subsystem shall create IEEE 1609.2 Anonymous Certificates based on input from the User Permissions Subsystem.
3.2.8.1.2.13	The User Trust Management Subsystem shall send System User IEEE 1609.2 Identity Certificates to the System User.
3.2.8.1.2.14	The User Trust Management Subsystem shall send System User IEEE 1609.2 Anonymous Certificates to the System User.
3.2.8.1.2.15	The User Trust Management Subsystem shall accept requests for IEEE 1609.2 Identify Certificates from System Users.
3.2.8.1.2.16	The User Trust Management Subsystem shall accept requests for IEEE 1609.2 Anonymous Certificates from System Users.
3.2.8.1.2.17	If the user validation is successful, the User Trust Management Subsystem shall provide a IEEE 1609.2 Anonymous certificate response message including a set of signed IEEE 1609.2 Anonymous certificates to the System User.
3.2.8.1.2.18	If the user validation fails, the User Trust Management Subsystem shall respond with a IEEE 1609.2 Anonymous certificate response message with a failure status to the System User.
3.2.8.1.2.19	The User Trust Management Subsystem shall accept certificate request messages for IEEE 1609.2 Identity certificates from the System Users.

Requirement ID	DSRC Security Related Requirements
3.2.8.1.2.20	If the user validation is successful, the User Trust Management Subsystem shall respond with a IEEE 1609.2 Identity certificate response message including a set of signed 1609.2 Identity certificates to the System User.
3.2.8.1.2.21	if the user validation fails, the User Trust Management Subsystem shall respond with a IEEE 1609.2 Identity certificate response message with a failure status to the System User.
3.2.8.1.2.22	The User Trust Management Subsystem shall accept IEEE 1609.2 root certificates retrieval requests from System Users.
3.2.8.1.3	*IEEE 1609.2 Certificate Revocation List (CRL) Processing*
3.2.8.1.3.1	The User Trust Management Subsystem shall generate a Certificate Revocation List (CRL) containing a list of revoked certificates as defined in IEEE Standard IEEE 1609.2.
3.2.8.1.3.2	The User Trust Management Subsystem shall accept IEEE 1609.2 certificate revocation list (CRL) complete retrieval requests from System Users.
3.2.8.1.3.3	The User Trust Management Subsystem shall accept IEEE 1609.2 certificate revocation list (CRL) delta update retrieval requests from System Users.
3.2.8.1.3.4	The User Permissions Subsystem shall send the complete IEEE 1609.2 certificate revocation list (CRL) to System Users.
3.2.8.1.3.5	The User Permissions Subsystem shall send delta updates of current IEEE 1609.2 certificate revocation list (CRL) to System Users.
3.2.8.1.3.6	The User Permissions Subsystem shall send the complete IEEE 1609.2 Certificate Revocation List (CRL) to other Core Systems.
3.2.8.1.3.7	The User Permissions Subsystem shall send delta updates of current IEEE 1609.2 Certificate Revocation List (CRL) to other Core Systems.
3.2.8.1.3.8	The User Permissions Subsystem shall accept the complete IEEE 1609.2 Certificate Revocation List (CRL) from other Core Systems.
3.2.8.1.3.9	The User Permissions Subsystem shall accept delta updates of IEEE 1609.2 Certificate Revocation List (CRL) from other Core Systems.
3.2.8.2	*User Trust Management Subsystem Performance Requirements*
3.2.8.2.1	The User Trust Management Subsystem shall process up to [TBD] IEEE 1609.2 Certificate Requests per second from System Users.
3.2.8.2.3	The User Trust Management Subsystem shall generate IEEE 1609.2 Certificate Revocation Lists (CRL) periodically at [TBD] rate.
3.2.8.3	*User Trust Management Subsystem Interface Requirements*
3.2.8.3.1.1	The User Trust Management Subsystem shall support an interface for IEEE 1609.2 Certificate Authority functions for System Users.
3.2.8.3.1.7	The User Trust Management shall enable a System Operator to revoke a System User's IEEE 1609.2 certificate which would subsequently be listed in the next generated IEEE 1609.2 Certificate Revocation List.

Requirement ID	DSRC Security Related Requirements
3.2.8.4	*User Trust Management Subsystem Data Requirements*
3.2.8.4.1	The User Trust Management Subsystem shall provide secure storage for [TBD] IEEE 1609.2 Anonymous Certificates.
3.2.8.4.2	The User Trust Management Subsystem shall provide secure storage for [TBD] IEEE 1609.2 Identity Certificates.
3.2.8.4.4	The User Trust Management Subsystem shall provide secure storage for [TBD] IEEE 1609.2 Certificate Revocation Lists (CRL).
3.2.8.4.10	The User Trust Management Subsystem shall provide secure storage for IEEE 1609.2 CA private keys.
3.2.8.4.11	The User Trust Management Subsystem shall provide secure storage for IEEE 1609.2 root.

6 Traceability Matrices

This section contains tables that trace the requirements in this document to and from Needs that drive the definition of the system as well as the Architecture definition.

6.1 Needs to Requirements Traceability

In this section the requirements of this document are traced to/from the Needs identified in the Core System Concept of Operations (ConOps) and listed in Table 5-1 of this document.

6.1.1 Core System Needs to System Requirements Matrix

Table 6-1 below shows the Core System Needs from the ConOps followed by one or more System Requirement (SR) Identifiers (IDs) that support that Need.

Table 6-1. Core System Needs to System Requirements Traceability Matrix

	Core System Need	SR ID
1	Data Protection	3.1.1.8.9
1	Data Protection	3.1.1.8.10
1	Data Protection	3.1.1.8.14
2	Core Trust	3.1.1.8.5
2	Core Trust	3.1.1.8.6
2	Core Trust	3.1.1.8.7
2	Core Trust	3.1.1.8.8
3	System User Trust	3.1.1.8.1
3	System User Trust	3.1.1.8.2
3	System User Trust	3.1.1.8.3
3	System User Trust	3.1.1.8.4
4	Core Trust Revocation	3.1.1.8.11
4	Core Trust Revocation	3.1.1.8.12
4	Core Trust Revocation	3.1.1.8.13
5	System User Trust Revocation	3.1.1.8.11
5	System User Trust Revocation	3.1.1.8.12
5	System User Trust Revocation	3.1.1.8.13
6	Authorization Management	3.1.1.7.1
6	Authorization Management	3.1.1.7.2
6	Authorization Management	3.1.1.7.3
6	Authorization Management	3.1.1.7.4
6	Authorization Management	3.1.1.7.5
7	Authorization Verification	3.1.1.7.6
8	Misbehavior Identification	3.1.1.3.1
8	Misbehavior Identification	3.1.1.3.2
8	Misbehavior Identification	3.1.1.3.3
8	Misbehavior Identification	3.1.1.3.4

	Core System Need	SR ID
8	Misbehavior Identification	3.1.1.3.5
9	Time Base	3.1.1.6.1
9	Time Base	3.1.3.3
10	Data Request	3.1.1.2.1
10	Data Request	3.1.1.2.2
10	Data Request	3.1.1.2.3
10	Data Request	3.1.3.2
11	Data Provision	3.1.1.2.4
11	Data Provision	3.1.1.2.5
11	Data Provision	3.1.1.2.6
11	Data Provision	3.1.3.2
12	Data Forward	3.1.1.2.11
12	Data Forward	3.1.1.4.1
12	Data Forward	3.1.1.4.2
12	Data Forward	3.1.3.2
13	Network Connectivity	3.1.3.5
14	Geographic Broadcast	3.1.1.2.7
14	Geographic Broadcast	3.1.1.2.8
14	Geographic Broadcast	3.1.1.2.9
14	Geographic Broadcast	3.1.1.2.10
15	Core System Service Status	3.1.1.5.1
15	Core System Service Status	3.1.1.5.5
15	Core System Service Status	3.1.1.5.6
15	Core System Service Status	3.1.1.5.7
15	Core System Service Status	3.1.1.5.8
15	Core System Service Status	3.1.1.5.9
15	Core System Service Status	3.1.1.5.10
15	Core System Service Status	3.1.1.5.11
15	Core System Service Status	3.1.1.5.12
15	Core System Service Status	3.1.1.5.13
16	System Integrity Protection	3.1.1.4.5
16	System Integrity Protection	3.1.1.4.6
17	System Availability	3.1.2.1
17	System Availability	3.1.4.2.1
17	System Availability	3.1.4.2.2
17	System Availability	3.1.4.2.3
17	System Availability	3.1.4.2.4
17	System Availability	3.1.4.2.5
17	System Availability	3.1.4.3.1
17	System Availability	3.1.4.3.2
17	System Availability	3.1.4.4.1
17	System Availability	3.1.4.4.2

	Core System Need	SR ID
18	System Operational Performance Monitoring	3.1.1.4.7
18	System Operational Performance Monitoring	3.1.1.5.4
18	System Operational Performance Monitoring	3.1.3.7
19	Core System Independence	3.1.1.5.2
19	Core System Independence	3.1.1.5.3
20	Core System Interoperability	3.1.1.4.3
20	Core System Interoperability	3.1.1.5.7
20	Core System Interoperability	3.1.1.5.8
20	Core System Interoperability	3.1.1.5.9
20	Core System Interoperability	3.1.1.5.9
20	Core System Interoperability	3.1.1.5.10
20	Core System Interoperability	3.1.1.5.10
20	Core System Interoperability	3.1.3.1
21	Core System Interdependence	3.1.1.1.1
21	Core System Interdependence	3.1.1.1.2
21	Core System Interdependence	3.1.1.1.3
21	Core System Interdependence	3.1.1.1.4
21	Core System Interdependence	3.1.1.1.5
21	Core System Interdependence	3.1.1.1.6
21	Core System Interdependence	3.1.1.1.7
21	Core System Interdependence	3.1.1.1.8
21	Core System Interdependence	3.1.1.1.9
21	Core System Interdependence	3.1.1.1.10
21	Core System Interdependence	3.1.1.1.11
21	Core System Interdependence	3.1.1.1.12
21	Core System Interdependence	3.1.1.1.13
21	Core System Interdependence	3.1.1.1.14
21	Core System Interdependence	3.1.1.1.15
21	Core System Interdependence	3.1.1.1.16
21	Core System Interdependence	3.1.1.1.17
21	Core System Interdependence	3.1.1.1.18
21	Core System Interdependence	3.1.1.1.19
21	Core System Interdependence	3.1.1.1.20
21	Core System Interdependence	3.1.1.1.21
21	Core System Interdependence	3.1.1.1.22
21	Core System Interdependence	3.1.1.1.23
21	Core System Interdependence	3.1.1.1.24
21	Core System Interdependence	3.1.1.1.25
21	Core System Interdependence	3.1.1.1.26
21	Core System Interdependence	3.1.1.1.27
21	Core System Interdependence	3.1.1.1.28
21	Core System Interdependence	3.1.1.1.29

	Core System Need	SR ID
21	Core System Interdependence	3.1.1.1.30
21	Core System Interdependence	3.1.1.1.31
21	Core System Interdependence	3.1.1.1.32
21	Core System Interdependence	3.1.1.1.33
22	Core System Data Protection	3.1.1.8.9
22	Core System Data Protection	3.1.1.8.10
22	Core System Data Protection	3.1.3.4
22	Core System Data Protection	3.1.4.1.1
23	Anonymity Preservation	3.1.5.1
24	Private Network Connectivity	3.1.3.6
25	Private Network Routing	3.1.1.4.4

6.1.2 System Requirements to Core System Needs Matrix

Table 6-2 below shows the Core System Requirement Identifiers (SR IDs) from Section 3.1 of this SyRS followed by one or more Core System Needs from the ConOps that are addressed by that requirement.

Table 6-2. System Requirements to Core System Needs Traceability

SR ID		Core System Need
3.1.1.1.1	21	Core System Interdependence
3.1.1.1.2	21	Core System Interdependence
3.1.1.1.3	21	Core System Interdependence
3.1.1.1.4	21	Core System Interdependence
3.1.1.1.5	21	Core System Interdependence
3.1.1.1.6	21	Core System Interdependence
3.1.1.1.7	21	Core System Interdependence
3.1.1.1.8	21	Core System Interdependence
3.1.1.1.9	21	Core System Interdependence
3.1.1.1.10	21	Core System Interdependence
3.1.1.1.11	21	Core System Interdependence
3.1.1.1.12	21	Core System Interdependence
3.1.1.1.13	21	Core System Interdependence
3.1.1.1.14	21	Core System Interdependence
3.1.1.1.15	21	Core System Interdependence
3.1.1.1.16	21	Core System Interdependence
3.1.1.1.17	21	Core System Interdependence
3.1.1.1.18	21	Core System Interdependence
3.1.1.1.19	21	Core System Interdependence
3.1.1.1.20	21	Core System Interdependence
3.1.1.1.21	21	Core System Interdependence

SR ID		Core System Need
3.1.1.1.22	21	Core System Interdependence
3.1.1.1.23	21	Core System Interdependence
3.1.1.1.24	21	Core System Interdependence
3.1.1.1.25	21	Core System Interdependence
3.1.1.1.26	21	Core System Interdependence
3.1.1.1.27	21	Core System Interdependence
3.1.1.1.28	21	Core System Interdependence
3.1.1.1.29	21	Core System Interdependence
3.1.1.1.30	21	Core System Interdependence
3.1.1.1.31	21	Core System Interdependence
3.1.1.1.32	21	Core System Interdependence
3.1.1.1.33	21	Core System Interdependence
3.1.1.2.1	10	Data Request
3.1.1.2.2	10	Data Request
3.1.1.2.3	10	Data Request
3.1.1.2.4	11	Data Provision
3.1.1.2.5	11	Data Provision
3.1.1.2.6	11	Data Provision
3.1.1.2.7	14	Geographic Broadcast
3.1.1.2.8	14	Geographic Broadcast
3.1.1.2.9	14	Geographic Broadcast
3.1.1.2.10	14	Geographic Broadcast
3.1.1.2.11	12	Data Forward
3.1.1.3.1	8	Misbehavior Identification
3.1.1.3.2	8	Misbehavior Identification
3.1.1.3.3	8	Misbehavior Identification
3.1.1.3.4	8	Misbehavior Identification
3.1.1.3.5	8	Misbehavior Identification
3.1.1.4.1	12	Data Forward
3.1.1.4.2	12	Data Forward
3.1.1.4.3	20	Core System Interoperability
3.1.1.4.4	25	Private Network Routing
3.1.1.4.5	16	System Integrity Protection
3.1.1.4.6	16	System Integrity Protection
3.1.1.4.7	18	System Operational Performance Monitoring
3.1.1.5.1	15	Core System Service Status
3.1.1.5.2	19	Core System Independence
3.1.1.5.3	19	Core System Independence
3.1.1.5.4	18	System Operational Performance Monitoring
3.1.1.5.5	15	Core System Service Status
3.1.1.5.6	15	Core System Service Status
3.1.1.5.7	15	Core System Service Status

SR ID		Core System Need
3.1.1.5.7	20	Core System Interoperability
3.1.1.5.8	15	Core System Service Status
3.1.1.5.8	20	Core System Interoperability
3.1.1.5.9	15	Core System Service Status
3.1.1.5.9	20	Core System Interoperability
3.1.1.5.9	20	Core System Interoperability
3.1.1.5.10	15	Core System Service Status
3.1.1.5.10	20	Core System Interoperability
3.1.1.5.10	20	Core System Interoperability
3.1.1.5.11	15	Core System Service Status
3.1.1.5.12	15	Core System Service Status
3.1.1.5.13	15	Core System Service Status
3.1.1.6.1	9	Time Base
3.1.1.7.1	6	Authorization Management
3.1.1.7.2	6	Authorization Management
3.1.1.7.3	6	Authorization Management
3.1.1.7.4	6	Authorization Management
3.1.1.7.5	6	Authorization Management
3.1.1.7.6	7	Authorization Verification
3.1.1.8.1	3	System User Trust
3.1.1.8.2	3	System User Trust
3.1.1.8.3	3	System User Trust
3.1.1.8.4	3	System User Trust
3.1.1.8.5	2	Core Trust
3.1.1.8.6	2	Core Trust
3.1.1.8.7	2	Core Trust
3.1.1.8.8	2	Core Trust
3.1.1.8.9	1	Data Protection
3.1.1.8.9	22	Core System Data Protection
3.1.1.8.10	1	Data Protection
3.1.1.8.10	22	Core System Data Protection
3.1.1.8.11	4	Core Trust Revocation
3.1.1.8.11	5	System User Trust Revocation
3.1.1.8.12	4	Core Trust Revocation
3.1.1.8.12	5	System User Trust Revocation
3.1.1.8.13	4	Core Trust Revocation
3.1.1.8.13	5	System User Trust Revocation
3.1.1.8.14	1	Data Protection
3.1.2.1	17	System Availability
3.1.3.1	20	Core System Interoperability
3.1.3.2	10	Data Request
3.1.3.2	11	Data Provision

SR ID		Core System Need
3.1.3.2	12	Data Forward
3.1.3.3	9	Time Base
3.1.3.4	22	Core System Data Protection
3.1.3.5	13	Network Connectivity
3.1.3.6	24	Private Network Connectivity
3.1.4.1.1	22	Core System Data Protection
3.1.4.2.1	17	System Availability
3.1.4.2.2	17	System Availability
3.1.4.2.3	17	System Availability
3.1.4.2.4	17	System Availability
3.1.4.2.5	17	System Availability
3.1.4.3.1	17	System Availability
3.1.4.3.2	17	System Availability
3.1.4.4.1	17	System Availability
3.1.4.4.2	17	System Availability
3.1.5.1	23	Anonymity Preservation

6.1.3 System to Subsystem Matrix

Table 6-3 below shows the mapping of System Requirements (SR IDs) to the lower level Subsystem Requirements (SSR IDs).

