

# Connected Vehicle Pilot Deployment Program Phase 1

## Security Management Operating Concept – New York City

[www.its.dot.gov/index.htm](http://www.its.dot.gov/index.htm)

**Final Report — May 18, 2016**

**FHWA-JPO-16-300**



U.S. Department of Transportation

Produced by New York City Connected Vehicle Pilot Deployment Program, Phase 1  
New York City Department of Transportation  
U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation Systems Joint Program Office

## 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.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

---

Cover photo courtesy of ITS JPO Resources, Connected Vehicle Basics 2016

## Technical Report Documentation Page

<b>1. Report No.</b> <b>FHWA-JPO-16-300</b>	<b>2. Government Accession No.</b>	<b>3. Recipient's Catalog No.</b>	
<b>4. Title and Subtitle</b> Connected Vehicle Pilot Deployment Program Phase 1, Security Management Operating Concept - New York City		<b>5. Report Date</b> May 18 <sup>th</sup> , 2016	<b>6. Performing Organization Code</b>
		<b>8. Performing Organization Report No.</b>	
<b>7. Author(s)</b> Steve Galgano, NYCDOT; Mohamad Talas, NYCDOT; William Whyte, Security Innovation; Jonathan Petit, Security Innovation; David Benevelli, TransCore, Robert Rausch, TransCore, Samuel Sim, TransCore		<b>10. Work Unit No. (TRAIS)</b>	
<b>9. Performing Organization Name And Address</b> New York City Department of Transportation (NYCDOT) Bureau of Traffic Operations 34-02 Queens Boulevard Long Island City, NY 11101		<b>11. Contract or Grant No.</b> DTFH6115C00036	
		<b>13. Type of Report and Period Covered</b> Final Security Management Operating Concept	
<b>12. Sponsoring Agency Name and Address</b> U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590		<b>14. Sponsoring Agency Code</b>	
		<b>15. Supplementary Notes</b> Program Manager: Kate Hartman Contracting Officer's Representative (COR): Jonathan Walker	
<b>16. Abstract</b> This document describes the Security Management Operating Concept (SMOC) for the New York City Department of Transportation (NYCDOT) Connected Vehicle Pilot Deployment (CVPD) Project. This SMOC outlines the security mechanisms that will be used to protect information flows within NYC CVPD, additional practices to protect privacy and security of data at rest, and management processes and procedures to ensure that security operations are carried out in a reliable and trustworthy way. This SMOC is one of the documents due for The Connected Vehicle Pilot Deployment Program, Phase 1 project funded by the United States Department of Transportation (USDOT)			
<b>17. Key Words</b> connected vehicles, DSRC, V2V, V2I, safety, security, security management, Security Management Operating Concept, New York City		<b>18. Distribution Statement</b>	
<b>19. Security Classif. (of this report)</b> Unclassified	<b>20. Security Classif. (of this page)</b> Unclassified	<b>21. No. of Pages</b> 156	<b>22. Price</b>

# Acknowledgements

The SMOC development team would like to thank the Tampa and Wyoming CV Pilot teams, for discussion and assistance on several sections of this document. The team would also like to thank everyone who reviewed this document, as well as everyone who participated in the cross-team working session. We acknowledge the timely and high-quality support offered by U.S. DOT, and the support contractor Noblis.

# Table of Contents

<b>Executive Summary .....</b>	<b>1</b>
<b>Chapter 1. Introduction .....</b>	<b>2</b>
1.1 General .....	2
1.2 Identification .....	3
1.3 Scope: Privacy and Security Objectives within NYC CVPD.....	3
1.3.1 Communications Security Objectives .....	3
1.3.2 Device Security Objectives.....	3
1.3.3 Privacy Objectives .....	3
1.4 Approach and Organization of this Document.....	4
1.4.1 General .....	4
1.4.2 SMOC Approach .....	5
1.4.3 CV Pilot Team Coordination.....	5
1.5 SMOC Limitations.....	6
<b>Chapter 2. System Overview.....</b>	<b>7</b>
2.1 Overview of the New York City Connected Vehicle Pilot Deployment .....	7
2.2 Types of View .....	10
2.3 Enterprise View .....	11
2.4 Network Architecture .....	12
2.5 Device Types and Interfaces .....	14
2.5.1 Aftermarket Safety Device (ASD).....	14
2.5.2 Personal Information Device (PID).....	15
2.6 Information Security Personnel .....	15
<b>Chapter 3. Security and Privacy Requirements for Usage Scenarios:     Information Flows and Device Classes.....</b>	<b>17</b>
3.1 Introduction .....	17
3.2 Existing CV Applications: BSM-based Safety .....	19
3.2.1 Overview.....	19
3.2.2 Information Flow Analysis.....	19
3.2.3 Device Classes.....	19
3.2.4 Additional Privacy Considerations.....	20
3.3 Existing CV Applications: Red Light Violation Warning.....	20
3.3.1 Overview.....	20
3.3.2 Information Flow Analysis.....	21
3.3.3 Device Classes.....	25
3.3.4 Additional Privacy Considerations.....	25
3.4 Traffic Manager: Speed Compliance / Speed Compliance in Work Zones / Curve Speed Compliance.....	25
3.4.1 Overview.....	25
3.4.2 Information Flow Analysis.....	26

3.4.3	Device Classes .....	28
3.4.4	Additional Privacy Considerations .....	28
3.5	Traffic Manager: Oversize Vehicle Compliance .....	28
3.5.1	Overview .....	28
3.5.2	Information Flow Analysis .....	29
3.5.3	Device Classes .....	30
3.5.4	Additional Privacy Considerations .....	30
3.6	Traffic Manager: Emergency Communications and Evacuation Information .....	31
3.6.1	Overview .....	31
3.6.2	Information Flow Analysis .....	31
3.6.3	Device Classes .....	32
3.6.4	Additional Privacy Considerations .....	32
3.7	Roadway User: Pedestrian in Signalized Intersection Warning .....	32
3.7.1	Overview .....	32
3.7.2	Information Flow Analysis .....	34
3.7.3	Device Classes .....	38
3.7.4	Additional Privacy Considerations .....	38
3.8	Roadway User: Mobile Accessible Pedestrian Signal System .....	38
3.8.1	Overview .....	38
3.8.2	Information Flow Analysis .....	40
3.8.3	Device Classes .....	43
3.8.4	Additional Privacy Considerations .....	43
3.9	System Manager: ASD CV Application Configuration Download and ASD Firmware Update .....	43
3.9.1	Overview .....	43
3.9.2	Information Flow Analysis .....	44
3.9.3	Device Classes .....	47
3.9.4	Additional Privacy Considerations .....	48
3.10	System Manager: RSE CV Application Configuration Download and RSE Firmware Update .....	48
3.10.1	Overview .....	48
3.10.2	Information Flow Analysis .....	49
3.10.3	Device Classes .....	50
3.10.4	Additional Privacy Considerations .....	50
3.11	System Manager: RSE RF Monitoring .....	51
3.11.1	Overview .....	51
3.11.2	Information Flow Analysis .....	51
3.11.3	Device Classes .....	52
3.11.4	Additional Privacy Considerations .....	52
3.12	System Manager: ASD RF Monitoring .....	52
3.12.1	Overview .....	52
3.12.2	Information Flow Analysis .....	52
3.12.3	Device Classes .....	53
3.12.4	Additional Privacy Considerations .....	53
3.13	Independent Evaluator: ASD Event Data Upload .....	53
3.13.1	Overview .....	53
3.13.2	Information Flow Analysis .....	54

3.13.3	Device Classes .....	54
3.13.4	Additional Privacy Considerations .....	55
3.14	Independent Evaluator: Performance Measurement Data Processing .....	56
3.14.1	Overview .....	56
3.14.2	Information Flow Analysis .....	56
3.14.3	Device Classes .....	57
3.14.4	Additional Privacy Considerations .....	57
3.15	Device Classes Considered in NYC Pilot Site .....	57
<b>Chapter 4. Communications Security and Privacy by Usage Scenario .....</b>		<b>59</b>
4.1	General .....	59
4.2	Overview of Existing Security Mechanisms .....	59
4.2.1	Current NYC DOT Approach .....	59
4.2.2	IEEE 1609.2 .....	60
4.2.3	SNMPv3 .....	64
4.2.4	VPN .....	66
4.2.5	TLS .....	67
4.3	Security Mechanisms per Information Flow .....	68
4.3.1	Overview .....	68
4.3.2	Existing CV Applications: BSM-based Safety .....	69
4.3.3	Existing CV Applications: Red Light Violation Warning .....	70
4.3.4	Traffic Manager: Speed Compliance / Speed Compliance in Work Zones / Curve Speed Compliance .....	72
4.3.5	Traffic Manager: Oversize Vehicle Compliance .....	74
4.3.6	Traffic Manager: Emergency Communications and Evacuation Information .....	75
4.3.7	Roadway User: Pedestrian in Signalized Intersection Warning .....	77
4.3.8	Roadway User: Mobile Accessible Pedestrian Signal System .....	79
4.3.9	System Manager: ASD CV Application Configuration Download and ASD Firmware Update .....	80
4.3.10	System Manager: RSE CV Application Configuration Download and RSE Firmware Update .....	83
4.3.11	System Manager: RSE RF Monitoring .....	85
4.3.12	System Manager: ASD RF Monitoring .....	85
4.3.13	Independent Evaluator: ASD Event Data Upload .....	87
4.3.14	Independent Evaluator: Performance Measurement Data Processing .....	88
4.4	Security Mechanisms per Device Type .....	91
<b>Chapter 5. Physical and Platform Security Controls .....</b>		<b>93</b>
5.1	General .....	93
5.1.1	Overview and Goals .....	93
5.1.2	Architectures .....	93
5.1.3	Host Processor .....	95
5.1.4	HSM .....	97
5.1.5	Architecture-specific Requirements .....	98
5.2	Physical Security Controls .....	98
5.3	Minimum Security Requirements per Device Classification .....	98
5.3.1	Class 1 (LMM) Device Minimum Security Requirements .....	99

5.3.2	Class 2 (MMM) Device Minimum Security Requirements.....	99
5.3.3	Class 3 (MHM) Device Minimum Security Requirements .....	99
5.3.4	Storage Requirements.....	100
5.3.5	Privacy of Stored Certificates .....	100
5.4	System and Device Testing.....	101
5.4.1	Conformance Testing .....	101
5.4.2	Physical Security Testing .....	101
5.5	Contingency Plan for Suitable Hardware Being Unavailable .....	101
5.6	Access Security .....	102
5.6.1	General.....	102
5.6.2	ASDs.....	102
5.6.3	RSEs.....	102
<b>Chapter 6. Management Considerations per Security Mechanism.....</b>		<b>103</b>
6.1	Introduction .....	103
6.2	IEEE 1609.2 .....	103
6.2.1	Introduction .....	103
6.2.2	Security Credential Management System Overview .....	104
6.2.3	Applications and PSIDs .....	106
6.2.4	SCMS-Core: Initial Provisioning .....	108
6.2.5	SCMS-Core: Initial Download.....	109
6.2.6	SCMS-Core: Certificate Update .....	110
6.2.7	SCMS-Core: Misbehavior Reporting .....	112
6.2.8	SCMS-Core: Revocation .....	114
6.2.9	SCMS-Core: Re-initialization.....	115
6.2.10	SCMS-Support: IP Connectivity via RSE .....	115
6.3	SNMPv3 Security Management Considerations .....	116
6.4	VPN Security Management Considerations .....	116
6.5	Physical Protection Security Management Considerations.....	116
<b>Chapter 7. Security Management Lifecycle Activities per Device Type .....</b>		<b>117</b>
7.1	RSE .....	117
7.1.1	Lifecycle.....	117
7.1.2	Geographic Constraints in Certificate.....	121
7.1.3	Tracking Use of RSE as a Pass-Through .....	122
7.2	Aftermarket Safety Device (ASD) .....	122
7.2.1	Lifecycle.....	122
7.3	Personal Information Device (PID) .....	125
7.3.1	Lifecycle.....	126
7.4	Traffic Management Center (TMC) .....	129
7.4.1	Lifecycle.....	129
<b>Chapter 8. Privacy and PII Data Protection.....</b>		<b>130</b>
8.1	Introduction/Background.....	130
8.2	Performance Data Collection.....	130
8.3	Tuning and Evaluation.....	131
8.4	Stakeholder Use of Logs .....	131
8.5	Other Performance Monitoring .....	132
8.6	Aggregated Mobility Data .....	132

8.7	Summary .....	133
8.8	Additional Notes .....	133
<b>Chapter 9.</b>	<b>Operation .....</b>	<b>134</b>
9.1	User Manual .....	134
9.2	Securing Initial Connections Between Devices .....	134
9.3	Encryption Registration Number .....	135
9.4	IPv6 Over IPv4 Tunneling.....	135
9.5	Network Security on NYCWiN .....	135
9.5.1	General .....	135
9.5.2	Penetration Testing .....	135
9.6	Availability.....	135
9.6.1	Denial of Service .....	135
9.6.2	Other Availability Considerations .....	136
9.7	Incident Response .....	136
9.8	Secure Transport of Devices .....	136
9.9	Physical Inspection.....	136
9.9.1	ASDs.....	136
9.9.2	RSEs.....	137
9.10	Contingency Plan .....	137
9.10.1	ASD .....	137
9.10.2	RSU .....	137
9.11	Evaluation .....	137
9.11.1	Security Evaluation .....	137
9.12	Business Relationship with the SCMS Operator .....	138
9.13	Certification.....	138
<b>Chapter 10.</b>	<b>Future Work to be Coordinated Between Pilot Deployment</b>	
	<b>Security Teams .....</b>	<b>139</b>
	<b>References.....</b>	<b>140</b>
	<b>APPENDIX A. List of Acronyms.....</b>	<b>142</b>
	<b>APPENDIX B. Physical View Legend.....</b>	<b>144</b>
	<b>APPENDIX C. Local Misbehavior Detection and Plausibility Checking</b>	
	<b>Recommendations from THEA PD .....</b>	<b>146</b>

## List of Tables

Table 2-1. CV Application ConOp References.....	9
Table 3-1. Source of C//A Analysis of the NYC CVPD Applications and Operational Scenarios.....	17
Table 3-2. C//A Analysis for BSM-based V2V Safety.....	19
Table 3-3. Baseline Device Classes for BSM-based V2V Safety.....	19
Table 3-4. CIA Analysis for Red Light Violation Application.....	21
Table 3-5. Device Classes for Red Light Violation Application.....	25
Table 3-6. CIA Analysis of Speed Compliance Applications.....	27
Table 3-7. Device Classes for Speed Compliance Applications.....	28
Table 3-8. CIA Analysis of Oversize Vehicle Compliance.....	29
Table 3-9. Device Classes for Oversize Vehicle Compliance.....	30
Table 3-10. CIA Analysis of Emergency Communication and Evacuation Information.....	32
Table 3-11. Device Classes for Emergency Communication and Evacuation Information Distribution.....	32
Table 3-12. CIA Analysis for Pedestrian in Signalized Intersection Warning.....	34
Table 3-13. Proposed Device Classes for Pedestrian in Signalized Intersection Warning.....	38
Table 3-14. CIA Analysis for Mobile Accessible PED-SIG Application.....	40
Table 3-15. NYC Proposed Device Classes for Mobile Accessible PED-SIG Application.....	43
Table 3-16. CIA Analysis for ASD CV Application Configuration Download and ASD Firmware Update.....	45
Table 3-17. NYC Proposed Device Classes for ASD CV Application Configuration Download and ASD Firmware Update.....	47
Table 3-18. CIA Analysis for RSE CV Application Configuration Download and RSE Firmware Update.....	49
Table 3-19. NYC Proposed Device Classes for RSE CV Application Configuration Download and RSE Firmware Update.....	50
Table 3-20. CIA Analysis for RSE RF Monitoring.....	51
Table 3-21. NYC Proposed Device Classes for RSE RF Monitoring.....	52
Table 3-22. CIA Analysis for ASD RF Monitoring.....	53
Table 3-23. NYC Proposed Device Classes for ASD RF Monitoring.....	53
Table 3-24. CIA Analysis for ASD Event Data Upload.....	54
Table 3-25. NYC Proposed Device Classes for ASD Event Data Upload.....	55
Table 3-26. NYC Proposed Device Classes for ASD Event Data Upload.....	55
Table 3-27. CIA Analysis for Performance Measurement Data Processing.....	56
Table 3-28. NYC Proposed Device Classes for Performance Measurement Data Processing.....	57
Table 3-29. Consolidated Device Classes by Type and Application / Usage Scenario.....	57
Table 4-1. SNMPv3 RFCs.....	64
Table 4-2. Security Mechanism Selection for BSM-based V2V Safety.....	70
Table 4-3. Security Mechanism Selection for Red Light Violation Warning.....	70
Table 4-4. Security Mechanism Selection for Speed Compliance applications.....	73

Table 4-5. Security Mechanism Selection for Oversize Vehicle Compliance .....	74
Table 4-6. Security Mechanism Selection for Emergency Communication and Evacuation Information.....	76
Table 4-7. Security Mechanism Selection for Pedestrian in Signalized Intersection Warning .....	77
Table 4-8. Security Mechanism Selection for Mobile Accessible PED-SIG Application.....	79
Table 4-9. Security Mechanism Selection for ASD CV Application Configuration Download and ASD Firmware Update.....	81
Table 4-10. CIA Analysis for RSE CV Application Configuration Download and RSE Firmware Update.....	84
Table 4-11. Security Mechanism Selection for RSE RF Monitoring Usage Scenario .....	85
Table 4-12. Security Mechanism Selection for ASD RF Monitoring Usage Scenario .....	86
Table 4-13. Security Mechanism Selection for ASD Event Data Upload Usage Scenario.....	88
Table 4-14. Security Mechanism Selection for Performance Measurement Data Processing.....	89
Table 4-15. Consolidated Security Mechanisms by Device Type and Application / Usage Scenario.....	91
Table 6-1. Mapping Between Applications and Application Activities That Use 1609.2 Certificates.....	106
Table 6-2. PSIDs That Require Certificates, By Device Type.....	108
Table 6-3. PSIDs that Will Not Appear in Certificates but Will Appear in WSAs .....	108
Table B-1. Physical/Application Interconnect Characteristics.....	145

## List of Figures

Figure 2-1. NYC CVPD System Concept .....	8
Figure 2-2. NYC CVPD Enterprise View (Layer 0 Roles).....	11
Figure 2-3. Network Connectivity Architecture.....	13
Figure 2-4. RSE Interfaces.....	14
Figure 2-5. ASD Interfaces .....	14
Figure 2-6. PID Interfaces .....	15
Figure 2-7. Organizational Chart for Security Operations .....	16
Figure 3-1. Physical View of Red Light Violation Application.....	20
Figure 3-2. Physical View of Speed Compliance Applications .....	26
Figure 3-3. Physical View of Oversize Vehicle Compliance .....	29
Figure 3-4. Physical View of Emergency Communication and Evacuation Information Distribution.....	31
Figure 3-5. Physical View of Pedestrian in Signalized Intersection Warning .....	33
Figure 3-6. Mobile Accessible Pedestrian Signal System .....	39
Figure 3-7. Physical View of ASD CV Application Configuration Download and ASD Firmware Update.....	44

Figure 3-8. Physical View of RSE Application Configuration Download and Firmware Update .....	48
Figure 3-9. RSE RF Monitoring .....	51
Figure 3-10. ASD RF Monitoring .....	52
Figure 3-11. ASD Event Data Upload .....	54
Figure 3-12. Performance Measurement Data Processing .....	56
Figure 4-1. Network Security in Current NYC DOT System .....	60
Figure 4-2. IEEE 1609.2 Verification Process .....	63
Figure 4-3. SNMPv3 Security Features .....	65
Figure 4-4. Legend for Diagrams in Chapter 4 .....	69
Figure 4-5. Security Mechanism Selection for BSM-based V2V Safety .....	70
Figure 4-6. Security Mechanism Selection for Red Light Violation Warning .....	72
Figure 4-7. Security Mechanism Selection for Curve Speed Compliance .....	73
Figure 4-8. Security Mechanism Selection for Oversize Vehicle Compliance .....	75
Figure 4-9. Security Mechanism Selection for Emergency Communications and Evacuation Information .....	76
Figure 4-10. Security Mechanism Selection for Emergency Communications and Evacuation Information .....	78
Figure 4-11. Security Mechanism Selection for Mobile Accessible PED-SIG .....	80
Figure 4-12. Security Mechanism Selection for ASD CV Application Configuration Download and ASD Firmware Update .....	82
Figure 4-13. Physical View of Infrastructure Management .....	84
Figure 4-14. Security Mechanism Selection for RSE RF Monitoring .....	85
Figure 4-15. Security Mechanism Selection for ASD RF Monitoring .....	87
Figure 4-16. Security Mechanism Selection for ASD Event Data Upload .....	88
Figure 4-17. Security Mechanism Selection for Performance Measurement Data Processing .....	90
Figure 5-1. Integrated Architecture .....	94
Figure 5-2. Connected Architecture .....	94
Figure 5-3. Networked Architecture .....	94
Figure 6-1. SCMS Diagram .....	104
Figure 6-2. Information Flows for 1609.2 Initial Provisioning .....	109
Figure 6-3. Information Flows for 1609.2 Initial Pseudonym Certificate Request .....	110
Figure 6-4. Information Flows for 1609.2 Application Certificate Request And Response .....	110
Figure 6-5. Information Flows for 1609.2 Pseudonym Certificate Issuance .....	111
Figure 6-6. Information Flows for 1609.2 Pseudonym Certificate Download .....	111
Figure 6-7. Information Flow for 1609.2 Misbehavior Reporting (Conjectured) .....	112
Figure 6-8. Information Flow For 1609.2 External Reporting .....	112
Figure 6-9. Information Flows for IP Connectivity via RSE .....	115
Figure B-1. Physical View Legend .....	144

# Executive Summary

The Privacy and Security Management Operating Concept (SMOC) of the New York City Department of Transportation (NYCDOT) Connected Vehicle Pilot Deployment (CVPD) Project outlines the security mechanisms that will be used to protect information flows within NYC CVPD, additional practices to protect privacy and security of data at rest, and management processes and procedures to ensure that security operations are carried out in a reliable and trustworthy way.

A Confidentiality / Integrity / Availability analysis has been performed on the 18 applications and usage scenarios envisioned in the NYC CVPD to identify the device security classes to be used. The main results are:

- Aftermarket Safety Device (ASD) is of security class 1;
- Personal Information Device (PID) is of security class 1 or 3 (depending on the applications);
- Roadside Equipment (RSE) is security class 1, 2 or 3 (depending on the applications);
- ITS-Roadway Equipment (ITS-RE) is of security class 1 or 3 (depending on the applications).
- Security-wise, the most stringent application is the Pedestrian in Signalized Crosswalk Warning, as requires ITS-RE, RSE and PID to be of security class 3.

The security mechanisms selected to ensure security are: TLS VPN, SNMPv3 with TLS, IEEE 1609.2 signature, IEEE 1609.2 encryption, physical protection of the link, and proprietary. The most frequently used mechanisms are IEEE 1609.2 signature and SNMPv3 with TLS. Therefore, it is clear that the NYC CVPD has to establish a relationship with the Security Credentials Management System (SCMS) in order to provide certificate provisioning and certificate refill to participating entities, and revocation (which is kept centrally).

SNMPv3 is an industry-standard network management protocol that will be used in the NYC CVPD to maintain ITS-REs, RSEs, and ASDs. Thanks to SNMP commands onto the MIBs, the TMC will be able to push firmware update and change configuration parameters. The TMC will have to run an X.509 certificate authority in order to prevent replay attack.

If a device were found faulty or compromised, this incident will be handled by replacing the units, which falls under the device supplier's responsibility.

Regarding privacy protection, we follow the seven concepts: transparency, participation, and redress, specification of purpose, minimization, use limitation, quality and integrity, accountability and auditing. Without getting into extensive detail (because the project's Performance Measurement and Evaluation Support Plan (FHWA-JPO-16-302) hasn't been completed yet), we explain data collection, data aggregation, and data use.

To summarize, this document covers the entire data lifecycle and specifies security and privacy mechanisms to ensure appropriate protection level during the CVPD.

# Chapter 1. Introduction

## 1.1 General

This document describes the Security Management Operating Concept (SMOC) for the New York City Department of Transportation (NYCDOT) Connected Vehicle Pilot Deployment (CVPD) Project. This SMOC outlines the security mechanisms that will be used to protect information flows within NYC CVPD, additional practices to protect privacy and security of data at rest, and management processes and procedures to ensure that security operations are carried out in a reliable and trustworthy way.

This SMOC is one of the documents due for The Connected Vehicle Pilot Deployment Program, Phase 1 project funded by the United States Department of Transportation (USDOT). Other planning documents, developed under this project phase, that are related to this SMOC include the Concept of Operations, Performance Measurement and Evaluation Plan, Safety Management Plan, and Human Use Approval.

Two other project phases are scheduled following the successful completion of Phase 1. Phase 2 consists of the design, deploy, and test project activities occurring over a 20-month period. A maintain and operate period comprises Phase 3 of the project over an 18-month period.

The SMOC is a foundational document for communicating this program's approach to security and security management to project stakeholders and system developers. Systems engineers will then use this SMOC to develop detailed technical specifications.

The intended audience for this document includes the following:

- New York City Department of Transportation (NYCDOT)
- New York City CV Architecture Team
- New York City CV Pilot Deployment Project Stakeholders
- Individuals interested in the NYC CV program
- ITS-JPO Program Leads and Support Staff
- ITS-JPO Program Engineering Teams
- Wave 1 CV Pilot Deployment Project Teams
- Future Connected Vehicle Deployment Project Teams

The document is organized to meet the requirements of the United States Department of Transportation (USDOT) System Engineering Process and IEEE Std 1362-1998 [2] as required by the USDOT Broad Agency Announcement (BAA) dated January 30, 2015 amended.

## 1.2 Identification

This document is identified as:

Agency: New York City Department of Transportation  
Organization: Bureau of Traffic Operations  
Project Name: New York City (NYC) Connected Vehicle Pilot Deployment (CVPD)  
Title: Connected Vehicle Pilot Deployment Program Phase 1  
Subtitle: Security Management Operating Concept – New York City  
Version: 1.0  
Date: 5/18/2016  
Status: Draft  
FHWA Publication: FHWA-JPO-16-300

## 1.3 Scope: Privacy and Security Objectives within NYC CVPD

This section outlines the privacy and security objectives within the NYC CVPD. The Scope of the document is to specify concrete mechanisms for achieving these objectives.

### 1.3.1 Communications Security Objectives

All communications between nodes operating an application shall provide at least the level of confidentiality, integrity, and availability (C//I/A) that is determined to be necessary through a security analysis as described in [14].

The system shall securely provide nodes with the security credentials necessary for them to be trusted by other nodes.

The system shall securely provide nodes with the security material necessary for them to trust other nodes.

The system shall securely provide nodes with the security material necessary for them to ensure confidential communications with other nodes.

The security mechanisms to be used to meet these requirements shall be specified unambiguously in order to allow multiple suppliers to interoperate.

### 1.3.2 Device Security Objectives

All field devices used in the NYC CVPD shall provide at least the level of confidentiality, integrity and availability (C//I/A) that is determined to be necessary through a security analysis as described in [14].

### 1.3.3 Privacy Objectives

In order to produce safety benefits consistent with the goals of the USDOT's connected vehicle program, the project will adopt the USDOT objective to "not collect or store any data on individuals or individual vehicles, [nor to] enable the government to do so." [4]

---

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

The time and location information collected in the project constitutes potentially Personally Identifiable Information (PII) because it could be merged with other records (e.g., police crash reports) and used in legal proceedings, disciplinary proceedings, or insurance negotiations. Keeping data with this time/location information is a potential infringement of an individual's privacy. If such records were known to exist, they could be subpoenaed for criminal and/or civil suits and would be subject to FOIA requests – which are very frequent in NYC.

The goal of privacy poses a formidable challenge for the deployment of the NYC CVPD project. While privacy is a fundamental concept embedded in the CV system design, the need to measure deployment benefits necessitates knowing details regarding the vehicle and its whereabouts. To balance these competing objectives, the NYC CVPD will provide detailed vehicle operational information only after it has been aggregated and normalized (i.e., scrubbed) of time and location details. Information shall be encrypted up to the time of scrubbing in order to prevent unauthorized access. This approach satisfies the detailed information needs for evaluation while protecting the privacy of the vehicle drivers/operators.

## **1.4 Approach and Organization of this Document**

### **1.4.1 General**

This document forms part of the systems engineering analysis of the New York City Connected Vehicle Pilot deployment per 23 CFR 940.11 [1].

Chapter 2 provides an overview of the security management, showing the network architecture, identifying device types and interfaces, identifying organizations involved in the security management, and identifying security management roles within NYC CVPD.

Chapter 3 provides (a) an overview in detail of the operational scenarios and (b) an analysis of the security requirements for the information flows in the Operational Scenarios, as described in [14]. The analysis of the information flows is based on Federal Information Processing Standard (FIPS) 199 [13]. Based on the aggregated security requirements for those information flows, we derive the required security device classes (also described in [14]) for each of the devices in the system that are specific to the NYC CVPD and make recommendations for security device classes for the existing devices.

Chapter 4 identifies mechanisms for protecting each of the information flows. A number of these mechanisms are based on IEEE 1609.2 [6]. Others are based on other standards which are identified in the body of the text.

Chapter 5 provides device and access security requirements for the devices in each class and specifies our approach to suppliers, acknowledging that it might not be possible for suppliers to produce devices that meet these requirements. This section also describes methods for system and device testing.

Chapter 6 addresses security management considerations for each of the security mechanisms identified in Chapter 4. This section (a) provides a background description of the Security Credentials

Management System (SCMS) that will provide IEEE 1609.2 certificates to devices within NYC CVPD; (b) describes the lifecycle of each system element from the point of view of security.

Chapter 7 specifies lifecycle security management operations for each of the relevant system components: ASD, RSE, TMC, and PID.

Chapter 8 specifies the operating concept for providing privacy to the participants in the system, particularly those participants whose activities are the raw material for reports provided to the external evaluator.

Chapter 9 specifies operation, incident response, and evaluation.

Chapter 10 notes future work to be done during Phase 1 that should be coordinated between the security teams for the different Pilot Deployment sites.

## 1.4.2 SMOC Approach

The SMOC was developed according to the following process:

- 1) Identify applications and usage scenarios
- 2) Analyze confidentiality / integrity / availability requirements on information flows within each application and usage scenario following [13] [14].
  - Based on the flows, identify the device classes necessary for each device to support each application per [14].
- 3) Identify security requirements for each device class.
- 4) For each information flow, select a specific security mechanism to secure that information flow.
- 5) For each security mechanism selected, identify general lifecycle management issues
- 6) For each device running an instance of an application, identify the specific lifecycle management steps to be carried out for
  - Provisioning
  - Start of operation
  - Ongoing operation
  - End of life
- 7) Identify privacy and confidentiality requirements for data at rest and privacy risks from access to that data: specify countermeasures to mitigate those privacy risks.

## 1.4.3 CV Pilot Team Coordination

Throughout concept development, the NYC team has coordinated with USDOT representatives and the other pilot teams to produce a broad, yet detailed security analysis and operating concept. This coordination was initiated and led by the THEA security team ensuring that valuable information from current and existing projects were shared with the CV Pilot teams. There were also biweekly coordination conference calls and a cross-team working session to review the status of concept development across the teams and request information from USDOT and the other pilot teams.

## 1.5 SMOC Limitations

(NOTE: This is based on the similar text in the THEA SMOC with grateful thanks)

While the NYC team took a comprehensive approach to the SMOC, there are still limitations to this concept as the overall pilot concept is still in the development process. As work continues on the remaining Pilot Deployment Concept tasks, the SMOC will likely have to be revisited and adjusted as necessary. Key limitations are listed below:

- While the draft concept will have security controls for devices identified per NIST SP 800-53, the full specification of those security controls will not be complete until the final deliverables of the Threat Definition of V2I Architecture project are published. However, we have coordinated with the project team and checked that we have the same device classifications. Based on the initial proposed list of specified security controls from the Threat Definition project (which will likely not be published until well after March 2016), suppliers would not be able to adjust devices and manufacturing processes in time to deliver devices for pilot deployment. For this concept, the CV Pilot teams have determined that the best course of action is to develop a minimum set of requirements that are realistic for device suppliers to meet in time for deployment
- SCMS Proof of Concept (POC) is not yet available for testing and current interface requirements documents will continue to be updated through September 2016 as the SCMS POC is built
- Security requirements recommended by this concept may be cost prohibitive (specifically FIPS 140-2 hardware security requirements) upon further review during the development of the System Requirements Specification document in Task 6
- Device suppliers may not be able to meet all recommended security requirements in time for the planned device deployment
- Full security certification testing by third parties will likely not be feasible. Testing and certification for interoperability and compliance with standards such as IEEE 1609.2 is definitely possible. However, new requirements such as compliance with specific FIPS 140-2 levels will likely have to be self-certified as these tests are expensive and time consuming to be conducted by accredited certification labs
- The concept and requirements may require updates based on the Application Deployment Plan (draft due April 2016), Human Use Approval Plan (draft due June 2016), Participant Training and Stakeholder Education Plan (draft due June 2016), and Outreach Plan (draft due June 2016)
- Misbehavior detection, plausibility checking, device management, and geographic encoding of zones are not fully specified and it would be useful for all the CVPD projects to have requirements that are as similar as possible.

# Chapter 2. System Overview

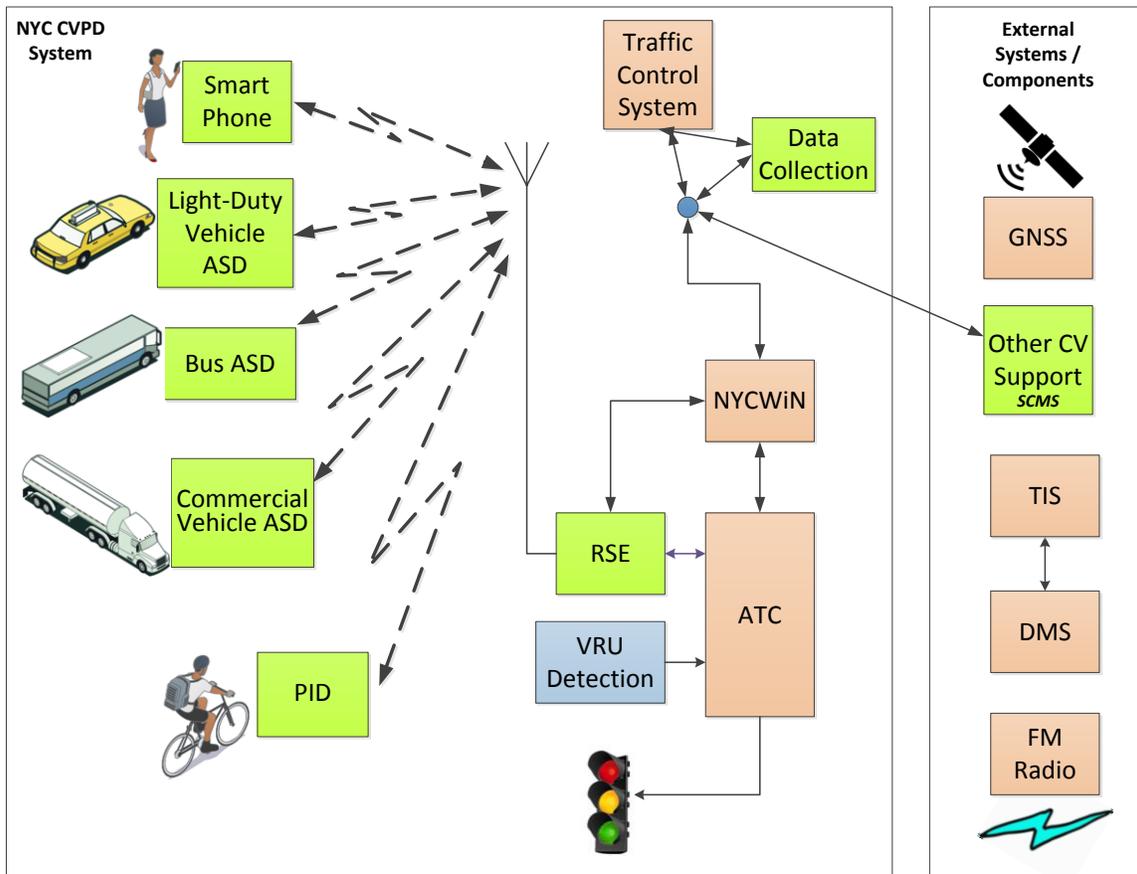
## 2.1 Overview of the New York City Connected Vehicle Pilot Deployment

This section, which is largely excerpted from the New York City Connected Vehicle Pilot Deployment (NYC CVPD) Concept of Operations document [5], will describe the key concepts for the NYC CVPD project.

The NYC CVPD project is one of three initial CV deployment projects that establish a base for growing a nationwide connected vehicle system. As such, its focus is on utilizing standards to build basic infrastructure in a manner that provides a foundation for future deployments of connected vehicle technology.

The key concept for the NYC CVPD project is to equip a large fleet of vehicles with CV technology in order to advance towards the Vision Zero goal of eliminating injuries and fatalities from traffic crashes. A small portion of New York City roadway network will have connected vehicle infrastructure installed (i.e., roadside equipment). Vehicle-to-Infrastructure (V2I) applications such as Red Light Violation Warning and Curve Speed Compliance will support connected vehicles operating in these areas. However, the geographic reach of the connected vehicle technology is much broader. Vehicles equipped with connected vehicle technology (i.e., aftermarket safety devices) will travel in this infrastructure equipped area *and throughout the City's transportation network*. Thus the connected vehicle technology that supports Vehicle-to-Vehicle (V2V) applications will function anywhere two equipped vehicles are within range of one another. Equipped vehicle encounters may occur on the surface streets, in the tunnels and bridges crossing the rivers, at the airports, and on the City's higher speed facilities such as the FDR Drive and the Long Island Expressway. The large fleet size means that there will be many opportunities for the connected vehicle technology to perform over a large geographic area and diverse roadway environments.

The envisioned NYC CVPD system is depicted in Figure 2-1. The existing system elements, critical to the operation of the pilot system, are illustrated with beige backgrounds. These existing elements include the traffic management system, the traffic controller (ASTC), and supporting NYCWiN communications infrastructure. New system elements which exist and will be reused, modified, or integrated into the NYC CVPD system have green backgrounds. Aftermarket safety devices (ASD), Personal Information Devices (PIDs), roadside equipment (RSE), and data collection/processing systems comprise the new system elements. The Vulnerable Road User (VRU) detection devices to be added to the system are shown with a blue background as these devices are relatively new and will be deployed on a very limited basis. PIDs will be specially equipped smartphones – i.e. it will not be possible for a smartphone to become a PID simply by downloading an app from a public source. The bicyclist is assumed to use the same application as the pedestrian to obtain similar system services and user notifications.



