DSRC ROADSIDE UNIT (RSU)

PROCUREMENT SPECIFICATION

Version 1.9
August 2017

Prepared for

NEW YORK CITY DEPARTMENT OF TRANSPORTATION

Prepared by

TransCore ITS – New York, P.C.
253 West 35th St, 3rd Floor
New York, NY 10001

REVISION CONTROL

Revision No.	Date	Description of Changes	Author	Checked
1.0	10/30/2016	Initial Release	SS	RGR
1.1	1/20/2017	Revised based on City review – added security	RGR	
1.2b	2/13/2017	Updates with DCAS comments – Submitted to DCAS February	RGR	
1.3	2/3/2017	Revised general formatting. Wordsmithed the requirement text and deleted duplicate requirements. Updated ReqID references in Appendix F.	SWS	
1.4	2/13/2017	Incorporated William Whyte's comments.	SWS	
1.5	2/16/2017	Final version	SWS	
1.7	4/20/2017	Revisions for harmonization with ASD and PID and SS comments and WW comments	RGR	
1.8	7/26/2017	Incorporated addendum to v1.7. Added requirements in new sections 4.8.9 and 4.8.10 as well as in Section 4.10.	SWS	
1.9	8/4/2017	Incorporated changes requested from DCAS	NB	

Table of Contents

List of Figures

List of Tables

1 NYCDOT Specification for DSRC Roadside Unit (RSU)

1.1 General Information

1.1.1.1 The purpose of this Specification is to describe the minimum requirements of a DSRC Roadside Unit (RSU) that will be used for the New York City (NYC) Connected Vehicle Pilot Deployment (CVPD) Project.

1.1.1.2 The RSU specification is based on the USDOT sponsored Version 4.1 with additions and modifications as identified herein.

1.1.1.3 The device discussed in this document is a DSRC RSU for roadside use to serve as the point of communications between the infrastructure and the vehicles and other mobile devices; it will also communicate with the traffic controller as necessary to obtain the information necessary or to provide input to the traffic controller located at signalized intersections.

1.1.1.4 All equipment and component parts furnished shall be new, be of the latest design and manufacture, and be in an operable condition at the time of delivery and installation. All parts shall be of high quality workmanship, and no part or attachment shall be substituted or applied contrary to the manufacturer's recommendations and standard practices.

1.1.1.5 The design shall be such as to prevent reversed assembly or improper installation of connectors, fasteners, etc. Each item of equipment shall be designed to protect personnel from exposure to high voltage during equipment operation, adjustments, and maintenance.

1.1.1.6 The RSU shall be designed for to operate continuously for a minimum of 10 years without operator intervention.

1.1.1.7 The Bidder for the RSU shall provide references to show that it has successfully deployed similar equipment in the street environment and has a working version of same operating in one or more of the USDOT connected vehicle (CV) pilot or demonstration CV systems currently in operation.

1.1.1.8 This equipment will be installed by third party contractors or the City based on the directions of the supplier. As noted later, the vendor shall be responsible for providing all incidental connectors, cables, fittings, mounting brackets, etc. that are necessary to complete a working installation.

1.1.1.9 Note that the word Vendor, Bidder, Supplier, and Contractor are used throughout this document to reflect the various stages of the project. A single contract will be awarded to the successful bidder who then becomes the vendor and contractor. The term bidder refers to the corporate entity which submits a bid to provide the equipment and services listed herein; the term contractor and vendor shall mean the entity which is awarded a contract to supply the equipment and services described herein.

1.2 General Contract Requirements

1.2.1 General

1.2.1.1 The following general requirements shall apply to this contract.

1.2.1.2 The New York City *Connected Vehicle* Project Development Team has produced a number of support documents during the first phase of this project. This has included (but is not limited to) a Concept of Operations (ConOps), Security Management Operational Concept (SMOC), System Requirements Document (SRD), Performance metrics and evaluation document, and a system architecture document (SAD). These are all available on-line at the US DOT web site or New York City Project site. The City is continuing to refine these documents and has incorporated these application requirements into these procurement specifications. However, many of the applications and data exchanges will require further adjustments and enhancements in order to meet all of the requirements stated herein. The contractor shall comply with the existing functional specifications and safety applications in this bid document to the satisfaction of the City and adhere to all future releases related to hardware and software modifications included herein or jointly developed with the City.

1.2.1.3 The apparent silence of these specifications as to any detail, or the apparent omission from them of a detailed description concerning any work to be done and materials to be furnished shall be regarded as meaning that only the best general practice is to prevail and that only the best material and workmanship is to be used. Interpretation of these Specifications shall be made upon that basis.