Table 6-3. System Requirements (SR) to Subsystem Requirements (SSR) Traceability

SR ID	SSR ID
3.1.1.1.1	3.2.1.1.3
3.1.1.1.1	3.2.1.1.4
3.1.1.1.1	3.2.1.1.5
3.1.1.1.1	3.2.7.1.10
3.1.1.1.1	3.2.7.1.12
3.1.1.1.1	3.2.1.2.1
3.1.1.1.2	3.2.1.1.2
3.1.1.1.3	3.2.1.1.6
3.1.1.1.4	3.2.1.1.7
3.1.1.1.4	3.2.1.1.9
3.1.1.1.4	3.2.1.1.10
3.1.1.1.5	3.2.1.1.8
3.1.1.1.6	3.2.1.1.11
3.1.1.1.7	3.2.1.1.14
3.1.1.1.7	3.2.1.1.12
3.1.1.1.8	3.2.1.1.13
3.1.1.1.9	3.2.1.1.15
3.1.1.1.10	3.2.5.1.1.9
3.1.1.1.10	3.2.8.1.5.12
3.1.1.1.10	3.2.8.1.5.11
3.1.1.1.10	3.2.3.1.10
3.1.1.1.10	3.2.1.1.16
3.1.1.1.10	3.2.1.1.28
3.1.1.1.10	3.2.1.1.29
3.1.1.1.10	3.2.1.1.30
3.1.1.1.10	3.2.1.1.31
3.1.1.1.10	3.2.1.1.32
3.1.1.1.10	3.2.2.1.2.16
3.1.1.1.10	3.2.7.1.25
3.1.1.1.10	3.2.3.1.9
3.1.1.1.10	3.2.7.1.24
3.1.1.1.10	3.2.4.1.3
3.1.1.1.10	3.2.4.1.4
3.1.1.1.10	3.2.5.1.1.8
3.1.1.1.10	3.2.2.1.2.17
3.1.1.1.11	3.2.1.1.18
3.1.1.1.12	3.2.1.1.22
3.1.1.1.12	3.2.1.1.20
3.1.1.1.12	3.2.1.1.19
3.1.1.1.13	3.2.1.1.21
3.1.1.1.14	3.2.1.1.23
3.1.1.1.15	3.2.1.1.25
3.1.1.1.15	3.2.1.1.27
3.1.1.1.15	3.2.1.1.24
3.1.1.1.16	3.2.1.1.26
3.1.1.1.17	3.2.1.1.33
3.1.1.1.18	3.2.1.1.34
3.1.1.1.19	3.2.1.1.35
3.1.1.1.20	3.2.1.1.36
3.1.1.1.21	3.2.1.1.44
3.1.1.1.21	3.2.8.1.5.13
3.1.1.1.21	3.2.7.1.26
3.1.1.1.21	3.2.5.1.1.11
3.1.1.1.21	3.2.5.1.1.10
3.1.1.1.21	3.2.4.1.5
3.1.1.1.21	3.2.3.1.11
3.1.1.1.21	3.2.2.1.2.18
3.1.1.1.21	3.2.1.1.39
3.1.1.1.22	3.2.1.1.41
3.1.1.1.22	3.2.1.1.40
3.1.1.1.22	3.2.1.1.43
3.1.1.1.23	3.2.1.1.42
3.1.1.1.24	3.2.1.1.37
3.1.1.1.25	3.2.1.1.38
3.1.1.1.26	3.2.1.1.45
3.1.1.1.26	3.2.1.1.50
3.1.1.1.26	3.2.1.1.51
3.1.1.1.27	3.2.1.1.47
3.1.1.1.27	3.2.1.1.49
3.1.1.1.27	3.2.1.1.46
3.1.1.1.28	3.2.1.1.48
3.1.1.1.29	3.2.1.1.52
3.1.1.1.30	3.2.1.1.56
3.1.1.1.30	3.2.8.1.5.7
3.1.1.1.30	3.2.7.1.11
3.1.1.1.30	3.2.5.1.1.15
3.1.1.1.30	3.2.5.1.1.14
3.1.1.1.30	3.2.5.1.1.13
3.1.1.1.30	3.2.1.1.53
3.1.1.1.30	3.2.1.1.54
3.1.1.1.30	3.2.2.1.2.20
3.1.1.1.31	3.2.1.1.55
3.1.1.1.32	3.2.1.1.50
3.1.1.1.33	3.2.1.1.51
3.1.1.2.1	3.2.2.1.1.2
3.1.1.2.1	3.2.2.1.1.1
3.1.1.2.2	3.2.2.1.1.5
3.1.1.2.2	3.2.2.1.1.3
3.1.1.2.3	3.2.2.1.1.7
3.1.1.2.3	3.2.2.1.1.4
3.1.1.2.3	3.2.2.1.1.6
3.1.1.2.4	3.2.2.1.2.1
3.1.1.2.4	3.2.2.1.2.2
3.1.1.2.4	3.2.2.1.2.5
3.1.1.2.4	3.2.2.1.2.6
3.1.1.2.5	3.2.2.1.2.3
3.1.1.2.6	3.2.2.1.2.4
3.1.1.2.7	3.2.2.1.4.1
3.1.1.2.7	3.2.2.1.4.4
3.1.1.2.7	3.2.2.1.4.2
3.1.1.2.7	3.2.2.1.4.6
3.1.1.2.7	3.2.2.1.4.5
3.1.1.2.8	3.2.2.1.4.3
3.1.1.2.9	3.2.2.1.2.7
3.1.1.2.9	3.2.2.1.2.8
3.1.1.2.9	3.2.2.1.2.10
3.1.1.2.10	3.2.2.1.2.9
3.1.1.2.11	3.2.2.1.3.3

SR ID	SSR ID
3.1.1.2.11	3.2.2.1.3.2
3.1.1.2.11	3.2.2.1.3.1
3.1.1.2.11	3.2.2.1.2.13
3.1.1.3.1	3.2.3.1.4
3.1.1.3.1	3.2.3.1.2
3.1.1.3.1	3.2.3.1.1
3.1.1.3.2	3.2.3.1.3
3.1.1.3.3	3.2.8.1.5.5
3.1.1.3.3	3.2.3.1.21
3.1.1.3.3	3.2.8.1.5.8
3.1.1.3.3	3.2.7.1.31
3.1.1.3.3	3.2.7.1.30
3.1.1.3.3	3.2.7.1.29
3.1.1.3.3	3.2.7.1.20
3.1.1.3.3	3.2.7.1.19
3.1.1.3.3	3.2.7.1.18
3.1.1.3.3	3.2.7.1.17
3.1.1.3.3	3.2.3.1.23
3.1.1.3.3	3.2.3.1.22
3.1.1.3.3	3.2.2.1.2.23
3.1.1.3.3	3.2.3.1.19
3.1.1.3.3	3.2.3.1.17
3.1.1.3.3	3.2.3.1.16
3.1.1.3.3	3.2.3.1.15
3.1.1.3.3	3.2.3.1.14
3.1.1.3.3	3.2.3.1.13
3.1.1.3.3	3.2.3.1.12.1
3.1.1.3.3	3.2.3.1.12.2
3.1.1.3.3	3.2.3.1.12.3
3.1.1.3.3	3.2.7.1.3.1
3.1.1.3.3	3.2.7.1.8.1
3.1.1.3.3	3.2.3.1.8
3.1.1.3.3	3.2.3.1.7
3.1.1.3.3	3.2.3.1.6
3.1.1.3.3	3.2.2.1.2.24
3.1.1.3.3	3.2.2.1.2.22
3.1.1.3.3	3.2.3.1.20
3.1.1.3.4	3.2.3.2.1
3.1.1.3.5	3.2.3.1.3
3.1.1.3.5	3.2.3.1.24
3.1.1.4.1	3.2.2.1.2.11
3.1.1.4.1	3.2.2.1.2.12
3.1.1.4.1	3.2.4.1.1
3.1.1.4.2	3.2.4.1.2
3.1.1.4.2	3.2.8.1.1.2
3.1.1.4.3	3.2.4.1.11
3.1.1.4.4	3.2.4.1.10
3.1.1.4.5	3.2.4.1.12.1
3.1.1.4.6	3.2.4.1.12.2
3.1.1.4.7	3.2.4.1.8
3.1.1.5.1	3.2.5.1.1.1
3.1.1.5.2	3.2.5.1.1.2
3.1.1.5.2	3.2.5.1.1.3
3.1.1.5.3	3.2.5.1.1.4
3.1.1.5.4	3.2.5.1.1.5
3.1.1.5.5	3.2.5.1.3.1
3.1.1.5.6	3.2.5.1.3.1
3.1.1.5.7	3.2.8.1.7.2
3.1.1.5.7	3.2.1.1.67.2
3.1.1.5.7	3.2.2.1.6.2
3.1.1.5.7	3.2.3.1.26.2
3.1.1.5.7	3.2.4.1.14.2
3.1.1.5.7	3.2.5.1.3.2
3.1.1.5.7	3.2.6.1.10.2
3.1.1.5.7	3.2.7.1.36.2
3.1.1.5.8	3.2.2.1.6.2
3.1.1.5.8	3.2.3.1.26.2
3.1.1.5.8	3.2.4.1.14.2
3.1.1.5.8	3.2.5.1.3.2
3.1.1.5.8	3.2.5.1.3.2
3.1.1.5.8	3.2.6.1.10.2
3.1.1.5.8	3.2.7.1.36.2
3.1.1.5.8	3.2.8.1.7.2
3.1.1.5.8	3.2.1.1.67.2
3.1.1.5.9	3.2.5.1.3.6
3.1.1.5.9	3.2.5.1.3.5
3.1.1.5.9	3.2.1.1.57
3.1.1.5.10	3.2.5.1.3.5
3.1.1.5.10	3.2.5.1.3.6
3.1.1.5.11	3.2.2.1.6.7
3.1.1.5.11	3.2.4.1.14.4
3.1.1.5.11	3.2.4.1.14.3
3.1.1.5.11	3.2.3.1.26.4
3.1.1.5.11	3.2.3.1.26.3
3.1.1.5.11	3.2.2.1.6.10
3.1.1.5.11	3.2.2.1.6.8
3.1.1.5.11	3.2.6.1.10.3
3.1.1.5.11	3.2.2.1.6.6
3.1.1.5.11	3.2.2.1.6.5
3.1.1.5.11	3.2.2.1.6.4
3.1.1.5.11	3.2.2.1.6.3
3.1.1.5.11	3.2.2.1.6.9
3.1.1.5.11	3.2.5.1.3.4
3.1.1.5.11	3.2.6.1.10.4
3.1.1.5.11	3.2.7.1.36.3
3.1.1.5.11	3.2.7.1.36.4
3.1.1.5.11	3.2.8.1.7.3
3.1.1.5.11	3.2.8.1.7.4
3.1.1.5.11	3.2.8.1.7.5
3.1.1.5.11	3.2.8.1.7.6
3.1.1.5.11	3.2.1.1.67.3
3.1.1.5.11	3.2.1.1.67.4
3.1.1.5.11	3.2.5.1.3.3
3.1.1.5.12	3.2.5.2.1
3.1.1.5.13	3.2.7.1.33
3.1.1.5.13	3.2.5.1.1.7
3.1.1.5.13	3.2.8.1.5.2
3.1.1.5.13	3.2.8.1.5.14
3.1.1.5.13	3.2.5.1.1.6
3.1.1.6.1	3.2.7.1.35.1
3.1.1.6.1	3.2.8.1.6.1
3.1.1.6.1	3.2.6.1.9
3.1.1.6.1	3.2.6.1.6
3.1.1.6.1	3.2.6.1.5
3.1.1.6.1	3.2.6.1.4
3.1.1.6.1	3.2.6.1.3
3.1.1.6.1	3.2.6.1.1
3.1.1.6.1	3.2.5.1.2.1
3.1.1.6.1	3.2.4.1.13.1
3.1.1.6.1	3.2.3.1.25.1
3.1.1.6.1	3.2.1.1.66.1
3.1.1.6.1	3.2.2.1.5.1
3.1.1.6.1	3.2.6.1.2
3.1.1.7.1	3.2.7.1.1
3.1.1.7.1	3.2.7.1.2
3.1.1.7.2	3.2.8.1.5.4

SR ID	SSR ID
3.1.1.7.2	3.2.7.1.3
3.1.1.7.3	3.2.7.1.4
3.1.1.7.4	3.2.7.1.6
3.1.1.7.4	3.2.7.1.9
3.1.1.7.4	3.2.7.1.5
3.1.1.7.5	3.2.7.1.7
3.1.1.7.6	3.2.7.1.8
3.1.1.8.1	3.2.8.1.1.3
3.1.1.8.2	3.2.8.1.1.4
3.1.1.8.3	3.2.8.1.2.7
3.1.1.8.3	3.2.8.1.2.1
3.1.1.8.3	3.2.8.1.2.2
3.1.1.8.3	3.2.8.1.2.8
3.1.1.8.3	3.2.8.1.2.5
3.1.1.8.4	3.2.8.1.2.3
3.1.1.8.5	3.2.8.1.2.4
3.1.1.8.6	3.2.8.1.2.6
3.1.1.8.7	3.2.8.1.2.9
3.1.1.8.8	3.2.8.1.2.14
3.1.1.8.8	3.2.8.1.2.10
3.1.1.8.8	3.2.8.1.2.11
3.1.1.8.8	3.2.8.1.2.13
3.1.1.8.8	3.2.8.1.2.12
3.1.1.8.9	3.2.8.1.4.6
3.1.1.8.9	3.2.8.1.4.5
3.1.1.8.9	3.2.8.1.4.4
3.1.1.8.9	3.2.8.1.4.3
3.1.1.8.10	3.2.8.1.5.1
3.1.1.8.10	3.2.8.1.4.1
3.1.1.8.10	3.2.6.1.7
3.1.1.8.10	3.2.7.1.32
3.1.1.8.10	3.2.5.1.1.16
3.1.1.8.10	3.2.4.1.7
3.1.1.8.10	3.2.2.1.2.21
3.1.1.8.10	3.2.1.1.59
3.1.1.8.10	3.2.8.1.4.2
3.1.1.8.11	3.2.8.1.3.2
3.1.1.8.11	3.2.8.1.3.4
3.1.1.8.11	3.2.8.1.3.1
3.1.1.8.12	3.2.8.1.3.3
3.1.1.8.13	3.2.8.1.3.6
3.1.1.8.13	3.2.8.1.3.5
3.1.1.8.13	3.2.8.1.3.9
3.1.1.8.13	3.2.8.1.3.8
3.1.1.8.13	3.2.8.1.3.7
3.1.1.8.14	3.2.8.1.5.3
3.1.1.8.14	3.2.7.1.22
3.1.1.8.14	3.2.8.1.5.10
3.1.1.8.14	3.2.8.1.5.9
3.1.1.8.14	3.2.8.1.5.6
3.1.1.8.14	3.2.7.1.13
3.1.1.8.14	3.2.1.1.17
3.1.1.8.14	3.2.1.1.58
3.1.1.8.14	3.2.2.1.2.14
3.1.1.8.14	3.2.2.1.2.15
3.1.1.8.14	3.2.2.1.2.19
3.1.1.8.14	3.2.3.1.5
3.1.1.8.14	3.2.3.1.12
3.1.1.8.14	3.2.3.1.18
3.1.1.8.14	3.2.4.1.6
3.1.1.8.14	3.2.4.1.9
3.1.1.8.14	3.2.7.1.27
3.1.1.8.14	3.2.6.1.8
3.1.1.8.14	3.2.8.1.4.8
3.1.1.8.14	3.2.7.1.14
3.1.1.8.14	3.2.7.1.15
3.1.1.8.14	3.2.7.1.16
3.1.1.8.14	3.2.7.1.21
3.1.1.8.14	3.2.7.1.23
3.1.1.8.14	3.2.7.1.28
3.1.1.8.14	3.2.7.1.34
3.1.1.8.14	3.2.8.1.1.1
3.1.1.8.14	3.2.8.1.4.7
3.1.1.8.14	3.2.5.1.1.12
3.1.2.1	3.2.4.2.3
3.1.2.1	3.2.4.2.2
3.1.2.1	3.2.1.1.33
3.1.3.1	3.2.1.1.60
3.1.3.1	3.2.1.1.61
3.1.3.1	3.2.1.2.3
3.1.3.2	3.2.4.2.2
3.1.3.3	3.2.6.2.1
3.1.3.4	3.2.6.2.2
3.1.3.4	3.2.8.2.2
3.1.3.4	3.2.8.2.1
3.1.3.4	3.2.7.2.2
3.1.3.4	3.2.6.2.3
3.1.3.4	3.2.5.2.2
3.1.3.4	3.2.5.2.1
3.1.3.4	3.2.4.2.4
3.1.3.4	3.2.1.2.4
3.1.3.4	3.2.1.2.1
3.1.3.4	3.2.7.2.1
3.1.3.4	3.2.4.2.1
3.1.3.4	3.2.1.2.2
3.1.3.4	3.2.2.2.1
3.1.3.4	3.2.2.2.2
3.1.3.4	3.2.3.2.1
3.1.3.4	3.2.3.2.2
3.1.3.5	3.2.6.2.1
3.1.3.5	3.2.6.1.1
3.1.3.5	3.2.4.2.2
3.1.3.6	3.2.8.2.1
3.1.3.6	3.2.3.2.2
3.1.3.6	3.2.8.1.7.1
3.1.3.6	3.2.1.2.4
3.1.3.6	3.2.2.2.2
3.1.3.6	3.2.4.2.4
3.1.3.6	3.2.8.2.2
3.1.3.6	3.2.5.2.2
3.1.3.6	3.2.7.2.2
3.1.3.6	3.2.7.2.1
3.1.3.6	3.2.1.2.2
3.1.3.6	3.2.6.2.3
3.1.3.6	3.2.6.2.2
3.1.3.6	3.2.6.1.10.1
3.1.3.6	3.2.4.2.3
3.1.3.6	3.2.4.2.1
3.1.3.6	3.2.4.1.14.1
3.1.3.6	3.2.3.1.26.1
3.1.3.6	3.2.2.1.6.1
3.1.3.6	3.2.1.2.1
3.1.3.6	3.2.1.1.67.1
3.1.3.6	3.2.7.1.36.1
3.1.3.6	3.2.2.2.1
3.1.3.7	3.2.5.2.3