(Source: NYCDOT, 2016)

**Figure 2-1. NYC CVPD System Concept**

The ASDs will be installed in fleet vehicles, not private vehicles. The concept of operations is that the fleet vehicles may include buses, taxis, UPS trucks, maintenance vehicles, and others. Maintenance for these vehicles will be provided in fleet terminals or “barns”; the exact location of the “barns” is still being resolved as part of our negotiations with the stakeholders and the specific vehicles to be used. There may be opportunities for the Auto OEMs to outfit and test their vehicles since the NYC Connected Vehicle Deployment Project will be adhering to the published standards and utilizing the SCMS. This type of option will be explored later once the contracted project is underway and is not covered in this SMOC.

The NYC CVPD will support the applications shown in Table 2-1 which are already defined as CV applications.

**Table 2-1. CV Application ConOp References**

<b>CV Application</b>	<b>Concept of Operations Reference</b>
Forward Crash Warning	SAE J2945/1-2016
Emergency Electronic Brake Lights	SAE J2945/1-2016
Blind Spot Warning	SAE J2945/1-2016
Lane Change Warning	SAE J2945/1-2016
Intersection Movement Assist	SAE J2945/1-2016
Red Light Violation Warning	Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications Concept of Operations Document Final Report —May 29, 2012 FHWA-JPO-13-058
Vehicle Turning Right in Front of Bus Warning	Transit Safety Retrofit Package Development TRP Concept of Operations Final Report – May 28, 2014 FHWA-JPO-14-117

Additionally, the NYC CVPD will support the following usage scenarios defined in the ConOps document [5]:

- **TRAFFIC MANAGER SCENARIOS**
  - Speed Compliance – provides warnings to the driver when they are exceeding the speed limit by a configurable amount or time.
  - Speed Compliance / Work Zones – provides over speed warnings for work or school zones that are either statically or dynamically located.
  - Curve Speed Compliance – provides warnings to the driver when they are exceeding the recommended speed for a curve.
  - Oversize Vehicle Compliance – provides warnings to vehicles over 9’6” in height traveling on FDR drive in Manhattan.
  - Emergency Communications and Evacuation Information – provides vehicles with emergency and evacuation information such as, for example, location-specific directions for evacuation, location restrictions for entry, global emergency information, and route-specific information.
- **ROADWAY USER SCENARIOS**
  - Vehicle Trip Initiation – the ASD notifies the driver that it has successfully turned on at the start of a trip
  - Driver Reporting Suspected ASD Failure – the driver notifies the fleet owner using a communications path outside the NYC CVPD (for example, by phone or email) that an ASD is not operating correctly.
  - Pedestrian in Signalized Intersection Warning – provides drivers with a warning when there is a pedestrian in a crosswalk at a signalized intersection; detects pedestrians either via current pedestrian detection technologies or using Personal Information Devices (PIDs) carried by the pedestrians.
  - Mobile Accessible Pedestrian Signal System – provides visually impaired pedestrians with information about crossing status; potentially, allows visually impaired pedestrians to request signal prioritization.

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

- SYSTEM MANAGER SCENARIOS
  - ASD CV Application Configuration Download – upload or download the configuration parameters of V2I and V2V applications to the ASD.
  - ASD Firmware Update – determine the ASD’s firmware version and perform over-the-air (OTA) firmware updates as needed
  - RSE RF Monitoring – RSEs monitor RF signal data to determine characteristics of the system such as effective operating range. The data is later uploaded to the TMC for analysis.
  - ASD RF Monitoring – ASDs monitor RF signal data to determine characteristics of the system such as effective operating range. The data is later uploaded to the TMC for analysis.
- INDEPENDENT EVALUATOR SCENARIOS
  - ASD Event Data Recording – ASDs record data around the time that an alert is triggered.
  - ASD Event Data Upload – Event data recorded in the previous bullet point is uploaded to the TMC for analysis
  - Performance Measurement Data Processing – The TMC analyses the data, and also aggregates it and normalizes it for transmission to the independent evaluator.

This document provides a Security Management Operating Concept (SMOC) to support the use scenarios in the ConOps.

For each of the applications above this Security Management Operating Concept covers the following:

- Communications security objectives
- Platform security objectives
- Privacy objectives

## 2.2 Types of View

In this Security Management Operating Concept for the NYC CVPD, the proposed system is described using different views. These include system architecture views based on USDOT's Connected Vehicle Reference Implementation Architecture (CVRIA) [3]. More information is described in the CVRIA website. This section provided an enterprise view and a (non-CVRIA-style) network view of the entire system. Later subsections provide information about the CV applications to be tailored for this deployment and make use of the CVRIA physical view.

The enterprise view describes the relationships between organizations and the roles those organizations play within the connected vehicle environment.

The physical view describes the physical objects (systems and devices) and their application objects, as well as the high-level interfaces between those physical objects. Functional and communications views can be included as subsets of the physical view components.

## 2.3 Enterprise View

Figure 2-2, extracted from the ConOps document [5], shows an Enterprise View of the relationships within the NYC CVPD.

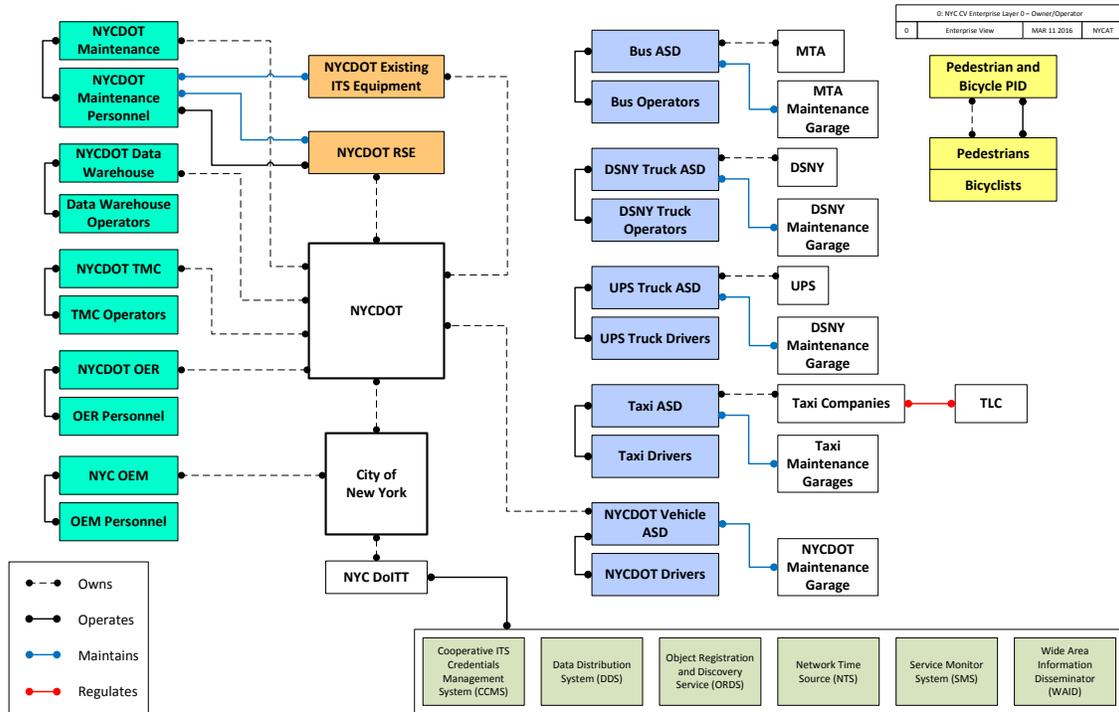


Figure 2-2. NYC CVPD Enterprise View (Layer 0 Roles)

Security management operations within the NYC CVPD are centered in NYC DOT. NYC DOT hosts the Traffic Management Center (TMC), which is operated by NYC DOT personnel. NYC Department of Information Technology and Telecommunications (DoITT) manages the networks and firewalls that connect TMC to the rest of the NYC network.

DoITT also provides the following support services:

- The **Network Time Source (NTS)** service provides time synchronized to the GNSS time used by in-vehicle equipment

NYC DOT also provides the following support services:

- The **Service Monitor System (SMS)** monitors, manages, and controls services for applications and equipment that are operating in the CV system environment. In the NYC CVPD, it will enable CV applications to provide services including device management, time synchronization, and trust management.
- The **Wide Area Information Disseminator (WAID)** represents the communications equipment in the CV system environment used to send messages to and from RSEs and, through the RSEs, to CV-equipped vehicles. The messages will be transmitted using DSRC at 5.9 GHz frequency and may be broadcasted to and from ASDs and RSEs.

The following support services are provided by external service providers:

- The **Data Distribution System (DDS)** is responsible for collecting, processing, and distributing near real-time CV data such as BSM, MAP, SPaT, and TIM messages. It will link the data produced by the roadway users with the research data exchange (RDE).
- The **Security Credentials Management System (SCMS)** provides certificate management services for certificates based on IEEE Std 1609.2 [6]

The physical interfaces for these support services are managed by DoITT. For each external service provider, there will be service level agreements putting security requirements on their operations as derived in Chapter 3.

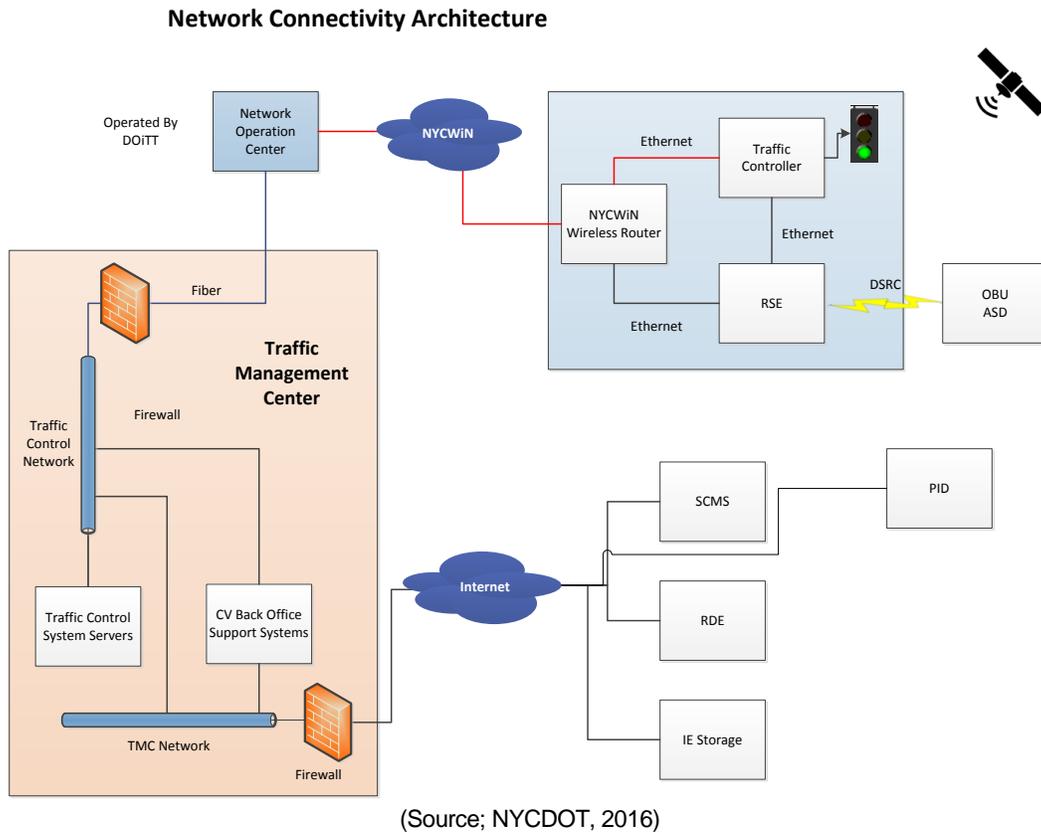
PIDs are provided by NYCDOT and can connect to Core Services directly via the Internet.

## 2.4 Network Architecture

Figure 2-3 provides an overview of the NYC CVPD network architecture, showing the physical partitioning and firewalls that will be implemented to maintain a system-level secure environment.

In this diagram, starting from the services on the Internet and working clockwise:

- The **Security Credentials Management System (SCMS)** is as described in Section 2.3.
- The **Research Data Exchange (RDE)** makes sanitized data available to third-party researchers.
- The **Independent Evaluator (IE)** storage makes data available to the independent evaluator.
- The **Traffic Management Center (TMC)** hosts back-office support systems and traffic control system services. These are operated within a firewall and with physical protection to prevent unauthorized logical or physical access. Back office support systems include the following:
  - Access to **SCMS**
  - **SMS** activities: Managing roadside equipment performance (failure identification, repair, maintenance); managing roadside equipment radio frequency (RF) footprints; managing CV application configuration
  - **DDS** activities: External data distribution (USDOT); Data collection from RSE/ASD; Data aggregation, data normalization, and system performance assessment
  - TMS.Existing security processes used in managing ITS components are described in Section 4.2.1.
- The **Network Operation Center (NOC)** manages underlying network operations. It is not an active participant in the NYC CVPD Usage Scenarios.
- The New York City Wireless Network is used to distribute data and commands to traffic controls and RSEs, and (via DSRC communications with the RSE) to participating field devices, i.e. ASDs and PIDs. NYCWiN is used only as a transport network and the security management operating concept does not rely on any security services provided within NYCWiN.



**Figure 2-3. Network Connectivity Architecture**

## 2.5 Device Types and Interfaces

Figure 2-4 shows the RSE and its interfaces.

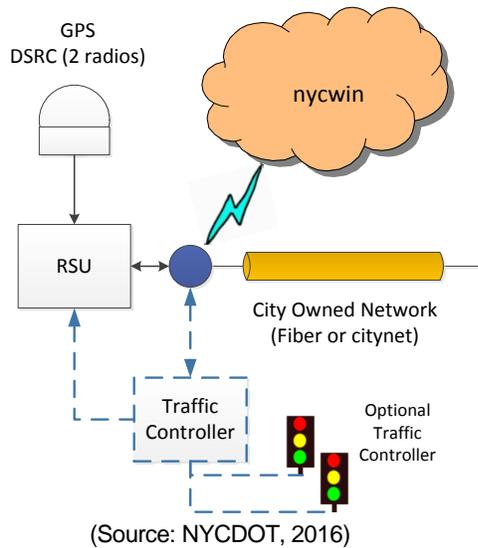


Figure 2-4. RSE Interfaces

### 2.5.1 Aftermarket Safety Device (ASD)

Figure 2-5 shows the ASD and its interfaces.

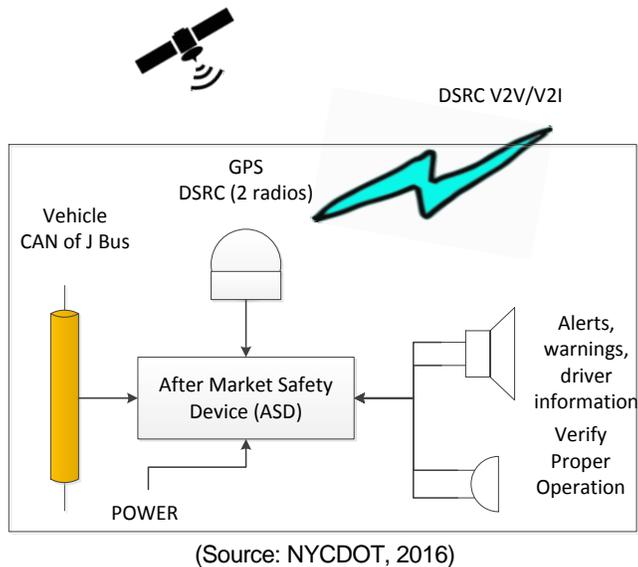
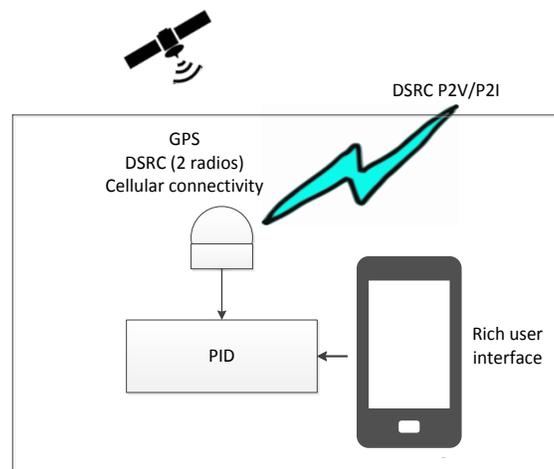


Figure 2-5. ASD Interfaces

## 2.5.2 Personal Information Device (PID)

Figure 2-6 shows the PID and its interfaces. It is currently intended that PID has two DSRC radios, but this will need to be reviewed with suppliers. Note that nothing in this SMOC relies on the PID having two DSRC radios.



(Source: NYCDOT, 2016)

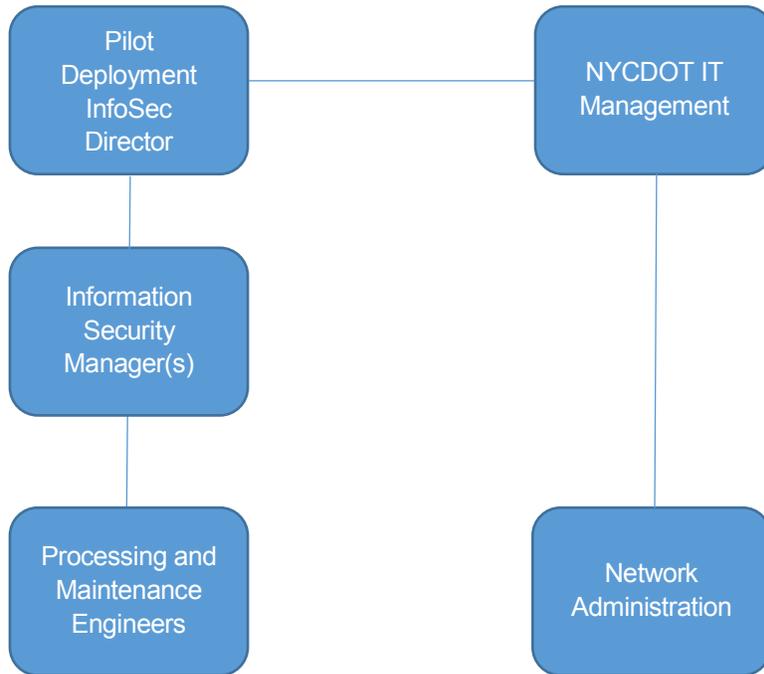
**Figure 2-6. PID Interfaces**

## 2.6 Information Security Personnel

The Pilot Deployment project will have the following roles related to information security and security management:

- **NYCDOT IT Management:** responsible for setting overall NYC DOT network security requirements and ensuring the correct operation of the backhaul. Will liaise with the Information Security Director to set policies and manage priorities.
- **Pilot deployment information security director:** responsible for overall execution of this Security Management Operating Concept, for setting policy on an ongoing basis, for liaison with SCMS Operator to ensure that requirements are clearly communicated and met, and for coordination with other Pilot Deployments and other field trials to share information about information security concerns, incidents and developments.
- **Information security manager:** may have day-to-day information security management activities delegated by the information security director.
- **Provisioning and maintenance engineers:** responsible for correct execution of security-related provisioning and maintenance activities according to this Security Management Operating Concept.
- **Network administration:** in charge of backhaul operations to ensure NYC DOT network security requirements are met.

The roles are shown in the organizational chart in Figure 2-7. Information security personnel may be existing members of NYC DOT IT staff or may be specifically hired for this task.



(Source: NYCDOT, 2016)

**Figure 2-7. Organizational Chart for Security Operations**

# Chapter 3. Security and Privacy Requirements for Usage Scenarios: Information Flows and Device Classes

## 3.1 Introduction

In this section we review security requirements of the applications and the sixteen different usage scenarios defined in the ConOps [5]. This analysis follows the methodology laid out in the Federal Highways Administration (FHWA)'s V2I Cyber Security analysis [14], which in turn is based on Federal Information Processing Standard (FIPS) 199 [13]. For each information flow we derive Confidentiality / Integrity / Availability requirements on information flows and hence the minimum acceptable security class (per the definitions of [14]) for each node within the system.

Analyses of all applications follow. Note that the security analyses for BSM-based V2V safety, Curve Speed Warning, and Mobile Accessible Pedestrian Signal System were provided by the Tampa-Hillsborough team. The analyses for Pedestrian in Signalized Crosswalk Warning and Speed Compliance in Work Zones were provided by or derived from the FHWA CIA Analysis project [14]. The sources of the C/I/A analysis for all usage scenarios is provided in Table 3-1.

Application descriptions include a diagram showing a Physical view of the application operations where appropriate. A legend for the Physical view is given in APPENDIX B.

**Table 3-1. Source of C/I/A Analysis of the NYC CVPD Applications and Operational Scenarios**

Application	Source of Analysis	Section
<b>Existing CV Applications</b>		
<b>BSM-Based Safety:</b>	THEA SMOC [18]	3.2
Blind Spot Warning		
Emergency Electronic Brake Light		
Forward Collision Warning		
Intersection Movement Assist		
Lane Change Warning/Assist		
Vehicle Turning Right in Front of Bus Warning		
<b>Red Light Violation Warning</b>	This document	3.3

Application	Source of Analysis	Section
<b>Traffic Manager Scenarios</b>		
<b>Speed Limit Compliance</b>	This document	3.4
<b>Speed Compliance / Work Zones</b>	FHWA CIA Analysis project [14], analysis is similar to Incident Scene Work Zone Alert	3.4
<b>Curve Speed Compliance</b>	THEA SMOC [18]	3.4
<b>Oversize Vehicle Compliance</b>	This document	3.5
<b>Emergency Communications and Evacuation</b>	This document	3.6
<b>Roadway User Scenarios</b>		
<b>Vehicle Trip Initiation</b>	No C//A analysis necessary, no machine-to-machine data flows	n/a
<b>Driver Reporting Suspected ASD Failure</b>	No C//A analysis necessary, no machine-to-machine data flows	n/a
<b>Pedestrian in Signalized Intersection Warning</b>	FHWA CIA Analysis project [14]	3.7
<b>Mobile Accessible Pedestrian Signal System</b>	THEA SMOC [18]	3.8
<b>System Manager Scenarios</b>		
<b>ASD CV Application Configuration Download</b>	This document	3.9
<b>ASD Firmware Update</b>	This document	3.10
<b>RSE RF Monitoring</b>	This document	3.11
<b>ASD RF Monitoring</b>	This document	3.12
<b>Independent Evaluator Scenarios</b>		
<b>ASD Event Data Recording (includes thresholds)</b>	No C//A analysis necessary, no machine-to-machine data flows	n/a
<b>ASD Event Data Upload</b>	This document	3.13
<b>Performance Measurement Data Processing</b>	This document	<b>3.14</b>

Device classes are:

- 1: Confidentiality **Low**, Integrity **Medium**, Availability **Medium**.
- 2: Confidentiality **Medium**, Integrity **Medium**, Availability **Medium**.
- 3: Confidentiality **Medium**, Integrity **High**, Availability **Medium**.
- 4: Confidentiality **High**, Integrity **High**, Availability **Medium**.

## 3.2 Existing CV Applications: BSM-based Safety

### 3.2.1 Overview

Vehicles transmit Basic Safety Messages (BSMs) up to ten times a second. Receiving vehicles use these to determine whether to alert the driver that a collision is imminent and should be avoided.

Vehicles carry out plausibility checking on BSMs before acting on them and do not act on messages that do not pass plausibility checking. Exact criteria for plausibility checking have yet to be defined and will be developed in coordination with the other Pilot Deployment sites. See APPENDIX C for discussion of one possible set of criteria for plausibility checking as proposed by the THEA CVPD team.

### 3.2.2 Information Flow Analysis

The following is the C//I/A analysis of the information flows within this family of applications. This analysis is based on that in the Tampa-Hillsborough Security Management Operating Concept [18] with grateful thanks.

**Table 3-2. C//I/A Analysis for BSM-based V2V Safety**

Source	Destination	Information Flow	C//I/A	Rationale
Remote Vehicle ASD	Vehicle ASD	Vehicle Control Event	C: L I: M A: M	C: Vehicle control event information is contained within BSM Part 2. BSM information is not confidential. I: BSM info needs to be accurate and should not be tampered with. Integrity would need to be high if there were no mitigations against bad data in incoming BSMs. In fact, there are two mitigations: plausibility checking, and misbehavior reporting plus revocation. Taking these into account we believe, with [18], that the security requirements are met by requiring an integrity level of Medium on these information flows. A: Even moderate availability of BSMs will enable a large majority of collisions between equipped vehicles to be avoided.
Vehicle ASD	Remote Vehicle ASD	Vehicle Control Event	C: L I: H A: H	See above

### 3.2.3 Device Classes

The C//I/A analysis presented in [18] identifies the following device classes for this application, with which we agree:

**Table 3-3. Baseline Device Classes for BSM-based V2V Safety**

Object	C	I	A	Class
Vehicle ASD	L	M	M	1

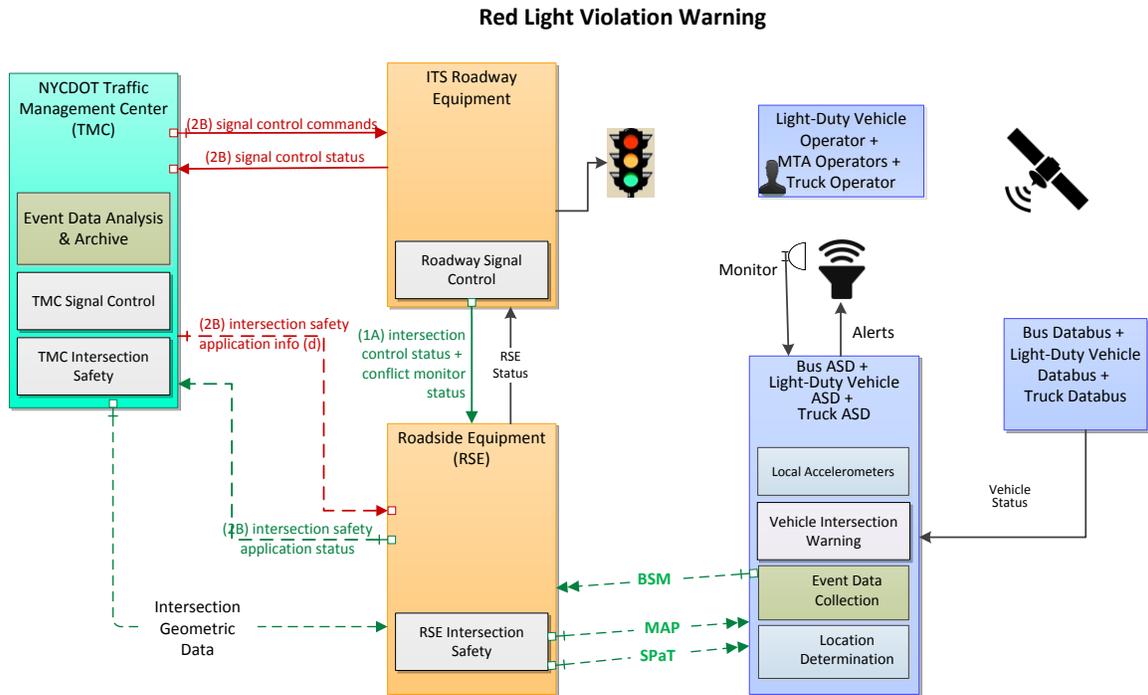
### 3.2.4 Additional Privacy Considerations

Vehicles can be tracked by their BSMs if they use a single fixed value for too long a time in any of the identifier fields (source MAC, certificate, BSM temporary ID).

## 3.3 Existing CV Applications: Red Light Violation Warning

### 3.3.1 Overview

The physical view of this application is given in Figure 3-1.



**Notes:**

1. The Security Credential Management System (SCMS) connections and support services are not shown here but are described further in this document. The SCMS will be used to secure and authenticate the data exchanges as described herein.
2. Each of the applications will include configurable event monitoring (Event Data Collection) capability which will be managed by the RSE and the data will be collected within the ASD. The RSE will advertise its ability to upload the data collected using the WSA and use DSRC to upload the data and purge the on-board temporary storage. This data will then be collected at the TMC where it will be processed on a daily basis for performance purposes.
3. All devices are synchronized to the same UTC clock reference accurate to 10 milliseconds which is used for all time points, data collection, and signal timing.

(Source: NYCDOT, 2016, modified from USDOT original)

**Figure 3-1. Physical View of Red Light Violation Application**

### 3.3.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application.

**Table 3-4. CIA Analysis for Red Light Violation Application**

Source	Destination	Information Flow	C//A	Rationale
ITS Roadway Equipment	Roadside Equipment	conflict monitor status	C: L I: H A: M	This flow tells the RSE that the traffic controller is in a failed state – typically flashing signals not timing.
ITS Roadway Equipment	Driver	driver information	C: L I: H A: M	C: “Data” (Signal condition) intentionally transmitted to everyone via a broadcast.  I: This is the primary signal trusted by the driver to decide whether to go through the intersection and what speed to go through the intersection at; if it’s wrong, accidents could happen.  A: If the lights are out you have to get a policeman to direct traffic – expensive and inefficient and may cause a cascading effect due to lack of coordination with other intersections.
ITS Roadway Equipment	Roadside Equipment	intersection control status	C: L I: H A: H	C: Data later intentionally transmitted to everyone via a broadcast.  I: If this is compromised, the Roadway Equipment and Roadside Equipment will be sending messages that are inconsistent with each other, leading to confusion and possible accidents and reducing the ability of the application to provide value. If this information is incorrect, it could lead to a collision between a vehicle and a pedestrian.  A: If this is down, the RSE doesn’t get the information it needs to stay in synch with the actual signal state, reducing or eliminating the value add from having this application. The RSE must detect a lack of availability and choose not to send out-of-date information, so a failure of availability cannot have worse consequences than a failure of integrity which we have previously assessed at HIGH.

Source	Destination	Information Flow	C//I/A	Rationale
ITS Roadway Equipment	Traffic Management Center	signal control status	C: L I: L A: L	<p>C: The current conditions of an ITS RE are completely observable, by design.</p> <p>I: TMC doesn't play an active role in this application, i.e. even if the information contained in this flow were incorrect, it is unlikely to affect the outcome of this application one way or the other.</p> <p>A: TMC doesn't play an active role in this application, i.e. even if it is unavailable, it is unlikely to affect the outcome of this application one way or the other.</p>
Roadside Equipment	Traffic Management Center	intersection safety application status	C: M I: M A: L	<p>C: This information could be of interest to a malicious individual who is attempting to determine the best way to accomplish a crime. As such it would be best to not make it easily accessible.</p> <p>I: If this is compromised, it could send unnecessary maintenance workers, or cause the appearance of excessive traffic violations, leading to further unnecessary investigation.</p> <p>A: A delay in reporting this may cause a delay in necessary maintenance, but (a) this is not time-critical and (b) there are other channels for reporting malfunctioning. Additionally, there is a message received notification, which means that RSE can ensure that all intersection safety issues are delivered.</p>
Roadside Equipment	Vehicle ASD	intersection safety warning	n/a	Explicit warnings are not used in Pilot Deployment: vehicles determine that hazard situations exist by analyzing SPAT / MAP messages
Roadside Equipment	Vehicle ASD	intersection status (Note this is the SPaT message)	C: L I: M A: M	<p>C: This data is intentionally transmitted to everyone via a broadcast. It can also be determined via other visual indicators.</p> <p>I: This information will be used by the vehicle ASD to determine whether or not to issue a red light violation warning to the driver. False information could lead to the vehicle ASD not issuing a warning when in fact it should have. The vehicle operator is not using this information to decide whether or not to travel through the intersection. They will still have visual cues, such as traffic lights, indicating whether or not they can travel through the intersection.</p> <p>A: Without this information, vehicle ASD may not properly issue a red light violation warning to the driver. The vehicle operator will still use</p>

Source	Destination	Information Flow	C//I/A	Rationale
				the traffic light to drive safely. A lack of this information will not directly cause harm.
Roadside Equipment	ITS Roadway Equipment	RSE status	C:L I: M A: M	This flow lets the traffic controller know that the RSE is operational and may be used to establish and maintain the data exchange for the SPaT data.
Traffic Management Center	Roadside Equipment	intersection safety application info	C: L I: H A: L	<p>C: Application configuration: The messages sent from the RSE are public and the warning parameters can be assumed to follow widely-known industry best practices, so management messages to configure these do not have a significant confidentiality requirement.</p> <p>C: Device management: As with TMC: Pedestrian Safety Warning Control, the device management may include proprietary information about the particular device being managed such as firmware details, memory size, processor limitations etc. The confidentiality requirement for the roadway equipment should be set by the supplier based on their understanding of the confidentiality requirements of the management messages. Note that the supplier can be assumed to provide devices that meet their own security requirements; however, the confidentiality requirements of this flow will also apply to the TMC.</p> <p>I: Fake instances of this information flow can cause drivers and pedestrians to get incorrect information (for example, swap the “crossing signal is on” and “crossing signal is off” messages so pedestrians cross at the wrong time). In particular, visually impaired people may rely on the message content to cross safely and may be endangered by bad message content. However, the impact is limited to a single crossing area and drivers still have primary responsibility for the safety of vulnerable road users, so the integrity requirement is MEDIUM rather than HIGH.</p> <p>A: Assuming that the traffic signal is configured reasonably well to start off with, the system should be robust if it goes an arbitrary amount of time without reconfiguration.</p>
Traffic Management Center	ITS Roadway Equipment	signal control commands	C: L I:M A: L	<p>C: The result of this will be directly observable</p> <p>I: The signal timing is critical to the intersection operation; incorrect signal timing can lead to significant congestion and unreliable operation;</p>

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

Source	Destination	Information Flow	C//I/A	Rationale
				<p>while unsafe operation is controlled by the cabinet monitoring system, attackers could “freeze” the signal or call a preemption.</p> <p>A: TMC doesn’t play an active role in this application, i.e. even if it is unavailable, it is unlikely to affect the outcome of this application one way or the other.</p>
Vehicle Databus	Vehicle ASD	vehicle status  <b>(not networked)</b>	C: L I: M A: M	<p>C: This can include some sensitive data. However, other data, such as vehicle location and motion will then be broadcast. There also may be proprietary information included in this.</p> <p>I: This is used later on to determine whether a vehicle is likely going to violate a red light. This needs to be correct in order for the application to work correctly.</p> <p>A: This information would need to be available immediately for the application to work. Late or missed messages would cause a warning to go unreported.</p>
Vehicle ASD	Vehicle Databus	driver update information	C: L I: M A: M	<p>C: this is just the configuration of the data requested from the data bus where a subscription is needed or where a request must be made.</p> <p>I: The data will be used to make decisions regarding warnings and must be authenticated but the data will not be sent to others.</p> <p>A: This is an important application and if not immediately available there may not be sufficient the driver to react.</p>
Vehicle ASD	Driver	driver updates (Alerts)	C: L I: M A: M	<p>C: This is a warning given to the driver. It should not contain anything sensitive, and does not matter if another person can observe it.</p> <p>I: This is a warning given to the driver. If they receive incorrect information, they may act in an unsafe manner. However, there are other indicators that would alert them to any hazards, such as flashing lights, or a flaming car in the middle of a road.</p> <p>A: If this information is not made available to the driver, then the system has not operated correctly.</p>
Vehicle ASD	Roadside Equipment	vehicle location and motion (BSM)	C: L I: M A: M	This is the standard BSM

### 3.3.3 Device Classes

Based on the C//A analysis, we have identified the following device classes for this application:

**Table 3-5. Device Classes for Red Light Violation Application**

Object	C	I	A	Class
ITS Roadway Equipment	L	H	H	3
Roadside Equipment	M	M	M	2
Traffic Management Center	M	H	L	3
Vehicle Databus	L	M	M	n/a
Vehicle ASD	L	M	M	1

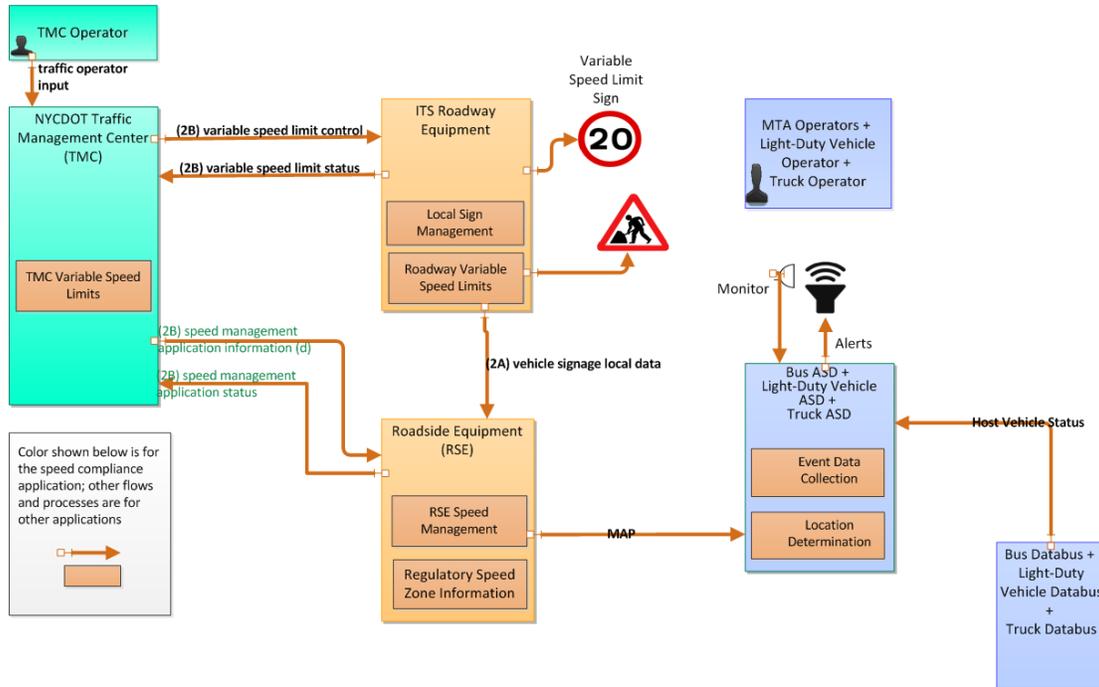
### 3.3.4 Additional Privacy Considerations

In addition to the privacy considerations noted in Section 3.2.4, it would be a violation of a driver's privacy for the fact that they have received a Red Light Violation warning to be made public.

## 3.4 Traffic Manager: Speed Compliance / Speed Compliance in Work Zones / Curve Speed Compliance

### 3.4.1 Overview

The physical view of this application as presented in the ConOps [5] is given in Figure 3-2. This is simplified from the CVRIA version of these applications (available via [3]).