1.2.1.4 The bidder shall read and review the Phase 1 contract documents – specifically the Concept of Operations (ConOps), Security Management Operating Concept (SMOC), Performance Measurement and Evaluation Support Plan, System Requirements Specifications (SyRS), and System Architecture Document (SAD). These provide a more complete set of requirements for the System and hence the RSU. Note that these documents are also being revised to ensure consistency.

1.2.1.5 The bidder shall also review and understand the ASD procurement document; the RSU supplier will be responsible for coordinating their efforts with the ASD suppliers and the New York Project team which is developing the TMC CV support systems such that the system meets the stated goals and requirements stated therein.

1.2.1.6 Many of the design details have not been included herein for either the RSU or the ASD as both systems are somewhat dependent on each other and the standards do not currently support all of the functionality required for this project. This requires some flexibility on the part of the suppliers to cooperate with each other to solve and resolve major and minor technical issues including RF operation, messages, dialogs, and application operation to build a successful system.

1.2.2 Requests for clarifications

1.2.2.1 The prospective bidder shall submit any questions for clarification or requests for changes in the specifications at least 10 days before the letting date advertised.

1.2.2.2 Requests for clarifications and questions regarding the bid documents shall be submitted in writing to the parties shown below.

Address:
Mr. Rashad LeMonier
New York City
Department of Citywide Administrative Services
Municipal Building (18th Floor)
1 Center Street
New York, NY 10007
Email: rlemonier@dcas.nyc.gov

1.2.2.3 All requests shall identify the specific section(s) of the specifications which are in doubt or for which clarification/change is requested.

1.2.2.4 Answers to questions will be transmitted to all bidders via first class mail, fax, and email.

1.2.2.5 All prospective bidders shall provide a valid email address. Email addresses provided shall be capable of accepting attachments at least 5 MB in size in PDF format. (Note: email may be used by the CITY to transmit information to perspective bidders throughout the bidding process.) The City will transmit both the documents and notice of the document availability on the City internet site such that vendors can pull such updates from the internet site if there are problems with email delivery.

1.2.2.6 The CITY shall not be responsible for the reliability of email as a form of distribution and communications. (Note: all email must also be transmitted in written form and received by NYCDOT at least 10 business days prior to the bid opening.) The prospective bidder shall ensure that email filters and spam filters are adjusted to permit the flow of email from NYCDOT to the bidder.

1.2.2.7 All prospective bidders shall provide a valid Fax number, which the City may use to transmit notices of addendum or changes to the specifications; (Clarification: the Fax may be used to notify the bidder that information has been transmitted via email or web posting such that the bidders are aware of same. However, the City is not responsible for improper receipt or loss of such fax transmissions.)

1.2.2.8 The CITY shall have no liability for the reliability or receipt of faxes transmitted to the bidders' identified fax number; acknowledgment of receipt by the CITY's fax equipment shall be sufficient proof that the fax was delivered.

1.2.2.9 The bidder shall provide acknowledgement of receipt of all updates and addendum transmitted by DCAS for this bid, including the cover page of the addendum. The cover sheet for each shall be included in the final bid submitted by the bidder.

1.2.3 Contract Delays and Work at Risk

1.2.3.1 The process of registering the contract with NYC purchasing after the submittal of bid documents is length and could take from 4 to 9 months depending on the

completeness and accuracy of the bidders business documentation, vacation schedules, and city personnel.

1.2.3.2 The project schedule for the delivery and installation of the connected vehicle demonstration project does not include schedule adjustments for this process. As a result, the contractor will be notified of their pending award and asked to proceed at risk with the development of the demonstrations and prototypes.

1.2.4 Vendor qualification demonstrations

1.2.4.1 Prior to the award of the contract, and within 10 business days of notification, the selected bidder shall demonstrate the operation of the RSU broadcasting the Signal, Phasing, and Timing (SPaT), the Map Data (MAP), the Radio Transmission Commission for Maritime Services (RTCM), and receiving and storing the Basic Safety Messages (BSM) from the vehicle ASDs.

1.2.4.2 The City will make a test facility available for such testing. It shall be the responsibility of the bidder to establish whatever infrastructure is necessary for their demonstration (i.e. ASDs, controller interface and traffic signal controller, and MAP message content and security certificates if required by the ASD).

1.2.4.3 The vendor shall show that its acquisition of GPS signals is adequate for the continuous operation of the RSU (i.e. operation without interruption due to GPS lock loss and recovery). This shall be demonstrated at the test site used for the ASD demonstration and at several additional locations in Manhattan selected by the City. If the RSU fails its continuous operation test the City may, at its option, award the contract to an alternate vendor. In this situation, the City shall have no obligation for any expense incurred by the bidder and the bidder agrees that they shall have no recourse against the City for any costs incurred or for the City's failure to award a contract. By submitting a bid for this contract the bidder acknowledges these terms and conditions and agrees to hold the City harmless for all expenses and its failure to award a contract.