6.1.4 Subsystem to System Matrix

The table below shows the mapping of Subsystem Requirements (SSR IDs) to the higher level System Requirements (SR IDs).

Table 6-4**. Subsystem Requirements (SSR) to System Requirements (SR) Traceability**

SSR ID	SR ID
3.2.1.1.1	3.1.1.1.1
3.2.1.1.2	3.1.1.1.2
3.2.1.1.3	3.1.1.1.1
3.2.1.1.4	3.1.1.1.1
3.2.1.1.5	3.1.1.1.1
3.2.1.1.6	3.1.1.1.3
3.2.1.1.7	3.1.1.1.4
3.2.1.1.8	3.1.1.1.5
3.2.1.1.9	3.1.1.1.4
3.2.1.1.10	3.1.1.1.4
3.2.1.1.11	3.1.1.1.6
3.2.1.1.12	3.1.1.1.7
3.2.1.1.13	3.1.1.1.8
3.2.1.1.14	3.1.1.1.7
3.2.1.1.15	3.1.1.1.9
3.2.1.1.16	3.1.1.1.10
3.2.1.1.17	3.1.1.8.14
3.2.1.1.18	3.1.1.1.11
3.2.1.1.19	3.1.1.1.12
3.2.1.1.20	3.1.1.1.12
3.2.1.1.21	3.1.1.1.13
3.2.1.1.22	3.1.1.1.12
3.2.1.1.23	3.1.1.1.14
3.2.1.1.24	3.1.1.1.15
3.2.1.1.25	3.1.1.1.15
3.2.1.1.26	3.1.1.1.16
3.2.1.1.27	3.1.1.1.15
3.2.1.1.28	3.1.1.1.10
3.2.1.1.29	3.1.1.1.10
3.2.1.1.30	3.1.1.1.10
3.2.1.1.31	3.1.1.1.10
3.2.1.1.32	3.1.1.1.10
3.2.1.1.33	3.1.1.1.17
3.2.1.1.33	3.1.2.1
3.2.1.1.34	3.1.1.1.18
3.2.1.1.35	3.1.1.1.19
3.2.1.1.36	3.1.1.1.20
3.2.1.1.37	3.1.1.1.24
3.2.1.1.38	3.1.1.1.25
3.2.1.1.39	3.1.1.1.21
3.2.1.1.40	3.1.1.1.22
3.2.1.1.41	3.1.1.1.22
3.2.1.1.42	3.1.1.1.23
3.2.1.1.43	3.1.1.1.22
3.2.1.1.44	3.1.1.1.21
3.2.1.1.45	3.1.1.1.26
3.2.1.1.46	3.1.1.1.27
3.2.1.1.47	3.1.1.1.27
3.2.1.1.48	3.1.1.1.28
3.2.1.1.49	3.1.1.1.27
3.2.1.1.50	3.1.1.1.26
3.2.1.1.50	3.1.1.1.32
3.2.1.1.51	3.1.1.1.26
3.2.1.1.51	3.1.1.1.33
3.2.1.1.52	3.1.1.1.29
3.2.1.1.53	3.1.1.1.30
3.2.1.1.54	3.1.1.1.30
3.2.1.1.55	3.1.1.1.31
3.2.1.1.56	3.1.1.1.30
3.2.1.1.57	3.1.1.5.9
3.2.1.1.58	3.1.1.8.14
3.2.1.1.59	3.1.1.8.10
3.2.1.1.60	3.1.3.1
3.2.1.1.61	3.1.3.1
3.2.1.1.66.1	3.1.1.6.1
3.2.1.1.67.1	3.1.3.6
3.2.1.1.67.2	3.1.1.5.7
3.2.1.1.67.2	3.1.1.5.8
3.2.1.1.67.3	3.1.1.5.11
3.2.1.1.67.4	3.1.1.5.11
3.2.1.2.1	3.1.1.1.1
3.2.1.2.1	3.1.3.4
3.2.1.2.1	3.1.3.6
3.2.1.2.2	3.1.3.4
3.2.1.2.2	3.1.3.6
3.2.1.2.3	3.1.3.1
3.2.1.2.4	3.1.3.4
3.2.1.2.4	3.1.3.6
3.2.2.1.1.1	3.1.1.2.1
3.2.2.1.1.2	3.1.1.2.1
3.2.2.1.1.3	3.1.1.2.2
3.2.2.1.1.4	3.1.1.2.3
3.2.2.1.1.5	3.1.1.2.2
3.2.2.1.1.6	3.1.1.2.3
3.2.2.1.1.7	3.1.1.2.3
3.2.2.1.2.1	3.1.1.2.4
3.2.2.1.2.2	3.1.1.2.4
3.2.2.1.2.3	3.1.1.2.5
3.2.2.1.2.4	3.1.1.2.6
3.2.2.1.2.5	3.1.1.2.4
3.2.2.1.2.6	3.1.1.2.4
3.2.2.1.2.7	3.1.1.2.9
3.2.2.1.2.8	3.1.1.2.9
3.2.2.1.2.9	3.1.1.2.10
3.2.2.1.2.10	3.1.1.2.9
3.2.2.1.2.11	3.1.1.4.1
3.2.2.1.2.12	3.1.1.4.1
3.2.2.1.2.13	3.1.1.2.11
3.2.2.1.2.14	3.1.1.8.14
3.2.2.1.2.15	3.1.1.8.14
3.2.2.1.2.16	3.1.1.1.10
3.2.2.1.2.17	3.1.1.1.10
3.2.2.1.2.18	3.1.1.1.21
3.2.2.1.2.19	3.1.1.8.14
3.2.2.1.2.20	3.1.1.1.30
3.2.2.1.2.21	3.1.1.8.10
3.2.2.1.2.22	3.1.1.3.3
3.2.2.1.3.1	3.1.1.2.11
3.2.2.1.3.2	3.1.1.2.11
3.2.2.1.3.3	3.1.1.2.11
3.2.2.1.4.1	3.1.1.2.7

SSR ID	SR ID
3.2.2.1.4.2	3.1.1.2.7
3.2.2.1.4.3	3.1.1.2.8
3.2.2.1.4.4	3.1.1.2.7
3.2.2.1.4.5	3.1.1.2.7
3.2.2.1.4.6	3.1.1.2.7
3.2.2.1.4.7	3.1.1.2.10
3.2.2.1.4.8	3.1.1.3.3
3.2.2.1.5.1	3.1.1.6.1
3.2.2.1.6.1	3.1.3.6
3.2.2.1.6.2	3.1.1.5.7
3.2.2.1.6.2	3.1.1.5.8
3.2.2.1.6.3	3.1.1.5.11
3.2.2.1.6.4	3.1.1.5.11
3.2.2.1.6.5	3.1.1.5.11
3.2.2.1.6.6	3.1.1.5.11
3.2.2.1.6.7	3.1.1.5.11
3.2.2.1.6.8	3.1.1.5.11
3.2.2.1.6.9	3.1.1.5.11
3.2.2.1.6.10	3.1.1.5.11
3.2.2.2.1	3.1.3.4
3.2.2.2.1	3.1.3.6
3.2.2.2.2	3.1.3.4
3.2.2.2.2	3.1.3.6
3.2.3.1.1	3.1.1.3.1
3.2.3.1.2	3.1.1.3.1
3.2.3.1.3	3.1.1.3.2
3.2.3.1.3	3.1.1.3.5
3.2.3.1.4	3.1.1.3.1
3.2.3.1.5	3.1.1.8.14
3.2.3.1.6	3.1.1.3.3
3.2.3.1.7	3.1.1.3.3
3.2.3.1.8	3.1.1.3.3
3.2.3.1.9	3.1.1.1.10
3.2.3.1.10	3.1.1.1.10
3.2.3.1.11	3.1.1.1.21
3.2.3.1.12	3.1.1.8.14
3.2.3.1.12.1	3.1.1.3.3
3.2.3.1.12.2	3.1.1.3.3
3.2.3.1.12.3	3.1.1.3.3
3.2.3.1.13	3.1.1.3.3
3.2.3.1.14	3.1.1.3.3
3.2.3.1.15	3.1.1.3.3

SSR ID	SR ID
3.2.3.1.16	3.1.1.3.3
3.2.3.1.17	3.1.1.3.3
3.2.3.1.18	3.1.1.8.14
3.2.3.1.19	3.1.1.3.3
3.2.3.1.20	3.1.1.3.3
3.2.3.1.21	3.1.1.3.3
3.2.3.1.22	3.1.1.3.3
3.2.3.1.23	3.1.1.3.3
3.2.3.1.24	3.1.1.3.5
3.2.3.1.25.1	3.1.1.6.1
3.2.3.1.26.1	3.1.3.6
3.2.3.1.26.2	3.1.1.5.7
3.2.3.1.26.2	3.1.1.5.8
3.2.3.1.26.3	3.1.1.5.11
3.2.3.1.26.4	3.1.1.5.11
3.2.3.2.1	3.1.1.3.4
3.2.3.2.1	3.1.3.4
3.2.3.2.2	3.1.3.4
3.2.3.2.2	3.1.3.6
3.2.4.1.1	3.1.1.4.1
3.2.4.1.2	3.1.1.4.2
3.2.4.1.3	3.1.1.1.10
3.2.4.1.4	3.1.1.1.10
3.2.4.1.5	3.1.1.1.21
3.2.4.1.6	3.1.1.8.14
3.2.4.1.7	3.1.1.8.10
3.2.4.1.8	3.1.1.4.7
3.2.4.1.9	3.1.1.8.14
3.2.4.1.10	3.1.1.4.4
3.2.4.1.11	3.1.1.4.3
3.2.4.1.12.1	3.1.1.4.5
3.2.4.1.12.2	3.1.1.4.6
3.2.4.1.13.1	3.1.1.6.1
3.2.4.1.14.1	3.1.3.6
3.2.4.1.14.2	3.1.1.5.7
3.2.4.1.14.2	3.1.1.5.8
3.2.4.1.14.3	3.1.1.5.11
3.2.4.1.14.4	3.1.1.5.11
3.2.4.2.1	3.1.3.4
3.2.4.2.1	3.1.3.6
3.2.4.2.2	3.1.2.1
3.2.4.2.2	3.1.3.2

SSR ID	SR ID
3.2.4.2.2	3.1.3.5
3.2.4.2.3	3.1.2.1
3.2.4.2.3	3.1.3.6
3.2.4.2.4	3.1.3.4
3.2.4.2.4	3.1.3.6
3.2.5.1.1.1	3.1.1.5.1
3.2.5.1.1.2	3.1.1.5.2
3.2.5.1.1.3	3.1.1.5.2
3.2.5.1.1.4	3.1.1.5.3
3.2.5.1.1.5	3.1.1.5.4
3.2.5.1.1.6	3.1.1.5.13
3.2.5.1.1.7	3.1.1.5.13
3.2.5.1.1.8	3.1.1.1.10
3.2.5.1.1.9	3.1.1.1.10
3.2.5.1.1.10	3.1.1.1.21
3.2.5.1.1.11	3.1.1.1.21
3.2.5.1.1.12	3.1.1.8.14
3.2.5.1.1.13	3.1.1.1.30
3.2.5.1.1.14	3.1.1.1.30
3.2.5.1.1.15	3.1.1.1.30
3.2.5.1.1.16	3.1.1.8.10
3.2.5.1.2.1	3.1.1.6.1
3.2.5.1.3.1	3.1.1.5.5
3.2.5.1.3.1	3.1.1.5.6
3.2.5.1.3.2	3.1.1.5.7
3.2.5.1.3.2	3.1.1.5.8
3.2.5.1.3.2	3.1.1.5.8
3.2.5.1.3.3	3.1.1.5.11
3.2.5.1.3.4	3.1.1.5.11
3.2.5.1.3.5	3.1.1.5.9
3.2.5.1.3.5	3.1.1.5.10
3.2.5.1.3.6	3.1.1.5.9
3.2.5.1.3.6	3.1.1.5.10
3.2.5.2.1	3.1.1.5.12
3.2.5.2.1	3.1.3.4
3.2.5.2.2	3.1.3.4
3.2.5.2.2	3.1.3.6
3.2.5.2.3	3.1.3.7
3.2.6.1.1	3.1.1.6.1
3.2.6.1.1	3.1.3.5
3.2.6.1.2	3.1.1.6.1
3.2.6.1.3	3.1.1.6.1