(Source: NYCDOT, 2016, modified from USDOT original)

**Figure 3-2. Physical View of Speed Compliance Applications**

This application will monitor the vehicle speed and provide an alert to the driver if the vehicle speed exceeds the configured speed limit for the area by more than a configurable amount. Thus, the OBU must “know” its location and the speed limit for that roadway segment and provide the audible alert.

All speed compliance applications use the same information flows and the same security requirements.

### 3.4.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application. Note that the information flow “Monitor” in the diagram is considered by us to be obtained from the Vehicle Databus.

**Table 3-6. CIA Analysis of Speed Compliance Applications**

Source	Destination	Information Flow	C//I/A	Rationale
ITS Roadway Equipment	Roadside Equipment	vehicle signage local data	C: L I: M A: M	C: This information is directly observable I: This information impacts the vehicle signage data sent to neighboring ASDs and should be trusted to avoid sending wrong information A: The system should know if these messages are not received.
ITS Roadway Equipment	Traffic Management Center	variable speed limit status	C: L I: M A: M	C: This information is directly observable I: The TMC will react based on current status of ITS-RE and thus this information should be trusted A: The information should be available to ensure timely response from TMC
Roadside Equipment	Traffic Management Center	speed management application status	C: L I: M A: L	C: This information is directly observable I/A: Per analysis of Pedestrian in Signalized Crosswalk Warning in V2I Cybersecurity (3.3.2.16)
Roadside Equipment	Vehicle ASD	speed management information (MAP)	C: L I: M A: M	C: This information is directly observable I: Wrong information would either falsely warn or advise the driver A: These notifications are helpful to a driver, if the driver does not receive this notification immediately, there should still be other visual cues
Roadside Equipment	Vehicle ASD	vehicle signage data (MAP)	C: L I: M A: M	Per analysis of Incident Scene Work Zone Alert for Drivers and Workers in V2I Cybersecurity (3.4.2.33)
Traffic Management Center	ITS Roadway Equipment	variable speed limit control	C: L I: H A: L	C: This information is directly observable I: The information sent from TMC directly affect the ITS-RE speed “announcement”. A: The ITS-RE can work accordingly or in fail-safe if information is not available.
Traffic Management Center	Roadside Equipment	speed management application information	C: L I: M A: M	Per analysis of Pedestrian in Signalized Crosswalk Warning in V2I Cybersecurity (3.3.2.18)
Traffic Operations Personnel	Traffic Management Center	traffic operator input	n/a	Not a networked data exchange

Source	Destination	Information Flow	C//I/A	Rationale
Vehicle Databus	Vehicle ASD	host vehicle status	C: L I: M A: M	Per analysis of Pedestrian in Signalized Crosswalk Warning in V2I Cybersecurity (3.3.2.24)

### 3.4.3 Device Classes

Based on the C//I/A analysis, we have identified the following device classes for this application:

**Table 3-7. Device Classes for Speed Compliance Applications**

Device name	C	I	A	Class
ITS Roadway Equipment	L	M	M	1
Roadside Equipment	L	M	M	1
Traffic Management Center	L	H	M	3
Vehicle ASD	L	n/a	n/a	1

### 3.4.4 Additional Privacy Considerations

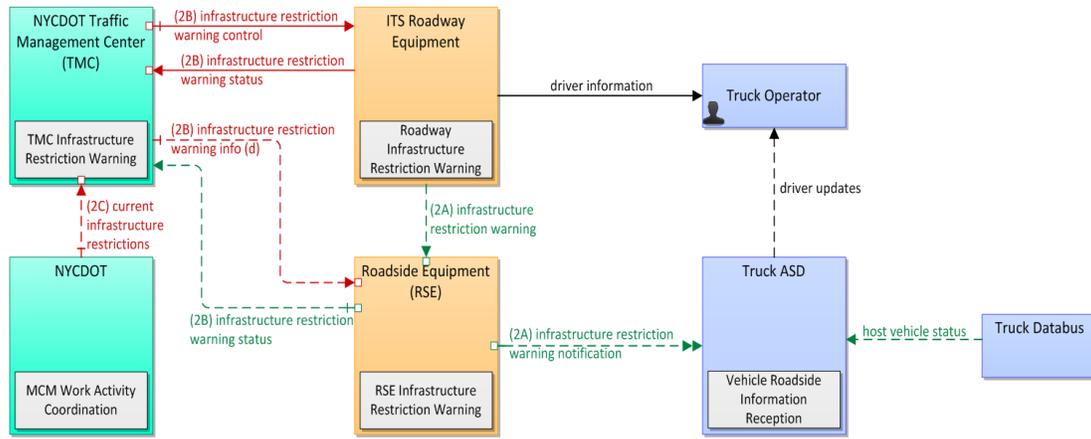
No additional privacy considerations.

## 3.5 Traffic Manager: Oversize Vehicle Compliance

### 3.5.1 Overview

The physical view of this application as presented in the ConOps [5] is given in Figure 3-3.

This application will provide an alert to the driver of an overweight vehicle if the vehicle height exceeds the permissible height on FDR Drive. Thus, the ASD must “know” the height of its host vehicle and compare it to restrictions received from the roadside equipment.



(Source: NYCDOT, 2016, modified from USDOT original)

**Figure 3-3. Physical View of Oversize Vehicle Compliance**

### 3.5.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application. Note that the information flow “Monitor” in the diagram is considered in this analysis to be obtained from the Vehicle Databas.

**Table 3-8. CIA Analysis of Oversize Vehicle Compliance**

Source	Destination	Information Flow	C//A	Rationale
ITS Roadway Equipment	Roadside Equipment	infrastructure restriction warning	C: L I: M A: M	C: This information is directly observable I: This information impacts the vehicle signage data sent to neighboring ASDs and should be trusted to avoid sending wrong information A: The system should know if these messages are not received.
ITS Roadway Equipment	Traffic Management Center	infrastructure restriction status	C: L I: M A: M	C: This information is directly observable I: The TMC will react based on current status of ITS-RE and thus this information should be trusted A: The information should be available to ensure timely response from TMC
NYCDOT	Traffic Management Center	current infrastructure restrictions	C: L I: H A: M	Per analysis of Cooperative Adaptive Cruise Control in V2I Cybersecurity (5.2.1.1.19)
Roadside Equipment	Traffic Management Center	infrastructure restriction warning status	C: L I: M A: L	C: This information is directly observable I/A: Per analysis of Pedestrian in Signalized Crosswalk Warning in V2I Cybersecurity (3.3.2.16)

Source	Destination	Information Flow	C//I/A	Rationale
Roadside Equipment	Truck ASD	Infrastructure restriction warning notification	C: L I: M A: M	C: This information is directly observable I: Wrong information would either falsely warn or advise the driver A: These notifications are helpful to a driver, if the driver does not receive this notification immediately, there should still be other visual cues
Traffic Management Center	ITS Roadway Equipment	infrastructure restriction warning control	C: L I: H A: L	C: This information is directly observable I: The information sent from TMC directly affect the ITS-RE speed “announcement”. A: The ITS-RE can work accordingly or in fail-safe if information is not available.
Traffic Management Center	Roadside Equipment	infrastructure restriction warning info	C: L I: M A: M	Per analysis of Pedestrian in Signalized Crosswalk Warning in V2I Cybersecurity (3.3.2.18)
Truck ASD	Truck Operator	driver updates	n/a	Not a networked data flow
Truck Databus	Truck ASD	host vehicle status	C: L I: M A: M	Per analysis of Pedestrian in Signalized Crosswalk Warning in V2I Cybersecurity (3.3.2.24)

### 3.5.3 Device Classes

Based on the C//I/A analysis, we have identified the following device classes for this application:

**Table 3-9. Device Classes for Oversize Vehicle Compliance**

Device name	C	I	A	Class
ITS Roadway Equipment	L	M	M	1
Roadside Equipment	L	M	M	1
Traffic Management Center	L	H	M	3
Vehicle ASD	L	M	M	1

### 3.5.4 Additional Privacy Considerations

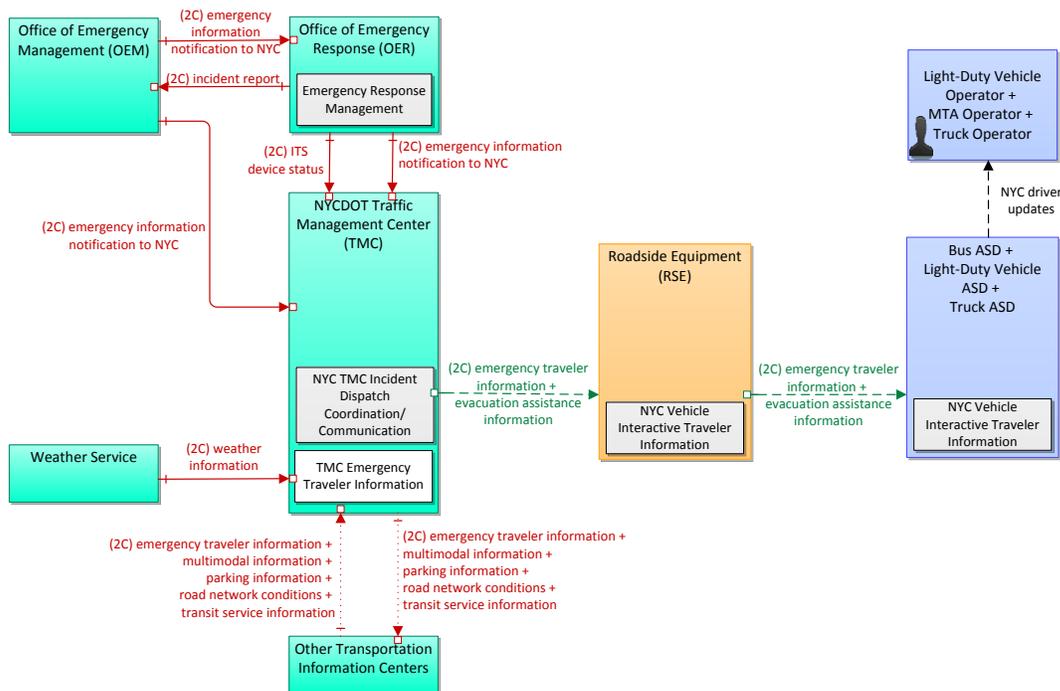
No additional privacy considerations as this application does not involve BSMs from the vehicle.

## 3.6 Traffic Manager: Emergency Communications and Evacuation Information

### 3.6.1 Overview

The physical view of this application as presented in the ConOps [5] is given in Figure 3-4.

2: Emergency Communications and Evacuation (Evacuation Traveler Information)			
2	Based on CVRIA Physical Diagram r3	Mar 01 2016	NYCAT



(Source: NYCDOT, 2016, modified from USDOT original)

**Figure 3-4. Physical View of Emergency Communication and Evacuation Information Distribution**

This application will coordinate emergency response information such as evacuation orders, routing information, and areas to avoid, and transmit it to the vehicles through the RSEs by evacuation zones. The information sent to vehicles will be encoded in TIM messages. TIM messages are sent from the TMC to the RSE, which simply acts as a repeater and does not add information to the TIM messages itself.

### 3.6.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application. Note that in this analysis we do not address flows that are purely between Center components as these flows already exist and are assumed to be secure to the task in hand.

**Table 3-10. CIA Analysis of Emergency Communication and Evacuation Information**

Source	Destination	Information Flow	C//I/A	Rationale
Traffic Management Center	Roadside Equipment	emergency traveler information + evacuation assistance information (TIM)	C: L I: H A: M	I: Incorrect information could lead to evacuation routes being taken that make the situation worse, rather than better, potentially leading to loss of life. It is better for the information to be unavailable than for it to be maliciously incorrect.
Roadside Equipment (pass-through)	Vehicle ASD	emergency traveler information + evacuation assistance information (TIM)	C: L I: M A: M	I: Incorrect information could lead to evacuation routes being taken that make the situation worse, rather than better, potentially leading to loss of life. It is better for the information to be unavailable than for it to be maliciously incorrect.
Roadside Equipment	Vehicle ASD	Service advertisement	C: L I: L A: L	This is standard WSA.

### 3.6.3 Device Classes

Based on the C//I/A analysis, we have identified the following device classes for this application:

**Table 3-11. Device Classes for Emergency Communication and Evacuation Information Distribution**

Device name	C	I	A	Class
Traffic Management Center	L	H	M	3
Vehicle ASD	L	M	M	1
Roadside Equipment	L	M	M	1

### 3.6.4 Additional Privacy Considerations

No additional privacy considerations.

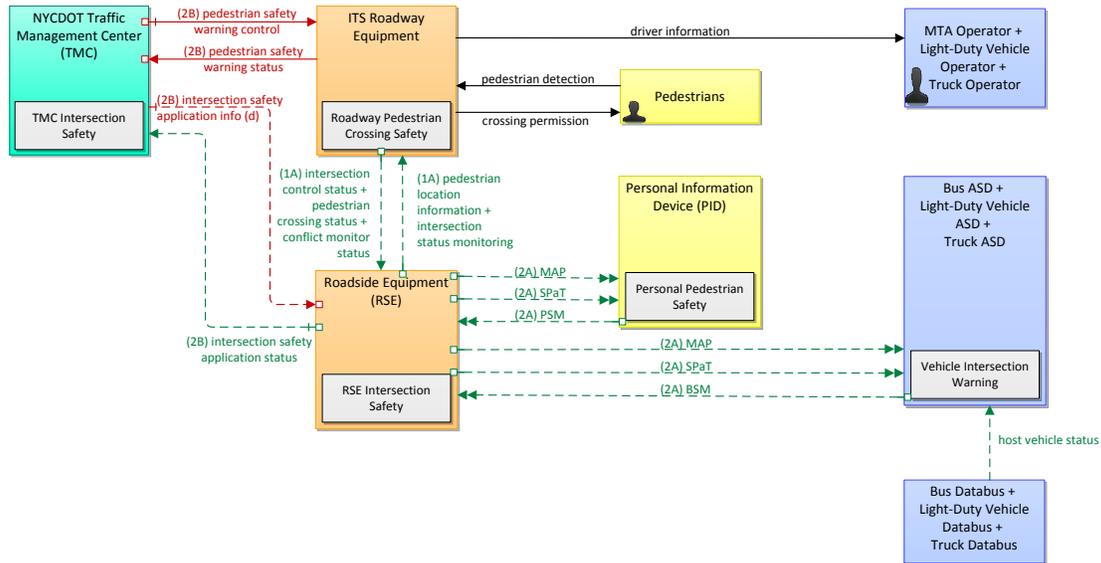
## 3.7 Roadway User: Pedestrian in Signalized Intersection Warning

### 3.7.1 Overview

This application will use the pedestrian detection information to indicate the presence of pedestrians in a crosswalk at a signalized intersection. As a pedestrian passes through a crosswalk at a signalized intersection with additional pedestrian detection equipment installed, the pedestrian’s presence will be

detected by the traffic control system. The traffic control system will notify the vehicle of a pedestrian's presence in the crosswalk. The Physical View of this application is given in Figure 3-5.

2: Pedestrian in Signalized Crosswalk Warning			
6	Based on CVRIA Physical Diagram r11	Jan 21 2016	NYCAT



(Source: NYCDOT, 2016, modified from USDOT original)

**Figure 3-5. Physical View of Pedestrian in Signalized Intersection Warning**

There are a number of different ways in which this could be implemented, and the final design has not yet been determined. In particular, there are some choices which significantly affect the security analysis:

- Will the system generate alerts when the pedestrian is crossing against the signal (i.e. to protect the pedestrian from vehicles going straight on), or only when they're crossing with the signal (i.e. to protect the pedestrian against turning vehicles)?
- If the alert can be generated when the pedestrian is crossing against the signal, it is more likely to lead to hard braking events, which carry their own risk. This therefore increases the integrity requirements on both the alert message and the inputs that trigger the alert message.
- Can the RSE generate Pedestrian Warning alert messages based only on the Pedestrian Safety Message (PSM) sent out by the PID, or does it require input from other sources such as proximity sensors?
- If the PSM can trigger warnings on its own, it has higher requirements for integrity than if proximity sensors are used

In the analysis below we distinguish between the scenarios based on the reliability needed for DSRC messages:

- Scenario R-1: RSE generates alerts for pedestrian crossing against the signal
- Scenario R-2: RSE generates alerts only for pedestrian crossing with the signal
- Scenario P-1: PID messages can be used on their own to cause RSE to generate alerts
- Scenario P-2: RSE needs input in addition to PSM to generate alerts

### 3.7.2 Information Flow Analysis

The following information flow analysis is based on the analysis carried out by the THEA project [18] with grateful thanks.

**Table 3-12. CIA Analysis for Pedestrian in Signalized Intersection Warning**

Source	Destination	Information flow	C//I/A	Rationale
ITS RE	RSE	Intersection Control Status	C: L I: H A: M	C: not encrypted and no harm should come from seeing this data  I: info needs to be accurate and should not be tampered so the RSE has correct phase info, priority status, etc.; if compromised, could lead to sending inconsistent messages which would greatly increase the possibility of collisions  A: should be immediately available so the RSE has correct phase info, priority status, etc.; however, the RSE could choose not to send out of date information
ITS RE	RSE	Conflict Monitor Status	C: L I: H A: M	C: info is not confidential or encrypted  I: if compromised, the ITS RE may not be able to support failsafe operating mode in the event of a conflict between the ITS RE and RSE  A: want this info to be available immediately but want to support wireless communication flows; the driver should also be able to see the traffic signal phases if there is a slight delay
ITS RE	RSE	Pedestrian Crossing Status	C: L I: H A: M	C: not encrypted and no harm should come from seeing this data  I: info needs to be accurate and should not be tampered so the RSE has correct crossing status, etc.  A: should be immediately available so the RSE has correct crossing status, etc. and can send that status to the PID; however, worst case is the RSE does not send out the information and the pedestrian waits to cross; also enables wireless communication

Source	Destination	Information flow	C//I/A	Rationale
ITS RE	TMC	Pedestrian Safety Warning Status	C: L I: M A: L	C: encrypted, but no harm should come from seeing this data; unless otherwise determined by the supplier because, for example it contains proprietary or security sensitive info  I: should be able to cope with some bad information on the status, because it shouldn't actually impact device control  A: want regular updates but does not have to be immediate; this could delay necessary maintenance but is not time critical
PID	RSE	Personal Location (PSM)	Scena rio P- 1:	C: Similar to Vehicle Location and Motion. Pedestrian location within the crosswalk is not confidential or encrypted. Want to protect pedestrians against being tracked, but revealing instantaneous location is key to the application  C: L I: H A: M  A: location needs to be immediately available to enable warnings and messages from the PID to RSE but availability cannot be guaranteed over a wireless medium
			Scena rio P- 2:	C: Similar to Vehicle Location and Motion. Pedestrian location within the crosswalk is not confidential or encrypted. Want to protect pedestrians against being tracked, but revealing instantaneous location is key to the application  C: L I: L A: M  I: location is informative only  A: location needs to be immediately available to enable warnings and messages from the PID to RSE but availability cannot be guaranteed over a wireless medium
RSE	TMC	Intersection Safety Application Status	C: L I: M A: L	C: not encrypted, no harm should come from seeing this data  I: should be able to cope with some bad information on the status and record of alerts/warnings; aggregate info; however could cause appearance of excessive traffic violations or unnecessary maintenance caused if data is compromised  A: want regular updates but does not have to be immediate

Source	Destination	Information flow	C//I/A	Rationale
RSE	Vehicle ASD	Intersection Safety Warning (MAP)	Scen ario R- 1	C: warning is not confidential; no harm caused from seeing warning I: warning must be accurate and not tampered with; causes safety issues if incorrect; false positive could cause unnecessary sudden braking and collisions from behind A: warning information needs to be provided to vehicle ASDs immediately in the event of a red light, etc. but cannot guarantee wireless communication
			C: L I: H A: M	
RSE	Vehicle ASD	Intersection Status (SPaT)	Scen ario R- 2:	C: warning is not confidential; no harm caused from seeing warning I: warning must be accurate and not tampered with; causes safety issues if incorrect; false positive could cause unnecessary braking and collisions from behind A: warning information needs to be provided to vehicle ASDs immediately in the event of a red light, etc. but cannot guarantee wireless communication
			C: L I: M A: M	
RSE	Vehicle ASD	Intersection Status (SPaT)	C: L I: M A: M	C: not encrypted and no harm should come from seeing this data I: info needs to be accurate and should not be tampered so the vehicle ASD has correct SPaT info for all lanes; however the driver can still see the traffic signals A: needs to be available so the vehicle ASD has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium
RSE	ITS RE	Intersection Status Monitoring	C: L I: H A: M	C: not encrypted and no harm should come from seeing this data I: info needs to be accurate and should not be tampered so the ITS RE has correct SPaT info for all lanes to be able to detect conflicts and support failsafe operating mode A: should be immediately available so the ITS RE has correct SPaT info; but should be able to support wireless communication and a slight delay
RSE	ITS RE	Pedestrian Location Information	C: L I: M A: L	C: pedestrian location within the crosswalk is not confidential or encrypted I: location should be accurate and should not be tampered; however, we assume the info is not able to cause the ITS RE to behave in extreme ways (i.e., there should be maximum different cycle phases) A: if down, the ITS RE should revert to default behavior which we assume is sensible

Source	Destination	Information flow	C//I/A	Rationale
RSE	PID	Pedestrian Safety Information	C: L I: M A: M	C: info is not confidential or encrypted I: info needs to be accurate and should not be tampered with (used to warn pedestrians of infringement, etc.); higher because enables accessibility; pedestrians may not be able to see/hear the information; however, overall I level is M, not H, because message is still just information and pedestrian needs to use their own awareness A: needs to be readily available to give permission to cross, time remaining, etc. but cannot guarantee wireless communication; however, worst case is the pedestrian has to wait; also cannot guarantee wireless communication
TMC	RSE	Intersection Safety Application Info	C: M I: H A: L	C: encrypted, authenticated, may contain proprietary information for device management I: proprietary info that should not be tampered with A: want updates but outdated information will not be serious assuming the signals are configured well to start with. Should be robust enough to go without reconfiguration for an arbitrary amount of time. However, this supports remote control of the application
TMC	ITS RE	Pedestrian Safety Warning Control	C: M I: H A: L	C: encrypted, authenticated, proprietary, but should not cause substantial risk I: proprietary info that should not be tampered with; equipment monitors and manages pedestrian crossings and provides visual displays and warnings A: System should be robust enough if it goes a while without reconfiguration
Vehicle Databus	Vehicle ASD	Host Vehicle Status	C: L I: H A: H	C: sensor data is not confidential; harm should not come from seeing status I: sensor data needs to be accurate and should not be tampered with A: sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle ASD	RSE	Vehicle Location & Motion (BSM)	C: L I: H A: M	C: BSM information is not confidential I: BSM info needs to be accurate and should not be tampered with A: BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium

### 3.7.3 Device Classes

Based on the C//A analysis, we propose the following device classes.

**Table 3-13. Proposed Device Classes for Pedestrian in Signalized Intersection Warning**

Object	C	I	A	Class
TMC	M	H	L	3
ITS RE	M	H	M	3
RSE (Scenario R-1)	M	H	M	3
RSE (Scenario R-2)	M	M	M	2
Vehicle ASD	L	M	M	1
PID (Scenario P-1)	L	H	M	3
PID (Scenario P-2)	L	L	M	1

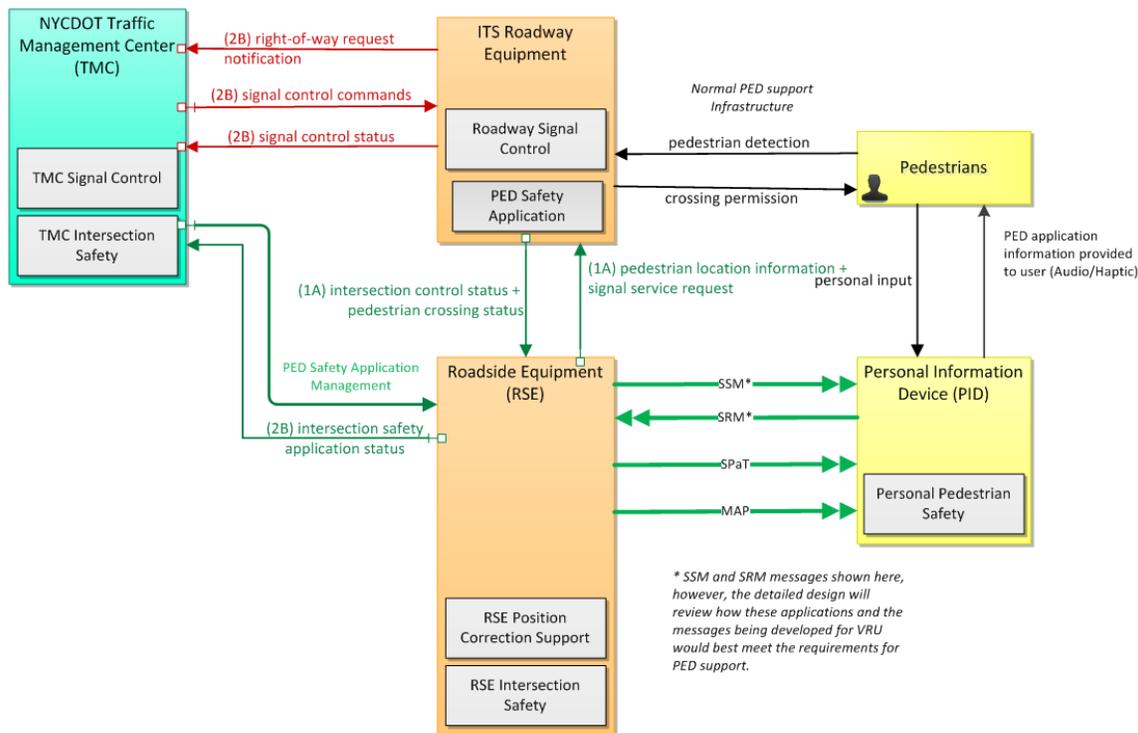
### 3.7.4 Additional Privacy Considerations

In addition to the privacy considerations noted in Section 3.2.4, both pedestrians and drivers could in principle be tracked by their safety messages.

## 3.8 Roadway User: Mobile Accessible Pedestrian Signal System

### 3.8.1 Overview

The physical view of this application is given in Figure 3-6.



(Source: NYCDOT, 2016, modified from USDOT original)

**Figure 3-6. Mobile Accessible Pedestrian Signal System**

This application supports visually impaired people in crossing the road. The application will be implemented using a portable personal device (e.g., smartphone) which supports both normal cellular operation and communications in the DSRC spectrum such that the pedestrian can monitor the messages associated with the CV applications and provide input to the traffic controller to request service where PED operation is actuated. Communications to/from the traffic controller will use DSRC (5.9 GHz. 1609.x, J2735) message sets and will be available at any intersection which includes an RSU.

The PED application will use the MAP and SPaT information received by the smart device to orient the pedestrian, assist the pedestrian in confirming their location (street and cross street), and provide verbal information regarding the signal state and thus improve their ability to safely cross the street.

The PED application will also allow the pedestrian to issue PED calls to the intersection using the DSRC and the J2735 messages that are normally used for the priority signal request management. The PED actuation is not treated as a preemption request; the PED request will be serviced in the normal phase sequence; however, under some conditions the signal timing for the PED crossing may be extended thus requiring a recovery period to re-establish the signal progression. In such circumstances, the traffic engineering review may limit the number of consecutive requests that may be honored during a configured period of time in order to minimize the impact on traffic flow.

### 3.8.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application. This analysis is based on that performed by the Tampa-Hillsborough Security Management Operating Concept with grateful thanks.

**Table 3-14. CIA Analysis for Mobile Accessible PED-SIG Application**

Source	Destination	Information type	C//A	Rationale
ITS RE	RSE	Intersection Control Status	C: L I: H A: M	C: not encrypted and no harm should come from seeing this data  I: info needs to be accurate and should not be tampered so the RSE has correct phase info, priority status, etc.; if compromised, could lead to sending inconsistent messages which would greatly increase the possibility of collisions  A: should be immediately available so the RSE has correct phase info, priority status, etc.; however, the RSE could choose not to send out of date information
ITS RE	RSE	Pedestrian Crossing Status	C: L I: H A: M	C: not encrypted and no harm should come from seeing this data  I: info needs to be accurate and should not be tampered so the RSE has correct crossing status, etc.  A: should be immediately available so the RSE has correct crossing status, etc. and can send that status to the PID; however, worst case is the RSE does not send out the information and the pedestrian waits to cross; also enables wireless communication
ITS RE	TMC	Right-of-Way Request Notification	C: L I: M A: L	C: encrypted and authenticated but no harm should come from seeing this data  I: invalid messages could lead to an unauthorized user gaining priority which could delay traffic etc.  A: not necessary for the app to work; can cope with not having immediately available data
ITS RE	TMC	Signal Control Status	C: L I: M A: M	C: encrypted and authenticated but no harm should come from seeing this data  I: info needs to be accurate and should not be tampered to enable effective monitoring and control by the TMC; should be as accurate as the right of way request  A: needs available to enable effective monitoring and control by the TMC; however if not immediately available, the app should still function

Source	Destination	Information type	C//I/A	Rationale
PID	RSE	Personal Signal Service Request	C: L I: M A: L	C: info is not confidential or encrypted I: requests should be accurate and not tampered with, otherwise incorrect or malicious requests could be granted which could lead to delays A: requests should be timely and available immediately but availability cannot be guaranteed over a wireless medium; also worst case scenario is the vehicle or pedestrian has to wait for the appropriate signal
RSE	ITS RE	Pedestrian Location Information	C: L I: M A: L	C: pedestrian location within the crosswalk is not confidential or encrypted I: location should be accurate and should not be tampered; however, we assume the info is not able to cause the ITS RE to behave in extreme ways (i.e., there should be maximum different cycle phases) A: if down, the ITS RE should revert to default behavior which we assume is sensible
RSE	ITS RE	Signal Service Request	C: L I: M A: L	C: info is not confidential or encrypted I: requests should be accurate and not tampered with, otherwise incorrect or malicious requests could be granted which could lead to delays A: requests should be timely and available immediately but availability cannot be guaranteed over a wireless medium; also worst case scenario is the vehicle or pedestrian has to wait for the appropriate signal
RSE	PID	Intersection Status	C: L I: M A: M	C: not encrypted and no harm should come from seeing this data I: info needs to be accurate and should not be tampered so the vehicle ASD has correct SPaT info for all lanes; however the driver can still see the traffic signals A: needs to be available so the vehicle ASD has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium

Source	Destination	Information type	C//I/A	Rationale
RSE	PID	Pedestrian Safety Information	C: L I: M A: M	<p>C: info is not confidential or encrypted</p> <p>I: info needs to be accurate and should not be tampered with (used to warn pedestrians of infringement, etc.); higher because enables accessibility; pedestrians may not be able to see/hear the information; however, pedestrians still need to use their own awareness, as the message simply indicates whether or not the crossing signal is not, not whether it is safe to cross.</p> <p>A: needs to be readily available to give permission to cross, time remaining, etc. but cannot guarantee wireless communication; however, worst case is the pedestrian has to wait; also cannot guarantee wireless communication</p>
RSE	TMC	Intersection Safety Application Status	C: L I: M A: L	<p>C: not encrypted, no harm should come from seeing this data</p> <p>I: should be able to cope with some bad information on the status and record of alerts/warnings; aggregate info; however could cause appearance of excessive traffic violations or unnecessary maintenance caused if data is compromised</p> <p>A: want regular updates but does not have to be immediate</p>
TMC	ITS RE	Signal Control Commands	C: L I: H A: M	<p>C: encrypted, authenticated, proprietary; but the result is directly observable</p> <p>I: proprietary info that should not be tampered with, could enable outside control of traffic signals</p> <p>A: should be able to issue immediate commands but the ITS RE should be able to continue to function using the default configuration</p>
TMC	RSE	Intersection Safety Application Info	C: M I: H A: L	<p>C: encrypted, authenticated, may contain proprietary information for device management</p> <p>I: proprietary info that should not be tampered with</p> <p>A: want updates but outdated information will not be serious assuming the signals are configured well to start with. Should be robust enough to go without reconfiguration for an arbitrary amount of time. However, this supports remote control of the application</p>

### 3.8.3 Device Classes

Based on the C//A analysis, we propose the following device classes:

**Table 3-15. NYC Proposed Device Classes for Mobile Accessible PED-SIG Application**

Object	C	I	A	Class
ITS RE	L	H	M	3
PID	L	M	L	1
RSE	M	M	M	2
TMC	M	H	M	3

### 3.8.4 Additional Privacy Considerations

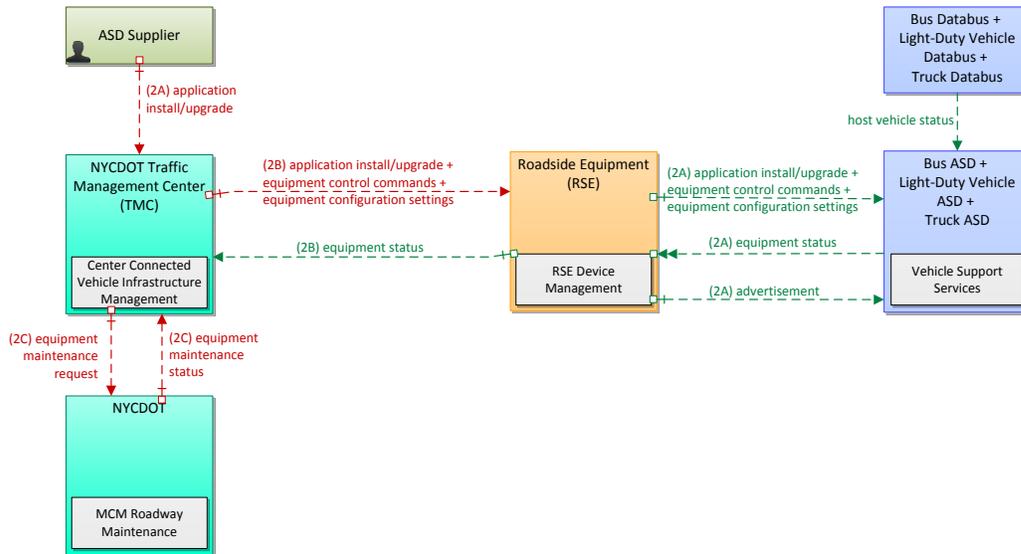
In addition to the privacy considerations noted in Section 3.2.4, pedestrians could in principle be tracked by their safety messages.

## 3.9 System Manager: ASD CV Application Configuration Download and ASD Firmware Update

### 3.9.1 Overview

The physical view of these usage scenarios is shown in Figure 3-7, following from the ConOps description [5] where both usage scenarios are shown in a single diagram. The rest of this section considers topics specific to one or other of the usage scenarios.

2: ASD Firmware Update			
5	Based on CVRIA Physical Diagram r3	May 05 2016	NYCAT



(Source: NYCDOT, 2016)

**Figure 3-7. Physical View of ASD CV Application Configuration Download and ASD Firmware Update**

**ASD CV Application Configuration:** In this application, the ConOps concept is that the TMC provide the RSE with parameter update information. When the vehicle arrives at the barn after hours, the RSE advertises the update and provide it to the ASD.

**ASD Firmware Update:** In this application, the ASD Supplier provides a firmware update to the TMC for distribution to the ASDs. The firmware update is made available via the RSEs.

### 3.9.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application.

NOTE: A number of information flows in this application are a pass-through from a component on one side of the source to a component on the other as described in [14]. A “pass through” component forwards datagrams unaltered, either live or in a store-and-forward sense. Information flows that are pass-through do not affect the I level or the C level of the pass through component.

**Table 3-16. CIA Analysis for ASD CV Application Configuration Download and ASD Firmware Update**

Source	Destination	Information flow	C//I/A	Rationale
ASD	RSE  <b>(pass-through)</b>	Equipment status	C: L I: L A: L	C: Status of equipment might be proprietary but this message will not include PII I: Forgery of equipment status messages might lead to unnecessary administrative work but will not lead to compromise of other devices A: Equipment status messages are used to determine whether or not parameter update is necessary (both centrally, whether an update should be prepared and locally, whether it should be pushed to this particular device); however, if there is a delay of a few visits to the barn before the status message is received, the impact is not severe.
ASD Supplier	TMC  <b>(pass-through)</b>	Application install / upgrade	C: L I: H A: M	C: Firmware is not confidential, anyone who wants to see it can buy an ASD for themselves. I: It is critical that malware cannot be installed on the ASDs as this would invalidate the results of the project A: System needs to be provided with firmware in a timely manner but given the time required to prepare the update, 5-9s availability for delivery of the update to the TMC is not necessary.
RSE	ASD	Advertisement	C: L I: L M: L	This is standard WSA
RSE  <b>(pass-through)</b>	ASD	Application install / upgrade	C: L I: H A: M	C: Firmware is not confidential, anyone who wants to see it can buy an ASD for themselves. I: It is critical that malware cannot be installed on the ASDs as this would invalidate the results of the project A: System needs to update firmware in a timely manner but this is not likely to be time critical.
RSE  <b>(pass-through)</b>	ASD	Equipment configuration settings	C: L I: H A: M	C: Configuration settings will not be device-specific, will not include PII, and will with high likelihood not be different among devices from different vendors. I: Malicious configuration settings could lead to widespread incorrect functioning of the system, causing it to do more harm than good. A: System needs to update configuration settings in a timely manner but this is not likely to be time critical.

Source	Destination	Information flow	C//I/A	Rationale
RSE  (pass-through)	ASD	Equipment control commands	C: L I: H A: M	<p>C: These commands will not be device-specific, will not include PII, and will with high likelihood not be different among devices from different vendors.</p> <p>I: Malicious device configuration could lead to widespread incorrect functioning of the system, causing it to do more harm than good.</p> <p>A: System needs to update device configuration in a timely manner but this is not likely to be time critical.</p>
RSE  (pass-through)	TMC	Equipment status	C: L I: L A: L	<p>C: Status of equipment might be proprietary but this message will not include PII</p> <p>I: Forgery of equipment status messages might lead to unnecessary administrative work but will not lead to compromise of other devices</p> <p>A: Equipment status messages are used to determine whether or not parameter update is necessary (both centrally, whether an update should be prepared and locally, whether it should be pushed to this particular device); however, if there is a delay of a few visits to the barn before the status message is received, the impact is not severe.</p>
TMC	RSE  (pass-through)	Application install / upgrade	C: L I: H A: M	<p>C: Firmware is not confidential, anyone who wants to see it can buy an ASD for themselves.</p> <p>I: It is critical that malware cannot be installed on the ASDs as this would invalidate the results of the project</p> <p>A: System needs to update firmware in a timely manner but this is not likely to be time critical.</p>
TMC	RSE  (pass-through)	Equipment configuration settings	C: L I: H A: M	<p>C: Configuration settings will not be device-specific, will not include PII, and will with high likelihood not be different among devices from different vendors.</p> <p>I: Malicious configuration settings could lead to widespread incorrect functioning of the system, causing it to do more harm than good.</p> <p>A: System needs to update configuration settings in a timely manner but this is not likely to be time critical.</p>

Source	Destination	Information flow	C//I/A	Rationale
TMC	RSE  (pass-through)	Equipment control commands	C: L I: H A: M	C: These commands will not be device-specific, will not include PII, and will with high likelihood not be different among devices from different vendors.  I: Malicious device configuration could lead to widespread incorrect functioning of the system, causing it to do more harm than good.  A: System needs to update device configuration in a timely manner but this is not likely to be time critical.
Vehicle Databus	ASD	Host vehicle status	C: L I: M A: L	C: Status of equipment might be proprietary but this message will not include PII  I: Incorrect information about the host vehicle should obviously be avoided: it might lead to new firmware or parameters being installed when the vehicle is in operation rather than at rest. However, it should not lead to incorrect firmware or parameters being installed and does not threaten life, because there is no control relationship from the ASD to the vehicle control systems.  A: Equipment status messages are used to determine whether or not parameter update is necessary (both centrally, whether an update should be prepared and locally, whether it should be pushed to this particular device); however, if there is a delay of a few visits to the barn before the status message is received, the impact is not severe.