1.2.4.4 The bidder shall cooperate and coordinate with the ASD bidder on the arrangements for the test demonstration. The RSU shall broadcast standards conformant SPaT, MAP, and RTCM messages for use by the ASD demonstrations as directed by the City. The traffic controller shall be supplied by the RSU bidder and shall interface with the RSU to provide the conformant message content based on the signal display. NYCDOT will assist the vendor in installation of power and traffic signals for the bidder demonstrations. The bidder shall provide a complete description of their requirements. The RSU bidder shall be responsible for the development of the MAP message content for the test location. The City will provide MAP content for any intersections within Manhattan.

1.2.4.5 The RSU shall also be responsible for managing the OTA software updates

1.2.5 RSU Procurement Program

1.2.5.1 The CONTRACTOR shall develop ten (10) prototype RSUs as per this procurement specification. (Note: the CONTRACTOR may be required to make minor modifications to the RSU design (with no change in cost) based upon City review. The

CONTRACTOR is encouraged to work closely with the City to avoid unnecessary rework and un-reimbursed costs due to interpretation of the specifications.)

1.2.5.2 The ten (10) ASD prototypes will be used to verify the vendor's quality (Software and Hardware operation) and support the software development of the Back-office CV support systems including SCMS interfaces, data collection, data analysis, OTA software updates, and OTA parameter changes.

1.2.5.3 Ten (10) RSU Installation Kits shall also be supplied which shall include all accessories including mounting brackets to complete the field installation. This shall include but not be limited to Ethernet cable, connectors, PoE inserter, power supply for the PoE if required (note the cabinet does not have a 48 VDC supply) and any necessary lightning protection. The RSU power supply shall derive its power from a 120 VAC source within the controller cabinet which already includes an RFI filter, surge protection, and circuit breaker.

1.2.5.4 Ten (10) Prototype installation Kits will be released for delivery to the City after verification of the proper operation and certification of the RSU prototypes.

1.2.5.5 The RSU vendor supply program shall undergo a ***prototype phase*** during which the City will work with the CONTRACTOR to ensure conformance to the requirements, and demonstrate various aspects of the technical challenges including support for the following:

(a.) "Tunable" applications (to compensate for the NYC driving environment)
(b.) Over-the-air (OTA) software updates
(c.) OTA tuning of the applications
(d.) Data collection (evaluation & operation)
(e.) Security system implementation (use of SCMS)
(f.) Software stability
(g.) Support for IPv4 and IPv6
(h.) Location determination accuracy
(i.) Hardware stability for the roadside environment including environmental (temperature, humidity, shock, vibration) and electrical (power interruption, surges, ESD)

1.2.5.6 During the prototype evaluation phase (or before), the RSU prototypes shall also be subjected to certification for standards conformance for the RF portion of device including messages which will invoke the appropriate SAE standards, IEEE standards, NEMA standards, and NTCIP standards (e.g. J2735, J2945/x, 802.11p, 1609.x, NEMA TS2 environmental).

1.2.5.7 Once the prototypes have been "proven", the City ***may*** release the production quantity. Note that this will be optional – i.e. there is no assurance that the production quantity will be released when the City awards the contract. Further, the CONTRACTOR will be required to provide timely submittals, design documents, and message proposals for review as they proceed.

1.2.5.8 During the prototype design and development, the CONTRACTOR shall be required to provide timely submittals, design documents, and message proposals for review as they proceed. These documents will be reviewed by NYCDOT and its subcontractors,

USDOT and its consultants to ensure conformance to the overall requirements of the project and the requirements documents.

1.2.6 Bid Items

Table 1. Proposed Bid items

Item #	Unit of Measure	Goods to Be Procured	Number To Be Procured	
1	Each	Roadside Units (RSU) - prototypes	10	
2	Each	RSU Installation Kits - prototypes	10	
3	Each	RSU Production Quantity (on approval)	390	
4	Each	RSU Installation Kits Production (on approval)	390	
5	Block of 1 week on site in NYC – See Section 1.2.9	On Site (NYC) Engineering Support Services Unit: week (optional)	8	
6	Lump Sum See Section 1.4.2	Software source code and development environment	LS	

All pricing must be submitted on the C pages included with the solicitation. Substitutions/variations of this document will not be accepted.

1.2.7 Proposed Delivery Period

1.2.7.1 Upon the request of the City, prototype designs/drawings shall be submitted during the evaluation of bids from proposed vendors and prior to award.

1.2.7.2 Multiple vendors may be asked to provide designs/drawings of the proposed RSU solution.

1.2.7.3 Prototypes are due within thirty (30) days after notification of award.

1.2.8 Preliminary production release

1.2.8.1 Once the prototypes have been “accepted”, the City may release a production quantity. Note that this will be optional – i.e. there is no assurance that the production quantity will be released when the City awards the contract. Further, the CONTRACTOR shall be required to provide timely submittals, design documents, and message proposals for review as they proceed.