SSR ID	SR ID
3.2.6.1.4	3.1.1.6.1
3.2.6.1.5	3.1.1.6.1
3.2.6.1.6	3.1.1.6.1
3.2.6.1.7	3.1.1.8.10
3.2.6.1.8	3.1.1.8.14
3.2.6.1.9	3.1.1.6.1
3.2.6.1.10.1	3.1.3.6
3.2.6.1.10.2	3.1.1.5.7
3.2.6.1.10.2	3.1.1.5.8
3.2.6.1.10.3	3.1.1.5.11
3.2.6.1.10.4	3.1.1.5.11
3.2.6.2.1	3.1.3.3
3.2.6.2.1	3.1.3.5
3.2.6.2.2	3.1.3.4
3.2.6.2.2	3.1.3.6
3.2.6.2.3	3.1.3.4
3.2.6.2.3	3.1.3.6
3.2.7.1.1	3.1.1.7.1
3.2.7.1.2	3.1.1.7.1
3.2.7.1.3	3.1.1.7.2
3.2.7.1.3.1	3.1.1.3.3
3.2.7.1.4	3.1.1.7.3
3.2.7.1.5	3.1.1.7.4
3.2.7.1.6	3.1.1.7.4
3.2.7.1.7	3.1.1.7.5
3.2.7.1.8	3.1.1.7.6
3.2.7.1.8.1	3.1.1.3.3
3.2.7.1.9	3.1.1.7.4
3.2.7.1.10	3.1.1.1.1
3.2.7.1.11	3.1.1.1.30
3.2.7.1.12	3.1.1.1.1
3.2.7.1.13	3.1.1.8.14
3.2.7.1.14	3.1.1.8.14
3.2.7.1.15	3.1.1.8.14
3.2.7.1.16	3.1.1.8.14
3.2.7.1.17	3.1.1.3.3
3.2.7.1.18	3.1.1.3.3
3.2.7.1.19	3.1.1.3.3
3.2.7.1.20	3.1.1.3.3
3.2.7.1.21	3.1.1.8.14
3.2.7.1.22	3.1.1.8.14
3.2.7.1.23	3.1.1.8.14
3.2.7.1.24	3.1.1.1.10
3.2.7.1.25	3.1.1.1.10
3.2.7.1.26	3.1.1.1.21
3.2.7.1.27	3.1.1.8.14
3.2.7.1.28	3.1.1.8.14
3.2.7.1.29	3.1.1.3.3
3.2.7.1.30	3.1.1.3.3
3.2.7.1.31	3.1.1.3.3
3.2.7.1.32	3.1.1.8.10
3.2.7.1.33	3.1.1.5.13
3.2.7.1.34	3.1.1.8.14
3.2.7.1.35.1	3.1.1.6.1
3.2.7.1.36.1	3.1.3.6
3.2.7.1.36.2	3.1.1.5.7
3.2.7.1.36.2	3.1.1.5.8
3.2.7.1.36.3	3.1.1.5.11
3.2.7.1.36.4	3.1.1.5.11
3.2.7.2.1	3.1.3.4
3.2.7.2.1	3.1.3.6
3.2.7.2.2	3.1.3.4
3.2.7.2.2	3.1.3.6
3.2.8.1.1.1	3.1.1.8.14
3.2.8.1.1.2	3.1.1.4.2
3.2.8.1.1.3	3.1.1.8.1
3.2.8.1.1.4	3.1.1.8.2
3.2.8.1.2.1	3.1.1.8.3
3.2.8.1.2.2	3.1.1.8.3
3.2.8.1.2.3	3.1.1.8.4
3.2.8.1.2.4	3.1.1.8.5
3.2.8.1.2.5	3.1.1.8.3
3.2.8.1.2.6	3.1.1.8.6
3.2.8.1.2.7	3.1.1.8.3
3.2.8.1.2.8	3.1.1.8.3
3.2.8.1.2.9	3.1.1.8.7
3.2.8.1.2.10	3.1.1.8.8
3.2.8.1.2.11	3.1.1.8.8
3.2.8.1.2.12	3.1.1.8.8
3.2.8.1.2.13	3.1.1.8.8
3.2.8.1.2.14	3.1.1.8.8
3.2.8.1.3.1	3.1.1.8.11
3.2.8.1.3.2	3.1.1.8.11
3.2.8.1.3.3	3.1.1.8.12
3.2.8.1.3.4	3.1.1.8.11
3.2.8.1.3.5	3.1.1.8.13
3.2.8.1.3.6	3.1.1.8.13
3.2.8.1.3.7	3.1.1.8.13
3.2.8.1.3.8	3.1.1.8.13
3.2.8.1.3.9	3.1.1.8.13
3.2.8.1.4.1	3.1.1.8.10
3.2.8.1.4.2	3.1.1.8.10
3.2.8.1.4.3	3.1.1.8.9
3.2.8.1.4.4	3.1.1.8.9
3.2.8.1.4.5	3.1.1.8.9
3.2.8.1.4.6	3.1.1.8.9
3.2.8.1.4.7	3.1.1.8.14
3.2.8.1.4.8	3.1.1.8.14
3.2.8.1.5.1	3.1.1.8.10
3.2.8.1.5.2	3.1.1.5.13
3.2.8.1.5.3	3.1.1.8.14
3.2.8.1.5.4	3.1.1.7.2
3.2.8.1.5.5	3.1.1.3.3
3.2.8.1.5.6	3.1.1.8.14
3.2.8.1.5.7	3.1.1.1.30
3.2.8.1.5.8	3.1.1.3.3
3.2.8.1.5.9	3.1.1.8.14
3.2.8.1.5.10	3.1.1.8.14
3.2.8.1.5.11	3.1.1.1.10
3.2.8.1.5.12	3.1.1.1.10
3.2.8.1.5.13	3.1.1.1.21
3.2.8.1.5.14	3.1.1.5.13
3.2.8.1.6.1	3.1.1.6.1
3.2.8.1.7.1	3.1.3.6
3.2.8.1.7.2	3.1.1.5.7
3.2.8.1.7.2	3.1.1.5.8
3.2.8.1.7.3	3.1.1.5.11
3.2.8.1.7.4	3.1.1.5.11
3.2.8.1.7.5	3.1.1.5.11
3.2.8.1.7.6	3.1.1.5.11
3.2.8.2.1	3.1.3.4
3.2.8.2.1	3.1.3.6
3.2.8.2.2	3.1.3.4
3.2.8.2.2	3.1.3.6

6.2 Requirements to Architecture Components

The relationships between objects or components of the architecture and requirements contained in this specification are documented in this section.

6.2.1 Subsystem Requirements to Architecture Traceability

The table below is a mapping between Subsystem Requirements to Architectural Views and the Architectural Object(s) that related to those requirements.

Table 6-5. Subsystem Requirement to Architecture Object Traceability

SSR ID	Architecture View	Arch Object ID
3.2.1.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core
3.2.1.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core
3.2.1.1.3	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.3	4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core
3.2.1.1.4	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.4	4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core
3.2.1.1.5	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.5	4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core
3.2.1.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core
3.2.1.1.7	4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores
3.2.1.1.8	4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores
3.2.1.1.9	4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores
3.2.1.1.10	4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores
3.2.1.1.11	4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores
3.2.1.1.12	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores

SSR ID	Architecture View	Arch Object ID
3.2.1.1.13	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.1.1.14	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.1.1.15	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.1.1.16	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.1.1.17	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.1.1.17	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.1.1.17	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.1.1.17	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.1.1.17	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.1.1.17	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.1.1.17	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.1.1.18	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.18	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.19	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.19	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.20	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.20	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.21	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.21	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.22	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.22	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.23	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.23	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.24	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL

SSR ID	Architecture View	Arch Object ID
3.2.1.1.24	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.25	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.25	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.26	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.26	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.27	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.1.1.27	4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores
3.2.1.1.28	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.1.1.29	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.1.1.30	4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores
3.2.1.1.31	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.1.1.32	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.1.1.33	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.1.1.34	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.1.1.35	4.2.3 Functional View – System Configuration	4.2.3.3.8 Identify Core Conflicts
3.2.1.1.36	4.2.3 Functional View – System Configuration	4.2.3.3.13 Receive Core Conflict Info
3.2.1.1.37	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.38	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.39	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.40	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.41	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.42	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.43	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.44	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.45	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.45	4.2.10 Functional View – Core Backup	4.2.10.3.20 Provide Other Core Data
3.2.1.1.46	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.46	4.2.10 Functional View – Core Backup	4.2.10.3.20 Provide Other Core Data
3.2.1.1.47	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.48	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data
3.2.1.1.49	4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data

SSR ID	Architecture View	Arch Object ID
3.2.1.1.50	4.2.10 Functional View – Core Backup	4.2.10.3.22 Request Core Takeover
3.2.1.1.51	4.2.10 Functional View – Core Backup	4.2.10.3.6 Core Takeover
3.2.1.1.52	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.53	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.54	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.55	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.56	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.1.1.57	4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores
3.2.1.1.57	4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users
3.2.1.1.58	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.1.1.58	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.1.1.58	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.1.1.58	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.1.1.58	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.1.1.58	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.1.1.58	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.1.1.59	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.1.1.60	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.1.1.61	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.1.66.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.1.1.67.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.1.1.67.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.14 Modify C2C Operational State
3.2.1.1.67.1	4.2.10 Functional View – Core Backup	4.2.10.3.15 Modify C2C Operational State
3.2.1.1.67.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.1.1.67.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.1.1.67.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.1.1.67.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.1.1.67.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component

SSR ID	Architecture View	Arch Object ID
3.2.1.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.1.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.1.2.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.19 Provide Operator Interface to C2C
3.2.1.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.1.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.10 Manually Modify Other Core Configs
3.2.1.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.1.2.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.19 Provide Operator Interface to C2C
3.2.1.2.3	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.1.2.4	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.1.2.4	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.2.1.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.1.1	4.2.10 Functional View – Core Backup	4.2.10.3.17 Modify System User Data Subscriptions
3.2.2.1.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.1.3	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.1.4	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.1.4	4.2.10 Functional View – Core Backup	4.2.10.3.17 Modify System User Data Subscriptions
3.2.2.1.1.5	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.1.6	4.2.10 Functional View – Core Backup	4.2.10.3.17 Modify System User Data Subscriptions
3.2.2.1.1.7	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.2.1	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.2.2	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.2.3	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.2.4	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.2.4	4.2.4 Functional View – User Configuration	4.2.4.3.17 Modify Data Acceptance Catalog
3.2.2.1.2.4	4.2.10 Functional View – Core Backup	4.2.10.3.16 Modify Data Acceptance Catalog

SSR ID	Architecture View	Arch Object ID
3.2.2.1.2.5	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.2.6	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.2.6	4.2.4 Functional View – User Configuration	4.2.4.3.17 Modify Data Acceptance Catalog
3.2.2.1.2.7	4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information
3.2.2.1.2.8	4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information
3.2.2.1.2.9	4.2.2 Functional View – Data Distribution	4.2.2.3.10 Match Data to Data Subscribers
3.2.2.1.2.9	4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users
3.2.2.1.2.9	4.2.10 Functional View – Core Backup	4.2.10.3.5 Configure Geo-cast Device Information
3.2.2.1.2.10	4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information
3.2.2.1.2.10	4.2.10 Functional View – Core Backup	4.2.10.3.5 Configure Geo-cast Device Information
3.2.2.1.2.11	4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data
3.2.2.1.2.11	4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users
3.2.2.1.2.12	4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data
3.2.2.1.2.12	4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users
3.2.2.1.2.13	4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data
3.2.2.1.2.13	4.2.2 Functional View – Data Distribution	4.2.2.3.14 Provide Data to Subscribing System Users
3.2.2.1.2.13	4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users
3.2.2.1.2.14	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.2.1.2.14	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.2.1.2.14	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.2.1.2.14	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.2.1.2.14	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.2.1.2.14	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.2.1.2.14	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.2.1.2.15	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission

SSR ID	Architecture View	Arch Object ID
3.2.2.1.2.15	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.2.1.2.15	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.2.1.2.15	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.2.1.2.15	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.2.1.2.15	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.2.1.2.15	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.2.1.2.16	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.2.1.2.17	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.2.1.2.18	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.2.1.2.18	4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up
3.2.2.1.2.19	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.2.1.2.19	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.2.1.2.19	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.2.1.2.19	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.2.1.2.19	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.2.1.2.19	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.2.1.2.19	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.2.1.2.20	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.2.1.2.21	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.2.1.2.22	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.2.1.3.1	4.2.2 Functional View – Data Distribution	4.2.2.3.3 Aggregate Data
3.2.2.1.3.1	4.2.2 Functional View – Data Distribution	4.2.2.3.17 Repackage Data
3.2.2.1.3.2	4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data
3.2.2.1.3.2	4.2.2 Functional View – Data Distribution	4.2.2.3.17 Repackage Data
3.2.2.1.3.3	4.2.2 Functional View – Data Distribution	4.2.2.3.17 Repackage Data
3.2.2.1.3.3	4.2.2 Functional View – Data Distribution	4.2.2.3.18 Sample Data

SSR ID	Architecture View	Arch Object ID
3.2.2.1.4.1	4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages
3.2.2.1.4.2	4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages
3.2.2.1.4.3	4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages
3.2.2.1.4.4	4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages
3.2.2.1.4.5	4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information
3.2.2.1.4.5	4.2.7 Functional View – Misbehavior Management	4.2.7.3.6 Disable Misbehaving Geo-Cast Device
3.2.2.1.4.6	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.2.1.5.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.2.1.6.1	4.2.2 Functional View – Data Distribution	4.2.2.3.12 Modify DD Operational State
3.2.2.1.6.1	4.2.4 Functional View – User Configuration	4.2.4.3.18 Modify DD Operational State
3.2.2.1.6.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.2.1.6.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.2.1.6.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.2.1.6.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.2.1.6.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.2.1.6.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.2.1.6.5	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.6.6	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.6.7	4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages
3.2.2.1.6.8	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.1.6.9	4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests
3.2.2.1.6.10	4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions
3.2.2.2.1	4.2.2 Functional View – Data Distribution	4.2.2.3.15 Provide Operator Interface to DD
3.2.2.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface

SSR ID	Architecture View	Arch Object ID
3.2.2.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.2.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.2.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.2.2.2	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.3.1.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports
3.2.3.1.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports
3.2.3.1.3	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.3	4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports
3.2.3.1.4	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.4	4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports
3.2.3.1.5	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.3.1.5	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.3.1.5	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.3.1.5	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.3.1.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.3.1.5	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.3.1.5	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.3.1.5	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.3.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status
3.2.3.1.7	4.2.7 Functional View – Misbehavior Management	4.2.7.3.3 Ask CA to Revoke
3.2.3.1.7	4.2.7 Functional View – Misbehavior Management	4.2.7.3.24 Revoke User Permissions
3.2.3.1.8	4.2.7 Functional View – Misbehavior Management	4.2.7.3.23 Revoke Operator Permissions
3.2.3.1.9	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration

SSR ID	Architecture View	Arch Object ID
3.2.3.1.10	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.3.1.11	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.3.1.11	4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up
3.2.3.1.12	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.3.1.12	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.3.1.12	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.3.1.12.1	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.3.1.12.2	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions
3.2.3.1.12.3	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.3.1.12.3	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permission
3.2.3.1.12	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.3.1.12	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.3.1.12	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.3.1.12	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.3.1.13	4.2.7 Functional View – Misbehavior Management	4.2.7.3.6 Disable Misbehaving Geo-Cast Device
3.2.3.1.14	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.3.1.15	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.3.1.15	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.16	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.3.1.16	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.17	4.2.9 Functional View – Networking	4.2.9.3.4 Intrusion Detection
3.2.3.1.18	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.3.1.18	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.3.1.19	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.3.1.19	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users

SSR ID	Architecture View	Arch Object ID
3.2.3.1.19	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.3.1.19	4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports
3.2.3.1.20	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.3.1.21	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.3.1.22	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.3.1.22	4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports
3.2.3.1.23	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.3.1.23	4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports
3.2.3.1.24	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.3.1.25.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.3.1.26.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.3.1.26.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.15 Modify MM Operational State
3.2.3.1.26.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.3.1.26.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.3.1.26.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.3.1.26.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.3.1.26.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.3.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.3.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.3.2.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.20 Provide Operator Interface to MM
3.2.3.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.3.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.3.2.2	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.4.1.1	4.2.2 Functional View – Data Distribution	4.2.2.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.3 Functional View – System Configuration	4.2.3.3.2.1 Decrypt Messages Received Encrypted

SSR ID	Architecture View	Arch Object ID
3.2.4.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.9 Functional View – Networking	4.2.9.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.1	4.2.10 Functional View – Core Backup	4.2.10.3.2.1 Decrypt Messages Received Encrypted
3.2.4.1.2	4.2.2 Functional View – Data Distribution	4.2.2.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.3 Functional View – System Configuration	4.2.3.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.9 Functional View – Networking	4.2.9.3.2.2 Encrypt Messages
3.2.4.1.2	4.2.10 Functional View – Core Backup	4.2.10.3.2.2 Encrypt Messages
3.2.4.1.3	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.4.1.4	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.4.1.5	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.4.1.5	4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up
3.2.4.1.6	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.4.1.6	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.4.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.4.1.6	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.4.1.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.4.1.6	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.4.1.6	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.4.1.7	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key