### 3.9.3 Device Classes

Based on the C//I/A analysis, we propose the following device classes:

**Table 3-17. NYC Proposed Device Classes for ASD CV Application Configuration Download and ASD Firmware Update**

Object	C	I	A	Class
ASD	L	L	L	1
ASD Supplier	L	H	M	3
RSE	L	L	M	1
TMC	L	H	M	3

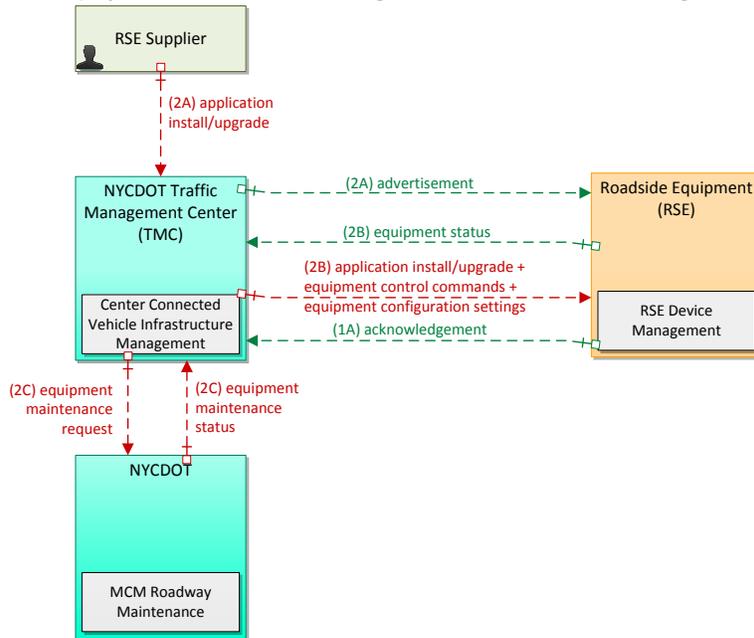
### 3.9.4 Additional Privacy Considerations

When the ASD identifies itself for purposes of receiving updates, if this identification can be overheard by an eavesdropper it will allow the eavesdropper to obtain information about the device’s behavior.

## 3.10 System Manager: RSE CV Application Configuration Download and RSE Firmware Update

### 3.10.1 Overview

This application is similar to Section 3.9 “ASD CV Application Configuration Download and ASD Firmware Update”. The physical view of these usage scenarios is shown in Figure 3-8.



(Source: NYCDOT, 2016)

**Figure 3-8. Physical View of RSE Application Configuration Download and Firmware Update**

**RSE CV Application Configuration:** In this application, the Traffic Management Center transmits parameter updates to the Roadside Equipment.

**RSE Firmware Update:** In this application, the RSE Supplier provides a firmware update to the TMC for distribution to the RSEs.

### 3.10.2 Information Flow Analysis

The following is the C//I/A analysis of the information flows within this application.

**Table 3-18. CIA Analysis for RSE CV Application Configuration Download and RSE Firmware Update**

Source	Destination	Information flow	C//I/A	Rationale
RSE Supplier	TMC  (pass-through)	Application install / upgrade	C: L I: H A: M	C: Firmware is not confidential, anyone who wants to see it can buy an RSE for themselves. I: It is critical that malware cannot be installed on the RSEs as this would invalidate the results of the project A: System needs to be provided with firmware in a timely manner but given the time required to prepare the update, 5-9s availability for delivery of the update to the TMC is not necessary.
RSE	TMC	Equipment status	C: L I: L A: L	C: Status of equipment might be proprietary but this message will not include PII I: Forgery of equipment status messages might lead to unnecessary administrative work but will not lead to compromise of other devices A: Equipment status messages are used to determine whether or not parameter update is necessary (both centrally, whether an update should be prepared and locally, whether it should be pushed to this particular device); however, if delayed, the impact is not severe.
RSE	TMC	Acknowledgement	C: L I: L A: L	C: Acknowledgment that firmware has been updated isn't device-specific and does not include PII I: Forgery of acknowledgment might lead to unnecessary administrative work but will not lead to compromise of other devices A: Acknowledgments are used to determine whether or not the update was successful, but can be determine later with the equipment status message

Source	Destination	Information flow	C//I/A	Rationale
TMC  (pass-through)	RSE	Application install / upgrade	C: L I: H A: M	C: Firmware is not confidential, anyone who wants to see it can buy an RSE for themselves. I: It is critical that malware cannot be installed on the RSEs as this would invalidate the results of the project A: System needs to update firmware in a timely manner but this is not likely to be time critical.
TMC	RSE	Equipment configuration settings	C: L I: H A: M	C: Configuration settings will not be device-specific, will not include PII, and will with high likelihood not be different among devices from different vendors. I: Malicious configuration settings could lead to widespread incorrect functioning of the system, causing it to do more harm than good. A: System needs to update configuration settings in a timely manner but this is not likely to be time critical.
TMC	RSE	Advertisement	C: L I: L A: L	This is standard WSA

### 3.10.3 Device Classes

Based on the C//I/A analysis, we propose the following device classes:

**Table 3-19. NYC Proposed Device Classes for RSE CV Application Configuration Download and RSE Firmware Update**

Object	C	I	A	Class
RSE Supplier	L	H	M	3
RSE	L	L	L	1
TMC	L	H	M	3

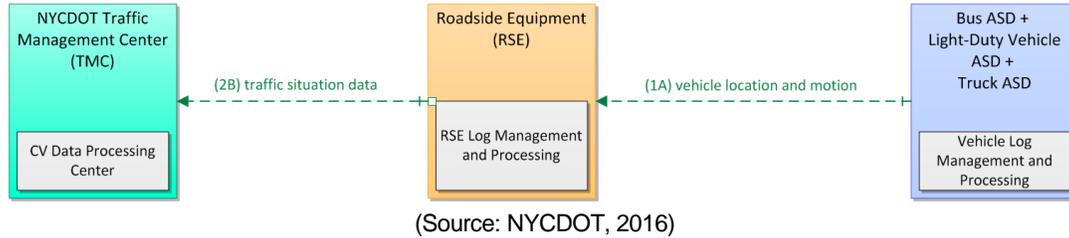
### 3.10.4 Additional Privacy Considerations

No additional privacy considerations.

## 3.11 System Manager: RSE RF Monitoring

### 3.11.1 Overview

The physical view of this usage scenario is shown in Figure 3-9.



**Figure 3-9. RSE RF Monitoring**

RSEs carry out RF monitoring using received BSMs. The RSE collects the received signal strength and the contents of the BSMs to enable analysis of the useful range of the DSRC wireless system. The first and last messages received from a source are recorded and uploaded to the TMC, where the analysis is carried out. The RSE does not continually upload, but instead stores the recorded data locally and periodically uploads it.

### 3.11.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application.

**Table 3-20. CIA Analysis for RSE RF Monitoring**

Source	Destination	Information type	C//A	Rationale
Vehicle ASD	RSE	vehicle location and motion	C: L I: M A: M	This is the standard BSM
RSE	TMC	traffic situation data	C: M I: M A: L	C: Aggregated messages may have more privacy implications than individual ones, especially if an attacker can attack more than one RSE-to-TMC connection at once.  I: as investigation might be triggered if RF quality is reported as low, this data should be trusted.  A: this data is purely for statistical purposes so low availability does not harm the application

### 3.11.3 Device Classes

Based on the C//A analysis, we propose the following device classes:

**Table 3-21. NYC Proposed Device Classes for RSE RF Monitoring**

Object	C	I	A	Class
Vehicle ASD	L	M	M	1
RSE	M	M	M	2
TMC	M	M	L	2

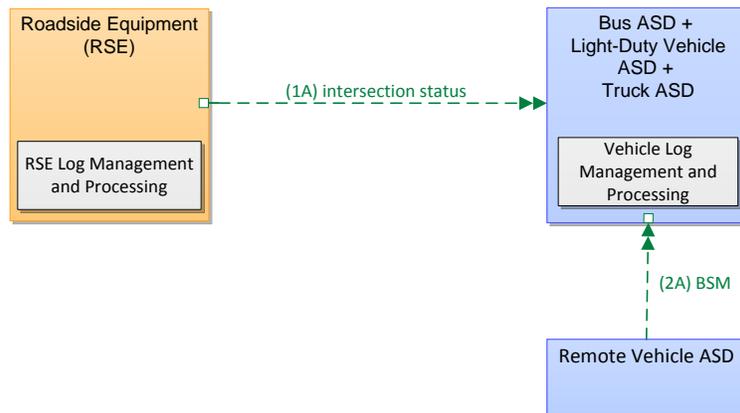
### 3.11.4 Additional Privacy Considerations

This involves collecting BSMs so is subject to the privacy considerations noted in Section 3.2.4.

## 3.12 System Manager: ASD RF Monitoring

### 3.12.1 Overview

The physical view of this application is given in Figure 3-10. Figure 3-10 covers only the monitoring part of RF monitoring. Upload is covered in Section 3.13.



(Source: NYCDOT, 2016)

**Figure 3-10. ASD RF Monitoring**

### 3.12.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application.

**Table 3-22. CIA Analysis for ASD RF Monitoring**

Source	Destination	Information type	C//A	Rationale
Remote Vehicle ASD	Vehicle ASD	vehicle location and motion (BSM)	C: L I: M A: M	This is the standard BSM
RSE	Vehicle ASD	intersection status	C: L I: M A: M	C: not encrypted and no harm should come from seeing this data I: info needs to be accurate and should not be tampered so the vehicle ASD has correct SPaT info for all lanes; however the driver can still see the traffic signals A: needs to be available so the vehicle ASD has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium

### 3.12.3 Device Classes

Based on the C//A analysis, we propose the following device classes:

**Table 3-23. NYC Proposed Device Classes for ASD RF Monitoring**

Object	C	I	A	Class
Vehicle ASD	L	n/a	n/a	1
RSE	L	M	M	1
Remote Vehicle ASD	L	M	M	1

### 3.12.4 Additional Privacy Considerations

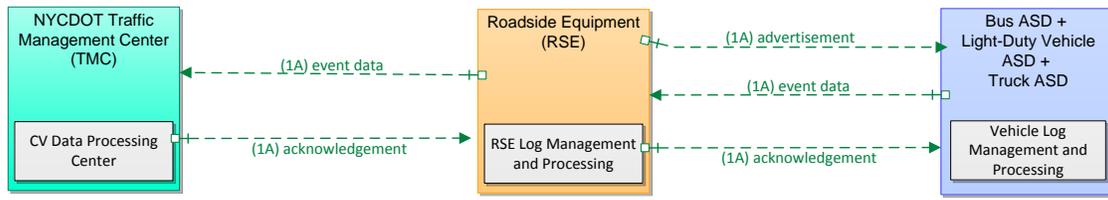
This involves collecting BSMs so is subject to the privacy considerations noted in Section 3.2.4.

## 3.13 Independent Evaluator: ASD Event Data Upload

### 3.13.1 Overview

The physical view of this application is given in Figure 3-11. In this application, the RSE acts as a buffer for the ASD event data. The RSE advertises event data collection; the ASD uploads its event log entries. The RSE does not carry out any processing on the data but instead forwards it, not necessarily immediately, to the TMC for analysis.

The TMC subsequently interacts with the ASD within the ASD CV Application Configuration usage scenario to confirm upload, allowing the ASD to purge successfully uploaded log file entries.



(Source: NYCDOT, 2016)

Figure 3-11. ASD Event Data Upload

### 3.13.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application.

Table 3-24. CIA Analysis for ASD Event Data Upload

Source	Destination	Information type	C//A	Rationale
ASD	RSE  (pass-through)	event data (BSM + MAP)	C: M I: M A: L	C: potentially PII, should not be easy for unauthorized parties to read. I: as investigation might be triggered if data quality is reported as low, this data should be trusted. A: this data is purely for statistical purposes so low availability does not harm the application
RSE	TMC  (pass-through)	event data	C: M I: M A: L	C: potentially PII, should not be easy for unauthorized parties to read. I: as investigation might be triggered if data quality is reported as low, this data should be trusted. A: this data is purely for statistical purposes so low availability does not harm the application
RSE	ASD	advertisement	C: L I: L A: L	This is standard WSA
RSE	ASD	acknowledgment	C: L I: M A: L	C: doesn't convey any sensitive information I: forging this information would enable attackers to force ASDs to delete their log files (thinking they were uploaded successfully to RSEs) A: the only risk is that the device doesn't purge its log files and runs out of storage space.

### 3.13.3 Device Classes

Based on the C//A analysis, we propose the following device classes:

**Table 3-25. NYC Proposed Device Classes for ASD Event Data Upload**

Object	C	I	A	Class
ASD	M	M	L	2
RSE	L	M	M	1
TMC	M	M	L	2

The result that the ASD needs to be class 2 is derived from the fact that the outgoing event data dataflow has confidentiality level M. However, as discussed in Section 4.3.13, the NYC CVPD team plans to encrypt event data immediately with the public key of the TMC, so that the event data is never available in cleartext even to a process running on the ASD. We consider that this allows us to level the ASD down to Class 1, resulting in the following device classes:

**Table 3-26. NYC Proposed Device Classes for ASD Event Data Upload**

Object	C	I	A	Class
ASD	L	M	L	1
RSE	L	M	M	1
TMC	M	M	L	2

### 3.13.4 Additional Privacy Considerations

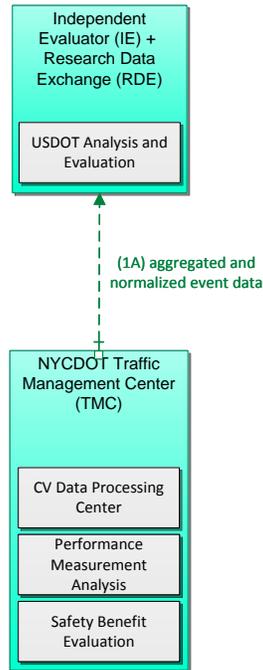
This involves collecting BSMs so is subject to the privacy considerations noted in Section 3.2.4.

Additionally, if the ASD repeatedly uploads identical packets, it can be tracked from location to location by those packets. The packets must be randomized so that two uploads of the same underlying log information cannot be identified as identical.

## 3.14 Independent Evaluator: Performance Measurement Data Processing

### 3.14.1 Overview

The physical view of this application is given in Figure 3-12.



(Source: NYCDOT, 2016)

Figure 3-12. Performance Measurement Data Processing

### 3.14.2 Information Flow Analysis

The following is the C//A analysis of the information flows within this application.

Table 3-27. CIA Analysis for Performance Measurement Data Processing

Source	Destination	Information type	C//A	Rationale
TMC	IE	aggregated and normalized event data	C: M I: M A: L	C: confidential data provided to independent evaluator is likely to have a lower level of aggregation and normalization than the one provided to RDE.  I: data should be trusted  A: this data is purely for statistical purposes so low availability does not harm the application

Source	Destination	Information type	C//I/A	Rationale
TMC	RDE	aggregated and normalized event data	C: M I: M A: L	C: access control to the data should be in place at the RDE I: data should be trusted A: this data is purely for statistical purposes so low availability does not harm the application

### 3.14.3 Device Classes

Based on the C//I/A analysis, we propose the following device classes:

**Table 3-28. NYC Proposed Device Classes for Performance Measurement Data Processing**

Object	C	I	A	Class
TMC	M	M	L	2
IE	M	n/a	n/a	2
RDE	M	n/a	n/a	2

### 3.14.4 Additional Privacy Considerations

The bulk data that is uploaded could, on its own or in combination with other databases, be used to track individual vehicles or learn PII about them or their behavior.

## 3.15 Device Classes Considered in NYC Pilot Site

In this section we review the security classes for the field devices and determine which classes can support which applications. The TMC is omitted from this analysis as the focus is on field devices.

**Table 3-29. Consolidated Device Classes by Type and Application / Usage Scenario**

Device type	Security class	Supports applications
ASD	1	V2V safety; Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Emergency Communication and Evacuation Information Distribution; Pedestrian in Signalized Intersection Warning; ASD CV Application Configuration Download and ASD Firmware Update; RSE RF Monitoring; ASD RF Monitoring; ASD Event Data Upload
PID	1	Mobile Accessible PED-SIG; Pedestrian in Signalized Crosswalk Warning (Scenario P-2)
	2	
	3	Pedestrian in Signalized Crosswalk Warning (Scenario P-1)

Device type	Security class	Supports applications
RSE	1	Speed Compliance; Oversize Vehicle Compliance; Emergency Communication and Evacuation Information Distribution; ASD CV Application Configuration Download and ASD Firmware Update; RSE CV Application Configuration Download and RSE Firmware Update; ASD Event Data Upload
	2	Red Light Violation; Pedestrian in Signalized Intersection Warning (scenario R-2); Mobile Accessible PED-SIG; RSE RF Monitoring
	3	Pedestrian in Signalized Intersection Warning (Scenario R-1)
ITS-RE	1	Red Light Violation; Speed Compliance; Oversize Vehicle Compliance
	2	
	3	Pedestrian in Signalized Intersection Warning; Mobile Accessible PED-SIG

Based on this analysis we make the following recommendation:

- **ASD:** All are Class 1 devices
- **PID:**
- If used for Mobile Accessible PED-SIG and/or for Pedestrian in Signalized Intersection Warning scenario P-2, PIDs are Class 1 devices.
- If used in Pedestrian in Signalized Intersection Warning scenario P-11, PIDs are Class 3 devices.
- **RSE:**
- There may be RSEs that support all applications except Pedestrian in Signalized Intersection Warning scenario R-1. These will be Class 2 devices.
- RSEs that support all applications including Pedestrian in Signalized Intersection Warning scenario R-2 will be Class 3 devices.
- **ITS-RE:** Although the requirements on information flows between ITS-RE and RSE suggest that some ITS-RE devices should be Class 3, we recognize that in practice it is unlikely that new, high security ITS-RE devices will be procured for all sites within this project. Where new ITS-RE devices are procured, they shall be Class 3, enabling them to be used in all applications. Existing ITS-RE devices within NYC have a cryptographic processor that enables TLS and IPsec. They have not been evaluated to be Class 3 compliant but will be grandfathered in.

# Chapter 4. Communications Security and Privacy by Usage Scenario

## 4.1 General

This section identifies the security mechanisms to be used to secure information flows within NYC CVPD. **This document identifies security mechanisms only for new flows**, i.e. for flows that involve an RSE, ASD or PID. The assumption is that existing flows are sufficiently secure already.

This section is structured as follows.

Section 4.2 provides an overview of the candidate security mechanisms and the security management that must be implemented in order for those security mechanisms to work.

- Section 4.2.1 describes existing NYC DOT practice (for illustration only; as noted above, this document assumes that this meets security requirements for existing information flows)
- Section 4.2.2 describes communications security based on IEEE 1609.2.
- Section 4.2.3 describes SNMPv3, which we recommend for device management in combination with Transport Layer Security (TLS).
- Section 4.2.4 describes the use of Virtual Private Networks (VPNs) and recommends the use of ones based on Transport Layer Security (TLS).
- Section 4.2.5 describes Transport Layer Security (TLS).

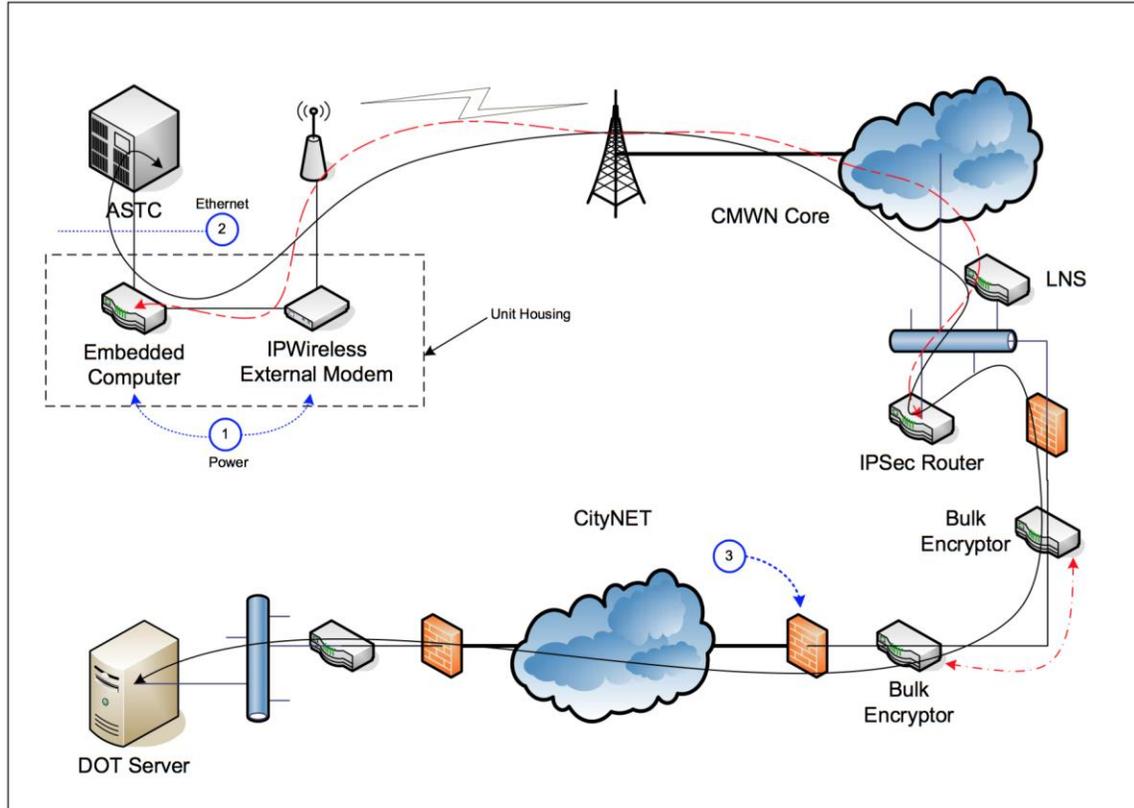
Section 4.3 then, for each of the NYC CVPD-specific information flows within each application, identifies which of the above security mechanisms is to be used within NYC CVPD.

## 4.2 Overview of Existing Security Mechanisms

### 4.2.1 Current NYC DOT Approach

Figure 4-1 shows the current NYC DOT approach. Commands are sent from the DOT server (bottom left) to the Traffic Signal Controller (ASTC, top left, referred to as the ITS-RE in this document); responses are sent back from the ASTC to the DOT. Authentication and confidentiality are provided by the use of the line encryptors. “CMWN Core” is the same as NYCWiN.

This approach does not provide end-to-end authentication or encryption and so does not meet the needs for new information flows in NYC CVPD. It is described for information only. Note that there is also no ability to navigate the network backward from the ASTC to the central systems since that is all protected by limiting the ports, and IP addresses.



(Source: NYCDOT, 2016)

**Figure 4-1. Network Security in Current NYC DOT System**

## 4.2.2 IEEE 1609.2

IEEE 1609.2 [6] provides mechanisms for communications security via digital signatures, encryption, and certificates.

Certificates are tied to a particular application activity and permit:

- The application that “owns” the certificate to participate in permitted activities associated with that application, which are indicated by the Provider Service Identifier (PSID) [8] and, if necessary, Service Specific Permissions (SSP) defined for use with that application.
- Peer applications on other devices to encrypt information for the owning application, to be transmitted in a store-and-forward manner to the owning application.

### 4.2.2.1 Authorization to Send

Security management is carried out by interactions with the Security Credential Management System (SCMS). These interactions are not defined in IEEE 1609.2 but will be carried out according to the interfaces defined by the Crash Avoidance Metrics Partnership (CAMP) [17].

- On initialization the host device obtains an *enrolment certificate* for the application. The enrolment certificate is used for security management. The application is identified using a Provider Service Identifier (PSID) in the certificate. Multiple applications may share an enrolment certificate, or different applications may use different enrolment certificates. The enrolment certificate typically has a lifetime approximately as long as the expected lifetime of the device.
- Each application (or set of applications sharing an enrolment certificate) uses that enrolment certificate to request one or more *authorization certificates*. An authorization certificate is used during operation of the applications to demonstrate authorization to peer instances of the application on other devices. CAMP identifies three different types of certificates:
  - *Application Certificates*: these are used by infrastructure entities to authenticate and authorize application messages (for example, RSEs authorizing WSA or SPaT, or TMC authorizing MAP or TIM). They typically have a lifetime of a week, with a small overlap between certificates so that the next one becomes valid shortly before the previous one expires. With the exception of the overlap period, the RSE typically has one application certificate valid for any given application at any given time.
  - *Vehicle Identified Certificates*: these are used by ASDs (and PIDs, despite the name) to authenticate and authorize application messages when the privacy of the ASD is not a significant consideration, for example when the ASD is requesting signal preemption or some similar highly-privileged action such that accountability in the use of that power is important. Like RSE application certificates, they typically have a lifetime of a week, with a small overlap between certificates so that the next one becomes valid shortly before the previous one expires. With the exception of the overlap period, each ASD identified application typically has one certificate valid at any given time. **These are not used in NYC CVPD.**
  - *Vehicle Pseudonym Certificates*: these are used by the ASD and PID in cases where it is not taking highly-privileged actions and there is more of a public interest in protecting the driver's privacy than in tracking the driver: for example, when sending Basic Safety Messages. They typically have a lifetime of a week, like the other two types of certificates, but in contrast to the other types of certificates the ASD will have several at a time: the recommended minimum that are valid at any given time is 20, and larger numbers are possible. This allows the certificate holder to change certificate from time to time, making it difficult for an eavesdropper to track the movements of that vehicle unless they were eavesdropping at the time the certificate changed. **These are used for all ASD based applications in NYC CVPD.**
- The device uses its authorization certificates, which contain an expiration date, until some configurable time before that expiration date arises. At that point it requests the SCMS for more authorization certificates, authenticating the request with its enrolment certificate.
- If the device is observed to be malfunctioning and outputting data that significantly endangers the integrity or correct functioning of the system, it can be *revoked*. In this case a data object known as a Certificate Revocation List (CRL) is distributed to field devices instructing them no longer to trust messages signed by the indicated certificates. (For pseudonym certificates the CRL contains information elements allowing all certificates for a single application instance to be revoked with a single entry on the CRL).

- If all of an application's authorization certificates have expired (for example, if it has not had connectivity to the SCMS since the last trigger time for certificate request) it does not send application messages until it has obtained more certificates.
- If an application's enrolment certificate has expired it must re-enroll. This is a manual process.

**NYC CVPD will use 1609.2 security for all messages sent over DSRC other than ASD configuration and ASD firmware update.**

#### **4.2.2.2 Verification on Receive**

On receiving a message, the receiver carries out a number of verification checks to ensure the message is valid. These are described in detail in [6] so the description below does not explain every term. The checks are:

- Check that the data is *relevant*, i.e. that it has been generated sufficiently close to the receiving device and sufficiently recently to be of interest. "Sufficiently close" and "sufficiently recently" are application-specific.
- Check that the data is *consistent* with the certificate, i.e. that all fields in the received data (both security header fields and message content) are within the range of values permitted by the certificate.
- Check that the signature on the message *cryptographically verifies* using the public key obtained from the sender's certificate.
- Check that the sender's certificate is part of a valid *certificate chain* constructed back to a known *root certificate authority (Root CA)*
- Check whether the sender's certificate, or any certificate in the chain, will appear on a revocation list, and for any certificate that will appear on a revocation list, check whether it has been revoked.

A message is considered valid only if none of these checks indicate that it is invalid. The verification process is illustrated in Figure 4-2.

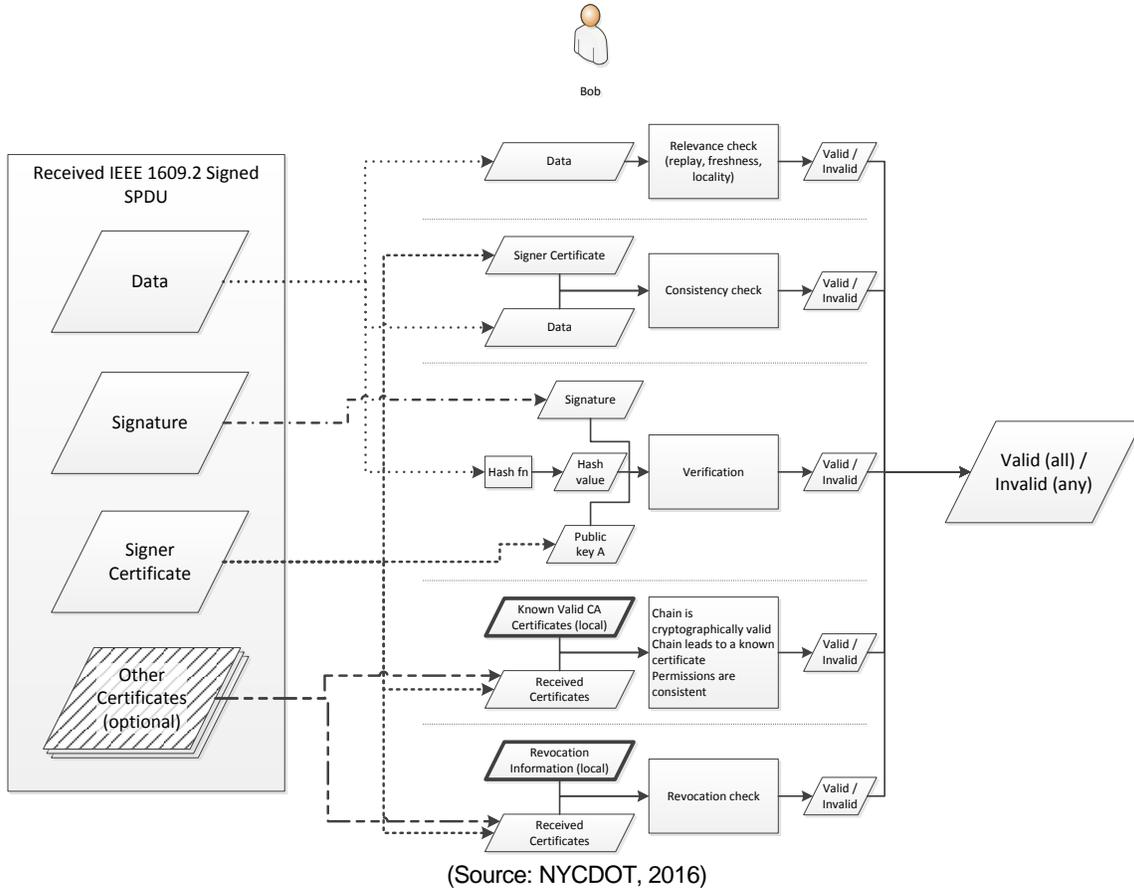


Figure 4-2. IEEE 1609.2 Verification Process

All devices that use 1609.2 verification shall ensure that the root certificates used to construct a chain for verification are stored in such a way that they are protected by secure hardware from modification. See Section 5.1.3.2 for further discussion.

No end-entity devices controlled by NYC CVPD will appear on CRLs. See Sections 5.3.4 and 6.2.8 for further discussion.

### 4.2.2.3 Choosing Which Entity Signs Infrastructure-Originating Messages

In this project, the decision has been made that the entity that takes responsibility for the data is the one who signs it. For example in the Emergency Communications and Evacuation Information application, the information regarding evacuation routes are the responsibility of the TMC. Therefore, the TMC will sign this data and the RSEs will only forward it without signing it. From the ASD point of view, even though the data is sent by the RSE, we refer to it as *centrally signed* when signed by the TMC, and *locally signed* when signed by the last sender in the chain. In the case where RSEs have to use their local data to augment TMC input, then the RSEs will sign the data, because should take responsibility for it. Moreover, choosing the *locally signed* approach would increase the computation load on the RSEs for no good reason and would not improve security or privacy.

### 4.2.3 SNMPv3

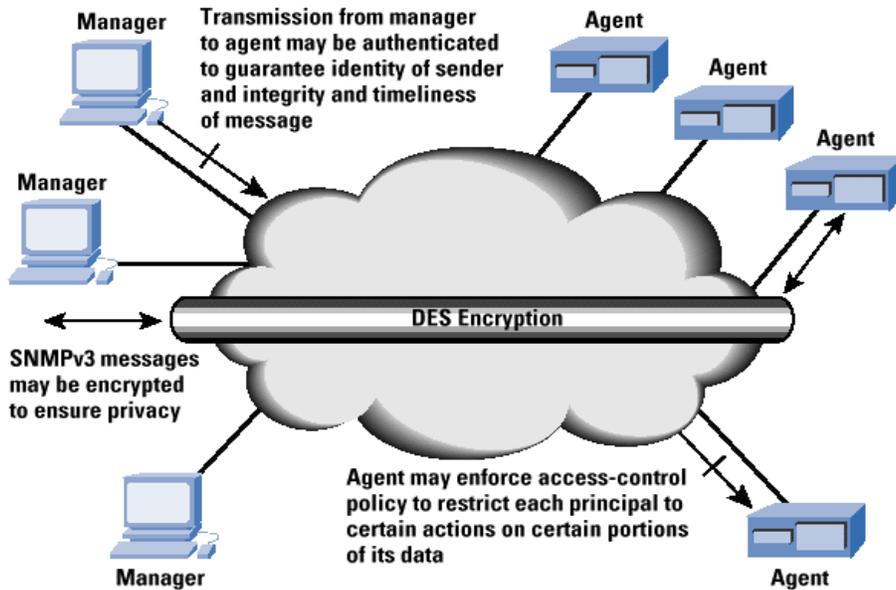
The Simple Network Management Protocol (SNMP) version 3 provides secure mechanisms for remotely managing devices. NYC CVPD will use SNMP for control of the RSEs and for configuring ASDs.

SNMP v3 is defined in the Internet Request for Comments (RFCs) identified in Table 4-1.

**Table 4-1. SNMPv3 RFCs**

RFC Number	Title
2271	An Architecture for Describing SNMP Management Frameworks
2272	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
2273	SNMPv3 Applications
2274	User-Based Security Model for SNMPv3
2275	View-Based Access Control Model (VACM) for SNMP
5591	Transport Security Model for SNMP

SNMPv3 includes three important services: authentication, privacy, and access control (Figure 4-3). To deliver these services in a flexible and efficient manner, SNMPv3 introduces the concept of a principal, which is the entity on whose behalf services are provided or processing takes place. A principal can be an individual acting in a particular role; a set of individuals, with each acting in a particular role; an application or set of applications; or combinations thereof. In essence, a principal operates from a management station and issues SNMP commands to agent systems. The identity of the principal and the target agent together determine the security features that will be invoked, including authentication, privacy, and access control. The use of principals allows security policies to be tailored to the specific principal, agent, and information exchange, and gives human security managers considerable flexibility in assigning network authorization to users.



(Source: [19], used by permission of the author)

**Figure 4-3. SNMPv3 Security Features**

The TMC will run the Network Management Station (i.e. ‘principal’ or ‘manager’), while RSEs and ASDs will run SNMP agent. SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

SNMP supports two security approaches, the User Security Model (USM) and Transport Layer Security (TLS).

In the USM, each user has a name (called a **securityName**) an authentication type (**authProtocol**) and a privacy type (**privProtocol**) as well as associated keys for each of these (**authKey** and **privKey**).

Authentication is performed by using a user's **authKey** to sign the message being sent. The **authProtocol** can be either *HMAC-SHA-2* [RFC7630]. **authKeys** (and **privKeys**) are generated from a passphrase that must be at least 8 characters in length.

Encryption is performed by using a user's **privKey** to encrypt the data portion of the message being sent. The **privProtocol** can be either *AES* or *DES*.

SNMPv3 can run with USM and recognizes three levels of security:

- Without authentication and without privacy (noAuthNoPriv).
- With authentication but without privacy (authNoPriv).
- With authentication and with privacy (authPriv).

Starting with version 5.6, Net-SNMP has the ability to tunnel SNMPv3 packets over the TLS and DTLS protocols. These protocols offer their own negotiation of security algorithms to use and thus the resulting security is dependent on that negotiation. It is possible to configure OpenSSL, which Net-SNMP relies on for the connections, to use stronger authentication and encryption algorithms than the ones that are offered by SNMPv3 with USM.

SNMP version 3 may be subject to brute force and dictionary attacks for guessing the authentication keys, or encryption keys, if these keys are generated from short (weak) passwords, or passwords that can be found in a dictionary. SNMPv3 allows both providing random uniformly distributed cryptographic keys, and generating cryptographic keys from password supplied by user, in which case caution is advised, and the risks are higher. The risk of guessing authentication strings is negligible, considering that for MD5- and SHA1-based authentication protocols the length of such a string is 96 bits, therefore the probability to successfully forge an authenticator is vanishingly small (being hit by lightning is likelier). Probability of finding two messages with the same authenticator is greater, but it still requires a pool of 248 valid messages to choose from, so is it not overly concerning, given the usage model (hard to accumulate that many messages for the same destination within the message lifetime of 5 minutes). With the acceptance of the HMAC-SHA-2 Authentication Protocol for USM, risks are even lower. The risk of guessing encrypted strings is too low to consider.

Because both the Transport Security Model, with TLS or DTLS, and the User-based Security Model offer comparable protection against security threats, the network manager can choose which should be used based on the type of key management system that works best for the organization. An organization with an existing system for managing SNMP's USM user keys need not migrate to a X.509-based security infrastructure solely for the purpose of security for SNMP. However, organizations that have already invested in an X.509 public key infrastructure can reap further benefit by managing SNMP users, applications, and devices under the same system. When implementing new configurations for transport-based security including TLS and DTLS, it is a good idea to also configure USM users as a backup measure.