SSR ID	Architecture View	Arch Object ID
3.2.4.1.8	4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance
3.2.4.1.8	4.2.9 Functional View – Networking	4.2.9.3.8 Monitor Service Control Node Performance
3.2.4.1.8	4.2.10 Functional View – Core Backup	4.2.10.3.18 Monitor Core Services Performance
3.2.4.1.9	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.4.1.9	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.4.1.9	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.4.1.9	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.4.1.9	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.4.1.9	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.4.1.9	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.4.1.10	4.2.9 Functional View – Networking	4.2.9.3.12 Route Data between Networks
3.2.4.1.10	4.2.9 Functional View – Networking	4.2.9.3.13 Route Data/Request
3.2.4.1.11	4.2.9 Functional View – Networking	4.2.9.3.9 Provide Internet Connectivity
3.2.4.1.11	4.2.9 Functional View – Networking	4.2.9.3.10 Provide Private Network Connectivity
3.2.4.1.12.1	4.2.9 Functional View – Networking	4.2.9.3.5 Intrusion Prevention
3.2.4.1.12.2	4.2.9 Functional View – Networking	4.2.9.3.4 Intrusion Detection
3.2.4.1.13.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.4.1.14.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.4.1.14.1	4.2.9 Functional View – Networking	4.2.9.3.7 Modify NS Operational State
3.2.4.1.14.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.4.1.14.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.4.1.14.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.4.1.14.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.4.1.14.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.4.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.4.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.4.2.1	4.2.9 Functional View – Networking	4.2.9.3.11 Provide Operator Interface to NS
3.2.4.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.4.2.2	4.2.9 Functional View – Networking	4.2.9.3.9 Provide Internet Connectivity
3.2.4.2.3	4.2.9 Functional View – Networking	4.2.9.3.10 Provide Private Network Connectivity

SSR ID	Architecture View	Arch Object ID
3.2.4.2.4	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.4.2.4	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.5.1.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status
3.2.5.1.1.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.5.1.1.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users
3.2.5.1.1.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.5.1.1.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users
3.2.5.1.1.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores
3.2.5.1.1.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users
3.2.5.1.1.5	4.2.5 Functional View – System Monitor and Control	4.2.5.3.15 Provide Record of System Performance
3.2.5.1.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.5.1.1.7	4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores
3.2.5.1.1.7	4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users
3.2.5.1.1.8	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.5.1.1.9	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.5.1.1.10	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.5.1.1.10	4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up
3.2.5.1.1.11	4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores
3.2.5.1.1.12	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.5.1.1.12	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.5.1.1.12	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.5.1.1.12	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.5.1.1.12	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.5.1.1.12	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.5.1.1.12	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission

SSR ID	Architecture View	Arch Object ID
3.2.5.1.1.13	4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status
3.2.5.1.1.14	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.5.1.1.15	4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance
3.2.5.1.1.16	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.5.1.2.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.5.1.3.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.5.1.3.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.10 Modify SM Operational State
3.2.5.1.3.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.5.1.3.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.5.1.3.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.5.1.3.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.5.1.3.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.5.1.3.5	4.2.5 Functional View – System Monitor and Control	4.2.5.3.12 Monitor Core Health and Safety
3.2.5.1.3.5	4.2.5 Functional View – System Monitor and Control	4.2.5.3.20 Take Action in Response to Environment Issue
3.2.5.1.3.6	4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance
3.2.5.1.3.6	4.2.9 Functional View – Networking	4.2.9.3.8 Monitor Service Control Node Performance
3.2.5.1.3.6	4.2.10 Functional View – Core Backup	4.2.10.3.18 Monitor Core Services Performance
3.2.5.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.5.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.5.2.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.5.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.5.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.5.2.2	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.5.2.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.15 Provide Record of System Performance
3.2.6.1.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.8 Get Time from External Available Source
3.2.6.1.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.8 Get Time from External Available Source

SSR ID	Architecture View	Arch Object ID
3.2.6.1.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.6.1.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.6.1.5	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.6.1.6	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.6.1.6	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.6.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.6.1.6	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.6.1.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.6.1.6	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.6.1.6	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.6.1.7	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.6.1.8	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.6.1.8	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.6.1.8	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.6.1.8	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.6.1.8	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.6.1.8	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.6.1.8	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.6.1.9	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.6.1.10.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.6.1.10.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.11 Modify TS Operational State
3.2.6.1.10.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.6.1.10.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.6.1.10.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.6.1.10.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component

SSR ID	Architecture View	Arch Object ID
3.2.6.1.10.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.6.2.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.8 Get Time from External Available Source
3.2.6.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.6.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.6.2.2	4.2.4 Functional View – User Configuration	4.2.4.3.10 Generic Provide Operator Interface
3.2.6.2.2	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.6.2.3	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.6.2.3	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.7.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions
3.2.7.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions
3.2.7.1.1	4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions
3.2.7.1.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions
3.2.7.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions
3.2.7.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions
3.2.7.1.2	4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions
3.2.7.1.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions
3.2.7.1.3	4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions
3.2.7.1.3	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions
3.2.7.1.3.1	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions
3.2.7.1.3	4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions
3.2.7.1.3	4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions
3.2.7.1.4	4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions
3.2.7.1.4	4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions
3.2.7.1.4	4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions
3.2.7.1.4	4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions

SSR ID	Architecture View	Arch Object ID
3.2.7.1.5	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.6	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.7	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.8	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.8.1	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.9	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.10	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.11	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.7.1.12	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.13	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.7.1.13	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.7.1.13	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.7.1.13	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.7.1.13	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.7.1.13	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.7.1.13	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.7.1.14	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.7.1.14	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.7.1.14	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.7.1.14	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.7.1.14	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.7.1.14	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.7.1.14	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.7.1.15	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.7.1.15	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission

SSR ID	Architecture View	Arch Object ID
3.2.7.1.15	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.7.1.15	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.7.1.15	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.7.1.15	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.7.1.15	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.7.1.16	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.7.1.16	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.7.1.16	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.7.1.16	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.7.1.16	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.7.1.16	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.7.1.16	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.7.1.17	4.2.7 Functional View – Misbehavior Management	4.2.7.3.3 Ask CA to Revoke
3.2.7.1.17	4.2.7 Functional View – Misbehavior Management	4.2.7.3.24 Revoke User Permissions
3.2.7.1.18	4.2.7 Functional View – Misbehavior Management	4.2.7.3.23 Revoke Operator Permissions
3.2.7.1.19	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.20	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.7.1.21	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.7.1.21	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.7.1.22	4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials
3.2.7.1.23	4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials
3.2.7.1.23	4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials
3.2.7.1.24	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.7.1.25	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.7.1.26	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data

SSR ID	Architecture View	Arch Object ID
3.2.7.1.26	4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up
3.2.7.1.27	4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status
3.2.7.1.28	4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status
3.2.7.1.29	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.7.1.29	4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports
3.2.7.1.30	4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators
3.2.7.1.31	4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users
3.2.7.1.32	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.7.1.33	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.7.1.34	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.7.1.35.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.7.1.36.1	4.2.4 Functional View – User Configuration	4.2.4.3.19 Modify UP Operational State
3.2.7.1.36.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.7.1.36.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.7.1.36.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.7.1.36.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.7.1.36.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.7.1.36.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.7.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface
3.2.7.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.7.2.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.7.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.7.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.7.2.2	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem
3.2.8.1.1.1	4.2.2 Functional View – Data Distribution	4.2.2.3.2.4 Verify Authenticity of Received Messages

SSR ID	Architecture View	Arch Object ID
3.2.8.1.1.1	4.2.3 Functional View – System Configuration	4.2.3.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.4 Functional View – User Configuration	4.2.4.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.8 Functional View – Core Decryption	4.2.8.3.1.2 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.9 Functional View – Networking	4.2.9.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.1	4.2.10 Functional View – Core Backup	4.2.10.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.1.2	4.2.2 Functional View – Data Distribution	4.2.2.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.3 Functional View – System Configuration	4.2.3.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.4 Functional View – User Configuration	4.2.4.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.9 Functional View – Networking	4.2.9.3.2.3 Sign Messages
3.2.8.1.1.2	4.2.10 Functional View – Core Backup	4.2.10.3.2.3 Sign Messages
3.2.8.1.1.3	4.2.6 Functional View – Credentials Distribution	4.2.6.3.13 Provide Special Permissions
3.2.8.1.1.4	4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs
3.2.8.1.2.1	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.2	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.3	4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials
3.2.8.1.2.3	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.4	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials

SSR ID	Architecture View	Arch Object ID
3.2.8.1.2.7	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.8	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.9	4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate
3.2.8.1.2.10	4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate
3.2.8.1.2.11	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.12	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.13	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.2.14	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.3.1	4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate
3.2.8.1.3.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs
3.2.8.1.3.2	4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate
3.2.8.1.3.2	4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs
3.2.8.1.3.3	4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs
3.2.8.1.3.4	4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate
3.2.8.1.3.4	4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs
3.2.8.1.3.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.8.1.3.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.14 System User Register to Receive CRL
3.2.8.1.3.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.8.1.3.7	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.8.1.3.8	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.8.1.3.9	4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL
3.2.8.1.4.1	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.8.1.4.2	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key

SSR ID	Architecture View	Arch Object ID
3.2.8.1.4.3	4.2.8 Functional View – Core Decryption	4.2.8.3.2 Service Component
3.2.8.1.4.3	4.2.8 Functional View – Core Decryption	4.2.8.3.5 Decrypt Locally Encrypted Message
3.2.8.1.4.3	4.2.8 Functional View – Core Decryption	4.2.8.3.6 Maintain Core Local Key
3.2.8.1.4.3	4.2.8 Functional View – Core Decryption	4.2.8.3.7 Maintain Core Private Key
3.2.8.1.4.3	4.2.8 Functional View – Core Decryption	4.2.8.3.9 Provide Encrypted Message to Decryptor
3.2.8.1.4.4	4.2.8 Functional View – Core Decryption	4.2.8.3.2 Service Component
3.2.8.1.4.4	4.2.8 Functional View – Core Decryption	4.2.8.3.5 Decrypt Locally Encrypted Message
3.2.8.1.4.4	4.2.8 Functional View – Core Decryption	4.2.8.3.6 Maintain Core Local Key
3.2.8.1.4.4	4.2.8 Functional View – Core Decryption	4.2.8.3.7 Maintain Core Private Key
3.2.8.1.4.4	4.2.8 Functional View – Core Decryption	4.2.8.3.9 Provide Encrypted Message to Decryptor
3.2.8.1.4.5	4.2.2 Functional View – Data Distribution	4.2.2.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.3 Functional View – System Configuration	4.2.3.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.4 Functional View – User Configuration	4.2.4.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.8 Functional View – Core Decryption	4.2.8.3.1.2 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.8 Functional View – Core Decryption	4.2.8.3.3 Decrypt Message Received Encrypted
3.2.8.1.4.5	4.2.9 Functional View – Networking	4.2.9.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.5	4.2.10 Functional View – Core Backup	4.2.10.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.2 Functional View – Data Distribution	4.2.2.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.3 Functional View – System Configuration	4.2.3.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.4 Functional View – User Configuration	4.2.4.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.4 Verify Authenticity of Received Messages

SSR ID	Architecture View	Arch Object ID
3.2.8.1.4.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.8.1.4.6	4.2.8 Functional View – Core Decryption	4.2.8.3.1.2 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports
3.2.8.1.4.6	4.2.8 Functional View – Core Decryption	4.2.8.3.8 Notify Misbehavior of Failed Decryption
3.2.8.1.4.6	4.2.9 Functional View – Networking	4.2.9.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.6	4.2.10 Functional View – Core Backup	4.2.10.3.2.4 Verify Authenticity of Received Messages
3.2.8.1.4.7	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.8.1.4.8	4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports
3.2.8.1.4.8	4.2.8 Functional View – Core Decryption	4.2.8.3.8 Notify Misbehavior of Failed Decryption
3.2.8.1.5.1	4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key
3.2.8.1.5.2	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.5.3	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.8.1.5.3	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.8.1.5.3	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.8.1.5.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.8.1.5.3	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.8.1.5.3	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.8.1.5.3	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.8.1.5.4	4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions
3.2.8.1.5.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.5.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials
3.2.8.1.5.7	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.8.1.5.8	4.2.7 Functional View – Misbehavior Management	4.2.7.3.12 Manage CRL

SSR ID	Architecture View	Arch Object ID
3.2.8.1.5.9	4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials
3.2.8.1.5.10	4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission
3.2.8.1.5.10	4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission
3.2.8.1.5.10	4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission
3.2.8.1.5.10	4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission
3.2.8.1.5.10	4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission
3.2.8.1.5.10	4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission
3.2.8.1.5.10	4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission
3.2.8.1.5.11	4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration
3.2.8.1.5.12	4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores
3.2.8.1.5.13	4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data
3.2.8.1.5.13	4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up
3.2.8.1.5.14	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.6.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems
3.2.8.1.7.1	4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State
3.2.8.1.7.1	4.2.6 Functional View – Credentials Distribution	4.2.6.3.10 Modify UTM Operational State
3.2.8.1.7.1	4.2.7 Functional View – Misbehavior Management	4.2.7.3.16 Modify UTM Operational State
3.2.8.1.7.2	4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface
3.2.8.1.7.3	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.8.1.7.3	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.8.1.7.4	4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component
3.2.8.1.7.4	4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component
3.2.8.1.7.5	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.1.7.6	4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials
3.2.8.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component
3.2.8.2.1	4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface

SSR ID	Architecture View	Arch Object ID
3.2.8.2.1	4.2.6 Functional View – Credentials Distribution	4.2.6.3.12 Provide Operator Interface to UTM
3.2.8.2.1	4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface
3.2.8.2.2	4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects
3.2.8.2.2	4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem

6.2.2 Architecture to Subsystem Requirements Traceability

The table below is a mapping between Architecture Views, their Objects and the Subsystem Requirements.

Table 6-6. Architecture View/Object to Subsystem Requirement Traceability

View ID	Arch Object ID	SSR ID
4.2.2 Functional View – Data Distribution	4.2.2.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.2 Functional View – Data Distribution	4.2.2.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.2 Functional View – Data Distribution	4.2.2.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.2 Functional View – Data Distribution	4.2.2.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.2 Functional View – Data Distribution	4.2.2.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.2 Functional View – Data Distribution	4.2.2.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.2 Functional View – Data Distribution	4.2.2.3.3 Aggregate Data	3.2.2.1.3.1
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.1.1.17
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.1.1.58
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.2.1.2.14
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.2.1.2.15
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.2.1.2.19
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.3.1.5
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.3.1.12
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.3.1.20
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.3.1.21
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.4.1.6
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.4.1.9
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.5.1.1.12
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.6.1.6
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.6.1.8
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.7.1.13
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.7.1.14
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.7.1.15
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.7.1.16
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.8.1.5.3
4.2.2 Functional View – Data Distribution	4.2.2.3.4 Check User Permission	3.2.8.1.5.10
4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages	3.2.2.1.4.1
4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages	3.2.2.1.4.2
4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages	3.2.2.1.4.3
4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages	3.2.2.1.4.4
4.2.2 Functional View – Data Distribution	4.2.2.3.9 Manage Geo-cast Messages	3.2.2.1.6.7
4.2.2 Functional View – Data Distribution	4.2.2.3.10 Match Data to Data Subscribers	3.2.2.1.2.9
4.2.2 Functional View – Data Distribution	4.2.2.3.12 Modify DD Operational State	3.2.2.1.6.1
4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data	3.2.2.1.2.11

View ID	Arch Object ID	SSR ID
4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data	3.2.2.1.2.12
4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data	3.2.2.1.2.13
4.2.2 Functional View – Data Distribution	4.2.2.3.13 Parse Data	3.2.2.1.3.2
4.2.2 Functional View – Data Distribution	4.2.2.3.14 Provide Data to Subscribing System Users	3.2.2.1.2.13
4.2.2 Functional View – Data Distribution	4.2.2.3.15 Provide Operator Interface to DD	3.2.2.2.1
4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users	3.2.2.1.2.9
4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users	3.2.2.1.2.11
4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users	3.2.2.1.2.12
4.2.2 Functional View – Data Distribution	4.2.2.3.16 Receive Data from System Users	3.2.2.1.2.13
4.2.2 Functional View – Data Distribution	4.2.2.3.17 Repackage Data	3.2.2.1.3.1
4.2.2 Functional View – Data Distribution	4.2.2.3.17 Repackage Data	3.2.2.1.3.2
4.2.2 Functional View – Data Distribution	4.2.2.3.17 Repackage Data	3.2.2.1.3.3
4.2.2 Functional View – Data Distribution	4.2.2.3.18 Sample Data	3.2.2.1.3.3
4.2.3 Functional View – System Configuration	4.2.3.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.3 Functional View – System Configuration	4.2.3.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.3 Functional View – System Configuration	4.2.3.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.3 Functional View – System Configuration	4.2.3.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.3 Functional View – System Configuration	4.2.3.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.3 Functional View – System Configuration	4.2.3.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.1.1.17
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.1.1.58
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.2.1.2.14
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.2.1.2.15
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.2.1.2.19
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.3.1.5
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.3.1.12
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.4.1.6
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.4.1.9
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.5.1.1.12
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.6.1.6
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.6.1.8
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.7.1.13
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.7.1.14
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.7.1.15
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.7.1.16
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.8.1.5.3
4.2.3 Functional View – System Configuration	4.2.3.3.3 Check User Permission	3.2.8.1.5.10
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.1.2.4
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.2.2.2

View ID	Arch Object ID	SSR ID
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.3.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.4.2.4
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.5.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.6.2.3
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.7.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.4 Configure [Subsystem] Objects	3.2.8.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.1.1.28
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.1.1.29
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.1.1.33
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.1.1.34
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.2.1.2.17
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.3.1.10
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.4.1.4
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.5.1.1.9
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.7.1.25
4.2.3 Functional View – System Configuration	4.2.3.3.6 Exchange Configuration Info with Other Cores	3.2.8.1.5.12
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.1.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.2.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.3.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.4.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.5.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.6.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.7.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.7 Generic [Subsystem] Component	3.2.8.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.8 Identify Core Conflicts	3.2.1.1.35
4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate	3.2.8.1.2.9
4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate	3.2.8.1.2.10
4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate	3.2.8.1.3.1
4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate	3.2.8.1.3.2
4.2.3 Functional View – System Configuration	4.2.3.3.9 Maintain Core X.509 Certificate	3.2.8.1.3.4
4.2.3 Functional View – System Configuration	4.2.3.3.10 Manually Modify Other Core Configs	3.2.1.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.1.2.1

View ID	Arch Object ID	SSR ID
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.1.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.2.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.3.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.4.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.5.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.6.2.2
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.7.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.12 Provide Operator Interface to [Subsystem] / Generic Subsystem Operator Interface	3.2.8.2.1
4.2.3 Functional View – System Configuration	4.2.3.3.13 Receive Core Conflict Info	3.2.1.1.36
4.2.4 Functional View – User Configuration	4.2.4.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.4 Functional View – User Configuration	4.2.4.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.1.1.17
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.1.1.58
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.2.1.2.14
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.2.1.2.15
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.2.1.2.19
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.3.1.5
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.3.1.12
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.4.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.4.1.9
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.5.1.1.12
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.6.1.6

View ID	Arch Object ID	SSR ID
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.6.1.8
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.7.1.13
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.7.1.14
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.7.1.15
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.7.1.16
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.8.1.5.3
4.2.4 Functional View – User Configuration	4.2.4.3.4 Check User Permission	3.2.8.1.5.10
4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information	3.2.2.1.2.7
4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information	3.2.2.1.2.8
4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information	3.2.2.1.2.10
4.2.4 Functional View – User Configuration	4.2.4.3.5 Configure Geo-cast Device Information	3.2.2.1.4.5
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.3
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.4
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.5
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.1.61
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.1.2.3
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.5.1.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.6 Core Register to Receive Status	3.2.5.1.1.13
4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core	3.2.1.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core	3.2.1.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core	3.2.1.1.3
4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core	3.2.1.1.4
4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core	3.2.1.1.5
4.2.4 Functional View – User Configuration	4.2.4.3.7 Core Register to Receive Status from Other Core	3.2.1.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.10 Generic Provide Operator Interface	3.2.6.2.2
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.2.1
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.2.2
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.2.3
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.2.4
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.2.5
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.2.6
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.6.6
4.2.4 Functional View – User Configuration	4.2.4.3.12 Manage Data Provision Requests	3.2.2.1.6.9
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.1

View ID	Arch Object ID	SSR ID
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.3
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.4
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.5
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.1.7
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.6.5
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.6.8
4.2.4 Functional View – User Configuration	4.2.4.3.13 Manage System User Data Subscriptions	3.2.2.1.6.10
4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions	3.2.7.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions	3.2.7.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions	3.2.7.1.3
4.2.4 Functional View – User Configuration	4.2.4.3.14 Manually Modify User Permissions	3.2.7.1.4
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.3.1.12.1
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.3.1.12.3
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.5
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.7
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.8
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.8.1
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.9
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.10
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.12
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.19
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.7.1.34
4.2.4 Functional View – User Configuration	4.2.4.3.16 Modify Application Permissions	3.2.8.1.5.4
4.2.4 Functional View – User Configuration	4.2.4.3.17 Modify Data Acceptance Catalog	3.2.2.1.2.4
4.2.4 Functional View – User Configuration	4.2.4.3.17 Modify Data Acceptance Catalog	3.2.2.1.2.6
4.2.4 Functional View – User Configuration	4.2.4.3.18 Modify DD Operational State	3.2.2.1.6.1
4.2.4 Functional View – User Configuration	4.2.4.3.19 Modify UP Operational State	3.2.7.1.36.1
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.3.1.12.2
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.3.1.12.3
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.7.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.7.1.2
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.7.1.3
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.7.1.3.1
4.2.4 Functional View – User Configuration	4.2.4.3.20 Modify User Permissions	3.2.7.1.4
4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status	3.2.3.1.6
4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status	3.2.5.1.1.1
4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status	3.2.7.1.27
4.2.4 Functional View – User Configuration	4.2.4.3.23 System User Register to Receive Status	3.2.7.1.28

View ID	Arch Object ID	SSR ID
4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.5 Functional View – System Monitor and Control	4.2.5.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.5 Functional View – System Monitor and Control	4.2.5.3.20 Take Action in Response to Environment Issue	3.2.5.1.3.5
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.1.1.17
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.1.1.58
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.2.1.2.14
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.2.1.2.15
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.2.1.2.19
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.3.1.5
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.3.1.12
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.4.1.6
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.4.1.9
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.5.1.1.12
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.6.1.6
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.6.1.8
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.7.1.13
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.7.1.14
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.7.1.15
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.7.1.16

View ID	Arch Object ID	SSR ID
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.8.1.5.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.3 Check User Permission	3.2.8.1.5.10
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.1.1.67.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.2.1.6.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.3.1.26.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.4.1.14.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.5.1.3.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.6.1.10.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.7.1.36.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.5 Generic Modify Subsystem Operational State	3.2.8.1.7.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.1.1.67.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.2.1.6.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.3.1.26.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.4.1.14.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.5.1.3.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.5.2.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.6.1.10.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.7.1.36.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.7.2.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.6 Generic Provide Operator Interface	3.2.8.1.7.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.1.1.67.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.1.1.67.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.2.1.6.3

View ID	Arch Object ID	SSR ID
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.2.1.6.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.3.1.26.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.3.1.26.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.4.1.14.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.4.1.14.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.5.1.3.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.5.1.3.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.6.1.9
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.6.1.10.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.6.1.10.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.7.1.36.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.7.1.36.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.8.1.7.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.7 Generic Service Component	3.2.8.1.7.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.8 Get Time from External Available Source	3.2.6.1.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.8 Get Time from External Available Source	3.2.6.1.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.8 Get Time from External Available Source	3.2.6.2.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.1.1.66.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.2.1.5.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.3.1.25.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.4.1.13.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.5.1.2.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.6.1.3

View ID	Arch Object ID	SSR ID
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.6.1.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.7.1.35.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.9 Make Time Available to All Subsystems	3.2.8.1.6.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.10 Modify SM Operational State	3.2.5.1.3.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.11 Modify TS Operational State	3.2.6.1.10.1
4.2.5 Functional View – System Monitor and Control	4.2.5.3.12 Monitor Core Health and Safety	3.2.5.1.3.5
4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance	3.2.4.1.8
4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance	3.2.5.1.1.5
4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance	3.2.5.1.1.15
4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance	3.2.5.1.3.6
4.2.5 Functional View – System Monitor and Control	4.2.5.3.13 Monitor Core Services Performance	3.2.5.2.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.1.1.12
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.1.1.13
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.1.1.14
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.1.1.15
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.1.1.16
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.1.1.60
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.5.1.1.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.5.1.1.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.14 Monitor Status of other Cores	3.2.5.1.1.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.15 Provide Record of System Performance	3.2.5.1.1.5
4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores	3.2.1.1.30
4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores	3.2.1.1.57

View ID	Arch Object ID	SSR ID
4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores	3.2.5.1.1.7
4.2.5 Functional View – System Monitor and Control	4.2.5.3.16 Provide Service Status to other Cores	3.2.5.1.1.11
4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users	3.2.1.1.57
4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users	3.2.5.1.1.2
4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users	3.2.5.1.1.3
4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users	3.2.5.1.1.4
4.2.5 Functional View – System Monitor and Control	4.2.5.3.17 Provide Service Status to System Users	3.2.5.1.1.7
4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.6 Functional View – Credentials Distribution	4.2.6.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.1.1.17
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.1.1.58
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.2.1.2.14
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.2.1.2.15
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.2.1.2.19
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.3.1.5
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.3.1.12
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.4.1.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.4.1.9
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.5.1.1.12
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.6.1.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.6.1.8
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.7.1.13
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.7.1.14
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.7.1.15
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.7.1.16
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.8.1.5.3
4.2.6 Functional View – Credentials Distribution	4.2.6.3.4 Check User Permission	3.2.8.1.5.10
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.18
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.19
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.20

View ID	Arch Object ID	SSR ID
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.21
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.22
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.23
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.24
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.25
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.26
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.1.1.27
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.8.1.3.5
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.8.1.3.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.8.1.3.7
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.8.1.3.8
4.2.6 Functional View – Credentials Distribution	4.2.6.3.7 Distribute CRL	3.2.8.1.3.9
4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials	3.2.7.1.22
4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials	3.2.7.1.23
4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials	3.2.7.1.23
4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials	3.2.8.1.2.3
4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials	3.2.8.1.5.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.8 Maintain Credentials	3.2.8.1.5.9
4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions	3.2.7.1.1
4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions	3.2.7.1.2
4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions	3.2.7.1.3
4.2.6 Functional View – Credentials Distribution	4.2.6.3.9 Modify User Permissions	3.2.7.1.4
4.2.6 Functional View – Credentials Distribution	4.2.6.3.10 Modify UTM Operational State	3.2.8.1.7.1
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.7.1.20
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.7.1.21
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.7.1.21
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.7.1.33
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.1
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.2
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.3
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.4
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.5
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.7
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.8
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.11
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.12
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.13
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.2.14
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.5.2
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.5.5
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.5.14

View ID	Arch Object ID	SSR ID
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.7.5
4.2.6 Functional View – Credentials Distribution	4.2.6.3.11 Provide Credentials	3.2.8.1.7.6
4.2.6 Functional View – Credentials Distribution	4.2.6.3.12 Provide Operator Interface to UTM	3.2.8.2.1
4.2.6 Functional View – Credentials Distribution	4.2.6.3.13 Provide Special Permissions	3.2.8.1.1.3
4.2.6 Functional View – Credentials Distribution	4.2.6.3.14 System User Register to Receive CRL	3.2.8.1.3.5
4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.7 Functional View – Misbehavior Management	4.2.7.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.7 Functional View – Misbehavior Management	4.2.7.3.20 Provide Operator Interface to MM	3.2.3.2.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.3.1.19
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.3.1.22
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.3.1.23
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.7.1.29
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.8.1.4.6
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.8.1.4.7
4.2.7 Functional View – Misbehavior Management	4.2.7.3.21 Receive Internal Misbehavior Reports	3.2.8.1.4.8
4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports	3.2.3.1.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports	3.2.3.1.2
4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports	3.2.3.1.3
4.2.7 Functional View – Misbehavior Management	4.2.7.3.22 Receive System User Misbehavior Reports	3.2.3.1.4
4.2.7 Functional View – Misbehavior Management	4.2.7.3.23 Revoke Operator Permissions	3.2.3.1.8
4.2.7 Functional View – Misbehavior Management	4.2.7.3.23 Revoke Operator Permissions	3.2.7.1.18

View ID	Arch Object ID	SSR ID
4.2.7 Functional View – Misbehavior Management	4.2.7.3.24 Revoke User Permissions	3.2.3.1.7
4.2.7 Functional View – Misbehavior Management	4.2.7.3.24 Revoke User Permissions	3.2.7.1.17
4.2.7 Functional View – Misbehavior Management	4.2.7.3.3 Ask CA to Revoke	3.2.3.1.7
4.2.7 Functional View – Misbehavior Management	4.2.7.3.3 Ask CA to Revoke	3.2.7.1.17
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.1.1.17
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.1.1.58
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.2.1.2.14
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.2.1.2.15
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.2.1.2.19
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.3.1.5
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.3.1.12
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.4.1.6
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.4.1.9
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.5.1.1.12
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.6.1.6
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.6.1.8
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.7.1.13
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.7.1.14
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.7.1.15
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.7.1.16
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.8.1.5.3
4.2.7 Functional View – Misbehavior Management	4.2.7.3.4 Check User Permission	3.2.8.1.5.10
4.2.7 Functional View – Misbehavior Management	4.2.7.3.6 Disable Misbehaving Geo-Cast Device	3.2.2.1.4.5

View ID	Arch Object ID	SSR ID
4.2.7 Functional View – Misbehavior Management	4.2.7.3.6 Disable Misbehaving Geo-Cast Device	3.2.3.1.13
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.18
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.19
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.20
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.21
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.22
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.23
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.24
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.25
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.26
4.2.7 Functional View – Misbehavior Management	4.2.7.3.7 Exchange CRLs with other Cores	3.2.1.1.27
4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores	3.2.1.1.7
4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores	3.2.1.1.8
4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores	3.2.1.1.9
4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores	3.2.1.1.10
4.2.7 Functional View – Misbehavior Management	4.2.7.3.8 Exchange Misbehavior Reports with other Cores	3.2.1.1.11
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.3.1.5
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.3.1.15
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.3.1.16
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.3.1.18
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.3.1.19
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.3.1.24
4.2.7 Functional View – Misbehavior Management	4.2.7.3.10 Identify Misbehaving Operators	3.2.7.1.30

View ID	Arch Object ID	SSR ID
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.2.1.2.22
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.2.1.4.6
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.2
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.3
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.4
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.15
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.16
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.18
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.3.1.19
4.2.7 Functional View – Misbehavior Management	4.2.7.3.11 Identify Misbehaving System Users	3.2.7.1.31
4.2.7 Functional View – Misbehavior Management	4.2.7.3.12 Manage CRL	3.2.8.1.5.8
4.2.7 Functional View – Misbehavior Management	4.2.7.3.14 Modify C2C Operational State	3.2.1.1.67.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.15 Modify MM Operational State	3.2.3.1.26.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.16 Modify UTM Operational State	3.2.8.1.7.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions	3.2.7.1.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions	3.2.7.1.2
4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions	3.2.7.1.3
4.2.7 Functional View – Misbehavior Management	4.2.7.3.17 Modify User Permissions	3.2.7.1.4
4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs	3.2.8.1.1.4
4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs	3.2.8.1.3.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs	3.2.8.1.3.2
4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs	3.2.8.1.3.3