**The NYC CV PD will use SNMPv3 with TLS per RFC5591 [10] to manage RSEs and to update ASD configuration. This will require the client and the server to be issued with X.509 certificates. These certificates will be issued with an in-house X.509 CA run on behalf of the TMC. ASDs and RSEs will obtain an X.509 certificate for SNMP with a five-year lifetime at provisioning time as specified in Section 4.2.5.**

**The ASDs and RSEs will be configured to trust only the in-house X.509 CA certificate for incoming SNMP authentication. A new trusted CA can only be added to the list of trusted CAs as part of a device reset.**

## 4.2.4 VPN

A VPN creates a virtual “tunnel” connecting the two endpoints. The traffic within the VPN tunnel is encrypted so that other users of the public Internet can not readily view intercepted communications.

There are two options, IPsec-based and SSL/TLS-based. Software supporting both approaches is widespread and easy to obtain. However, SSL VPNs allow more precise access control. First of all they provide tunnels to specific applications rather than to the entire corporate LAN. So, users on SSL VPN connections can only access the applications that they are configured to access rather than the

whole network. Second, it is easier to provide different access rights to different users and have more granular control over user access.

Best practices:

- Restricting physical access to server that runs VPN server.
- Using strong authentication and encryption: Transport Level Security (TLS) with client certificates
- Operating system and domain functional level: enforce software and system configurations for RSE
- Assigning IP addresses: it is not a good idea to let VPN clients specify their own IP addresses. This should be done by the VPN server or the DHCP server. If the VPN server handles more than 20 concurrent connections, use the VPN server to allocate IP address leases to remote access clients. When creating a pool of IP addresses make sure that none of them are already in use by the DHCP server or servers on the network.
- Use real-time end-point monitoring

RECOMMENDATION: OpenVPN with **TLS** -- Use SSL/TLS + certificates for authentication and key exchange.

- CRL
- Specify TLS cipher-suites: AES 256
- Client-side certificate: generate with the software bundled with OpenVPN

**Note:** In SSL/TLS mode, an SSL session is established with bidirectional authentication (i.e. each side of the connection must present its own certificate). If the SSL/TLS authentication succeeds, encryption/decryption and HMAC key source material is then randomly generated by OpenSSL's RAND\_bytes function and exchanged over the SSL/TLS connection. Both sides of the connection contribute random source material. This mode never uses any key bidirectionally, so each peer has a distinct send HMAC, receive HMAC, packet encrypt, and packet decrypt key. If **--key-method 2** is used, the actual keys are generated from the random source material using the TLS PRF function. If **--key-method 1** is used, the keys are generated directly from the OpenSSL RAND\_bytes function. **--key-method 2** was introduced with OpenVPN 1.5.0 and is the default in OpenVPN 2.0.

During SSL/TLS rekeying, there is a transition-window parameter that permits overlap between old and new key usage, so there is no time pressure or latency bottleneck during SSL/TLS renegotiations.

**The NYC CVPD will use persistent TLS-based VPN connectivity to the RSEs to provide for bulk data upload.**

## 4.2.5 TLS

Transport Layer Security (TLS) is an internet standard defined in RFC 5246 [9] and associated IETF documents. In the NYC CVPD, TLS will be used directly to encrypt and/or authenticate a number of information flows. Where used, **TLS will obey the following requirements:**

- Both client and server authentication is used
- Implementations will follow the appropriate Best Practices given in RFC 7525 [11].
- The TMC has a certificate with subjectAltName equal to tmc.cvpd.dot.nyc.gov.
- ASDs have a certificate with subjectAltName equal to asd-XXXX.cvpd.dot.nyc.gov, where XXXX is a four-hex digit serial number for the ASD, allowing for up to 65536 distinct ASDs.
- RSEs have a certificate with subjectAltName equal to rse-XXXX.cvpd.dot.nyc.gov, where XXXX is a four-hex digit serial number for the RSE, allowing for up to 65536 distinct RSEs.
- ITS-REs have a certificate with subjectAltName equal to its-re-XXXX.cvpd.dot.nyc.gov, where XXXX is a four-hex digit serial number for the RSE, allowing for up to 65536 distinct RSEs.
- The TLS configuration will be based on elliptic curve cryptography with 256-bit keys and support forward secrecy.
- For efficiency, session resumption may be supported

#### MANAGEMENT REQUIREMENTS:

- Client-side:
  - A client-side implementation must have access to at least one trusted X.509 CA certificate that issues the server-side certificate.
  - A client-side implementation should trust as few X.509 CA certificates as necessary
  - A client-side implementation that uses client certificate authentication must have an X.509 certificate and corresponding private key of its own.
- Server-side:
  - A server-side implementation must have access to an X.509 certificate and corresponding private key.
  - A server-side implementation that uses client authentication must have a mechanism for determining whether to trust incoming client certificates. **In NYC CVPD this will be done by whitelisting known good client certificates.**

## 4.3 Security Mechanisms per Information Flow

### 4.3.1 Overview

The following security mechanisms will be used:

- IEEE 1609.2 signatures only – used for protection of messages broadcast over 5.9 GHz DSRC
- IEEE 1609.2 encryption and signature – used to protect data that is stored on the ASD and then forwarded to the TMC when connectivity is available.
- Physical protection of link – used for protection of messages between Vehicle Databus and ASD
- SNMPv3 over TLS – used for management of RSE and ASD

- TLS + IEEE 1609.2 encryption and signature – used for data upload
- VPN with client certificate authentication – used to authenticate messages from the RSE to the TMC, and between the ITS-RE and RSE

The following subsections identify which security mechanism will be used on each information flow in NYC CVPD. For each usage scenario the security mechanism for each information flow is given in a table and in a diagram. Figure 4-4 gives the legend for the diagrams in this section. The security mechanism for each flow is identified by line color and dash type, and by an abbreviated name for the mechanism given after each flow name.

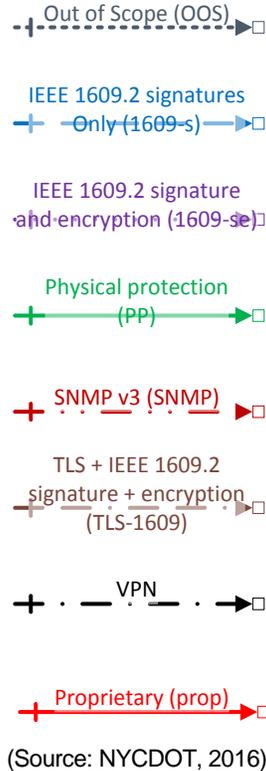


Figure 4-4. Legend for Diagrams in Chapter 4

### 4.3.2 Existing CV Applications: BSM-based Safety

Security mechanisms for BSM-based safety are given in Table 4-2 and Figure 4-5. All messages are protected with IEEE 1609.2 signatures.

**Privacy.** ASDs shall change their source MAC address, BSM signing certificate, and BSM Temporary ID from time to time as specified in J2945/1 [20].

**Table 4-2. Security Mechanism Selection for BSM-based V2V Safety**

Source	Destination	Information Flow	C//I/A	Mechanism
Remote Vehicle ASD	Vehicle ASD	Vehicle Control Event	C: L I: H A: H	IEEE 1609.2 signatures
Vehicle ASD	Remote Vehicle ASD	Vehicle Control Event	C: L I: H A: H	IEEE 1609.2 signatures



(Source: NYCDOT, 2016)

**Figure 4-5. Security Mechanism Selection for BSM-based V2V Safety**

### 4.3.3 Existing CV Applications: Red Light Violation Warning

Security mechanisms for Red Light Violation Warning are given in Table 4-3 and Figure 4-6.

The TMC exchanges information with the RSE via SNMP v3. MAP messages are generated at the TMC and signed with 1609.2 signatures per Section 4.2.2.3, and then delivered to the RSE via SNMP v3. The RSE acts as a repeater for these messages. The RSE generates SPaT messages based on local information provided by BSMs or from the ITS-RE (protected by TLS), and on information provided by the TMC (over SNMPv3). The RSE protects the SPaT messages with 1609.2 signatures. The BSMs generated by the ASD are also protected with 1609.2 signatures.

**Privacy.** If RSE detects potential red light violations and stores them, it will (a) strip the identifying data from the relevant BSMs and (b) encrypt the stored data with the TMC encryption key prior to local storage.

**Table 4-3. Security Mechanism Selection for Red Light Violation Warning**

Source	Destination	Information Flow	C//I/A	Mechanism
ITS Roadway Equipment	Roadside Equipment	conflict monitor status	C: L I: H A: M	VPN
ITS Roadway Equipment	Roadside Equipment	intersection control status	C: L I: H A: M	VPN

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

Source	Destination	Information Flow	C//I/A	Mechanism
Roadside Equipment	Traffic Management Center	intersection safety application status	C: M I: M A: L	SNMP v3
Roadside Equipment	Vehicle ASD	intersection status (Note this is the SPaT message)	C: L I: M A: M	IEEE 1609.2 signatures
Roadside Equipment	ITS Roadway Equipment	RSE status	C:L I: M A: M	VPN
Traffic Management Center	Roadside Equipment	intersection safety application info	C: L I: H A: L	SNMP v3
Vehicle Databus	Vehicle ASD	host vehicle status	C: L I: M A: M	Physical protection of link
Vehicle ASD	Vehicle Databus	driver update information	C: L I: M A: M	Physical protection of link
Vehicle ASD	Roadside Equipment	vehicle location and motion	C: L I: M A: M	IEEE 1609.2 signatures

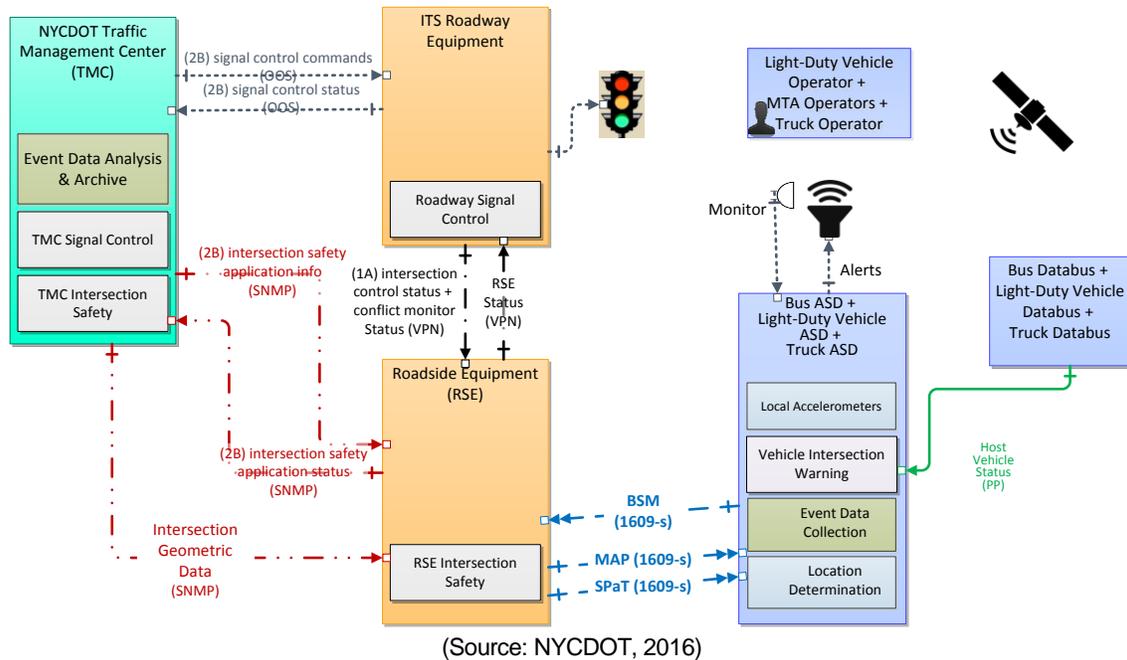


Figure 4-6. Security Mechanism Selection for Red Light Violation Warning

### 4.3.4 Traffic Manager: Speed Compliance / Speed Compliance in Work Zones / Curve Speed Compliance

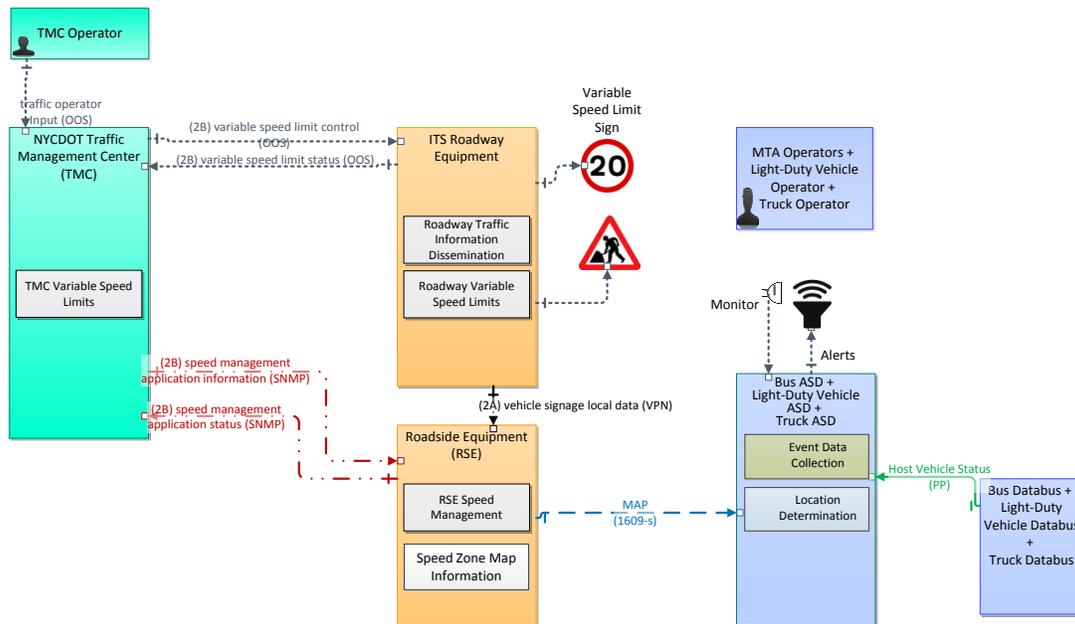
Security mechanisms for speed compliance applications are given in Table 4-4 and Figure 4-7.

The TMC exchanges information with the RSE via SNMP v3. MAP messages are generated at the TMC and signed with 1609.2 signatures, and then delivered to the RSE via SNMP v3. The RSE acts as a repeater for these messages. The RSE generates SPaT messages based on local information provided by BSMs or from the ITS-RE (protected by TLS), and on information provided by the TMC (over SNMPv3). The RSE protects the SPaT messages with 1609.2 signatures. The BSMs generated by the ASD are also protected with 1609.2 signatures.

**Privacy.** No additional privacy considerations.

**Table 4-4. Security Mechanism Selection for Speed Compliance applications**

Source	Destination	Information Flow	C//I/A	Mechanisms
ITS Roadway Equipment	Roadside Equipment	vehicle signage local data	C: L I: M A: M	VPN
Roadside Equipment	Traffic Management Center	speed management application status	C: L I: M A: L	SNMP v3
Roadside Equipment	Vehicle ASD	speed management information (MAP)	C: L I: M A: M	IEEE 1609.2 signature
Roadside Equipment	Vehicle ASD	vehicle signage data (MAP)	C: L I: M A: M	IEEE 1609.2 signature
Traffic Management Center	Roadside Equipment	speed management application information	C: L I: M A: M	SNMP v3
Vehicle Databus	Vehicle ASD	host vehicle status	C: L I: M A: M	Physical protection of link



(Source: NYCDOT, 2016)

**Figure 4-7. Security Mechanism Selection for Curve Speed Compliance**

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

### 4.3.5 Traffic Manager: Oversize Vehicle Compliance

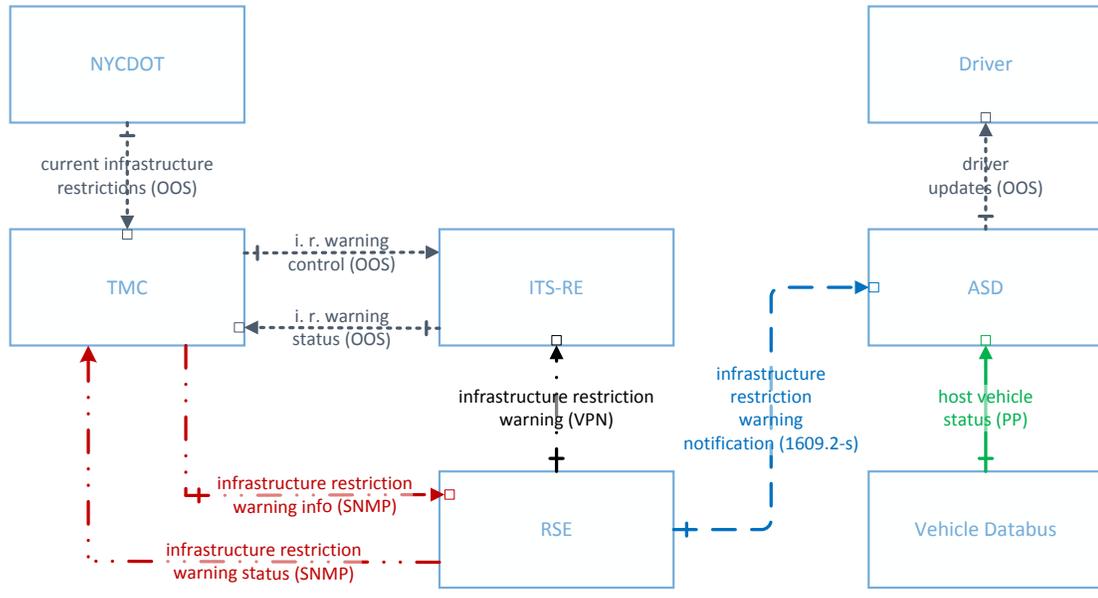
Security for oversize vehicle compliance applications are given in Table 4-5 and Figure 4-8.

The TMC exchanges information with the RSE via SNMP v3. This information includes signed infrastructure restriction messages in the form of MAP messages which are signed by the TMC. The RSE acts as a repeater for these messages and does not sign any messages itself. The BSMs generated by the ASD are also protected with 1609.2 signatures.

**Privacy.** No additional privacy considerations.

**Table 4-5. Security Mechanism Selection for Oversize Vehicle Compliance**

Source	Destination	Information Flow	C//I/A	Mechanisms
ITS Roadway Equipment	Roadside Equipment	infrastructure restriction warning	C: L I: M A: M	VPN
Roadside Equipment	Traffic Management Center	infrastructure restriction warning info	C: L I: M A: L	SNMP v3
Roadside Equipment	Truck ASD	Infrastructure restriction warning notification	C: L I: M A: M	IEEE 1609.2 signature
Traffic Management Center	Roadside Equipment	infrastructure restriction warning status	C: L I: M A: M	SNMP v3
Truck Databus	Truck ASD	host vehicle status	C: L I: M A: M	Physical protection of link



(Source: NYCDOT, 2016)

**Figure 4-8. Security Mechanism Selection for Oversize Vehicle Compliance**

### 4.3.6 Traffic Manager: Emergency Communications and Evacuation Information

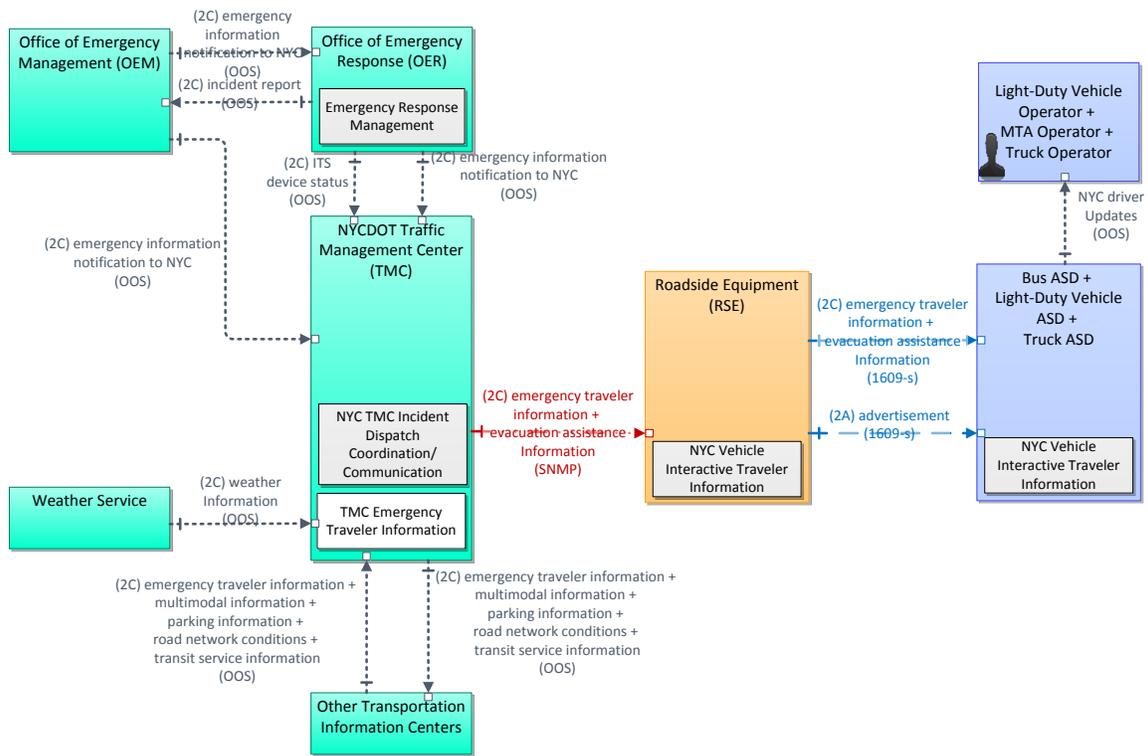
Security mechanisms for Emergency Communications and Evacuation Information are given in Table 4-6 and Figure 4-9.

The TMC generates signed TIM messages and provides them to the RSE via SNMP. The RSE broadcasts a WAVE Service Advertisement indicating that TIM messages are available on a service channel; the WSA is signed with 1609.2 certificates. On the indicated service channel, the RSE rebroadcasts the TIM messages that the TMC originally generated.

**Privacy.** No additional privacy considerations.

**Table 4-6. Security Mechanism Selection for Emergency Communication and Evacuation Information**

Source	Destination	Information Flow	C//I/A	Mechanism
Traffic Management Center	Roadside Equipment	emergency traveler information + evacuation assistance information (TIM)	C: L I: H A: M	SNMP v3 for update of RSE MB; IEEE 1609.2 signatures for TIM message
Roadside Equipment (pass-through)	Vehicle ASD	emergency traveler information + evacuation assistance information (TIM)	C: L I: M A: M	IEEE 1609.2 signatures generated by TMC
Roadside Equipment	Vehicle ASD	Service advertisement	C: L I: L A: L	IEEE 1609.2 signatures



(Source: NYCDOT, 2016)

**Figure 4-9. Security Mechanism Selection for Emergency Communications and Evacuation Information**

### 4.3.7 Roadway User: Pedestrian in Signalized Intersection Warning

Security mechanisms for Pedestrian in Signalized Intersection Warning are given in Table 4-7 and Figure 4-10.

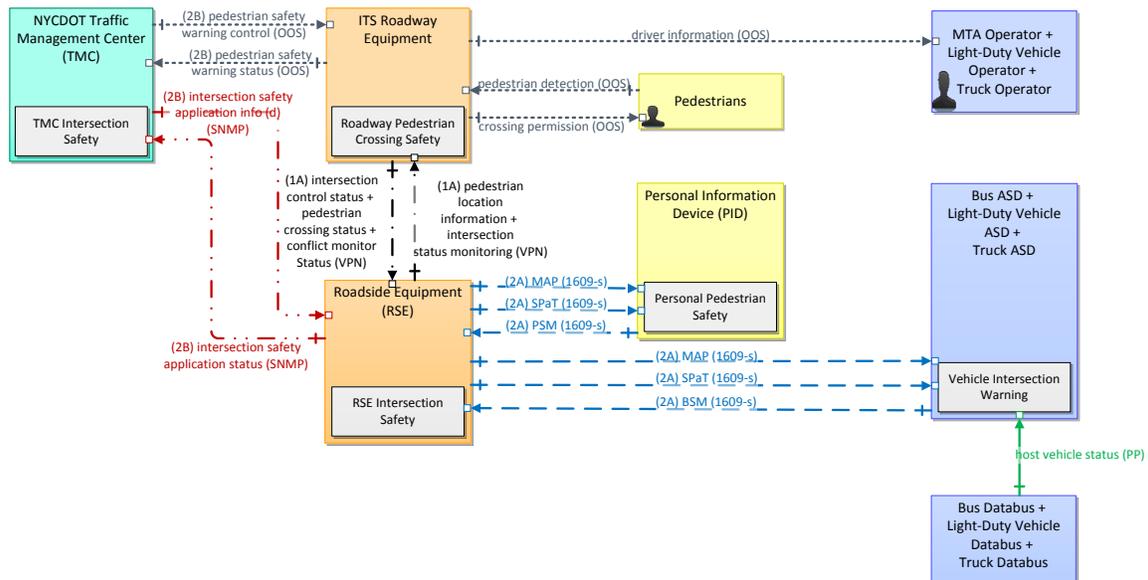
The TMC exchanges information with the RSE via SNMP v3. MAP messages are generated at the TMC and signed with 1609.2 signatures, and then delivered to the RSE via SNMP v3. The RSE acts as a repeater for these messages. The RSE generates SPaT messages based on local information provided by BSMs or from the ITS-RE (protected by TLS), and on information provided by the TMC (over SNMPv3). The RSE protects the SPaT messages with 1609.2 signatures. Messages from the ASD and the PID are also signed with 1609.2 certificates.

**Privacy.** ASDs and PIDs shall change their source MAC address, BSM signing certificate, and BSM Temporary ID from time to time as specified in J2945/1 [20]. If RSE detects potential pedestrian / vehicle encounters and stores them, it will (a) strip the identifying data from the relevant BSMs and PSMs and (b) encrypt the stored data with the TMC encryption key prior to local storage.

**Table 4-7. Security Mechanism Selection for Pedestrian in Signalized Intersection Warning**

Source	Destination	Information flow	C//I/A	Mechanism
ITS RE	RSE	Intersection Control Status, Conflict Monitor Status, Pedestrian Crossing Status	C: L I: H A: M	VPN
PID	RSE	Personal Location (PSM)	C: L I: H A: M	IEEE 1609.2 signatures
RSE	TMC	Intersection Safety Application Status	C: L I: M A: L	SNMP v3
RSE	Vehicle ASD	MAP, SPaT	C: L I: H A: M	IEEE 1609.2 signatures, either from RSE or from TMC
RSE	ITS RE	Intersection Status Monitoring	C: L I: H A: M	VPN
RSE	ITS RE	Pedestrian Location Information	C: L I: M A: L	VPN

Source	Destination	Information flow	C//I/A	Mechanism
RSE	PID	Pedestrian Safety Information	C: L I: H A: M	IEEE 1609.2 signatures
TMC	RSE	Intersection Safety Application Info	C: M I: H A: L	SNMP v3; potentially IEEE 1609.2 signatures
Vehicle Databus	Vehicle ASD	Host Vehicle Status	C: L I: H A: H	Physical protection of link
Vehicle ASD	RSE	Vehicle Location & Motion (BSM)	C: L I: H A: M	IEEE 1609.2 signatures



(Source: NYCDOT, 2016)

**Figure 4-10. Security Mechanism Selection for Emergency Communications and Evacuation Information**

### 4.3.8 Roadway User: Mobile Accessible Pedestrian Signal System

Security mechanisms for Mobile Accessible Pedestrian Signal System are given in Table 4-8 and Figure 4-11.

The TMC exchanges information with the RSE via SNMP v3. MAP messages are generated at the TMC and signed with 1609.2 signatures, and then delivered to the RSE via SNMP v3. The RSE acts as a repeater for these messages. The RSE generates SPaT messages based on local information provided by BSMs or from the ITS-RE (protected by TLS), and on information provided by the TMC (over SNMPv3). The RSE protects the SPaT messages with 1609.2 signatures.

The PID requests signal change via SRMs, which are signed with 1609.2. The RSE provides status updates via SSMs, which are signed with 1609.2.

**Privacy.** PIDs shall change their source MAC address, BSM signing certificate, and BSM Temporary ID from time to time. If RSE stores signal requests it will encrypt the stored data with the TMC encryption key prior to local storage. It will not strip identifying information because this will be used by the TMC to detect misbehaving devices.

**Table 4-8. Security Mechanism Selection for Mobile Accessible PED-SIG Application**

Source	Destination	Information type	C//I/A	Mechanism
ITS RE	RSE	Intersection Control Status	C: L I: H A: M	VPN
ITS RE	RSE	Pedestrian Crossing Status	C: L I: H A: M	VPN
PID	RSE	Personal Signal Service Request	C: L I: M A: L	IEEE 1609.2 signatures
RSE	ITS RE	Pedestrian Location Information	C: L I: M A: L	VPN
RSE	ITS RE	Signal Service Request	C: L I: M A: L	VPN
RSE	PID	Intersection Status	C: L I: M A: M	IEEE 1609.2 signatures

Source	Destination	Information type	C//I/A	Mechanism
RSE	PID	Pedestrian Safety Information	C: L I: H A: M	IEEE 1609.2 signatures
RSE	TMC	Intersection Safety Application Status	C: L I: M A: L	SNMP v3
TMC	RSE	Intersection Safety Application Info	C: M I: H A: L	SNMP v3

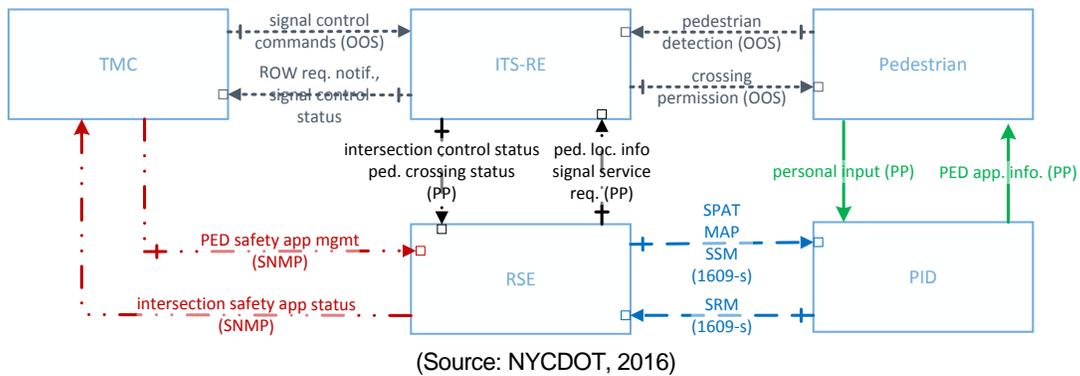


Figure 4-11. Security Mechanism Selection for Mobile Accessible PED-SIG

### 4.3.9 System Manager: ASD CV Application Configuration Download and ASD Firmware Update

Security mechanisms for ASD CV Application Configuration Download and ASD Firmware Update are given in Table 4-9 and Figure 4-12.

At manufacturing time, the ASD supplier implements a secure firmware update method that does not require live communications with the ASD supplier, i.e. it can start with an image stored at the TMC. The secure update method shall use cryptographic mechanisms that have at least 128-bit security against known attacks. Any secure firmware update that meets this requirement is acceptable and NYC CVPD will not require ASD suppliers to change existing secure update mechanisms if they meet this requirement.

As necessary, the ASD supplier provides authenticated firmware update images to the TMC. NYC CVPD discourages the supplier from providing encrypted firmware images: anyone who wants to see the firmware can simply buy a device directly from the supplier, and having a plaintext firmware image allows better audit within NYCDOT of what exact software has been installed on each device. **NYC CVPD will not permit direct connection from the supplier to the ASD for purposes of firmware update.**

The RSE advertises availability of firmware update or of SNMP v3 management for the ASD. This advertisement is signed with a 1609.2 application certificate containing the PSID for WSA signing.

In either case, the ASD connects over secured SNMP to the TMC and its status is queried by the TMC.

If the ASD is due for a configuration update, this is provided via secured SNMP over TLS, authenticated by X.509 certificates.

If the ASD is due for a firmware update, this is provided by the TMC over a client-certificate authenticated VPN connection to the ASD, tunneled through the RSE. This download is thus double-protected, once by the VPN connection (which authenticates the device to the TMC) and once by the proprietary firmware update security (which authenticates the firmware update as a valid one for installation).

Once the configuration update or firmware update has been installed, the TMC again queries the device status over SNMPv3 to ensure that the update has been successful.

**Privacy.** The ASD should authenticate itself to the TMC only within an encrypted session.

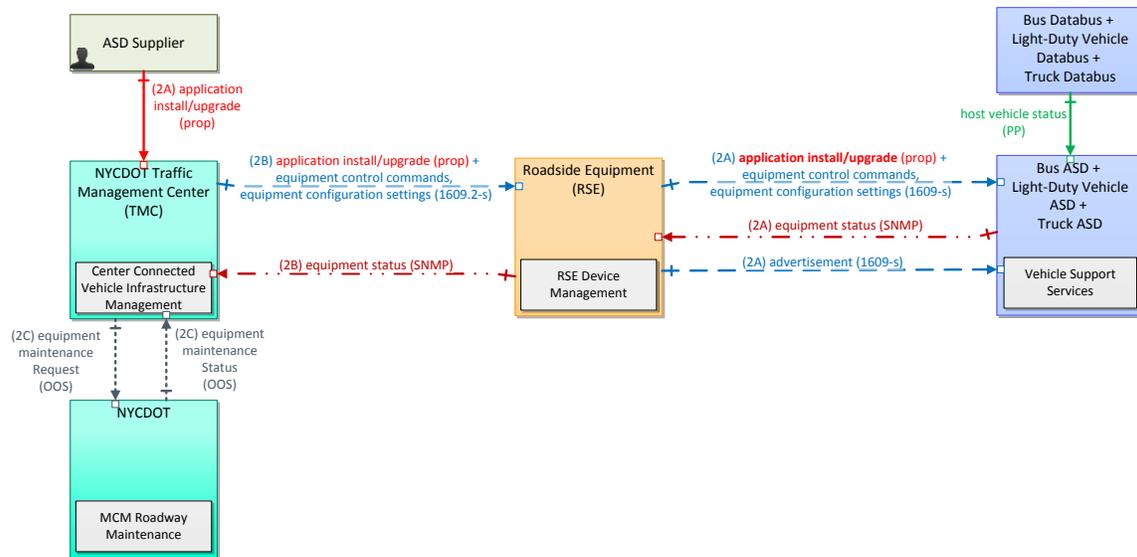
NOTE:

- A PSID will need to be allocated for advertising firmware image update.
- If other Pilot Deployment projects are defining similar functionality, the Pilot Deployments should all collaborate to develop the specification to simplify life for suppliers..

**Table 4-9. Security Mechanism Selection for ASD CV Application Configuration Download and ASD Firmware Update**

Source	Destination	Information flow	C//I/A	Mechanism
ASD	RSE (pass-through)	Equipment status	C: L I: L A: L	SNMP v3 over TLS connection to TMC
ASD Supplier	TMC (pass-through)	Application install / upgrade	C: L I: H A: M	Proprietary
RSE (pass-through)	ASD	Application install / upgrade	C: L I: H A: M	Proprietary, authenticated by ASD Supplier
RSE (pass-through)	ASD	Equipment configuration settings / control commands	C: L I: H A: M	SNMP v3 over TLS connection to TMC

Source	Destination	Information flow	C//I/A	Mechanism
RSE (pass-through)	TMC	Equipment status	C: L I: L A: L	SNMP v3 over TLS connection to TMC
TMC	RSE (pass-through)	Application install / upgrade	C: L I: H A: M	Proprietary
TMC	RSE (pass-through)	Equipment configuration settings / control commands	C: L I: H A: M	SNMP v3 over TLS connection to TMC
Vehicle Databus	ASD	Host vehicle status	C: L I: M A: L	Physical protection of link



(Source: NYCDOT, 2016)

**Figure 4-12. Security Mechanism Selection for ASD CV Application Configuration Download and ASD Firmware Update**

### 4.3.10 System Manager: RSE CV Application Configuration Download and RSE Firmware Update

Security mechanisms for RSE CV Application Configuration Download and RSE Firmware Update are given in Table 4-10 and Figure 4-13.

At manufacturing time, the RSE supplier implements a secure firmware update method that does not require live communications with the RSE supplier, i.e. it can start with an image stored at the TMC. The secure update method shall use cryptographic mechanisms that have at least 128-bit security against known attacks. Any secure firmware update that meets this requirement is acceptable and NYC CVPD will not require RSE suppliers to change existing secure update mechanisms if they meet this requirement.

As necessary, the RSE supplier provides authenticated firmware update images to the TMC. NYC CVPD discourages the supplier from providing encrypted firmware images: anyone who wants to see the firmware can simply buy a device directly from the supplier, and having a plaintext firmware image allows better audit within NYCDOT of what exact software has been installed on each device. **NYC CVPD will not permit direct connection from the supplier to the ASD for purposes of firmware update.**

From time to time, the RSE connects over secured SNMP to the TMC and its status is queried by the TMC.

If the RSE is due for a configuration update, this is provided via secured SNMP over TLS, authenticated by X.509 certificates.

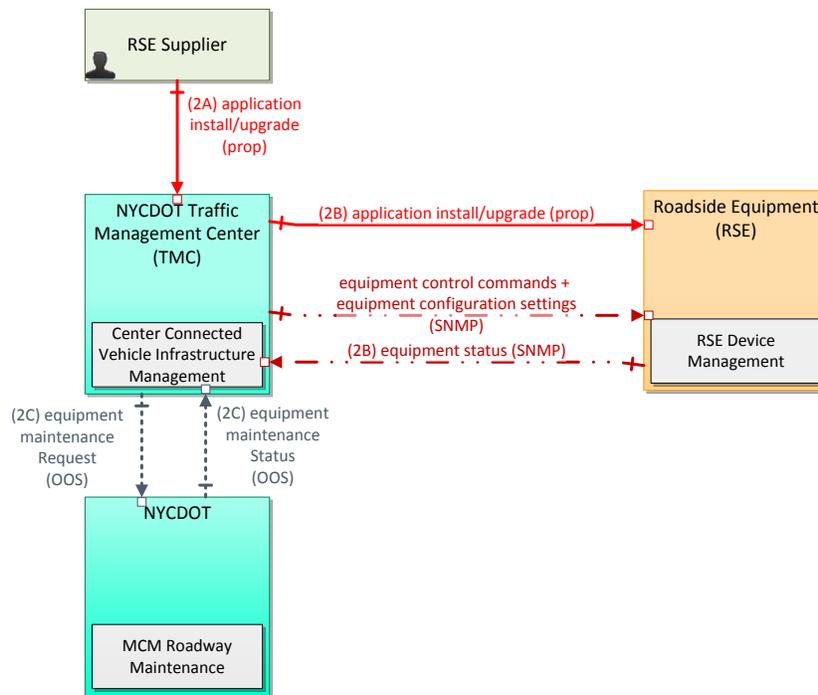
If the RSE is due for a firmware update, this is provided by the TMC over a client-certificate authenticated VPN connection. This download is thus double-protected, once by the VPN connection (which authenticates the device to the TMC) and once by the proprietary firmware update security (which authenticates the firmware update as a valid one for installation).