View ID	Arch Object ID	SSR ID
4.2.7 Functional View – Misbehavior Management	4.2.7.3.18 Obtain CRLs	3.2.8.1.3.4
4.2.7 Functional View – Misbehavior Management	4.2.7.3.19 Provide Operator Interface to C2C	3.2.1.2.1
4.2.7 Functional View – Misbehavior Management	4.2.7.3.19 Provide Operator Interface to C2C	3.2.1.2.2
4.2.8 Functional View – Core Decryption	4.2.8.3.1.2 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.8 Functional View – Core Decryption	4.2.8.3.1.2 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.8 Functional View – Core Decryption	4.2.8.3.1.2 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.8 Functional View – Core Decryption	4.2.8.3.2 Service Component	3.2.8.1.4.3
4.2.8 Functional View – Core Decryption	4.2.8.3.2 Service Component	3.2.8.1.4.4
4.2.8 Functional View – Core Decryption	4.2.8.3.3 Decrypt Message Received Encrypted	3.2.8.1.4.5
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.1.1.59
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.2.1.2.21
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.4.1.7
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.5.1.1.16
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.6.1.7
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.7.1.32
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.8.1.4.1
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.8.1.4.2
4.2.8 Functional View – Core Decryption	4.2.8.3.4 Encrypt Message Using Core Local Key	3.2.8.1.5.1
4.2.8 Functional View – Core Decryption	4.2.8.3.5 Decrypt Locally Encrypted Message	3.2.8.1.4.3
4.2.8 Functional View – Core Decryption	4.2.8.3.5 Decrypt Locally Encrypted Message	3.2.8.1.4.4
4.2.8 Functional View – Core Decryption	4.2.8.3.6 Maintain Core Local Key	3.2.8.1.4.3
4.2.8 Functional View – Core Decryption	4.2.8.3.6 Maintain Core Local Key	3.2.8.1.4.4
4.2.8 Functional View – Core Decryption	4.2.8.3.7 Maintain Core Private Key	3.2.8.1.4.3
4.2.8 Functional View – Core Decryption	4.2.8.3.7 Maintain Core Private Key	3.2.8.1.4.4
4.2.8 Functional View – Core Decryption	4.2.8.3.8 Notify Misbehavior of Failed Decryption	3.2.8.1.4.6
4.2.8 Functional View – Core Decryption	4.2.8.3.8 Notify Misbehavior of Failed Decryption	3.2.8.1.4.8
4.2.8 Functional View – Core Decryption	4.2.8.3.9 Provide Encrypted Message to Decryptor	3.2.8.1.4.3
4.2.8 Functional View – Core Decryption	4.2.8.3.9 Provide Encrypted Message to Decryptor	3.2.8.1.4.4
4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports	3.2.3.1.19
4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports	3.2.3.1.22
4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports	3.2.3.1.23
4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports	3.2.7.1.29
4.2.8 Functional View – Core Decryption	4.2.8.3.10 Receive Internal Misbehavior Reports	3.2.8.1.4.6
4.2.9 Functional View – Networking	4.2.9.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.9 Functional View – Networking	4.2.9.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.9 Functional View – Networking	4.2.9.3.2.3 Sign Messages	3.2.8.1.1.2

View ID	Arch Object ID	SSR ID
4.2.9 Functional View – Networking	4.2.9.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1
4.2.9 Functional View – Networking	4.2.9.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.9 Functional View – Networking	4.2.9.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.1.1.67.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.1.1.67.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.2.1.6.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.2.1.6.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.3.1.26.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.3.1.26.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.4.1.14.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.4.1.14.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.5.1.3.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.5.1.3.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.6.1.10.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.6.1.10.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.7.1.36.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.7.1.36.4
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.8.1.7.3
4.2.9 Functional View – Networking	4.2.9.3.3 Generic Service Component	3.2.8.1.7.4
4.2.9 Functional View – Networking	4.2.9.3.4 Intrusion Detection	3.2.3.1.17
4.2.9 Functional View – Networking	4.2.9.3.4 Intrusion Detection	3.2.4.1.12.2
4.2.9 Functional View – Networking	4.2.9.3.5 Intrusion Prevention	3.2.4.1.12.1
4.2.9 Functional View – Networking	4.2.9.3.7 Modify NS Operational State	3.2.4.1.14.1
4.2.9 Functional View – Networking	4.2.9.3.8 Monitor Service Control Node Performance	3.2.4.1.8
4.2.9 Functional View – Networking	4.2.9.3.8 Monitor Service Control Node Performance	3.2.5.1.3.6
4.2.9 Functional View – Networking	4.2.9.3.9 Provide Internet Connectivity	3.2.4.1.11
4.2.9 Functional View – Networking	4.2.9.3.9 Provide Internet Connectivity	3.2.4.2.2
4.2.9 Functional View – Networking	4.2.9.3.10 Provide Private Network Connectivity	3.2.4.1.11
4.2.9 Functional View – Networking	4.2.9.3.10 Provide Private Network Connectivity	3.2.4.2.3
4.2.9 Functional View – Networking	4.2.9.3.11 Provide Operator Interface to NS	3.2.4.2.1
4.2.9 Functional View – Networking	4.2.9.3.12 Route Data between Networks	3.2.4.1.10
4.2.9 Functional View – Networking	4.2.9.3.13 Route Data/Request	3.2.4.1.10
4.2.10 Functional View – Core Backup	4.2.10.3.2.1 Decrypt Messages Received Encrypted	3.2.4.1.1
4.2.10 Functional View – Core Backup	4.2.10.3.2.2 Encrypt Messages	3.2.4.1.2
4.2.10 Functional View – Core Backup	4.2.10.3.2.3 Sign Messages	3.2.8.1.1.2
4.2.10 Functional View – Core Backup	4.2.10.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.1.1

View ID	Arch Object ID	SSR ID
4.2.10 Functional View – Core Backup	4.2.10.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.5
4.2.10 Functional View – Core Backup	4.2.10.3.2.4 Verify Authenticity of Received Messages	3.2.8.1.4.6
4.2.10 Functional View – Core Backup	4.2.10.3.20 Provide Other Core Data	3.2.1.1.45
4.2.10 Functional View – Core Backup	4.2.10.3.20 Provide Other Core Data	3.2.1.1.46
4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up	3.2.2.1.2.18
4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up	3.2.3.1.11
4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up	3.2.4.1.5
4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up	3.2.5.1.1.10
4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up	3.2.7.1.26
4.2.10 Functional View – Core Backup	4.2.10.3.21 Provide Data to be Backed Up	3.2.8.1.5.13
4.2.10 Functional View – Core Backup	4.2.10.3.22 Request Core Takeover	3.2.1.1.50
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.39
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.40
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.41
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.42
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.43
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.44
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.45
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.46
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.47
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.48
4.2.10 Functional View – Core Backup	4.2.10.3.3 Backup Other Core Data	3.2.1.1.49
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.1.1.17
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.1.1.58
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.2.1.2.14
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.2.1.2.15
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.2.1.2.19
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.3.1.5
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.3.1.12
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.4.1.6
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.4.1.9
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.5.1.1.12
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.6.1.6
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.6.1.8
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.7.1.13
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.7.1.14
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.7.1.15
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.7.1.16
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.8.1.5.3
4.2.10 Functional View – Core Backup	4.2.10.3.4 Check User Permission	3.2.8.1.5.10

View ID	Arch Object ID	SSR ID
4.2.10 Functional View – Core Backup	4.2.10.3.5 Configure Geo-cast Device Information	3.2.2.1.2.9
4.2.10 Functional View – Core Backup	4.2.10.3.5 Configure Geo-cast Device Information	3.2.2.1.2.10
4.2.10 Functional View – Core Backup	4.2.10.3.6 Core Takeover	3.2.1.1.51
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.1.2.4
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.2.2.2
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.3.2.2
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.4.2.4
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.5.2.2
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.6.2.3
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.7.2.2
4.2.10 Functional View – Core Backup	4.2.10.3.9 Generic Configure Subsystem	3.2.8.2.2
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.1.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.2.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.3.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.4.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.5.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.6.2.2
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.7.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.11 Generic Provide Operator Interface	3.2.8.2.1
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.1.1.31
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.1.1.32
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.2.1.2.16
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.3.1.9
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.4.1.3
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.5.1.1.8
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.7.1.24
4.2.10 Functional View – Core Backup	4.2.10.3.12 Generic Subsystem Configuration	3.2.8.1.5.11
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.37
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.38
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.52
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.53
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.54
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.55
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.1.1.56
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.2.1.2.18
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.2.1.2.20
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.3.1.11
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.3.1.14
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.4.1.5
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.5.1.1.10
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.5.1.1.14
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.6.1.5

View ID	Arch Object ID	SSR ID
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.7.1.11
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.7.1.26
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.8.1.5.7
4.2.10 Functional View – Core Backup	4.2.10.3.14 Get Backed Up Data	3.2.8.1.5.13
4.2.10 Functional View – Core Backup	4.2.10.3.15 Modify C2C Operational State	3.2.1.1.67.1
4.2.10 Functional View – Core Backup	4.2.10.3.16 Modify Data Acceptance Catalog	3.2.2.1.2.4
4.2.10 Functional View – Core Backup	4.2.10.3.17 Modify System User Data Subscriptions	3.2.2.1.1.1
4.2.10 Functional View – Core Backup	4.2.10.3.17 Modify System User Data Subscriptions	3.2.2.1.1.4
4.2.10 Functional View – Core Backup	4.2.10.3.17 Modify System User Data Subscriptions	3.2.2.1.1.6
4.2.10 Functional View – Core Backup	4.2.10.3.18 Monitor Core Services Performance	3.2.4.1.8
4.2.10 Functional View – Core Backup	4.2.10.3.18 Monitor Core Services Performance	3.2.5.1.3.6

6.2.3 System Requirements to Architecture Traceability

Virtually all of the System Requirements map to one or more Subsystem Requirements. The next table shows the architecture mapping for those non-functional requirements and one constraint that did not have any subsystem requirements.

Table 6-7. System Requirement to Architecture Object Traceability

SR ID	Arch Object ID	View ID
3.1.4.1.1	Monitor Core Health and Safety	4.2.5 System Monitor and Control
3.1.4.2.1	Monitor Core Health and Safety	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.4.2.2	Monitor Core Health and Safety	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.4.2.3	Monitor Core Health and Safety	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.4.2.4	Monitor Core Health and Safety	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.4.2.5	Monitor Core Health and Safety	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.4.3.1	Monitor Core Health and Safety	4.2.5 System Monitor and Control
3.1.4.3.2	Monitor Core Health and Safety	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.4.3.3	Monitor Core Physical Security	4.2.5 System Monitor and Control
	Take Action in Response to Environment Issue	4.2.5 System Monitor and Control
3.1.5.1	User Permission Registry	4.2.5 System Monitor and Control
	Data Subscription Catalog	4.2.2 Data Distribution

7 Terminology

This section includes definition of key terms and a list of Abbreviations and Acronyms used in this document.

7.1 Glossary

Table 7-1. Glossary

Term	Definition
Access Control	Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.
Administrator	These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.
Analysis	The process of studying a system by partitioning the system into parts (functions, components, or objects) and determining how the parts relate to each other.
Anonymity	Lacking individuality, distinction, and recognizability within message exchanges.
Anonymous Certificates	A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the *connected vehicle* program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
Application	One or more pieces of software designed to perform some specific function; it is a configuration of interacting Engineering Objects. A computer software program with an interface, enabling people to use a computer as a tool to accomplish a specific task.
Application User	One who interfaces with Application Layer-based software for a function or feature.
Authentication	The process of determining the identity of a user that is attempting to access a network.
Authenticity	The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source.

Term	**Definition**
Authorization	The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.
Assumption	A judgment about unknown factors and the future which is made in analyzing alternative courses of action.
Aggregation	The process of combining data elements of similar format into a single data element that is a statistical representation of the original elements.
Available	Ready or able to be used
Back Office	See Center.
Backup	The ability of one Core System replacing another Core System’s functionality (including Core Services) upon a system failure.
Bad Actor	A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope.
Boundaries	The area of management and control for a Core System. It could be by latitude/longitude or by county or by regional jurisdictions.
Catalog	Used by the Data Distribution Subsystem as a repository for maintaining data publishers information including the type of data they are transmitting, frequency of that data, address, data source, etc.
Center	An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms “back office” and “center” are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of the Core System ConOps these are considered the same.
Class of Service (CoS)	Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority.
Commanded	When a privileged System Operator has initiated an instruction to execute a software or hardware action.
Compatibility issues	Conflict with two Core Systems, such as different Core System software versions that aren’t compatible.

Term **Definition**

Concept of Operations (ConOps)
A user-oriented document that describes a system's operational characteristics from the end user's viewpoint.

Configure
The process of selecting from a set of option(s) or alternative values in order to create a custom system.

Configuration
Data that is used to customizes the environment for a user, program, application or hardware item.

Constraint
An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.

Contract
In project management, a legally binding document agreed upon by the customer and the hardware or software developer or supplier; includes the technical, organizational, cost, and/or scheduling requirements of a project.

Control
To exercise influence over.

Coordinate coverage
When two Core System boundaries are near or overlapping, there needs to be an agreement between the two Core Systems who should be the one to provide coverage.

Coordinated Universal Time (UTC)
The primary time standard by which the world regulates clocks and time. UTC serves to accommodate the timekeeping differences that arise between atomic time (which is derived from atomic clocks) and solar time (which is derived from astronomical measurements of the Earth's rotation on its axis relative to the Sun). Since Jan. 1, 1972, UTC has been modified by adding "leap seconds" when necessary.

Core Services
A set of functions within the Core System subsystems that interact with System Users.

Core System Personnel-controlled rules
The conditions to identify misbehavior activity, including the need to revoke credentials from such reported misbehaving users.

Core System Personnel
This represents the staff that operates and maintains the Core System. In addition to network managers and operations personnel, Core System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployers and Testers.

Core System User
See System User.

Correlation processing
To process data for misbehavior pattern matching and to look for signatures of known misbehavior users.

Coverage Area
A geographic jurisdiction within which a Core System provides Core Services.

Term	**Definition**
Critical Failure	When the Core System's Core Services do not operate as expected or their overall performance is sub-optimal.
Data Acceptance Criteria	Criteria describing the data a Core System accepts as part of Data Distribution. Includes data type, source type, location, and time criteria.
Data Consumer	A user or system that is receiving or using data from another user or system.
Data Provider	A System User that is supplying or transmitting data to another user or system. A data provider is likely to be an aggregator of data.
Data Provisioning	The act of a System User providing data to a consumer.
Decrypt	To decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access. See Encryption.
Degraded Mode	In the degraded mode, the subsystem is impaired to a significant extent: its ability to provide services is greatly reduced or eliminated completely. Also, Service Monitor's ability to manage the subsystem may be impaired.
Degraded/Restricted Mode	If during the course of operating in a restricted mode there is a loss of functionality, or if while in degraded mode there is a need to enter restricted mode, the subsystem may enter the degraded/restricted mode. This mode is a combination of the restricted and degraded modes, where subsystem services are offered only to particular users, but performance is degraded.
Delta updates	Only the data that is new since the last block of data that was downloaded.
Denial of Service (DoS) attack	An explicit attempt by an attacker to prevent legitimate users of that system from accessing information or services. Examples include flooding the network with useless messages or attempting an overflow condition.
Deployability	Able to be deployed in existing roadway environments, without requiring replacement of existing systems in order to provide measurable improvements.
Deployers	These users represent the initial installers for a Core System. Their interaction with the Core System itself will be similar to an administrator or maintainer in that they will be accessing system configuration files, setting parameters and policies as part of the initial installation and check out of the system before turning it over to the other Core System Personnel for regular operations.
Desirable features	Features that should be provided by the Core System.

Term	**Definition**
Developers	These users are the actual software developers that build software enhancements for the system. They will be accessing the published interface definitions and configuration data about the Core System in order to develop additional features or expanded capabilities.
Digital Certificate or Signature	A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Note: From the SysAdmin, Audit, Network, Security Institute - www.sans.org website.
DNS (Domain Name System)	The internet protocol for mapping host names, domain names and aliases to IP addresses.
Encryption	Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.
End-User	The ultimate user of a product or service, especially of a computer system, application, or network.
Environment	The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system must do or how it will do it.
Error Messages	Messages from Mobile Users that indicate issues with cross-jurisdictional compatibility, scope coverage service or service availability.
Essential features	Features that shall be provided by the Core System.
Extensibility	The ability to add or modify functionality or features with little or no design changes.
External source-to-point	When the data provider communicates data directly to data consumers. No data is sent through the Core System; however, the Core System is involved with checking user permissions and maintains provider addresses to consumers as part of its data catalog.
External Support System	An entity that provides a service the Core needs to deliver. This service is provided by the ESS because it makes more sense to manage, maintain and share the service between multiple Cores due to overriding institutional, performance or functional constraints.
Facility	A building or group of buildings housing a Core System with access restrictions.

Term	**Definition**
Faculty backup services	When failed services of a Core System has been backed up by another Core System that has those same services available.
Field	These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSE and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure.
Flexibility	The ability to adjust or adapt to external changes with little or no design changes.
Forwarding	The process of forward sending data onto another entity (system user) without modifying or storing the data for any substantial length of time.
Functionality	The capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product.
Geocast	The delivery of a message to a group of network destinations identified by their geographic locations.
Geo-Referencing	The process of scaling, rotating, translating and de-skewing the image to match a particular size and position. To define something in terms of its physical location in space.
Hardware	Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners.
Health of the Core System	The overall Core System’s operational condition. This includes not only errors and alerts from the system; but intermittent errors and slow performance conditions that may not currently degrade the system, but is not necessarily a healthy system. Intermittent and slow performance conditions can be mitigated before it does degrade the system.
Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Installation State	This state includes all pre-operational activities necessary to plan, develop, install and verify the procedures and system configurations used to support the Core System.

Term **Definition**

Integrity

To maintain a system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible.

Internet

An interconnected system of networks that connects computers around the world via the TCP/IP protocol.

Issuance

a) For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User’s real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA).

b) For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA).

Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.

Jurisdictional Scope

The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.

Link

A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.

Local Cache

Reserved areas of computer memory that are used to speed up instruction execution, data retrieval and data updating.

Logical Security

Safeguards that include user identification and password access, authentication, access rights and authority levels.

Maintainability

To keep in an existing operational state preserved from failure or decline of services (with minimum repair, efficiency, or validity).

Maintenance State

The administrator commands this state for a particular subsystem or to the whole Core System to replace an impaired component or to upgrade a component(s). Depending on the nature of maintenance planned, the impact on the Core System’s ability to provide services may be impacted. Also, its ability to manage itself and provide visibility into how it is performing may be impacted.

Maintainers

These users interact with the system to install updated software; repair or upgrade hardware components to keep the system up to date and running efficiently.

Term	**Definition**
Misbehavior	The act of providing false or misleading data, operating in such a fashion as to impede other users, or to operate outside of their authorized scope. This includes suspicions behavior as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages, etc; either purposeful or unintended.
Misbehavior Information	Includes Misbehavior Reports from System Users, as well as other improper System User acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages and other inappropriate System User behavior.
Misbehavior Report	Data from a System User identifying suspicious behavior from another System User that can be characterized as misbehavior.
Misbehaving user	A user who exhibits misbehavior.
Mobile	These are vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travelers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information.
Modes	Modes are typically phases within a State. Degraded Mode occurs automatically due to certain conditions. Such as, when in Operational State, there is an automatic transition to Degraded Mode because of a detected hardware failure. Modes are Normal, Degraded, Restricted and Degraded/Restricted.
Modifiable parameter	Non-static data that can be adjustable and updated when needed.
NIST Time	National Institute of Science and Technology (NIST) is the standard for Internet time using the Year, Month, Day, Hour, Minute, Second format. NIST adjusts and compensates for time zones and Daylight Savings Time.
Node	A Node is a physical hardware Engineering Object that is a run-time computational resource and generally has at least memory and processing capability. Run-time software Engineering Objects reside on nodes. A Node has some well-understood, possibly rapidly moving, location. A Node may be composed of two or more (sub) Nodes.
Normal Mode	In the normal mode, there is little or no functional or performance impacts on the ability of the subsystem to provide its services. In addition, the Service Monitor provides good visibility into how the subsystem is performing.

Term **Definition**

Open Standard

Is a standard that is publicly available and has various rights to use associated with it, and may also have various properties of how it was designed (e.g. open process). Open Standards may not mean open source. A true open source is typically free to both acquire and implement.

Operational State

This state includes all activities during the normal conduct of operations. This state also needs to be able to handle support for services from other Cores including fail-over and/or degraded services.

Optional features

Features that might be provided by the Core System.

On-Board Equipment (OBE)

Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment.

Operators

These are the day-to-day users of the Core System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.

Parsing

The process of splitting or breaking down aggregate data into relevant parts.

Persistent connection

A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received. This is opposite of Session-oriented Connection.

Permission

Authorization granted to do something. To the Core System, permissions are granted to System Users and Operators determining what actions they are allowed to take when interacting with the Core.

Physical Security

Safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information. This can include simply a locked door, badge access controls, or armed security guards.

Point of Service

The Core System which provides a “gatekeeping arrangement” to connected System Users with functions and capabilities.

Port

A Port is the physical element of a Node where a Link is connected. Nodes may have one or more Ports. Each Port may connect to one or more physical Ports on (sub) Nodes that are contained within the Node.

Term	**Definition**
Priority	A rank order of status, activities, or tasks. Priority is particularly important when resources are limited.
Privacy	From the VII Privacy Policies Framework: the respect for individual choices about, and control over an individual's personal information.
Private Network	A network belonging to a person, company or organization that uses a public network (usually the Internet) to connect its' remote sites or users together.
Privileged System Operator	A user that runs the day-to-day operations of the system and who has the permissions or rights to manage that system.
Problem domain	A set of similar problems that occur in an environment and lend themselves to common solutions.
Process	A series of actions, changes, or functions bringing about a result.
Public Key	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).
Registration characteristics	Attributes of the System User's enrollment process into the Core System. This would include the System User's role(s) and permission(s) that have been granted by the Core System.
Repackage Data	Data that is broken down for aggregation, parsing or sampling.
Registry	A repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.
Reliability	Providing consistent and dependable system output or results.
Request for Quotation (RFQ)	A request for services, research, or a product prepared by a customer and delivered to a contractor with the expectation that the contractor will respond with their proposed cost, schedule, and development approach.

Term	**Definition**
Restricted mode	In the restricted mode, the subsystem is capable of performing as expected; however certain services or features are disabled to support a specific event such as an evacuation. The restriction is determined by operators/entities outside of the system and subsequently implemented by the system in response to an authorized operation (command) from the external entity. This may also be implemented via a policy-based management system whereby policies (as specified by an authorized external entity) are automatically implemented by the Core System in response to detection of events, behaviors or performance thresholds. In a restricted mode, the Core System could curtail the use of particular subsystems to privileged users, such first responders and other emergency personnel.
Sampling	To process of selecting a subset of data as a representation of that data.
Scalability	The capable of being easily grown, expanded or upgraded upon demand without requiring a redesign.
Scenario	A step-by-step description of a series of events that may occur concurrently or sequentially.
Secure/Securely	Referring to storage, which consists of both logical and physical safeguards
Secure Storage	Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off.
Secure Transmission	To protect the transfer of confidential or sensitive data usually by encryption, Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS) or similar secure communications.
Session-oriented Connection	A connection between two networked devices that is established intermittently and to handle few requests thereafter. The connection is meant to be temporary lasting for minutes, hours, but likely not more than a day before it is closed. This is opposite of Persistent Connection.
Software	Software is a general term that describes computer programs. Terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software.
States	A distinct system setting in which the same user input will produce different results than it would in other settings. The Core System as a whole is always in one state. A state is typically commanded or placed in that state by an operator. States are Installation, Operational, Maintenance, Training, and Standby.

Term **Definition**

Standby

The Core System or subsystem operating in a Standby state will be providing backup to one or more other Cores or other Core subsystems. From the standby state the Core or subsystem may take over the functions of another Core or subsystem if required. When operating in Standby state, the Core or subsystem should be continually evaluated on its ability to switch-in and take provide services for the Core or subsystem it is supporting.

Status

Anomalies, actions, intermittent and other conditions used to inform the System Operator for reparation or maintenance.

Subsystem

An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.

Synchronization

the act or results of occurrence or operating at the same time or rate

System

(A) A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment.

(B) A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.

System Need

A capability that is identified and supported within the Core System to accomplish a specific goal or solve a problem

System User

System Users refers to Mobile, Field, and Center Systems.

Testers

These users verify the Core System’s operation when any changes are made to its operating hardware or software.

Time

A measurable period during which an action, process or condition occurs.

Time-of-Day

Current hours, minutes and seconds within a day.

Time synchronization

Calibration adjustment of date, hour, minutes and seconds for keeping the same time within a system.

Term	**Definition**
Traceability	The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test.
Training	The administrator commands this state when it is used for imparting training on the Core features. Certain features like real-time display of log messages and debug messages may be enabled in the Training state which may not otherwise be accessible under normal conditions.
Transition	A passage from one state, stage, subject, or place to another
Trust Credentials	A user's authentication information which determines permissions and/or allowed actions with a system and other users.
Unicast	The sending of a message to a single network destination identified by a unique address.
User	An entity that uses a computer, program, network, and related services of a hardware and/or software system. In the case of the Core System this includes System Users that refers to the combination of Mobile, Field, and Center based devices and applications. The term End User refers to the human user of the System User device. End Users do not interact directly with the Core System, but are referred to as the ultimate beneficiaries or participants in the *connected vehicle* environment.
User Classes	A category of user, typically with different user profiles and access rights to the system.
User Need	A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system.
Valid	When data values within a message are acceptable and logical (e.g., numbers fall within a range, numeric data are all digits).

7.2 Abbreviations and Acronyms

This section contains an alphabetical listing of abbreviations and acronyms used in this document.

Table 7-2. Abbreviation and Acronym List

Abbreviation or Acronym	**Definition**
AMS	Analysis, Modeling, and Simulation
AASHTO	American Association of State Highway and Transportation Officials
AMDS	Advisory Message Distribution Service
ANSI	American National Standards Institute
APTA	American Public Transportation Association
ASOS	Automated Surface Observing System
AWOS	Automated Weather Observing System
BAH	Booz Allen Hamilton
CA	Certification Authority
CALM	Communications Access for Land Mobile Standards
CAMP	Crash Avoidance Metrics Partnership
CCH	Control Channel (interval)
CCTV	Closed Circuit Television
CICAS	Cooperative Intersection Collision Avoidance Systems
CMP	Certificate Management Protocol
COM eSafety	Communications for eSafety
ConOps	Concept of Operations
COOPERS	Cooperative Systems for Intelligent Road Safety
COTS	Commercial off-the-shelf
CRL	Certification Revocation Lists
CVIS	Cooperative Vehicle Infrastructure System
CVO	Commercial Vehicles Operation
DCM	Data Capture Management
DGPS	Differential GPS
DMA	Dynamic Mobility Applications
DMS	Dynamic Message Signs

Abbreviation or Acronym	**Definition**
DNS	Domain Name System
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
EC	European Commission
EEBL	Emergency Electronic Break Light
ENOC	Enterprise Network Operations Center
ETSI	European Telecommunications Standards Institute
INCOSE	International Council on Systems Engineering
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FRAME	Framework Architecture Made for Europe
FTA	Federal Transit Administration
GADS	Green Action Decider System
GCS	Geocasting Service
GHz	Gigahertz
GIS	Geographical Information Systems
GPS	Global Positioning System
HIA	“Here I am” basic safety message
HOV	High Occupancy Vehicle
HRI	Highway Rail Intersection
ICM	Integrated Corridor Management
ID	Identifier or Identification
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INCOSE	International Council of Systems Engineers
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Standards Office
ISP	Internet Service Provider or Information Service Provider
IT	Information Technology

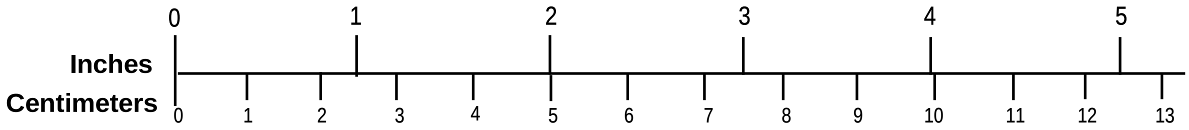
Abbreviation or Acronym	Definition
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
ITU	International Telecommunications Union
IVBSS	Integrated Vehicle-Based Safety Systems
JPO	Joint Program Office
LTE	Long Term Evolution
Mbps	Megabits per second
MIB	Management Information Base
NAVTEQ	Navigational Technology and Data Used to Develop Maps
NCAR	National Center for Atmospheric Research
NEMA	National Electrical Manufacturer’s Association
NIST	National Institute of Standards and Technology
NSR	National System Requirements
NTCIP	National Transportation Communication for ITS Protocol
OBE	Onboard Equipment
OBU	On Board Unit
OEM	Original Equipment Manufacturer
OSI	Open System Interconnection
PDS	Probe Data Service
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure based on X.509 certificates
PII	Personally Identifiable Information
POC	Proof of Concept
PMP	Project Management Plan
PMU	Private Mobile User
PSMU	Public Service Mobile User
QC	Quality Control
RA	Registration Authority
RFC	Request for Comments
RITA	Research and Innovative Technology Administration's

Abbreviation or Acronym	**Definition**
RSE	Roadside Equipment
RSU	Roadside Unit
SAE	Society of Automobile Engineers
SCH	Service Channel (interval)
SDN	Service Delivery Node
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SPAT	Signal Phase and Timing
SRS	Software Requirements Specification
stm	State Machine
SUV	Sport Utility Vehicle
SyRS	System Requirements Specification
TBD	To Be Determined
TC	Technical Committee
TIA	Telecommunications Industry Association
TMC	Transportation Management Center
TRSP	Traffic Responsive (Signal Control)
US	United States
USDOT	US Department of Transportation
USNO	US Naval Observatory
UTC	Coordinated Universal Time
VDT	Vehicle Data Translator
VII	Vehicle Infrastructure Integration
VIIC	Vehicle Infrastructure Integration Consortium
VMS	Variable Message Signal
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WAVE	Wireless Access in Vehicle Environment
WiMAX	Worldwide Interoperability for Microwave Access

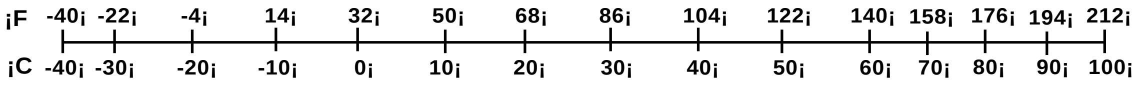
8 Metric/English Conversion Factors

ENGLISH TO METRIC			METRIC TO ENGLISH		
LENGTH (APPROXIMATE)			**LENGTH (APPROXIMATE)**		
1 inch (in)	=	2.5 centimeters (cm)	1 millimeter (mm)	=	0.04 inch (in)
1 foot (ft)	=	30 centimeters (cm)	1 centimeter (cm)	=	0.4 inch (in)
1 yard (yd)	=	0.9 meter (m)	1 meter (m)	=	3.3 feet (ft)
1 mile (mi)	=	1.6 kilometers (km)	1 meter (m)	=	1.1 yards (yd)
			1 kilometer (km)	=	0.6 mile (mi)
AREA (APPROXIMATE)			**AREA (APPROXIMATE)**		
1 square inch (sq in, in^2)	=	6.5 square centimeters (cm^2)	1 square centimeter (cm^2)	=	0.16 square inch (sq in, in^2)
1 square foot (sq ft, ft^2)	=	0.09 square meter (m^2)	1 square meter (m^2)	=	1.2 square yards (sq yd, yd^2)
1 square yard (sq yd, yd^2)	=	0.8 square meter (m^2)	1 square kilometer (km^2)	=	0.4 square mile (sq mi, mi^2)
1 square mile (sq mi, mi^2)	=	2.6 square kilometers (km^2)	10,000 square meters (m^2)	=	1 hectare (ha) = 2.5 acres
1 acre = 0.4 hectare (he)	=	4,000 square meters (m^2)			
MASS - WEIGHT (APPROXIMATE)			**MASS - WEIGHT (APPROXIMATE)**		
1 ounce (oz)	=	28 grams (gm)	1 gram (gm)	=	0.036 ounce (oz)
1 pound (lb)	=	0.45 kilogram (kg)	1 kilogram (kg)	=	2.2 pounds (lb)
1 short ton = 2,000 pounds (lb)	=	0.9 tonne (t)	1 tonne (t)	=	1,000 kilograms (kg)
				=	1.1 short tons
VOLUME (APPROXIMATE)			**VOLUME (APPROXIMATE)**		
1 teaspoon (tsp)	=	5 milliliters (ml)	1 milliliter (ml)	=	0.03 fluid ounce (fl oz)
1 tablespoon (tbsp)	=	15 milliliters (ml)	1 liter (l)	=	2.1 pints (pt)
1 fluid ounce (fl oz)	=	30 milliliters (ml)	1 liter (l)	=	1.06 quarts (qt)
1 cup (c)	=	0.24 liter (l)	1 liter (l)	=	0.26 gallon (gal)
1 pint (pt)	=	0.47 liter (l)			
1 quart (qt)	=	0.96 liter (l)			
1 gallon (gal)	=	3.8 liters (l)			
1 cubic foot (cu ft, ft^3)	=	0.03 cubic meter (m^3)	1 cubic meter (m^3)	=	36 cubic feet (cu ft, ft^3)
1 cubic yard (cu yd, yd^3)	=	0.76 cubic meter (m^3)	1 cubic meter (m^3)	=	1.3 cubic yards (cu yd, yd^3)
TEMPERATURE (EXACT)			**TEMPERATURE (EXACT)**		
[(x-32)(5/9)] °F	=	y °C	[(9/5) y + 32] °C	=	x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSIO



For more exact and or other conversion factors, see NIST Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50 SD Catalog No. C13 10286