Once the configuration update or firmware update has been installed, the TMC again queries the device status over SNMPv3 to ensure that the update has been successful.

**Privacy.** No additional privacy considerations.

**Table 4-10. CIA Analysis for RSE CV Application Configuration Download and RSE Firmware Update**

Source	Destination	Information flow	C//I/A	Mechanism
RSE Supplier	TMC (pass-through)	Application install / upgrade	C: L I: H A: M	Proprietary
RSE	TMC	Equipment status	C: L I: L A: L	SNMP v3 over TLS
TMC (pass-through)	RSE	Application install / upgrade	C: L I: H A: M	Proprietary
TMC	RSE	Equipment configuration settings	C: L I: H A: M	SNMP v3 over TLS



(Source: NYCDOT, 2016)

**Figure 4-13. Physical View of Infrastructure Management**

### 4.3.11 System Manager: RSE RF Monitoring

Security mechanisms for RSE RF Monitoring are given in Table 4-11 and Figure 4-14.

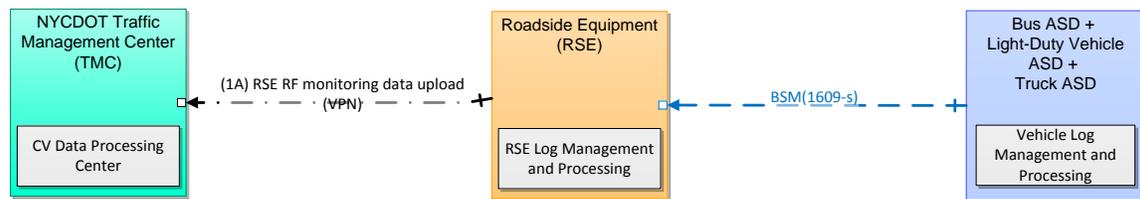
The RSE carries out the monitoring using incoming BSMs, which are signed with IEEE 1609.2 certificates.

The RSE carries out local data aggregation and periodically uploads the data over a client-certificate authenticated VPN connection to the TMC. Each instance of aggregated data is encrypted with the TMC’s encryption key (see Section 7.4) and periodically uploaded to the TMC.

**Privacy.** BSMs will be stripped of identifying information and encrypted with the TMC’s encryption key before being stored on the RSE.

**Table 4-11. Security Mechanism Selection for RSE RF Monitoring Usage Scenario**

Source	Destination	Information type	C//I/A	Mechanism
Vehicle ASD	RSE	vehicle location and motion	C: L I: M A: M	IEEE 1609.2 signatures
RSE	TMC	traffic situation data	C: L I: M A: L	VPN



(Source: NYCDOT, 2016)

**Figure 4-14. Security Mechanism Selection for RSE RF Monitoring**

### 4.3.12 System Manager: ASD RF Monitoring

Security mechanisms for ASD RF Monitoring are given in Table 4-12 and Figure 4-15. Note that this section just addresses security mechanisms for monitoring; security mechanisms for upload are addressed in Section 4.3.13.

The ASD receives RF monitoring messages, which are signed with IEEE 1609.2. It aggregates the data, signs it with its current BSM certificate, encrypts it with an encryption key belonging to the TMC, and stores it for later upload. The encryption key is stored in a MIB on the ASD and can be updated via SNMP as part of the Application Configuration Usage Scenario.

All log file entries will be signed with the BSM signing key that is currently in use if there is such a key. Signed log file entries will be encapsulated in a IEEE1609Dot2Data as defined in IEEE 1609.2, of type signed, using the PSID (0x28) for misbehavior detection which is included in the current BSM-signing certificate profile. The signed log file entries will then be encrypted with the TMC's encryption key. If the ASD has no valid BSM signing certificates, it shall format log file entries as IEEE1609Dot2Data of type unsecured and then encrypt them with the TMC's encryption key.

**REQUIREMENT:**

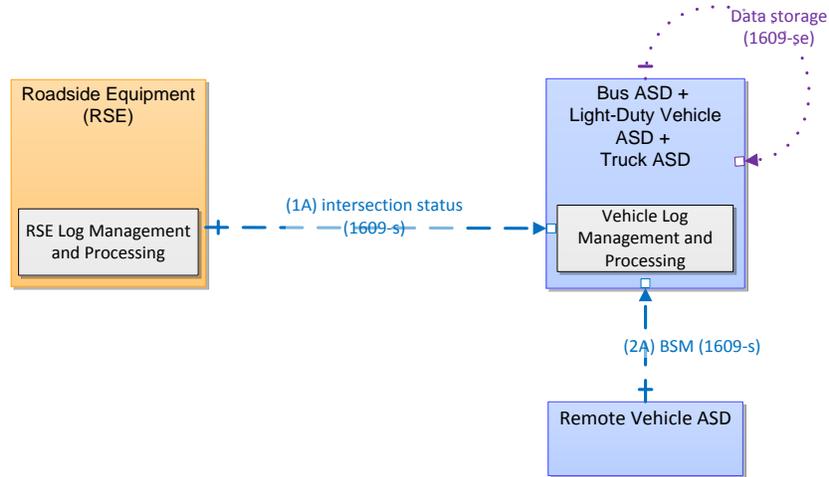
- The log file signing application shall have access to the BSM signing keys.
- The OS on the ASD will prevent the log file signing application from sending messages on channel 172.

**NOTE:** the log entries will in general include BSMs the device just sent out, so its current BSM cert is in there anyway. Signing the entry with the current BSM cert therefore doesn't significantly impact privacy. Distinct log file entries are distinct and can in principle not be correlated. However, the TMC will be able to tell which log file entries belong together because they will all be received at the same time. This is addressed in Sections 4.3.13 and 4.3.14.

**Privacy.** BSMs will be stripped of identifying information and encrypted with the TMC's encryption key before being stored on the ASD.

**Table 4-12. Security Mechanism Selection for ASD RF Monitoring Usage Scenario**

Source	Destination	Information type	C//I/A	Mechanism
Vehicle ASD	RSE <b>(pass-through)</b>	RF data upload	C: L I: M A: M	IEEE 1609.2 signatures
RSE <b>(pass-through)</b>	TMC	ASD RF monitoring data upload	C: L I: M A: L	VPN from RSE to TMC; IEEE 1609.2 signatures + encryption from ASD to TMC
Remote Vehicle ASD	Vehicle ASD	vehicle location and motion (BSM)	C: L I: M A: M	IEEE 1609.2 signatures
RSE	Vehicle ASD	Advertisement	C: L I: L A: L	IEEE 1609.2 signatures
RSE	Vehicle ASD	intersection status	C: L I: M A: M	IEEE 1609.2 signatures



(Source: NYCDOT, 2016)

**Figure 4-15. Security Mechanism Selection for ASD RF Monitoring**

### 4.3.13 Independent Evaluator: ASD Event Data Upload

Security mechanisms for ASD Event Data Upload are given in Table 4-13 and Figure 4-16. This section covers:

- Event Data Upload
- RF Monitoring Data Upload
- Probe Data Upload.

Log File entries for all these evaluation activities are protected at the time of generation as described in Section 4.3.12. This section only describes the upload process.

The RSE sends a WSA indicating that data upload services are available. The ASD uploads log file entries to the RSE. The RSE subsequently uploads the log file entries to the TMC. The log file entries are encrypted twice by the ASD for the TMC (see Privacy below) so the upload to the RSE does not need to take place over an authenticated or encrypted RSE-ASD connection.

**The data traffic usage shall be monitored by the TMC to detect abuse of the IP connection.** In particular, if an RSE at a barn is generating more IP traffic than would be warranted by the number of ASDs known to be associated with that barn, the information security manager shall investigate to determine the reason.

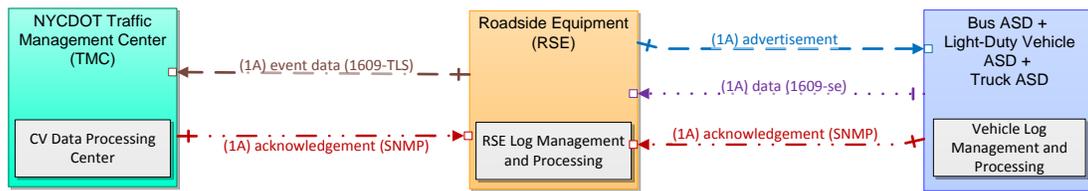
Distinct log file entries are distinct and can in principle not be correlated. However, the TMC will be able to tell which log file entries belong together because they will all be received at the same time. **The TMC shall discard information about time of receipt of log file entries at the time the entries are received.**

**Privacy.** To protect the senders of the original BSMs, those BSMs will be stripped of identifying information and encrypted with the TMC’s encryption key before being stored on the ASD.

To protect the ASDs that upload the logs against tracking, the ASD shall encrypt each log entry **again** with the TMC encryption key before uploading it. The encryption is randomized so this ensures that the same encrypted log entry, uploaded twice, will look difference each time.

**Table 4-13. Security Mechanism Selection for ASD Event Data Upload Usage Scenario**

Source	Destination	Information type	C//I/A	Mechanism
ASD	RSE <b>(pass-through)</b>	event data (BSM + MAP)	C: M I: M A: L	IEEE 1609.2 signature and encryption
RSE <b>(pass-through)</b>	TMC	event data	C: M I: M A: L	IEEE 1609.2 signature and encryption from the ASD
RSE	ASD	advertisement	C: L I: L A: L	IEEE 1609.2 signature
RSE <b>(pass-through)</b>	ASD	Acknowledgment	C: L I: L A: L	IEEE 1609.2 signature
TMC	RSE <b>(pass-through)</b>	Acknowledgment	C: L I: L A: L	IEEE 1609.2 signature



(Source: NYCDOT, 2016)

**Figure 4-16. Security Mechanism Selection for ASD Event Data Upload**

### 4.3.14 Independent Evaluator: Performance Measurement Data Processing

Security mechanisms for Performance Measurement Data Processing are given in Table 4-14 and Figure 4-17.

We anticipate that DOT will publish specs for this upload protocol and that they will provide adequate security, in that:

- The IE and RDE will authenticate themselves to the TMC before data is uploaded
- The data upload will be authenticated as coming from the TMC
- Data will be encrypted in transit
- Data will be sanitized to the greatest extent possible consistent with allowing legitimate research and evaluation activities
- All cryptographic mechanisms will provide at least 128 bits of security against the best known current attacks.

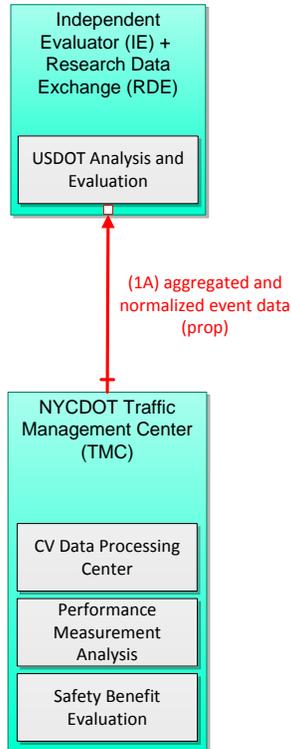
At the time of writing we do not have access to the interface specifications.

As noted in Section 4.3.12, although individual distinct log file entries are distinct and can in principle not be correlated, the TMC will be able to tell which log file entries belong together because they will all be received at the same time. **The TMC shall discard information about time of receipt of log file entries at the time the entries are received.**

**Privacy.** See Chapter 8 for discussion of privacy of bulk data.

**Table 4-14. Security Mechanism Selection for Performance Measurement Data Processing**

Source	Destination	Information type	C//I//A	Mechanism
TMC	USDOT	aggregated and normalized event data	C: M I: M A: L	Proprietary



(Source: NYCDOT, 2016)

**Figure 4-17. Security Mechanism Selection for Performance Measurement Data Processing**

## 4.4 Security Mechanisms per Device Type

Table 4-15 summarizes the security mechanisms that are to be supported by each device type.

**Table 4-15. Consolidated Security Mechanisms by Device Type and Application / Usage Scenario**

Device type	Security mechanisms	Supports applications
<b>ASD</b>	IEEE 1609.2 signatures (send and receive)	V2V safety; Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Emergency Communication and Evacuation Information Distribution; Pedestrian in Signalized Intersection Warning; RSE RF Monitoring; ASD RF Monitoring;
	SNMP v3 with TLS (client-side)	ASD CV Application Configuration Download and ASD Firmware Update;
	TLS VPN	
	Physical Protection of the link (to the Vehicle Databus)	Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Pedestrian in Signalized Intersection Warning; ASD CV Application Configuration Download and ASD Firmware Update;
	IEEE 1609.2 signature and encryption (send only)	ASD RF Monitoring; ASD Event Data Upload
	Proprietary	ASD CV Application Configuration Download and ASD Firmware Update;
<b>PID</b>	IEEE 1609.2 signatures (send and receive)	Pedestrian in Signalized Intersection Warning; Mobile Accessible Pedestrian Signal System;
	SNMP v3 with TLS	
	TLS VPN	
	Physical Protection of the link	
	IEEE 1609.2 signature and encryption	
<b>RSE</b>	IEEE 1609.2 signatures (send and receive)	Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Emergency Communication and Evacuation Information Distribution; Pedestrian in Signalized Intersection Warning; Mobile Accessible Pedestrian Signal System; RSE RF Monitoring; ASD RF Monitoring; ASD Event Data Upload
	SNMP v3 with TLS (client-side with authentication)	Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Emergency Communication and Evacuation Information Distribution; Pedestrian in Signalized Intersection Warning; Mobile Accessible Pedestrian Signal System; ASD CV Application Configuration Download and ASD Firmware Update; RSE CV Application Configuration Download and RSE Firmware Update;

Device type	Security mechanisms	Supports applications
	TLS VPN (Client side with authentication, to ITS-RE and TMC)	RSE RF Monitoring; ASD RF Monitoring; Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Pedestrian in Signalized Intersection Warning; Mobile Accessible Pedestrian Signal System;
	Physical Protection of the link	
	IEEE 1609.2 signature and encryption (Send only)	
	Proprietary	ASD CV Application Configuration Download and ASD Firmware Update;
<b>ITS-RE</b>	IEEE 1609.2 signatures	
	SNMP v3 with TLS	
	TLS VPN (to RSE)	Red Light Violation; Speed Compliance; Oversize Vehicle Compliance; Pedestrian in Signalized Intersection Warning; Mobile Accessible Pedestrian Signal System;
	Physical Protection of the link	
	IEEE 1609.2 signature and encryption	

# Chapter 5. Physical and Platform Security Controls

## 5.1 General

### 5.1.1 Overview and Goals

This section describes hardware, software, and operating system security for systems that run DSRC applications that use cryptographic private keys and certificates in the format specified by IEEE Std 1609.2-2016 and that are issued by the Security Credentials Management System (SCMS).

The security requirements apply to two logically distinct sets of functional blocks:

- **Privileged applications:** These are applications that run autonomously (i.e. do not require human intervention to start running) and either send or receive signed messages. They run on the **host processor**.
- **Cryptographic operations:** These are operations that use secret keys from symmetric cryptographic algorithms, or private keys from asymmetric cryptographic algorithms. They run on the **Hardware security module (HSM)**.

The goals of these requirements are:

1. Different privileged applications can have different sets of keys such that
  - a. A privileged application is able to sign with its own keys
  - b. A privileged application is not able to sign with keys reserved for use by a different privileged application
  - c. Non-privileged applications do not have any access to keys that are reserved for use by privileged applications.
- 2) No application has read access to key material – all key material is execute- or write-only.
- 3) Keys used for verification are protected against unauthorized replacement.
- 4) The system supports software/firmware update in such a way that the above properties continue to hold.

This document does not address processes for certifying that systems meet the requirements: its purpose is simply to state the requirements.

### 5.1.2 Architectures

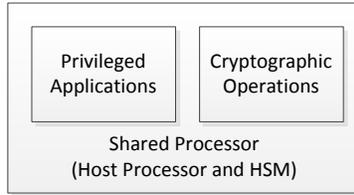
The requirements below cover three architectures.

- **Integrated architecture** (Figure 5-1): The host processor and the HSM are the same processor.
- **Connected architecture** (Figure 5-2): The host processor and the HSM are different, but they are physically connected using a connector that connects only those two processors,

such that the only way to read or write data flowing between the two processors is by physically tapping into that connector, and the only access to the HSM is via the host processor.

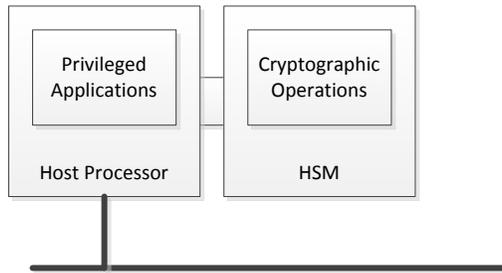
- **Networked architecture** (Figure 5-3): The host processor and the HSM are different and are connected over a network or bus that has other processors connected to it.

The document provides requirements for the host processor and the HSM separately in Sections 5.1.3 and 5.1.4 respectively, and then provides architecture-specific requirements in Section 5.1.5.



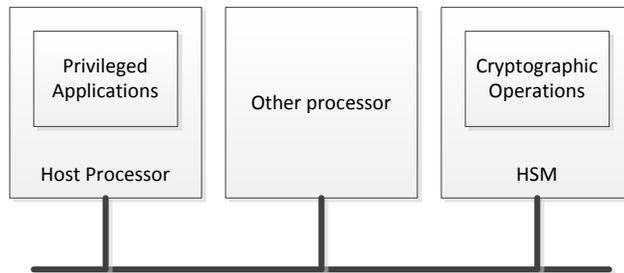
(Source: NYC DOT, 2016)

**Figure 5-1. Integrated Architecture**



(Source: NYC DOT, 2016)

**Figure 5-2. Connected Architecture**



(Source: NYC DOT, 2016)

**Figure 5-3. Networked Architecture**

## 5.1.3 Host Processor

### 5.1.3.1 Manufacturing and Operational States

The host processor and its software shall be delivered in an *operational state* that implements all the protections below.

The host processor may be initialized while in a *manufacturing state* that does not implement all the protections.

A device may be designed so it can return from the operational state to the manufacturing state. If this functionality is provided, the transition shall wipe all privileged applications from the host processor and all keys from the HSM. The device may allow a user to perform a reset to a manufacturing state without any authentication if the mechanism for a reset guarantees that the user is physically present.

### 5.1.3.2 Secure Boot

The host processor shall perform integrity checks on boot to ensure that it is in a known good software state. The integrity checks shall require the use of a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified. Examples of these integrity checks include signing the software such that the verification key is protected by hardware, or storing hashes via the Platform Configuration Registry (PCR) mechanism of the Trusted Computing Group (TCG)'s Trusted Platform Module (TPM).

The host processor integrity check shall verify the software and firmware configuration of the host processor such that:

- The host processor shall not allow any privileged application to sign until the integrity checks have passed.
- If the host processor fails the integrity checks it shall not grant access for any process to private keys.
- If the host processor fails the integrity checks it shall not allow any privileged application to operate.

The host processor integrity check shall carry out a check that stored root CA certificates have not been modified since they were last accessed such that:

- If this integrity check fails, the device shall reject all incoming signed messages that chain back to those root CA certificates as invalid.

### 5.1.3.3 Operating System

The host processor operating system shall meet the following requirements (derived from FIPS 140-2 [12] Section 4.6.1):

- The operating system shall support roles which are used as specified below. Each privileged application shall map to a role.
- The discretionary access control mechanisms of the operating system shall be configured to:

- Specify the set of roles that has execute permissions on each private key stored within the HSM.
- Specify the set of roles that can modify (i.e., write, replace, and delete) programs and plaintext data stored at various locations within the host processor boundary.
- Specify the set of roles that can read data stored within the host processor boundary and which data can be read by those roles.
- Specify the set of roles that can enter cryptographic keys. (It is permissible for the host to require that all keys are generated on the device and that keys cannot be entered directly)
- The OS shall allow the following roles to operate without explicit authentication by a user:
  - Processes that correspond to privileged applications, i.e. applications that are intended to run without user initiation or intervention, and that have execute access to private keys.
  - Processes that update private key material within the HSM, for example to implement the butterfly key process specified within the SCMS documentation.
- The OS may allow the following roles to operate without explicit authentication, or may require authentication:
  - Processes that install new software or firmware if that software or firmware is signed.
  - Processes that write private key material to the HSM. (It is permissible for the host to require that all keys are generated on the device and that keys cannot be entered directly)
- The OS may support the following roles and, if it supports them, shall require explicit authentication:
  - Processes that modify or inspect executing processes
- The OS shall not allow the following roles to exist:
  - Processes that read private cryptographic key material from the HSM (NOTE: The HSM must also not provide this functionality)

#### **5.1.3.4 Secure Updates**

The host processor shall use the following mechanisms to ensure that its software and firmware can be securely updated:

- The host processor requires that all software installed is signed: in other words, when requested to install software, the host processor OS ensures that the software is signed by an authority with appropriate permissions before proceeding with the installation and rejects the installation if the signature or any of the validity checks on the software or its signing certificate fail.
  - The integrity of the verification key shall be protected by local hardware, either by directly storing the key in local hardware, or by creating a chain of trust from the key to a hardware-protected key. The hardware protection shall be equivalent to FIPS 140-2 at the level appropriate to the device as a whole.
- In addition, the host processor may require that software can be installed only by an authenticated user.

The update mechanism shall include mechanisms to prevent updates being rolled back.

## 5.1.4 HSM

### 5.1.4.1 General

The HSM shall meet the requirements for an operating system given in FIPS 140-2 Level 2 except for the audit requirements and certain additional exceptions. The baseline requirements are the following:

- All cryptographic software and firmware shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification.
- A cryptographic mechanism using an Approved integrity technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the HSM.
  - The message authentication code may be used in the following circumstances only:
    - If the HSM itself calculates the MAC when the software is installed using a secret key known only to the HSM, and uses this secret key to verify the software on boot
    - If the software/firmware provider has a unique shared key with each distinct device and uses this to authenticate the software.
  - A message authentication code (MAC) may not be used to protect the software unless the MAC key is unique to the HSM.
- All cryptographic software and firmware, cryptographic keys, and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles listed in FIPS 140-2 Annex B and is capable of evaluation at the CC evaluation assurance level EAL2, or an equivalent trusted operating system.
- To protect plaintext data, cryptographic software and firmware, cryptographic keys, and authentication data, the discretionary access control mechanisms of the operating system shall be configured to:
  - Specify the set of roles that can execute stored cryptographic software and firmware.
  - Specify the set of roles that can modify (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), and plaintext data.
  - Specify the set of roles that can read the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), and plaintext data.
  - Specify the set of roles that can enter cryptographic keys.
- The discretionary access control mechanisms may allow a role without explicit authorization to execute stored cryptographic software and firmware if the device follows the Integrated or Connected Architectures specified in Section 5.1.2. The discretionary access control mechanisms shall require explicit authorization to execute stored cryptographic software and firmware if the device follows the Networked Architecture specified in Section 5.1.2.
- The discretionary access control mechanisms of the OS shall allow an unauthenticated role to create a new cryptographic key by combining an existing key with new input.

- The discretionary access control mechanisms of the OS may allow automated software and firmware update if that update is carried out by a process that includes cryptographic checks to ensure the validity of the update prior to installation.
- The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.
- The operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

## 5.1.5 Architecture-specific Requirements

### 5.1.5.1 *Integrated Architecture*

An integrated processor meets the complete set of requirements identified in Sections 5.1.3 and 5.1.4.

### 5.1.5.2 *Connected Architecture*

An integrated processor meets the complete set of requirements identified in Sections 5.1.3 and 5.1.4.

### 5.1.5.3 *Networked Architecture*

Modifications are the following:

- All of the Connected architecture requirements above
- In addition, the host processor shall authenticate itself to the HSM with an authentication mechanism based in hardware with the same physical security level as the HSM itself.

## 5.2 Physical Security Controls

In addition to the platform security controls specified above, devices shall follow the following physical security controls:

The device shall provide tamper evidence to detect tampering of the device (e.g. opening of the case). All unused media ports (e.g. USB) shall be sealed. Examples of a tamper evident seal are tamper evident stickers above screw holes.

There will be no removable media.

## 5.3 Minimum Security Requirements per Device Classification

This section will list the minimum security requirements per device classification to ensure security and privacy while facilitating timely development and delivery by suppliers. Full, detailed security controls from NIST SP 800-53 will not be available in time for the suppliers to modify designs, manufacturing

practices, etc. as necessary. The final security controls from the Threat Definition of V2I Architecture should be used as guidelines for the next lifecycle of devices, while these requirements are used for the CV Pilots to ensure reasonable security, privacy, and interoperability.

This section is derived from the corresponding section in the THEA SMOC [18] with grateful thanks. Only requirements that differ from the common requirements in Section 5.1 are recorded below.

### **5.3.1 Class 1 (LMM) Device Minimum Security Requirements**

#### **5.3.1.1 Hardware**

- LMM devices shall be compliant with FIPS 140-2 Level 2 physical security requirements

#### **5.3.1.2 Access**

- LMM devices may support remote and physical management via SNMPv3 over TLS.
- LMM devices shall not otherwise support remote login.

### **5.3.2 Class 2 (MMM) Device Minimum Security Requirements**

#### **5.3.2.1 Hardware**

- MMM devices shall be compliant with FIPS 140-2 Level 2 physical security requirements

#### **5.3.2.2 Access**

- MMM devices shall support remote and physical management via SNMPv3 over TLS.
- MMM devices shall not otherwise support remote login.

### **5.3.3 Class 3 (MHM) Device Minimum Security Requirements**

**Note:** The USDOT FHWA DSRC Roadside Unit (RSU) Specifications Document, Version 4.0 April 15, 2014, includes basic security requirements for RSEs. All of the existing requirements should be followed as stated, except the requirement on FIPS 140-2 level. The RSE shall be compliant with FIPS 140-2 Level 3, not Level 2 as stated within the specifications document.

#### **5.3.3.1 Hardware**

- MHM devices shall be compliant with FIPS 140-2 Level 3 physical security requirements

#### **5.3.3.2 Access**

- MHM devices shall support remote and physical management via SNMP. The device shall require role- remote authentication in both cases.
- MHM devices shall not otherwise support remote login.

### 5.3.4 Storage Requirements

NYC CVPD devices will have good connectivity to the SCMS and will be able to renew certificates every day if necessary. **Therefore, the plan is for devices to carry no more than two weeks' worth of valid certificates at any time** (usually one week's worth, but the day before a new week becomes valid the devices will download the next week's worth of certificates and so will have valid certificates for two separate weeks). It will be a requirement for our devices that they can be configured to request download of this small a number rather than the three years' worth of certificates that we understand will be the default.

Storage requirements for certificates are therefore minimal, less than 50Kb.

**Given this short timescale for which certificates are held, the NYC Pilot Deployment does not plan to issue Certificate Revocation Lists (CRLs).** Instead, if a device is noted to be misbehaving, we will notify the SCMS and prevent that device from obtaining more authorization certificates by putting that device on a blacklist which is internal to the SCMS and does not need to be distributed to vehicles. We note here that there is no defined protocol for distribution of CRLs and as such it is not possible to procure devices that are certified as obtaining CRLs correctly.

#### ASSUMPTIONS:

We make the following assumptions about SCMS behavior. If any of them are false the Security Management Operating Concept will have to be reconsidered.

- The SCMS supports downloading certificates to one or two weeks in the future rather than three years in the future as is currently stated to be the default.
- The SCMS provides an interface which allows a trusted operator to configure the “maximum future downloaded certificate period” for a device or set of devices, for example by linking this configuration choice to an enrolment certificate or by including it in the certificate itself (these options are just for illustration; the interface will be worked out with or provided by the SCMS Manager)
- The SCMS is responsive to requests to no longer issue or download certificates to blacklisted devices.
- The SCMS supports a mechanism to blacklist an enrollment certificate – such as email, HTTPS, etc.

#### REQUIREMENTS:

The following requirements will be passed to device suppliers.

- The devices support downloading certificates to one or two weeks in the future rather than three years in the future as is currently stated to be the default.

### 5.3.5 Privacy of Stored Certificates

If an attacker can read the pseudonym certificates of a device, they can track the device. This attack is unlikely, but if it can be carried out undetectably it is still a concern. Therefore, **a device shall not store its pseudonym certificates unencrypted in persistent storage.** Pseudonym certificates may be stored unencrypted in volatile memory so long as that memory is not swapped unencrypted to persistent storage.

## 5.4 System and Device Testing

Devices from suppliers will:

- Correctly implement the parts of IEEE 1609.2 necessary to support the NYC CVPD applications;
- Conform to the security requirements described in Chapter 5.

The supplier will provide proof that their devices meet these conditions and will operate a Device Configuration Manager, i.e. a secure environment including a secured connection to the ECA which it uses to request enrolment certificates from the ECA.

### 5.4.1 Conformance Testing

NYCDOT will acquire devices that have been tested for conformance to IEEE 1609.2 by the USDOT-sponsored conformance test labs.

If the conformance test labs also test for conformance to the CAMP certificate management interfaces, NYCDOT will use these conformance test results. Otherwise, NYCDOT will require a documented test plan from suppliers indicating the tests run against the “dummy” SCMS instance and the results of those tests.

### 5.4.2 Physical Security Testing

Devices will be self-certified for physical security unless USDOT provides conformance testing services. See Section 5.5 for further discussion.

## 5.5 Contingency Plan for Suitable Hardware Being Unavailable

Suppliers will be provided with the requirements in this document, and will be required to provide written documentation indicating that the device conforms to those requirements. If we cannot obtain devices that meet the security requirements we will work with suppliers to establish the best possible match with the security requirements.

If devices meet only a subset of the security requirements, there is increased risk of key compromise. We mitigate this by:

- Ensuring that no device has certificates for more than eight days in advance of the current date;
- Storing more than 20 spares of each device, to increase our ability to swap out devices that appear to have been compromised and swap in a replacement.

## 5.6 Access Security

### 5.6.1 General

DOT poses the following questions:

- How are the security materials stored internally?
- Which users are allowed to access to the device?
- What are the user name and password policies for authorized users?
- Is remote access to the device allowed?

Although these questions are addressed by the Platform and Physical Security requirements, we answer them directly in this section.

### 5.6.2 ASDs

#### **How are the security materials stored internally?**

Security materials are stored as specified in this section.

#### **Which users are allowed to access to the device?**

#### **What are the user name and password policies for authorized users?**

#### **Is remote access to the device allowed?**

Access to ASDs is provided by SNMPv3 over TLS as specified in Section 4.2.3. There is no remote login as such.

### 5.6.3 RSEs

#### **How are the security materials stored internally?**

Security materials are stored as specified in this section.

#### **Which users are allowed to access to the device?**

#### **What are the user name and password policies for authorized users?**

#### **Is remote access to the device allowed?**

Access to RSEs is provided by SNMPv3 over TLS as specified in Section 4.2.3. There is no remote login as such.

# Chapter 6. Management Considerations per Security Mechanism

## 6.1 Introduction

This section describes management and implementation considerations for each security mechanism specified for use in Chapter 4. The focus of this section is on usage scenarios that arise in NYC CVPD due to security management, identifying information flows and how they are protected as well as giving background on the context in which those information flows are used. The following section, Chapter 7, presents security management lifecycle activities for each device, referring back to the considerations in this section and identifying application-specific activities

## 6.2 IEEE 1609.2

### 6.2.1 Introduction

This section provides an overview of IEEE 1609.2 security management considerations.

In this section we define usage scenarios associated with 1609.2 security management. There are two types of usage scenario:

- SCMS-Core: usage scenarios that involve “live” communications between the SCMS and NYC CVPD devices or components
- SCMS-Support: usage scenarios that are necessary because of SCMS operations but involve only NYC CVPD devices or components.

SCMS-Core usage scenarios are:

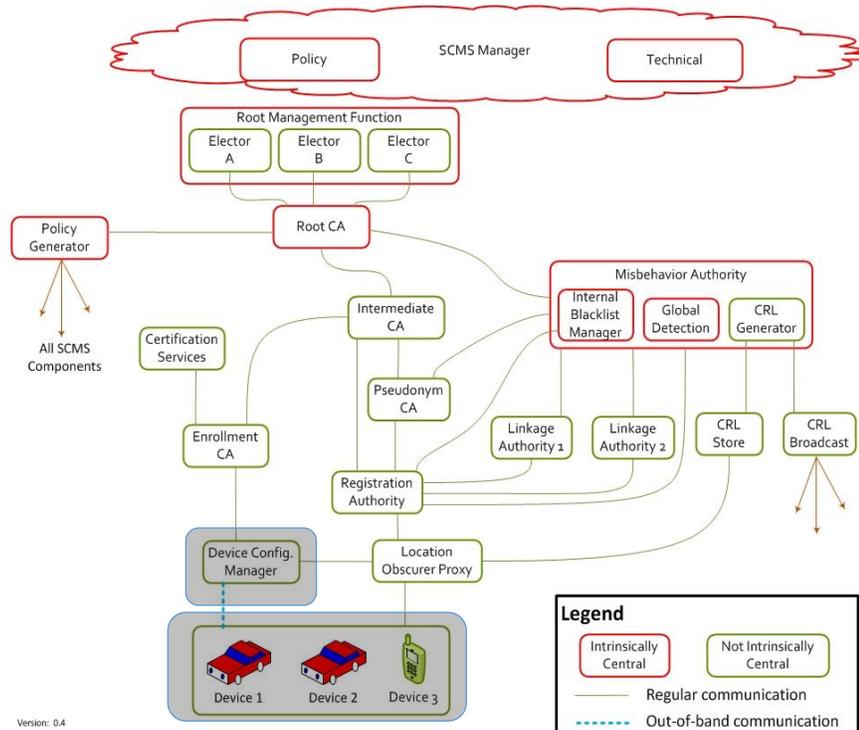
- **Initial provisioning:** ECA -> Device Configuration Manager -> ASD / RSE
- Initial certificate request and download: PCA->RA -> ASD / RSE
- Certificate update (for RSE): RA-> RSE (as endpoint)
- **Certificate update (for ASD):** RA-> RSE (as IP connectivity) -> ASD (via DSRC Interface)
- **CRL distribution:** same interfaces as certificate update. **Note:** Although the SCMS supports CRL distribution, we do not intend to distribute CRLs within the NYC Pilot Deployment as discussed in Sections 6.2.7 and 6.2.8.
- **Re-initialization:** creating a new certificate

SCMS-Support usage scenarios are:

- IPv6 Connectivity via RSE
- Connectivity Log Upload

## 6.2.2 Security Credential Management System Overview

Figure 6-1 provides an overview of the Security Credential Management System (SCMS) that manages IEEE 1609.2 certificates. In this diagram, a component is called *central* if there is only one instance of it in the system, and *non-central* if there could be more than one.



(Source: USDOT, 2016)

**Figure 6-1. SCMS Diagram**

- The **SCMS Manager** sets policy, including operational policy for all the other SCMS components.
- The **Root Management Function** manages root Certificate Authorities (CAs) via endorsements from Electors.
- The **Root CA** is the top of the trust chain for the Public Key Infrastructure (PKI). Directly or indirectly, it issues certificates for all entities in the system that use 1609.2 certificates.
- The **Intermediate CA** (ICA) issues certificates to other CAs, which in turn issue certificates to End Entities. The purpose of the ICA is to firewall the Root CA; it is more complicated and expensive to replace a Root CA than an ICA, so using an ICA allows the Root CA to be used as little as possible. For Pilot Deployments our understanding is that there will be a single ICA that supports all the deployments. As well as issuing certificates to lower-tier CAs, the ICA issues certificates to other non-central SCMS components.

- The **Enrollment CA (ECA)** issues enrollment certificates to end-entities. Enrollment certificates are used to request application certificates, i.e. certificates that are used to authorize messages used in the context of an application. Enrollment certificates are distinguished from application certificates because revocation can be managed more easily by having long-lived enrollment certificates and short-lived application certificates. The Enrollment CA gets assurance that a device is in fact entitled to an enrollment certificate of the type requested from the Device Configuration Manager (DCM).
- The **Registration Authority (RA)** receives requests from end-entity devices for application certificates, approves them, and forwards them to the Pseudonym CA (PCA) for the certificates to be issued. When the certificates are issued the RA makes them available for download by the end-entity. When necessary, the RA protects end-entities from having their location or identity revealed to the PCA.
- The **Pseudonym CA (PCA)** issues certificates to end-entities.
- The **Linkage Authorities (LAs)** create Linkage Values which are used to support revocation while still preserving privacy to the greatest possible extent.
- The **Misbehavior Authority (MA)** collects misbehavior reports, submitted by field devices or by other means (see Section 6.2.7 for discussion) and determines whether a device is to be revoked. If the device is revoked:
  - The CRL Generator signs the Certificate Revocation List (CRL)
  - The CRL Store component makes the CRL available for direct download on request (a “pull” mechanism)
  - The CRL broadcast component broadcasts the CRL to field devices (a “push” mechanism).
  - **Note** that in NYC CVPD our intent is to avoid the use of Certificate Revocation Lists altogether.
- The **Location Obscurer Proxy (LOP)** protects an end-entity from having its location be known to the RA, to protect its privacy.
- The **Device Configuration Manager (DCM)** is responsible for initializing devices and for providing assurance to the ECA that devices are entitled to the enrollment certificates that are being requested. The role of the DCM is key in the SCMS as it is wholly trusted to ensure that only valid devices can get certificates – there is no way to get an application certificate without an enrollment certificate, and a device that is incorrectly issued with an enrollment certificate may be able to obtain a large number of application certificates before it is detected and the certificates removed.
- The **Certification Services** work with the ECA to define and enforce requirements for device security that the DCM must attest are met by candidate devices for enrollment. In NYC CVPD certification services for interoperability will be provided by USDOT, and certification services for physical security will be provided by self-certification as described in Sections 5.4 and 5.5.

From the NYC CVPD point of view, the most important components are:

- **Enrollment Certificate Authority (ECA)** – interfaces with DCM to issue Enrollment certificates
- **Registration Authority (RA)** – interfaces with devices to provide Authorization certificates
- **Pseudonym Certificate Authority (PCA)** – issues Authorization certificates but does not interface directly with devices

- **Misbehavior Authority (MA)** – interfaces with devices to receive misbehavior reports and to distribute Certificate Revocation Lists (CRLs) if necessary. Our understanding is that this will not be in operation on day 1 of the Pilot Deployment, although if it is in operation we will support it by procuring devices that implement documented misbehavior detection processes. See Section 6.2.7 for further details.

NYC CVPD will not operate any SCMS components itself.

- The DCM will be operated by the supplier
- All other SCMS components will be operated by the SCMS Operator

### 6.2.3 Applications and PSIDs

IEEE 1609.2 certificates allow the holder to carry out specific application activities, for example sending messages drawn from a particular message set. The permitted application activities are identified at a high level by the PSID and at a lower level by a PSID-specific SSP field in the certificates. In this section we identify the PSIDs that will be used in 1609.2 certificates in the NYC CVPD and which will be managed by the SCMS. Table 6-1 lists all the usage scenarios and the corresponding message types.

**Table 6-1. Mapping Between Applications and Application Activities That Use 1609.2 Certificates**

CV Application / Usage Scenario	Application Message Utilization									
	BSM	MAP	SPaT	SRM	TIM	RSA	SSM	PSM	WSA advertising?	Data up-load
<b>BSM-Based Safety:</b>	BSM									
Blind Spot Warning										
Emergency Electronic Brake Light										
Forward Collision Warning										
Intersection Movement Assist										
Lane Change Warning/Assist										
Vehicle Turning Right in Front of Bus Warning										
<b>Red Light Violation Warning</b>	BSM	MAP	SPaT							
<b>Speed Limit Compliance</b>	BSM	MAP								
<b>Speed Compliance / Work Zones</b>	BSM	MAP			TIM	RSA			TIM	

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

CV Application / Usage Scenario	Application Message Utilization									
	BSM	MAP	SPaT	SRM	TIM	RSA	SSM	PSM	WSA advertising?	Data upload
Curve Speed Compliance	BSM	MAP								
Oversize Vehicle Compliance	BSM	MAP			TIM				TIM	
Emergency Communications and Evacuation	BSM				TIM				TIM	
Pedestrian in Signalized Intersection Warning	BSM	MAP	SPaT					PSM		
Mobile Accessible Pedestrian Signal System	BSM	MAP	SPaT	SRM			SSM			
ASD Application Configuration Download and Firmware Update									Firmware update, config update	
RSE Application Configuration Download and Firmware Update						--none--				
RSE RF Monitoring	BSM									
ASD RF Monitoring	BSM	MAP	SPaT							DUp
ASD Data Upload									Data Upload	
Performance measurement data processing						--none identified--				

Table 6-2 shows the PSIDs that will appear in certificates and what devices will need certificates with those PSIDs. The PSID is shown in “p-encoded” form, i.e. the hex representation of the octet string used in IEEE 1609.3 [7] to encode the PSID value. PSID allocations are given in IEEE 1609.12 [8].

**The devices identified in Table 6-2 will interact with the SCMS to obtain certificates with the PSIDs or PSID combinations identified in Table 6-2.**

Table 6-2 also identifies:

- Whether PSIDs appear in multiple simultaneous certificates, to help protect privacy as discussed in Section 4.2.2.
- Whether a given PSID appears in the same certificate as a different PSID (because they are used by the same device type and in a similar way)

**Table 6-2. PSIDs That Require Certificates, By Device Type**

Application activity (PSID)	Device type				PSID allocated?	Multiple simultaneous certificates?	Shares certificate with
	ASD	PID	RSE	TMC			
BSM	X				0p20	X	Data Upload
MAP				X	0p80-03		n/a
SPaT			X		0p80-03		n/a
TIM				X	0p80-02		n/a
RSA				X	No		n/a
PSM		X			0p27		n/a
WSA			X		0p80-07		n/a
SRM		X					
SSM			X				
Data Upload	X				0p26	X	BSM

NOTES on Table 6-2:

1. MAP and SPaT will need to be distinguished by SSP in the certificates so that a compromised SPaT-signing RSE won't be able to create a MAP.
2. RSA PSID is anticipated to be the same as TIM; this will be determined during Phase 2.
3. 0p26 is allocated for misbehavior reporting but can be used for data upload.

Table 6-3 shows the PSIDs that will not appear in certificates but will appear in WSAs.

**Table 6-3. PSIDs that Will Not Appear in Certificates but Will Appear in WSAs**

Application Activity (PSID)	PSID Allocated?
Firmware update	No
Configuration update	No

For each application that uses 1609.2 certificates, the specification of that application is intended to provide a Security Profile that specifies options for how 1609.2 services are to be invoked.

**ACTIONS:**

- Work with stakeholders to ensure that all required PSIDs are allocated.
- Work with application definition organizations to ensure that the security profile for all relevant applications will be available to the SCMS operator in time for correct certificates to be issued.
- Work with SCMS to ensure that all PSIDs that need to be allocated in certificates can be allocated by Pilot Deployment SCMS implementation.

### 6.2.4 SCMS-Core: Initial Provisioning

In the Initial Provisioning usage scenario for an application running on a device or component, the device or component obtains an enrolment certificate and submits a request for its first pseudonym

certificate or batch of pseudonym certificates. The Device Configuration Manager has responsibility in the SCMS architecture for providing assurance that the devices that obtain credentials from the SCMS are in fact eligible to receive those credentials. Figure 6-2 shows information flows for initial provisioning.



(Source: NYCDOT, 2016)

**Figure 6-2. Information Flows for 1609.2 Initial Provisioning**

**In the NYC Pilot Deployment, the DCM will be implemented at the device supplier – i.e. the devices will be provisioned with enrolment certs by the supplier. The Supplier will create and make available to the NYC CVPD a list of enrolment certificates cross-referenced to the serial number of each device in order to support efficient removal of misbehaving devices.**

**RISKS.** Since NYC CVPD does not control the SCMS, the following risks exist. All of these risks potentially impact the time to procure devices and so the ability to deploy devices in NYC CVPD in a timely manner.

- The interface to the SCMS might not be published in time for suppliers to build to.
- The interface to the SCMS might not be fully specified enough to be implementable.
- It may not be possible for suppliers to test their implementation against an SCMS instance and so device-side certificate management implementation may have undiscovered bugs.
- The SCMS Manager may not make physical and OS security requirements clear in time for suppliers to build to.
- The physical and OS security requirements, when published, may not be attainable for devices that need to be robust in the environmental conditions that obtain
- The process for demonstrating that devices meet SCMS requirements may not be clear or consistent enough for suppliers to follow
- The definition of the physical and process security requirements on the DCM may not be available in time for the suppliers to conform to it
- Even if the definition of the physical and process security requirements on the DCM is made available in time, it may not be possible for suppliers to comply with it.

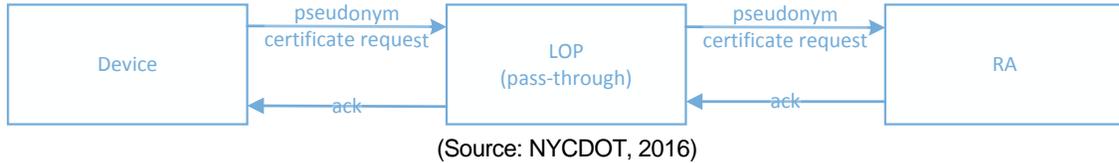
## 6.2.5 SCMS-Core: Initial Download

In the Initial Download usage scenario for an application running on a device or component, the device or component downloads its first pseudonym certificate or batch of pseudonym certificates.

In the NYC CVPD, this is either done at the same time as provisioning (i.e. through the supplier's internet connection) or by the same mechanism as certificate update. If it is carried out at the same time as provisioning it is carried out using the SCMS-defined interfaces. See the next section for security management considerations relevant to certificate update.

**Neither the supplier nor any entity operated by the NYC CVPD will record or have access to information indicating which pseudonym certificates are held by a given device.** According to the SCMS design, no individual SCMS component will have this information either, although SCMS components can cooperate to derive this information if necessary for revocation.

Figure 6-3 shows information flows for initial pseudonym certificate request. Figure 6-4 shows information flows for request and download for application certificates..



**Figure 6-3. Information Flows for 1609.2 Initial Pseudonym Certificate Request**



**Figure 6-4. Information FLOws for 1609.2 Application Certificate Request And Response**

## 6.2.6 SCMS-Core: Certificate Update

In the SCMS concept:

- 1) The RA manages requests from multiple client devices and submits them to the PCA for the PCA to issue certificates
- 2) The PCA issues certificates and returns them to the RA, encrypted for the client device
- 3) The RA stores them in a location accessible over the public internet and identified by a URL
- 4) The client devices use DNS lookup to contact the RA
- 5) The RA sets up a TLS-protected session with the client device that features server-side authentication of the RA with an X.509 certificate
- 6) The client device authenticates to the RA with its enrolment certificate
- 7) The RA makes the appropriate certificates available to the client device via a download protocol that supports robust delivery, session resumption, etc.

In NYC CVPD, it is a strong goal to avoid live connections from the TMC to the Internet, and in particular to allow pass-through connections from field devices over NYCWiN through the TMC to a service remote on the Internet. However, it does not seem that we can avoid this in this case.

**The NYC CVPD preference is to enable holes in the firewall to allow the devices to contact the RA directly.** The firewall will allow the following outbound connections to the internet from communications passing through or originating at the RSE:

- Connections the Pilot Deployment RA/LOP for certificate download.

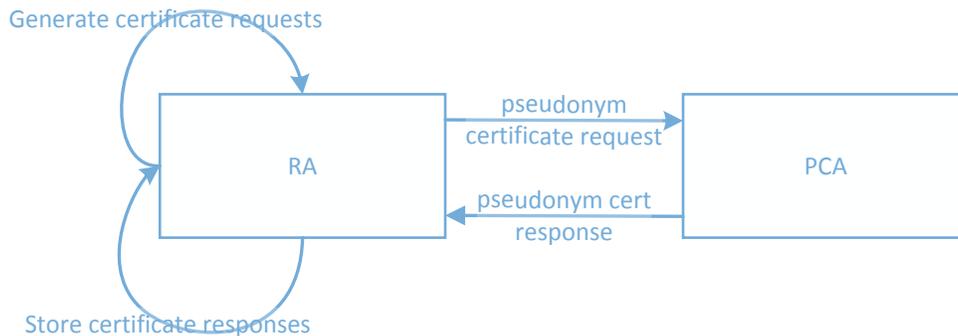
The TMC will host a DNS resolver and will populate the internal IP address of this DNS resolver to the WRA field in the WSA to allow ASDs to do a DNS lookup of the RA.

**NOTE 1:** When updating ASD certificates, the ASD needs to connect through the RSE and the TMC to the RA. When updating RSE certificates, the RSE needs to connect through the TMC to the RA. When updating TMC certificates, the TMC needs to connect to the RA. When the ASD is connecting the RSE needs to provide IPv6 connectivity. This is addressed in Section 6.2.10.

**NOTE 2:** If this approach (of having the RA remote over the internet) does not meet performance requirements, the NYC CVPD will work with the SCMS Operator to see if a mirror of the RA certificate download functionality can be hosted at the TMC.

**Communications shall be protected between ASDs/RSEs and the SCMS in an end-to-end fashion (i.e. encryption between device and SCMS) based on the published SCMS interface. There will be no additional security mechanisms provided at the network or transport level.** This protection ensures that the TMC does not have access to the contents of the communications and will not know which ASD is requesting certificate download, although they will know what RSE the activity is originating at.

Information flow within the SCMS for pseudonym certificate issuance is shown in Figure 6-5. Information flow between a device that uses pseudonym certificates and the RA via the RSE and TMC is shown in Figure 6-6.



(Source: NYCDOT, 2016)

**Figure 6-5. Information Flows for 1609.2 Pseudonym Certificate Issuance**



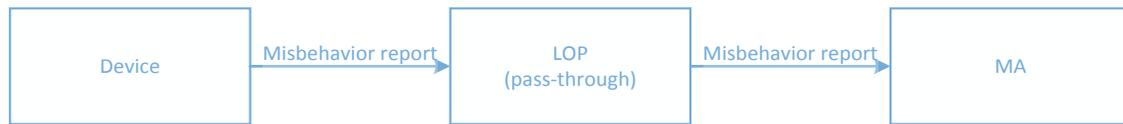
(Source: NYCDOT, 2016)

**Figure 6-6. Information Flows for 1609.2 Pseudonym Certificate Download**

## 6.2.7 SCMS-Core: Misbehavior Reporting

To protect the system, the SCMS must have mechanisms to determine that devices have been compromised or removed and should no longer be issued pseudonym or application certificates. There are two processes for doing this:

- *Misbehavior reporting* is the process by which field devices, having received messages from other field devices, determine that those messages are likely to be false or malicious and report that information to the SCMS. The SCMS carries out analysis on the misbehaving messages to determine if a single device is misbehaving sufficiently badly to be revoked. The information flow for misbehavior reporting is shown in Figure 6-7, though note that misbehavior reporting is not yet standardized so the flow in the figure is conjectured rather than certain.
- *External reporting* is the process of determining that a device should be revoked using some mechanism other than “in-band” revocation. For example, a maintenance engineer might determine that a device has been tampered with and the keys extracted, or an information security officer might discover that the keys from a device have been posted on the internet. The information flow for external reporting is shown in Figure 6-8.



(Source: NYCDOT, 2016)

**Figure 6-7. Information Flow for 1609.2 Misbehavior Reporting (Conjectured)**



(Source: NYCDOT, 2016)

**Figure 6-8. Information Flow For 1609.2 External Reporting**

### 6.2.7.1 Misbehavior Detection

The ability for misbehavior detection to operate depends on two specification bodies:

- For each application, the full specification needs to include a definition of what constitutes misbehavior to be detected. This is application-specific because misbehavior consists of sending messages that may be interpreted within an application.
- The SCMS interface must include a protocol for reporting misbehavior.

At the time of writing, to the best of our knowledge neither of these specifications exist:

- There is no misbehavior report payload for BSM or for any other application or message set.
- There is no misbehavior reporting protocol.

As such, **devices within the NYC CVPD will not support misbehavior reporting to the SCMS on day 1**. If a specification becomes available for misbehavior reports for any given application, and if CAMP provides a misbehavior reporting protocol, suppliers will be requested to provide support for misbehavior detection as part of the standard software support / patch / update cycle.

### **6.2.7.2 External Reporting**

- **ASDs/RSEs:** Maintenance engineers will check for physical tampering with the security module as part of the normal maintenance cycle. If they notice tampering they will escalate to an information security manager. If the information security manager determines that there is sufficient risk of the keys having been extracted they will notify the SCMS and request that the device is blacklisted. In this case the device will be removed from the vehicle (if a mobile device) or from its mounting (if an RSE) and returned to the supplier or the provisioning center for re-initialization (see Section 6.2.9). (and possible recertification)
- **Field reporting by participants:** If participants report an unusual number of false alerts, the information security manager will attempt to determine which device was involved by (a) understanding the location of the alerts and notifying operators of devices that might have been in that location (b) instructing maintenance engineers to be particularly vigilant for signs of device compromise. An email address and automated telephone answering service will be provided for participants to report suspicious events, and maintenance personnel will be trained to ask drivers, when they bring vehicles for maintenance, if anything unusual happened during driving.
- **Event data upload:** We will collaboratively define misbehavior scenarios with the other CV Pilot Deployment teams and investigate whether the event data upload channel can be used to report misbehavior.
- **Monitoring:** The information security manager(s) will monitor internet security news for any indication that devices have been compromised. If a device's keys are posted online, the information security manager will coordinate with the SCMS Operator to revoke that device. If it seems likely that a device has been compromised, but there is no information to identify the device, the information security manager will instruct maintenance engineers to be particularly vigilant for signs of device compromise.

**The Supplier will create and make available to the NYC CVPD a list of enrolment certificates cross-referenced to the serial number of each device in order to support efficient removal of misbehaving devices.**

**ACTION:** Ensure that the following is true about the SCMS. If it is not, manual reporting will not be possible and the only way to remove devices will be to physically remove and deactivate them.

- The SCMS will provide an interface and process for reporting enrolment and pseudonym certificates that should be revoked. (This could be, for example, email to the SCMS Operator, or there could be a machine-to-machine protocol; there is a wide range of acceptable

- solutions, and our requirement is simply that there is a documented and operational process on day 1.)
- The SCMS will be able to determine the enrolment certificate to revoke from pseudonym certificates or keys that are published.

## 6.2.8 SCMS-Core: Revocation

Revocation is the process of protecting correctly-operating devices from the risks arising from trusting incorrect messages by removing compromised or seriously malfunctioning devices from the system. Revocation can in principle happen by two mechanisms:

- *Certificate Revocation Lists (CRLs)*: These are distributed to field devices and identify the certificates that are no longer trusted. Before trusting a received message, the field devices check that the certificate that signed the message is not on the CRL; if it is on the CRL, the receiving device rejects the message. CRLs must be periodically updated and re-distributed.
- *SCMS Internal Blacklist*: The SCMS maintains a blacklist of devices that are revoked and ensures that they do not receive pseudonym certificates. This means that once a revoked device's currently downloaded batch of certificates expires, the device no longer has current certificates and cannot create signed messages that will be trusted. If a device does not have current certificates it need not appear on a CRL.

**The NYC Pilot Deployment does not intend to distribute Certificate Revocation Lists over the air. Revocation will be supported by internal blacklisting within the SCMS only. To support this, we will request the SCMS operator to issue end-entity certificates with the CrlSeries field set to 0, which is used in IEEE 1609.2 to indicate that the certificate will not appear on a CRL.**

### RISK:

- The lack of a requirement to support CRLs poses a risk if devices from other locations: (a) have been provisioned with several years of certificates; (b) chain back to the same root certificate and so are trusted by NYC CVPD devices; (c) have been compromised; (d) can send authenticated messages within the NYC DP site, for example because the compromised device itself is transported to NYC or because the keys are extracted and used in a different device. If all of these conditions hold, devices from other sites can be used to send invalid but trusted messages within the NYC CVPD site, disrupting NYC CVPD operations. **We consider this risk remote and do not see it as sufficient to require support of CRLs .**

If the CAMP project develops a spec for CRL distribution, and our suppliers are willing to provide client software to support it, we will support CRL distribution via the RSEs in the maintenance facility that also support certificate download.

**NOTE:** NYC CVPD does not have control over (a) whether CA certificates appear on a CRL (b) how often the CRLs for CA certificates are updated. Our understanding is that there will be a CRL to support the potential revocation of these certificates, but that the SCMS design supports distributing this as part of the certificate update process rather than separately, over the air. **Our Operating Concept is therefore that no CRLs, including CRLs for CAs, will be distributed other than**

**through the certificate update process.** We will modify this concept if, in consultation with the SCMS Operator, this turns out not to be the case.

## 6.2.9 SCMS-Core: Re-initialization

If a device needs to be re-initialized it will be returned to the supplier, who may re-initialize it or replace it. The device will be swapped out for a device of the same type in storage that is already provisioned with certificates as specified in Section 6.2.4. The device will be taken from the pool of spare devices located at the fleet barn. The supplier will provide a correctly provisioned replacement. How this device is provided – whether it is a new device or an old one that has in some way been re-initialized – is not the concern of the NYC CVPD.

## 6.2.10 SCMS-Support: IP Connectivity via RSE



(Source: NYCDOT, 2016)

**Figure 6-9. Information Flows for IP Connectivity via RSE**

RSEs at barns provide an IP connection for vehicle based devices to the SCMS for certificate update and to the TMC for log file upload. Other RSEs may have a permanent connection to the TMC.

The RSE broadcasts a secured WSA to announce the IP connection. For each application that is accessed over IP, the RSE includes a PSID for the application and the IP address to which the connection should be made.

The RSE will implement a firewall blocking all IP access from mobile devices to any IP address other than those approved for specific applications. The approved applications at the time of writing are the following and no others:

- Certificate download
- Event data upload
- Configuration management
- DNS lookup

The firewall settings need to be updated if the IP address (range) for the RA or RA agent or (if used) DNS lookup service changes. This will be done via the Configuration Management usage scenario described in Sections 3.10 and 4.3.10.

The TMC shall monitor the data traffic usage to detect abuse of the IP connection. In particular, if an RSE at a barn is generating more IP traffic than would be warranted by the number of ASDs known to be associated with that barn, the information security manager shall investigate to determine the reason.

The RSE maintains a log of security management related connections. This log is anonymized so all identifying information is removed from it. The log information shall be made available to the TMC via SNMP over TLS.

### **6.2.10.1 Detection of Abuse**

The data traffic usage shall be monitored to detect abuse of the IP connection. In particular, if an RSE at a barn is generating more IP traffic than would be warranted by the number of ASDs known to be associated with that barn, the information security manager shall investigate to determine the reason.

## **6.3 SNMPv3 Security Management Considerations**

SNMPv3 will use TLS authentication as specified in RFC 5953.

TLS will be configured as specified in Section 4.2.5 of this document, including the subjectAltNames in the certificates for the TMC and the managed devices.

The NYC CVPD system will run a CA internally to issue certificates to the TMC. The TMC SNMP certificate shall have a lifetime of one day to remove the need for certificate revocation lists.

The suppliers of the ASDs and the RSEs shall issue the devices with a client certificate with a five-year lifetime and shall send the client certificate to NYC CVPD to allow for it to be whitelisted.

## **6.4 VPN Security Management Considerations**

VPN connectivity will use TLS as specified in Section 4.2.5 of this document, including the subjectAltNames in the certificates for the TMC and the managed devices.

The NYC CVPD system will run a CA internally to issue certificates to the TMC. The TMC SNMP certificate shall have a lifetime of one day to remove the need for certificate revocation lists.

The suppliers of the ASDs and the RSEs shall issue the devices with a client certificate with a five-year lifetime and shall send the client certificate to NYC CVPD to allow for it to be whitelisted.

## **6.5 Physical Protection Security Management Considerations**

For RSEs connected to ITS-REs, physical protection shall be provided by running the cable inside the mast arm supporting the devices. Note however that this connection does not primarily rely on physical protection for its security.

For ASDs protected to vehicle databuses, the ASD shall record all instances when connectivity to the vehicle databus is lost during power-on and shall report them as part of its status report when next queried.

# Chapter 7. Security Management

## Lifecycle Activities per Device Type

### 7.1 RSE

RSEs will be initially provisioned by the Supplier and thereafter will manage their own certificates live by downloading them from the RA operated by the SCMS Operator, via the LOP operated by the SCMS Operator.

RSEs, when installed, will have a permanent internet connection with sufficient connectivity to the SCMS to ensure they are always up-to-date. RSEs at barns will have internet connectivity sufficient to update the certificates of all devices as they pass by unless there is a network outage beyond the control of NYCDOT. There will be one RSE at each barn for an equipped fleet. These RSEs will be maintained primarily by the owners of the respective barns. There may be additional RSEs providing internet connectivity, placed at busy intersections and maintained by the NYC CVPD team, to act as a backup in case of service outage at the barns.

#### 7.1.1 Lifecycle

The RSE lifecycle may be any one of the following. The requirements below support all of the lifecycles.

- RSE is delivered from supplier and installed in a fixed location, and stays there
- RSE is delivered from a supplier and installed in a series of fixed locations
- RSE is delivered from a supplier and placed on a slowly moving vehicle, for example for work zone warnings
- RSE is delivered from a supplier and placed in storage. When an RSE in the field fails or has to be replaced, the RSE in storage is quickly provisioned appropriately to the location and placed there.

The general process for RSE is as follows.

##### 7.1.1.1 Provisioning

- 1609.2:
  - The Supplier runs a DCM and initializes the RSE with the following enrollment certificates:
    - One authorizing it to send SPAT messages anywhere within the Pilot Deployment site.
    - One authorizing it to send WSAs anywhere within the Pilot Deployment site.

- One authorizing it to send SSMs anywhere within the Pilot Deployment site.
- The enrolment certificates have a lifetime of three years.
- X.509:
  - The TMC provides the Supplier with the CA certificate that issues the TMC's X.509 certificate as specified in Section 4.2.5. The Supplier installs this on the RSE and configures the RSE so that this is the only CA trusted to authorize SNMP or VPN connections. The Supplier also locks down the RSE so that new CA certificates can only be installed if the RSE is wiped.
  - The Supplier generates a client X.509 certificate for the RSE with subjectAltName equal to rse-XXXX.cvpd.dot.nyc.gov, where XXXX is a four-hex digit serial number for the RSE that has been provided by NYC CVPD.
- Software:
  - The Supplier installs a TLS-based VPN client and a TLS-based SNMP v3 client
  - The Supplier installs a 1609.2 certificate management application that can read geographic regions from a MIB and use them to form certificate requests.
- The Supplier sends the RSE and the X.509 client certificate to the TMC. The TMC adds the client certificate to the list of whitelisted certificates for TLS connections.

### **7.1.1.2 Initial Download**

- The RSE is delivered to the Provisioning Center,
  - In the Provisioning Center it is configured via SNMP to request 1609.2 application certificates as appropriate for SPAT and WSA, but this time with a geographic validity region set to a circular region with the center at the center of the intersection and the radius of the validity region set equal to 30 meters (for stationary RSEs) or the relevant work zone (for mobile RSEs).
  - The device also requests a CrIseries value of 0 to appear in the application certificate.
  - ASSUMPTION: The SCMS supports application certificates with a different geographic validity region than the associated enrolment certificate. IF THIS IS NOT TRUE, the application certificates will have a validity region equal to the entire NYC CVPD site.
  - ASSUMPTION: The SCMS allows devices to be issued with application certificates with a CrIseries value equal to 0 and allows devices to indicate that they wish to have that CrIseries value, either by explicitly setting that field in the certificate request or through out-of-band communication of that desire.
- Once the geographic region of the RSE has been set via SNMP, it requests and receives an initial set of application certificates via the RA (the PCA actually issues the certificates, but the RA provides the interface). This will be done through an IP connection through the TMC to the RA.
  - If the RA is not hosted at the TMC, the TMC will implement a firewall so that communications to the RA's IP address are permitted.
  - The application certificates have a lifetime of one week + 1 hour overlap.

### 7.1.1.3 Operations

- The RSE is installed on site. When installed on site it has a permanent connection to the Internet.
- The RSE establishes a TLS VPN connection to the TMC.
- The RSE is configured via SNMP to attempt a TLS connection with the ITS-RE and to accept only the ITS-RE certificate as a server certificate.
  - The RSE logs the result of the connection attempt in the MIB. If the connection attempt was successful it puts itself in a state where it will not attempt to initiate additional TLS connections.
- If the RSE supports IP connectivity, it is configured to log connectivity requests per Section 6.2.10 and to periodically upload logs per Section 4.3.10.
- A day before the current application certificate expires for any provisioned application (SPaT, WSA) the RSE requests and receives a new application certificate via the RA.
- The new and the old application certificate have an overlap of one hour. The RSE will stop using the old one and start using the new one as soon as the new one becomes available, unless the application is in a state where continuing to use the old one is vital.
- If at any point connectivity is not available for requesting and receiving new certificates the RSE waits until connectivity is available and requests the certificates again.
- If the RSE has no currently valid application certificate for a given application, i.e. it has not received any application certificate or all its application certificates have expired, it stops sending messages associated with that application until it is able to contact the RA and receive more application certificates
- If the RSE enrolment certificate expires, or if it receives a notification that its application or enrolment certificate have been revoked, it sends a notification to the System Management component via SNMP.
- REQUIREMENT: This notification needs to be specified.
- If the RSE is moved from one location to another, it can be reconfigured to request new certificates bound to the new location.
- If the RSE was originally anticipated to support just SPAT, but later a requirement comes up for it to support WSA (or vice versa), it shall be reconfigured in the field to request those certificates via SNMP.

### 7.1.1.4 Assumptions on Credentialing Process

#### **SCMS**

- **Interface:** The SCMS interface supports
  - Requesting enrolment / application certificates for arbitrary PSIDs
  - Requesting an enrolment certificate
  - Requesting one application certificate at a time with a week's validity and an hour's overlap with the next certificate
  - Requesting an application certificate a day before the current application certificate expires

- Requesting an application certificate with a validity region within but not identical to the corresponding enrolment certificates.
- Notifying the device if its enrolment certificate has been revoked
- Setting the CrlSeries value to 0 in application certificates.
- **Performance:** If connectivity is available, the SCMS supports the following performance:
  - Issuing enrolment certificates within the amount of time it takes to initialize a device.
    - ASSUMPTION: This takes one second or less.
  - Issuing application certificates within the amount of time it takes to provision a device at the provisioning center
    - ASSUMPTION: This takes one second or less.
  - Issuing subsequent application certificates in response to a valid request within one second of the request being received at the RA.
  - Notifying a device that its application or enrolment certificate has been revoked within a day of the SCMS making the decision to revoke it.

### **Device**

- **Interface with SCMS:** The device supports the SCMS interface functionality specified above.
- **Configuration interface:** The device can be configured to specify:
  - The PSIDs/SSPs that are to appear in the enrolment / application certificates
  - Which distinct PSIDs appear in separate certificates and which distinct PSIDs appear in the same certificate
  - The length of time that certificates are to be valid and the overlap period
  - The length of time remaining in the validity period necessary to trigger the certificate request
    - NOTE: some of these quantities may be determined by the PSID and may therefore be specified implicitly by specifying the PSID; this will need to be established in coordination with the SCMS Operator
  - That a CrlSeries value of 0 is desired.
- **Management interface:**
  - The device supports sending a notification to System Management that it has been revoked and can be configured with a fixed IP address for this notification.
  - The device can be configured to report its application and enrolment certificates to System Management both at initialization and when new application certificates are received.

### **System Management:**

- System management supports an interface where it receives notifications from the SCMS as to whether devices have been revoked.
- System management supports an interface where it receives notifications from devices themselves noting that they have been revoked.
- System management supports a database matching the enrolment and application certificates to the location of the device.

**Provisioning:**

- The staff carrying out the provisioning are trained in how to carry out the appropriate device configuration.
- The Provisioning Center provides a secure communications link to the SCMS
- The Provisioning Center is physically secure in a way that is acceptable to the SCMS.

## 7.1.2 Geographic Constraints in Certificate

1609.2 certificates allow the inclusion of geographic constraints in the form of a validity region. If a signed message has a generation location that falls outside the validity region of the signing certificate, it is rejected. This constrains the generation location to be inside the validity region of the signing certificate. Since receivers of SPaTs, WSAs, and other RSE-originating messages will reject them if their generation location is too far away, a tight geographic restriction means that even if an RSE is compromised it can only send messages from very close to its original location. This provides a useful tool for controlling the damage that can be done by a compromised RSE. **NYC CVPD will in general use RSE application certificates with as small a geographic region as is practical and enrolment certificates with a validity region that covers the entire Pilot Deployment site.**

There will be two types of RSEs: fixed and mobile.

Fixed RSEs will be sited at fixed locations. They will have a geographical validity region of a circle centered at the location of RSE is initially sited at and with a radius of 30m to allow the RSE to be relocated at the same site without needing the data in its certificate to be changed.

Mobile RSEs as might be used for a work zone (e.g. utility repairs) or a moving work zone (e.g. pothole repairs), will need to be provisioned for each “project site”. However, they will only operate as an RSE (broadcasting MAP and SPaT and other messages such as BIM, TIM) when they are stationary at the site. (Note: the FCC does not permit an RSE to transmit while in motion.) When moving, they may be able to operate as an ASD (changing operating modes) broadcasting their BSM for any approaching vehicles to support applications such as FCW; in this mode they would use a different set of credentials – as required for an ASD. Thus, a pothole “work zone” may be configured for a large area, and operate [as an RSE] anywhere within the planned work zone only when stationary. Note that the RSE will can acquire certificates using it’s continuous access to NYCWiN to acquire the correct operating certificates for the area once it is stationary.

Mobile RSEs will have a geographic validity region that includes the relevant Work Zone. Exactly how this region is to be encoded is still TBD.

NOTE: If enrolment certificate size can be significantly reduced by indicating a geographic region larger than but containing the Pilot Deployment site, we will consider doing this.

- RISK: If the enrolment certificate indicates an area larger than but containing the Pilot Deployment site, an attacker who compromises the enrolment cert can request certificates to run a false device outside the intended area. We consider that this risk does not need to be mitigated.

### 7.1.3 Tracking Use of RSE as a Pass-Through

The RSE maintains a log of security management related connections in a series of MIB entries. This log is anonymized so all identifying information is removed from it. The log may be obtained by the TMC using SNMPv3 over TLS as specified in Section 4.2.3.

## 7.2 Aftermarket Safety Device (ASD)

ASDs will be initially provisioned by the Supplier and thereafter will manage their own certificates by downloading them from the RA operated by the SCMS Operator, via an RSE offering internet connectivity, the TMC, and a LOP operated by the SCMS Operator.

ASDs will primarily be maintained by the fleet owners.

### 7.2.1 Lifecycle

The general process for ASD is as follows.

#### 7.2.1.1 Provisioning

- 1609.2:
  - The Supplier runs a DCM and initializes the ASD with a single enrolment certificate that will allow it to request pseudonym certificates to sign BSM (0x20) and misbehavior reporting (0x28) messages. The geographic validity region of the certificate shall be at least the continental USA and may be larger depending on SCMS Operator policy. The lifetime of the enrolment certificate will be at least three years and will be agreed in consultation with the SCMS Operator.
  - The enrolment certificate will be provided by the ASD to the Supplier.
  - While in the possession of the supplier, the ASD requests and receives its initial pseudonym certificates. The ASD will have fifty certificates simultaneously valid for a period of one week + one hour overlap period. The pseudonym certificates will have the same PSIDs and geographic validity region as the enrollment certificate. The Supplier will confirm that the ASD has successfully received the first batch of pseudonym certificates before shipping the device. The ASD will not reveal the pseudonym certificates.
    - ASSUMPTION: The SCMS supports issuing fifty certificates per week. If it does not, the ASD will request twenty certificates per week.
  - The device also requests a CrIseries value of 0 to appear in the application certificate.
    - ASSUMPTION: The SCMS allows devices to be issued with application certificates with a CrIseries value equal to 0 and allows devices to indicate that they wish to have that CrIseries value, either by explicitly setting that field in the certificate request or through out-of-band communication of that desire.
  - The TMC provides the Supplier with its current event data encryption key, which is an Elliptic Curve Integrated Encryption Scheme public key over the NIST p256 curve. The Supplier installs this on the ASD in such a way that it can be updated via SNMP (see Section 7.4).

- X.509:
  - The TMC provides the Supplier with the CA certificate that issues the TMC's X.509 certificate as specified in Section 4.2.5. The Supplier installs this on the ASD and configures the RSE so that this is the only CA trusted to authorize SNMP or VPN connections. The Supplier also locks down the ASD so that new CA certificates can only be installed if the ASD is wiped.
  - The Supplier generates a client X.509 certificate for the ASD with subjectAltName equal to asd-XXXX.cvpd.dot.nyc.gov, where XXXX is a four-hex digit serial number for the ASD that has been provided by NYC CVPD.
- Software:
  - The Supplier installs a TLS-based VPN client and a TLS-based SNMP v3 client
  - The Supplier installs a 1609.2 certificate management application that can read geographic regions from a MIB and use them to form certificate requests.
  - The Supplier sends the ASD to the fleet operator, and the X.509 client certificate and enrolment certificate to the TMC. The TMC adds the client certificate to the list of whitelisted certificates for TLS connections.

### **7.2.1.2 Operations**

- The ASD signs BSMs with one of its currently valid pseudonym certificates.
- The ASD changes the pseudonym certificate that is currently in use from time to time per J2945/1.
- When events occur that are to be logged and uploaded (location sampling for probe data purposes, RF monitoring data, collisions or near-collisions), the ASD creates an event log entry; signs it with its current pseudonym certificate; and encrypts it with the TMC's encryption key.
- The ASD has access at least once a day to an RSE offering internet connectivity for certificate download.
- Starting 24 hours before the current batch of certificates expires, whenever the ASD gets internet connectivity it requests download of the next batch of certificates via an IPv6 connection through the RSE and the LOP. The RA provides the certificates as specified in the CAMP interface document [17].
- The ASD shall not store its pseudonym certificates unencrypted in persistent storage. Pseudonym certificates may be stored unencrypted in volatile memory so long as that memory is not swapped unencrypted to persistent storage.
- The new and the old pseudonym certificate batches have an overlap of one hour. The ASD will stop using the old one and start using the new one as soon as the new one becomes valid, unless the application is in a state where continuing to use the old one is vital (for example, the BSM is in an ALERT state)
  - ASSUMPTION: The specification of all applications includes a clear definition of an alert state, if one exists for that application, and indicates for how long an alert state may prevent certificates from changing.

- If the ASD has no currently valid pseudonym certificates:
  - **BSM:** it stops sending BSMS until it is able to contact the RA and receive more application certificates
  - **Log file entries:** It stores log file entries as leee1609Dot2Messages of type unsecured, encrypted with the TMC's encryption key.
- When the ASD has connectivity it uses SNMP v3 to send a notification to the TMC that it has that connectivity. The TMC may use SNMP v3 to obtain ASD status and to update configuration. In particular, the TMC may set a new encryption key to use to encrypt event log entries and set a time when the new key should start to be used.
- If the ASD enrolment certificate expires, or if it receives a notification that its application or enrolment certificate have been revoked, it behaves as specified above for the case where it has no valid pseudonym certificates.
- System Management shall track the expected expiry times of ASD enrolment certificates and re-enroll them when necessary (by replacing them in the vehicles with newer ASDs from supply).
- System Management shall be notified if an ASD is revoked and shall organize for the host vehicle to have its ASD replaced with one from supply.
- Maintenance engineers at the barn shall be instructed to visually inspect the ASDs at least once a week to see if the tamper-evident seal has been interfered with or the blocked physical ports have been unblocked.

Assumptions on credentialing process:

### **SCMS**

- **Interface:** The SCMS interface supports
  - Requesting enrolment / pseudonym certificates for the identified PSIDs
  - Requesting an enrolment certificate
  - Requesting fifty simultaneous application certificates at a time with a week's validity and an hour's overlap with the next certificate
  - Requesting download of the next week's worth of certificates a day before the current week's batch expires.
  - Restricting a device (based on its enrollment cert) to download only certificates that are valid in the next seven days
  - Notifying the device if its enrolment certificate has been revoked
  - Setting the CrlSeries value to 0 in application certificates.
- **Performance:** If connectivity is available, the SCMS supports the following performance:
  - Issuing enrolment certificates within one second or less.
  - Issuing an initial batch of pseudonym certificates within a time consistent with manufacturing processes.
  - Making certificates available in response to a download request in one second or less.

### **Device**

- **Interface with SCMS:** The device supports the SCMS interface functionality specified above.
- **Configuration interface:** The device can be configured to specify:
  - The PSIDs/SSPs that are to appear in the enrolment / pseudonym certificates
  - Which distinct PSIDs appear in separate certificates and which distinct PSIDs appear in the same certificate
  - The length of time that certificates are to be valid and the overlap period
  - The length of time remaining in the validity period necessary to trigger the certificate request
    - NOTE: some of these quantities may be determined by the PSID and may therefore be specified implicitly by specifying the PSID; this will need to be established in coordination with the SCMS Operator
  - That a CrlSeries value of 0 is desired
- **Management interface:**
  - The device supports sending a notification to System Management via SNMPv4 that it has been revoked.
  - The device cannot be configured to report its application certificate(s) to System Management at any time, to preserve privacy.
  - The device may be configurable to report its enrolment certificate to System Management.

### **System Management:**

- System management supports an interface where it receives notifications from the SCMS as to whether devices using pseudonym certificates have been revoked.

### **Provisioning:**

- The staff carrying out the provisioning are trained in how to carry out the appropriate device configuration.
- The Provisioning Center provides a secure communications link to the SCMS
- The Provisioning Center is physically secure in a way that is acceptable to the SCMS.

RISKS: For success, we require that either the certificate download protocol is robust against interruptions or the download and performance of access to the RA is fast enough to allow this transaction to be completed fast enough to manage the transaction during a single session with a single RSE. If neither of these is the case there is a risk that the ASD will run out of certificates.

## **7.3 Personal Information Device (PID)**

PIDs will be initially provisioned by the Supplier and thereafter will manage their own certificates by downloading them from the RA operated by the SCMS Operator, via an RSE offering internet connectivity, the TMC, and a LOP operated by the SCMS Operator.

PIDs will primarily be maintained by the device users themselves.

## 7.3.1 Lifecycle

The general process for PID is as follows.

### 7.3.1.1 Provisioning

- 1609.2:
  - The Supplier runs a DCM and initializes the PID with:
    - An enrolment certificate that will allow it to request pseudonym certificates to sign PSM (0x27) messages.
    - An enrolment certificate that will allow it to request pseudonym certificates to sign SRM message.

The geographic validity region of the certificates shall be at least the continental USA and may be larger depending on SCMS Operator policy. The lifetime of the enrolment certificate will be at least three years and will be agreed in consultation with the SCMS Operator.
  - The enrolment certificate will be provided by the PID to the Supplier.
  - While in the possession of the supplier, the PID requests and receives its initial pseudonym certificates. The PID will have fifty certificates simultaneously valid for a period of one week + one hour overlap period. The pseudonym certificates will have the same PSIDs and geographic validity region as the enrollment certificate. The Supplier will confirm that the PID has successfully received the first batch of pseudonym certificates before shipping the device. The PID will not reveal the pseudonym certificates.
    - ASSUMPTION: The SCMS supports issuing fifty certificates per week. If it does not, the PID will request twenty certificates per week.
  - The device also requests a CrIseries value of 0 to appear in the application certificate.
    - ASSUMPTION: The SCMS allows devices to be issued with application certificates with a CrIseries value equal to 0 and allows devices to indicate that they wish to have that CrIseries value, either by explicitly setting that field in the certificate request or through out-of-band communication of that desire.
- Software:
  - The Supplier installs an application update channel (e.g. Google Play Store)

### 7.3.1.2 Operations

- The PID signs PSMs with one of its currently valid pseudonym certificates.
- The PID changes the pseudonym certificate that is currently in use from time to time per J2945/1.
- The PID has cellular access to the internet at least once a day for certificate download.
- Starting 24 hours before the current batch of certificates expires, whenever the PID gets internet connectivity it requests download of the next batch of certificates via an IPv6

connection through the RSE and the LOP. The RA provides the certificates as specified in the CAMP interface document.

- The PID shall not store its pseudonym certificates unencrypted in persistent storage. Pseudonym certificates may be stored unencrypted in volatile memory so long as that memory is not swapped unencrypted to persistent storage.
- The new and the old pseudonym certificate batches have an overlap of one hour. The PID will stop using the old one and start using the new one as soon as the new one becomes valid, unless the application is in a state where continuing to use the old one is vital.
  - **ASSUMPTION:** The specification of all applications includes a clear definition of an alert state, if one exists for that application, and indicates for how long an alert state may prevent certificates from changing.
- If the PID has no currently valid pseudonym certificates:
  - **PSM:** it stops sending PSMs until it is able to contact the RA and receive more application certificates
- When the PID has connectivity it uses the application update channel to update configuration.
- If the PID enrolment certificate expires, or if it receives a notification that its application or enrolment certificate have been revoked, it behaves as specified above for the case where it has no valid pseudonym certificates.
- System Management shall track the expected expiry times of PID enrolment certificates and re-enroll them when necessary (by replacing them in the vehicles with newer PIDs from supply).
- System Management shall be notified if an PID is revoked and shall organize for the vulnerable road user to have its PID replaced with one from supply.
- Maintenance engineers at the barn shall be instructed to visually inspect the PIDs at least once a week to see if the tamper-evident seal has been interfered with or the blocked physical ports have been unblocked.

Assumptions on credentialing process:

### **SCMS**

- **Interface:** The SCMS interface supports
  - Requesting enrolment / pseudonym certificates for the identified PSIDs
  - Requesting an enrolment certificate
  - Requesting fifty simultaneous application certificates at a time with a week's validity and an hour's overlap with the next certificate
  - Requesting download of the next week's worth of certificates a day before the current week's batch expires.
  - Restricting a device (based on its enrollment cert) to download only certificates that are valid in the next seven days
  - Notifying the device if its enrolment certificate has been revoked
  - Setting the CrISeries value to 0 in application certificates.

- **Performance:** If connectivity is available, the SCMS supports the following performance:
  - Issuing enrolment certificates within one second or less.
  - Issuing an initial batch of pseudonym certificates within a time consistent with manufacturing processes.
  - Making certificates available in response to a download request in one second or less.

### **Device**

- **Interface with SCMS:** The device supports the SCMS interface functionality specified above.
- **Configuration interface:** The device can be configured to specify:
  - The PSIDs/SSPs that are to appear in the enrolment / pseudonym certificates
  - Which distinct PSIDs appear in separate certificates and which distinct PSIDs appear in the same certificate
  - The length of time that certificates are to be valid and the overlap period
  - The length of time remaining in the validity period necessary to trigger the certificate request
    - NOTE: some of these quantities may be determined by the PSID and may therefore be specified implicitly by specifying the PSID; this will need to be established in coordination with the SCMS Operator
  - That a CrlSeries value of 0 is desired.
- **Management interface:**
  - The device supports sending a notification to System Management that it has been revoked and can be configured with a fixed IP address for this notification.
  - The device cannot be configured to report its application certificate(s) to System Management at any time, to preserve privacy.
  - The device may be configurable to report its enrolment certificate to System Management.

### **System Management:**

- System management supports an interface where it receives notifications from the SCMS as to whether devices using pseudonym certificates have been revoked.

### **Provisioning:**

- The staff carrying out the provisioning are trained in how to carry out the appropriate device configuration.
- The Provisioning Center provides a secure communications link to the SCMS
- The Provisioning Center is physically secure in a way that is acceptable to the SCMS.

**RISKS:** For success, we require that either the certificate download protocol is robust against interruptions or the download and performance of access to the RA is fast enough to allow this transaction to be completed fast enough to manage the transaction during a single session with a single RSE. If neither of these is the case there is a risk that the PID will run out of certificates.

## 7.4 Traffic Management Center (TMC)

The TMC will have 1609.2 certificates for signing MAP, TIM and RSE. It will also have an encryption public key pair used to encrypt log uploads. The 1609.2 certificates will be updated every week and the encryption key will also be updated every week. The encryption key will be provided to ASDs and RSEs over SNMP to enable log file entries to be encrypted.

The TMC will have an X.509 certificate with subjectAltName equal to tmc.cvdpd.dot.nyc.gov and a lifetime of a day and will run an X.509 CA that will issue a new certificate every day. This will be used for authentication of connections over TLS for data upload and configuration management.

### 7.4.1 Lifecycle

#### 7.4.1.1 Initialization

These steps must be carried out before any devices can be provisioned.

- 1609.2:
  - The TMC generates an encryption key and provides it to the supplier.
  - The TMC obtains an enrolment certificate for MAP over the published SCMS interface.
  - The TMC obtains an enrolment certificate for RSA over the published SCMS interface.
  - The TMC obtains an enrolment certificate for TIM over the published SCMS interface.
- X.509:
  - The TMC stands up a lightweight internal X.509 CA, generates a CA certificate, and provides it to the supplier.

#### 7.4.1.2 Operations

- The X.509 CA daily generates a new X.509 server certificate for the TMC.
- The TMC generates a new encryption keypair every week and pushes the new encryption key and the date when it is to be used to field devices via SNMP.
- Log files that are received are decrypted with the decryption key corresponding to the key they were encrypted with.
- Encryption keypairs are deleted a week after the next encryption keypair starts to be used.
- The TMC weekly requests new application certificates for MAP, RSE and TIM
  - The TMC also requests a CrIseries value of 0 to appear in the application certificate.
    - ASSUMPTION: The SCMS allows devices to be issued with application certificates with a CrIseries value equal to 0 and allows devices to indicate that they wish to have that CrIseries value, either by explicitly setting that field in the certificate request or through out-of-band communication of that desire.
- The TMC establishes a VPN server connection with all RSEs and refreshes this daily with its new certificate

# Chapter 8. Privacy and PII Data Protection

## 8.1 Introduction/Background

Some of the data generated by vehicles during pilot deployment is considered Personal Identifiable Information (PII). Although the data generated does not identify the specific vehicle or the driver, because it includes a specific time and place, it can be merged with other data sources to provide extensive information regarding what happened in the case of a “incident”, potentially up to and including identifying individual drivers.

It is a concern of all stakeholders that any data generated could, if collected, be used for driver evaluation or that such data could be subpoenaed for criminal and/or civil suits or the subject of a freedom of information act (FOIA) request for any and all records available that could then be merged with other records (e.g. police accident reports) and used in legal proceedings, disciplinary proceedings, or insurance negotiations.

## 8.2 Performance Data Collection

The NYC CV Pilot project is primarily focused on improving safety through the reduction of vehicle crashes and pedestrian injuries and fatalities. This is consistent with the City’s focus and dedication of resources to achieve its **Vision Zero**.

To implement this project, NYCDOT will be installing Aftermarket Safety Devices (ASDs) in roughly 10,000 vehicles including 7,500 Taxis that frequent the lower half of Manhattan, 1,500 MTA buses that service this area, 500 UPS vehicles that service this area, and approximately 500 Sanitation and other City vehicles that also frequent this area. The ASDs will support a variety of safety applications including Red Light Violation Warning, School/work zone warnings, Over Speed Warning, Pedestrian in roadway warning, Vehicle/Transit bus collision warning, curve speed warning, and over-height and restricted route warnings. In addition the ASDs will support a number of V2V safety applications including Forward Collision Warning, Emergency Electronic Brake Light warning, Blind Spot Warning, Lane Change warning/assist, Intersection Movement Assist, and Stationary Vehicle Ahead warning.

The ASDs are expected to connect to the vehicle CAN bus (or other bus) such that additional vehicle dynamics can be monitored such as directional signals, hard braking, steering wheel angle, trajectory, and speed. The ASDs will use UTC time, and will include accelerometers (X, Y, Z) that can be used to detect vehicle actions.

To collect data associated with the issuance of warnings or when events occur (without warnings), ASDs will log the information (at 1/10 sec intervals) from all sources available during the time surrounding an event. The time will be configurable but is expected to be on the order of 10-20 seconds leading up to and 20-50 seconds after the event, and the duration of collection may be

---

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

modified depending on the type of warning issued. NYCDOT has suggested that the time duration may be on the order of the cycle length (e.g. 90, 120, 150 seconds) such that the analysis can perform correlations with longer term signal activity. However, data will be limited to the data that the ASD can provide and vehicle data available from the vehicle bus. (The ASD would typically log the SPaT message content, other BSM content from vehicles within a range of the subject vehicle, and SPaT/map messages within a range of the subject vehicle.)

Thus, “microscopic” data would not be continuously collected, but collected whenever an “event” occurs. The definition of an “event” will be configurable so it can be used to collect short term driver behavioral data (hard break, steering turns, accelerations, etc.) or vehicle actions (e.g. based on accelerometers) for aggregation and use for the performance measure analysis. However, such data will be held only temporarily until used for daily or weekly aggregation before being cleansed of any traceable data (e.g. exact location and time).

Selected Roadside Units (RSU) will issue a wave service announcement (WSA) indicating that they can upload log data stored in the vehicle. When the ASD receives this message, it will respond by transmitting the logged data on the specified channel and then purging its log after confirmation of receipt.

It is expected that this data will also be used in tuning the ASD warning thresholds and operation. During the implementation period (Phase 2) but prior to the activation of the audible warnings, the system will be operating in a “silent” mode such that the project can gather statistics for both vehicle and driver actions throughout the subject area. This will include logging BSMs at the RSUs and SPaT and MAP messages at the vehicles such that we can verify the proper operation of the equipment. However, except as noted below, this data will be purged once the tuning process has been completed. It can be activated periodically for additional adjustments throughout the project.

Because the detailed data is not to be kept such that it is available for FOIA requests or subpoena, this microscopic data will not be sent to the USDOT data distribution clearing house or the USDOT data warehouse. Data to be distributed externally will be cleansed and aggregated such that it minimizes the risk of privacy inference by correlating databases that might provide incriminating information for a specific driver or vehicle.

## 8.3 Tuning and Evaluation

The project will need to conduct interviews with a small selection of drivers to gain feedback on the false positives, efficiency of the Driver Interface, and apparent utility for the applications. Such data will be collected on an opt-in basis. In such cases, the target drivers need to be identified and the specific vehicle and time of operation will need to be identified such that the logged data can be retained for analysis.

## 8.4 Stakeholder Use of Logs

If a stakeholder (vehicle owner) wishes to receive this type of information for the vehicle fleet they own, then such data for their vehicles can be transmitted to them on a daily basis for their exclusive use. Such data will not be stored at the TMC or passed along to FHWA without the stakeholder’s explicit written request.

To date, none of the stakeholders have requested such data. Most have already implemented some sort of monitoring system that either provides limited real time GPS data or off-line logging of the data such that the vehicle location history can be analyzed. This data does not include the type of data being collected by the CVPD project.

## 8.5 Other Performance Monitoring

The applications listed above require the analysis of the **event** oriented data to determine the safety benefits achieved. In addition to the safety benefits, it is essential that we consider monitoring the performance of the equipment and the RF (DSRC) communications system.

Aggregated and anonymous statistics will be recorded for the individual units to monitor the DSRC activity. OBUs will record the first SPaT and MAP and BSM heard from any RSU or other vehicle (with time stamp, location, and signal strength if known) and the last message heard for each of the above. RSUs will record the first BSM heard from each vehicle (with time stamp, location, and signal strength if known) and the last location. This data can be used to monitor the RF signal issues and develop a general map of the RF coverage for each vehicle and RSU. The exact criteria for the “first” or “last” such message need to be determined and should consider some “reliability” check such as when 3 of 5 or heard or when less than 3 of 5 are heard; however, this approach works well for 10 Hz operation but may change because of changing message rates because of channel congestion or changes to transmission rates. In addition to the above, each RSU will periodically log SPaT and map messages received from other RSUs. It is important to note that not all of the BSM/SPaT/MAP messages received will be logged – only the select few such that the system can determine the RF characteristics of each RSU and OBU. While this data can be tracked to specific locations for RSUs, such data is not traceable to Personally Identifiable Information (PII) for any participant. The actual logged data (from OBUs) could be further aggregated if necessary such that only the RF information is used for further analysis.

We also want the OBU to report major system activity such as down time, lost signals on ASDs, and other system performance measurements to be determined.

Note that while this data collection is described above, there is a more complete description in the concept of operations and the Performance Measurement documents and is subject to change and refinement during subsequent development of the detailed design. It is presented here for the purpose of investigating the needed security and privacy protections for the data handling.

## 8.6 Aggregated Mobility Data

USDOT has expressed a need to collect ongoing vehicle situation data and infrastructure situational data that can be used by other applications through the CV data distribution system and stored into the CV data warehouse for analysis of network performance.

For this type of data, it should be possible to log and upload a subset of the BSM data that does not provide possible incriminating data. The rate of collection could be lengthened to once per second or longer. Since there are a significant number of vehicles within the area, collection of this type of data without vehicle identifiers can then be used to monitor network performance because the logged

BSMs act as breadcrumbs for the vehicle's history noting location and speed (and such speed could be averaged over several samples).

For the NYC project, this data will be used to provide input to the midtown-in-motion (MIM) adaptive control system and the speed detection system. Both are currently using RFID readers and monitoring the travel times of vehicles with toll tags. The MIM also used the volume and occupancy from midblock microwave detectors (RTMS) providing volume and occupancy.

## 8.7 Summary

As Connected Vehicle applications proliferate and systems grow with increasing infrastructure deployment and increased vehicle deployment, it is important to adopt data collection and data sharing guidelines and rules that maximize the benefit of such data. While people seem to accept that their every move is trackable by simply carrying a cell phone, tracking our motor vehicles seems to create issues.

Until there are clear rules governing the collection and use of such data, most stakeholders do not want to participate if there is a chance that this data can be subpoenaed or FOIA requested where it can be merged with other databases to incriminate an individual driver or vehicle. While it is also true that such data can be used to exonerate an individual or vehicle – they would rather the data not be available.

## 8.8 Additional Notes

A full privacy impact assessment (PIA) has not been carried out, but the nature of the data and the existing data flows have been reviewed and the CV pilot deployment project will be guided by the principles stated in this chapter. We follow the seven concepts to ensure privacy protection: transparency, participation and redress, specification of purpose, minimization, use limitation, quality and integrity, accountability and auditing. The SMOC provides safeguards against loss or unauthorized access, destruction, use, modification and disclosure.

To specify minimization, use limitation, and quality, we have to define the purpose of aggregated data (“why do we need this data in the first place?”) and the use of aggregated data (“How do we use the aggregated data?”). Moreover, one should note that a vehicle will constantly store at least 20 seconds of data (SPaT/BSM/MAP/WSA, CAN bus traffic) until an event is detected. Unfortunately, no exact definition of “event” has been specified yet. We feel that this has to be formalized in order to prevent collection of unnecessary data. Whereas this Security Management Operations Concept document has been prepared midway in the project's planning phase, the project's Performance Measurement and Evaluation Support Plan (FHWA-JPO-16-302) hasn't been completed yet and should be referenced for additional details regarding the system's performance measurement, especially aggregation and data use. Any specifications described in the Performance Measurement and Evaluation Support Plan (FHWA-JPO-16-302) will supersede this document on that matter.

# Chapter 9. Operation

## 9.1 User Manual

There will be no user interface for security operations provided to the operators of devices within the NYC CVPD.

## 9.2 Securing Initial Connections Between Devices

By “initial connection” we mean the establishment of a shared key for a secure communications session, such as TLS.

There are two types of initial connections: those between the TMC and a device, and those between two field devices.

Initial connections between the TMC and a device are described in Chapter 7, leaving only the initial connections between field devices. The only secure connection between field devices to be considered is the one between the ITS-RE and RSE.

The ITS-RE and RSE will be connected as follows.

- Both ITS-RE and RSE will have X.509 certificates, self-signed or signed by a private CA.
  - These certificates will have a lifetime of five years.
  - The subjectAltNames in the certificate shall be as specified in Section 4.2.5.
- The certificate will be stored in a MIB entry and made available to the TMC via SNMP v3.
- When an ITS-RE and RSE are to be connected in the field, the TMC will use SNMPv3 to configure both as follows:
  - A MIB entry indicating what certificates may be trusted to set up a TLS session will be modified to include the certificate of the peer device
  - A MIB entry indicating that the device will accept incoming TLS sessions will be set to TRUE
- As part of the RSE installation process, the RSE will act as the client to set up a mutually authenticated TLS session between it and the RSE.
- After the installation, the TMC will carry out a status query on the ITS-RE and RSE. If this indicates that the secure session has been set up, the TMC will set the MIB entry indicating that the device will accept incoming TLS sessions to FALSE.

## 9.3 Encryption Registration Number

There is no requirement for Encryption Registration Numbers for NYC CVPD devices.

## 9.4 IPv6 Over IPv4 Tunneling

IEEE 1609.3 [7] specifies Wave Service Advertisements (WSAs) that advertise services as available over IPv6, but not over IPv4. However, NYCWIN supports IPv4 only. This affects all networked IP traffic from the ASD, specifically traffic that supports the following:

- Certificate download
- Event Data upload

**To address this:**

- RSEs shall support tunneling IPv6 over IPv4 from the RSE to at least the TMC
- The TMC shall support being the endpoint of an IPv6 over IPv4 tunnel

## 9.5 Network Security on NYCWiN

### 9.5.1 General

Security on NYCWiN will be carried out in accordance with existing NYCDOT Network security practices [15] [16]. This includes monitoring, logging and intrusion detection. We do not anticipate that additional staff will be necessary to support this security task.

### 9.5.2 Penetration Testing

It is not currently planned to carry out penetration testing specifically against Pilot Deployment applications.

## 9.6 Availability

### 9.6.1 Denial of Service

Denial of service attacks within the NYC network shall be addressed by existing practices within NYC DOT IT.

Denial of service attacks on the DSRC communications channel shall be addressed as follows:

- RSEs shall report over a management interface if channel busy ratios go above a threshold to be determined
- ASDs shall log an event report every second for which channel busy ratios are above a threshold to be determined.

These shall both be done as part of the RF monitoring application. If a significant level of high channel busy ratios is observed, the Information Security Manager shall organize an investigation.

## 9.6.2 Other Availability Considerations

If IP connectivity from a barn RSE fails the barn RSE will be replaced in no more than five (5) working days.

## 9.7 Incident Response

Incident response for network intrusion incidents on the NYCDOT network will be managed according to existing NYCDOT IT security policy 15[[16].

There will be an email address and phone number for an answering service to receive reports of unusual behavior from field devices – for example, unusually high numbers of false alerts.

- If the alerts are reported as occurring in a single location, a maintenance engineer and an information security manager will be sent to the indicated site. How soon they are sent to the site depends on the frequency of the false alerts. If more than 100 false alerts are reported as happening at a location in a single day, the incident response team will report to the location no more than one working day after the threshold is reached. If more than 20 false alerts are reported as happening at a location in a single day, the incident response team will report to the location no more than a week after that threshold is reached. We will monitor these thresholds as the project progresses and change them if appropriate.
- If the alerts are reported as coming from a single device, the device will be swapped out for a device of the same type in storage that is already provisioned with certificates as specified in the sub-section of Chapter 7 relevant to that device type. The swapped-out device will have its log files uploaded to the TMC for inspection and will then be returned to the supplier for re-initialization.

## 9.8 Secure Transport of Devices

Suppliers will ensure that devices are kept in a secure location and transported in a secure way, to reduce the risk that a device capable of receiving certificates will be intercepted.

The NYC CVPD will use best practices to ensure that devices are not lost or stolen from the test site.

## 9.9 Physical Inspection

### 9.9.1 ASDs

Maintenance engineers at barns will carry out physical inspection of all ASDs at least once a month (subject to discussion with NYC DOT). If the tamper-evident seal on the ASD is broken, then the device will be swapped out for a device of the same type in storage that is already provisioned with certificates as specified in Section 7.2. The swapped-out device will have its log files uploaded to the TMC for inspection and will then be returned to the supplier for re-initialization.

## 9.9.2 RSEs

NYCDOT maintenance engineers will carry out physical inspection of all RSEs at least once every six months. This will include examining the tamper-evident seal. If the tamper-evident seal is broken, then the device will be swapped out for a device of the same type in storage that is already provisioned with certificates as specified in Section 7.1. The swapped-out device will have its log files uploaded to the TMC for inspection and will then be returned to the supplier for re-initialization.

## 9.10 Contingency Plan

### 9.10.1 ASD

20 ASDs from each supplier in excess of what is needed will be held centrally. These units will be kept powered off in a secure location. There will be an RSE offering connectivity to update certificates at the central secure location. When the RSE is retrieved from the secure inventory location, it will be powered on and allowed to acquire its initial batch of operating certificates.

**REQUIREMENT:** ASDs from a supplier will be able to update certificates when not physically connected to a vehicle.

### 9.10.2 RSU

20 RSUs from each supplier in excess of what is needed will be held centrally. These units will be kept powered off in a secure location. They will be provisioned with an enrolment certificate but no application certificate. If there is a need to replace an RSU, a replacement will be selected from the store of centrally held RSUs and configured to request an application certificate for its location.

**REQUIREMENT:** RSUs can be configured to request an application certificate for a particular location at deployment time; the location does not need to be selected at provisioning or manufacturing time.

## 9.11 Evaluation

### 9.11.1 Security Evaluation

There will be weekly calls with the Information Security Manager to ensure that the Information Security Manager is up to date with all incidents.

The Information Security Manager will produce a detailed report every month listing all known incidents involving suspected malfunctioning of the Pilot Deployment Applications. The Information Security Manager will develop a database schema for storing information about these malfunctions.

The Information Security Manager will produce a high-level report every quarter providing a review of information security incidents associated with the Pilot Deployment. Incidents deemed to be serious that occurred more than a month before the report is issued will contain a full treatment, identifying where in the system the security breach happened that allowed the incident to occur. Incidents deemed to be serious that occurred a month or less before the report is issued will be highlighted in the report and investigated in full for the following report.

Feedback arising from study of information security incidents will be provided to the SCMS manager, the suppliers, USDOT, and the conformance test team at least quarterly. If the incidents are serious enough to warrant providing feedback outside the quarterly cycle, this will be done. An outstanding task is to develop, maintain, and (if necessary) modify the criteria that make an incident count as serious. These criteria will be developed in partnership with USDOT and with the other Pilot Deployments for any applications that run in multiple Pilot Deployment sites.

## 9.12 Business Relationship with the SCMS Operator

We make the following assumptions. If they are incorrect it could jeopardize NYCDOT's legal or budgetary ability to host the NYC CVPD.

- SCMS services will be provided free of charge
- SCMS supports everything here fully operational by end of this year.
- There will be an acceptable business and legal relationship in place that is explicit about liability issues, for example if certificates are incorrectly provisioned to a device that is not eligible to them or to a hacker's device. NYC CVPD project assumes that NYC will not bear any liability arising from incorrect provisioning of certificates and has not budgeted for such a liability event.

## 9.13 Certification

The DCM has responsibility in the SCMS architecture for providing assurance that the devices that obtain credentials from the SCMS are in fact eligible to receive those credentials. Testing for compliance with existing standards and message specifications, such as IEEE 1609.2, SCMS POC interfaces, and SPaT information broadcast system specification, should be handled by the testing services that will be provided, for a fee, by the Certification Operating Council that is currently working with USDOT to standardize testing processes. However, additional requirements introduced by the NYC CVPD team, such as specific hardware and software security requirements, will be specified and/or self-certified by equipment suppliers and the pilot team. Third-party testing of these requirements usually requires submitting the devices and design documents to an accredited certification lab which is very costly and time consuming. Given the tight timelines for developing these new devices and overall deployment, formal lab testing for additional imposed requirements is likely not realistic.

# Chapter 10. Future Work to be Coordinated Between Pilot Deployment Security Teams

The following work items will be developed during the course of Phase 1 and would benefit strongly from coordination between the security teams for the different Pilot Deployment sites. The NYC CVPD team will work with the other teams to ensure that coordination happens.

- Coordinated definition of misbehavior reporting
- Coordinated definition of device management – ideally a consensus on SNMP v3 over TLS
- Coordinated definition of plausibility checking
- Coordinated approach to certification
- Coordinated approach to geographic encoding of small irregular zones such as work zones.
- Define SSPs to distinguish permissions to sign SPaT only, MAP only, or both.
- Ensure that security profiles have been defined for all applications to be deployed in the Pilot Deployments. If they have not been defined, define them.
- Specification of security-related MIB entries.
- Profile of RFC 7525 [11] to highlight the areas of relevance to the Pilot Deployments.

# References

1. Code of Federal Regulations Title 23: Highways, Subtitle I: FHWA, Subchapter K: Intelligent Transportation System, Part 940: Architecture and Standards, Section 11: Project implementation (23 CFR 940.11), available from [http://www.ecfr.gov/cgi-bin/text-idx?node=se23.1.940\\_111](http://www.ecfr.gov/cgi-bin/text-idx?node=se23.1.940_111).
2. 1362-1998 - IEEE Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document
3. Connected Vehicle Reference Implementation Architecture (CVRIA), available via <http://www.iteris.com/cvria/>.
4. U.S. DOT Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communication Technology (NHTSA 34-14; dated Aug. 18, 2014)
5. Connected Vehicle Pilot Deployment Program Phase 1, Concept of Operations (ConOps) - New York City, Final ConOps — April 8, 2016: FHWA-JPO-16-299
6. IEEE Std 1609.2-2016, IEEE Standard for Wireless Access in Vehicular Environments— Security Services for Applications and Management Messages
7. IEEE Std 1609.3-2016, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Networking Services
8. IEEE 1609.12, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Identifier Allocations
9. IETF Request For Comments (RFC) 5246, The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008, available from <https://tools.ietf.org/html/rfc5246>
10. IETF Request for Comments (RFC) 5591, Transport Security Model for the Simple Network Management Protocol (SNMP), June 2009, available from <https://tools.ietf.org/html/rfc5591>.
11. IETF Request For Comments (RFC) 7525 / Best Current Practice (BCP) 195, Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), May 2015, available from <https://tools.ietf.org/html/rfc7525>
12. National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules
13. National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
14. Federal Highways Administration, Threat definition of V2I architecture: Confidentiality, integrity, availability analysis of sample CVRIA information flows, Draft, July 2015.
15. New York City Department of Information Technology & Telecommunications, IT Security main page, available from <http://www1.nyc.gov/site/doitt/agencies/it-security.page>
16. New York City Department of Information Technology & Telecommunications, IT Security Requirements for Vendors and Contractors, available from <http://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page>

17. Crash Avoidance Metrics Partnership (CAMP), Security Credentials Management System (SCMS) Proof-of-Concept Interface Requirements, not yet available.
18. Connected Vehicle Pilot Deployment Program Phase I – Tampa (THEA): Security Management Operational Concept (SMOC), FHWA report number FHWA-JPO-16-312.
19. W. Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2 (3rd Edition), Addison Wesley, 1999
20. SAE Surface Vehicle Standard J2945/1, On-Board System Requirements for V2V Safety Communications.

# APPENDIX A. List of Acronyms

Acronym / Abbreviation	Definition
ASD	Aftermarket Safety Device
ASTC	Advanced Solid-state Traffic Controller
BSM	Basic Safety Message
CIA	Confidentiality / Integrity / Availability
CRL	Certificate Revocation List
CVPD	Connected Vehicle Pilot Deployment
DCM	Device Configuration Manager
ECA	Enrolment Certificate Authority
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
IE	Independent Evaluator
LOP	Location Obscurer Proxy
MA	Misbehavior Authority
MAP	Map
MTA	New York City Transit
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NYC	New York City
NYCDOT	New York City Department of Transportation
NYCWiN	New York City Wireless Network
PCA	Pseudonym Certificate Authority
PID	Personal Information Device
PSID	Provider Service Identifier
RA	Registration Authority
RDE	Research Data Exchange
RSA	Roadside Alert
RSE	Roadside Equipment
SCMS	Security Credential Management System
SMOC	Security Management Operating Concept

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

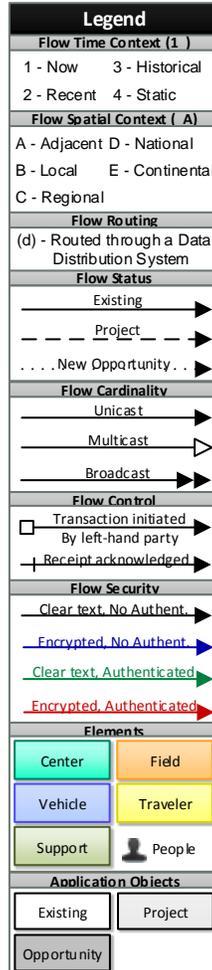
## APPENDIX A. List of Acronyms

---

<b>Acronym / Abbreviation</b>	<b>Definition</b>
SNMP	Simple Network Management Protocol
SP	Special Publication
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SSL	Secure Sockets Layer
TIM	Traveler Information Message
TLS	Transport Layer Security
USM	User Security Model
VRU	Vulnerable Road User
VSM	Vehicle Situation (Data) Message
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement

# APPENDIX B. Physical View Legend

The legend in Figure B-1 includes the definitions of the physical interconnects, the lines between the elements, shown in the Physical diagrams in Chapter 3.



(Source: USDOT, 2016)

**Figure B-1. Physical View Legend**

Each interconnect in Layer 0 or 1 includes a set of defining characteristics. These characteristics are described in Table B-1.

## APPENDIX B. Physical View Legend

**Table B-1. Physical/Application Interconnect Characteristics**

<b>Interconnect Characteristics</b>	<b>Values</b>	<b>Characteristic Value Description</b>	<b>Graphic Appearance</b>
<b>Encryption</b>	True	Information flows on this interconnect must be encrypted	Red, if Authenticability is also True; Blue if Authenticability is False
	False	Information flow encryption is not required	Black, if Authenticability is also False; Green if Authenticability is True
<b>Authenticability</b>	True	Information flows on this interconnect must include a digital signature (signed certificate credential)	Red, if Encryption is also True; Green if Encryption is False
	False	Information flow signature is not required	Black, if Encryption is also False; Blue if Encryption is True
<b>Cardinality</b>	Broadcast	Information flows on this interconnect are sent to all potential recipients that are within range	Double, filled arrowheads on the destination
	Multicast	Information is sent to multiple specific recipients	Single, open arrowhead on the destination
	Unicast	Information is sent to a single specific recipient	Single, filled arrowhead on the destination
<b>Bidirectional</b>	Yes	Information flows on this interconnect may flow in either direction	Arrowheads on both the source and destination end
	No	Information flows on this interconnect flow in one direction only	Arrowheads on the destination end
<b>Status</b>	Existing	Information flows on this interconnect are deployed today	Solid line
	Project	Information flows are going to be developed and deployed as part of this New York City (NYC) Connected Vehicle Pilot Deployment (CVPD)	Dashed line
	New Opportunity	Information flows on this interconnect are not planned currently but may be part of a future deployment	Dotted line

# APPENDIX C. Local Misbehavior Detection and Plausibility Checking Recommendations from THEA PD

*NOTE: The following text from the THEA SMOC describes their proposed approach to local misbehavior detection and plausibility checking. NYC CVPD proposes to use this as a baseline for developing a single set of misbehavior detection and plausibility checking requirements that are shared across all the PD sites.*

Local misbehavior detection is the act of a V2X device analyzing a message from another device to determine whether the message from the source device is valid or invalid as a result of malfunction or malfeasance. Local misbehavior detection strategies have not been finalized by the SCMS POC. Based on the current SCMS POC Implementation EE Requirements and Specifications and recent USDOT technical assistance webinars, the SCMS POC is in the process of testing prototype misbehavior detection methods through 2016 and will integrate global misbehavior detection functionality from mid-2016 to mid-2017 for use in version 2.0 of the SCMS POC. Members of the current THEA team developed recommendations for potential local misbehavior detection strategies. However, testing these strategies is not within the scope of the current THEA CV Pilot. Working to develop these misbehavior checks and conduct tests would be added work that could be done with additional resources or an outside contractor.

Recommended local misbehavior detection strategies focus on detecting ASD misbehavior, not RSE misbehavior. Per the SCMS POC, RSEs will have application certificates with short validity periods (e.g., daily, hourly) and require frequent certificate renewal, and hence no RSE CRL is necessary except under exceptional circumstances. We do not suggest any strategies to detect RSE misbehavior at this time. The TMC should be able to provide sufficient monitoring to determine if a RSE is not functioning properly or has been compromised.

While the ASD should obviously report any message that does not have a valid signature and/or certificate, the project team also developed some strategies that could be deployed with additional resources or an outside contractor to conduct plausibility testing. These potential requirements are not part of a current device specification and would have to be developed as new capabilities.

- Level 1 Plausibility: The ASD [and RSE] shall identify as a suspect or implausible message any BSM for which the components of the vehicle dynamic state (position, speed, acceleration, and yaw rate) are outside the values as noted below
- Speed: More than 70 m/s (252 kmph, 156 mph) which only excludes various supercars; well over any typical speed limits
- Longitudinal acceleration: 0-100 kmph in under 2.3 second (Less than 12 m/s<sup>2</sup>). Based on Ariel Atom, fastest accelerating production vehicle
- Longitudinal deceleration: 100-0 kmph in under 95 feet (Less than -12 m/s<sup>2</sup>). Based on Corvette Z6, fastest stopping production vehicle
- Lateral Acceleration: More than 11 m/s<sup>2</sup> (1.12 G). Few production vehicles can exceed 1.0 G
- Yaw Rate: Less than 1.5 radian/s, Rationale: 1.5 radian/sec is about equivalent to taking a 15 mph right turn at 27 mph (1G); tighter corners are not feasible (>1G), and softer corners are lower yaw rate at 1G acceleration

---

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation System Joint Program Office

- Values in BSM need to be internally consistent: Speed, lateral acceleration, and yaw rate are linked mathematically by the relation:  $V^2 = ac^2 / (\gamma)^2$ . As a result, if the BSM includes speed, lateral acceleration, and yaw rate, the values in the BSM must follow this relationship within some allowable tolerance. For example, dividing the lateral acceleration value by the yaw rate should yield a speed value that is equal to (within some small tolerance) the speed value in the BSM.
- Level 2 plausibility: If a BSM would result in a positive application warning decision, the ASD shall identify as a message that fails level 2 plausibility any BSM for which the vehicle dynamic state (position, speed, acceleration, heading, and yaw rate) as described by the most recent BSM falls outside the 2 sigma distribution for the vehicle state as projected from the prior BSM to the time of the current BSM (i.e., the message is implausible if it is not on its expected trajectory within 2 sigma based on the received BSMs). If such a message fails the level 2 plausibility check, the ASD shall not raise an alert to the driver on the basis of that message and shall prioritize the message for misbehavior reporting
- The ASD [and RSE] shall log within a misbehavior report (a) any message that (1) results in a warning or (2) would result in a warning but failed a level 2 plausibility check, or (b) any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility Level 1 checks
- The ASD [and RSE] shall perform intrusion detection activities and shall flag as misbehaving any message detected as intruding

The feasibility of these plausibility strategies, especially Level 2, is dependent on vehicle sensors feeding accurate information to generate an accurate BSM. This also brings about considerations of hazard detection reliability. Depending on available resources and priorities, the team believes there would be value in testing the impact of tighter BSM parameter error tolerances than those specified in SAE J2945/1 (shown in Table 2-1). Again, these tests would be outside the scope of the THEA CV Pilot and would be added work that could be done with additional resources or an outside contractor.

Tighter error tolerances present a technical challenge but should also provide a reliable and consistent collision prediction, and thereby enable user applications to provide consistent safety benefits and support plausibility and misbehavior detection strategies. However, this is all dependent on current vehicle sensors and equipment being able to meet tighter error tolerances which may not be feasible.

U.S. Department of Transportation  
ITS Joint Program Office-HOIT  
1200 New Jersey Avenue, SE  
Washington, DC 20590

Toll-Free "Help Line" 866-367-7487  
[www.its.dot.gov](http://www.its.dot.gov)

FHWA-JPO-16-300



U.S. Department of Transportation