1.2.8.2 The commitment to purchase the 390 production units will be dependent on the vendor’s conformance to the schedule and the overall reliability of their device. If there are no problems with the prototype units, the City has the option of releasing the balance of the 390 production units or cancelling the contract paying only for the prototypes already delivered.

1.2.8.3 The City will reserve the right to purchase additional RSU's and installation kits for the line item bid amount for the production units in lots of twenty five (25). With a nominal 12 week or faster delivery.

1.2.8.4 By submitting a bid to supply this equipment, the bidder acknowledges that the City shall have the right to terminate the contract during the delivery of the prototypes and prior to notification of release of the production units without any further expense or obligation if it is deemed to be in the best interest of the City.

1.2.9 Engineering Services

1.2.9.1 This contract includes the purchase of on-site engineering support services for up to 8 weeks on site in NYC.

1.2.9.2 The line item will be purchased in lots of 1 week at a time. The actual number of weeks purchased will depend on the needs of the contract and may be extended to a maximum of 12 weeks.

1.2.9.3 Under this bid item, the vendor shall provide the onsite services of a qualified engineer to assist the City and its consultants and subcontractors in such tasks as troubleshooting apparent problems and training.

1.2.9.4 The engineer shall report to a location within NYC as specified by the City and be prepared to work with the City staff and its consultants as scheduled by the City for not less than 32 man hours between 10 AM Monday morning and 2 PM Friday afternoon.

1.2.9.5 The City will provide 7 day advance notice for the request and the vendor shall provide the onsite engineer within 7 days after notification or as otherwise allowed by the City.

1.2.9.6 The engineer or expert provided by the vendor shall have full knowledge of the equipment being furnished, the software, its operations, and the technology involved and shall be prepared to assist the City with whatever information and tools may be required.

1.2.9.7 The purpose of this item is to significantly shorten the time required to troubleshoot and correct difficult system "problems" by bringing the right resources to the situation rather than waste valuable time and resources trying to remotely isolate the problem or establish responsibility for the problem. It also provides the City with access to the experts necessary to work through design and deployment issues as necessary.

1.2.9.8 However, if the source of the problem for which the Vendor was called to NY City for this purpose turns out to be a defect in the product or software/equipment provided by the Vendor, then the City is not be obligated to pay for the site visit, the Vendor shall not invoice for the support call, and all costs shall be the responsibility of the Vendor. Otherwise, the Vendor shall invoice the City for this line item for each week as specified above.

1.2.9.9 The City's judgment as to the cause of the problem shall determine whether the engineering support call is billable as stated above.

1.2.10 Manufacture's Qualifications

1.2.10.1 The manufacturer shall have manufactured and integrated and demonstrated a minimum of 10 RSUs for the US domestic market during the last 3 years.

1.2.10.2 At least 5 RSUs shall have been in operation on the street for a minimum of 6 months.

1.2.10.3 The RSU shall consist of three major 'assemblies': 1) the Roadside Unit (RSU) including all processing and DSRC radios as required herein, 2) the antennae and installation cables, mounting brackets and hardware, and 3) software/firmware providing the J2735 Messages as described herein and connecting to the central sytem using either IPv4 or IPv6.

1.2.10.4 Note: it is the intent of these requirements that the bidder be able to demonstrate that they can meet this qualification for each (and all) of these categories by at least one member of their team and that the named member/supplier will be providing these specific assemblies.

1.2.10.5 If the bidder proposes a team to meet these qualification requirements, then the CONTRACTOR shall not change team composition without written approval from the CITY. (Clarification: if the bidder submits multiple team members to meet specific requirements, each submitted team member must meet these qualification requirements for the proposed items. The bidder must name which items will be supplied by which team member. Failure of a team member to meet these qualifications will cause the team to be considered non-qualified.)

1.2.10.6 Failure to comply with all of these requirements (above) shall constitute grounds for disqualification.

1.2.10.7 The prospective bidder shall provide the names, dates, contract numbers, and contact information with their bid proposal to substantiate their qualification. (Note: the CITY will review this qualification information and determine the acceptability of the response prior to the award of the contract.)

1.3 Correspondence and Contract Documents

1.3.1.1 The CONTRACTOR shall submit all requests to the CITY in written (hard copy) form. (Note: this will include but not be limited to requests for changes, time extensions, project submittals, drawings, requests for clarifications, schedules, etc. The number of copies is listed elsewhere herein.)

1.3.1.2 The CONTRACTOR shall commit all verbal discussions, telephone calls, etc. to a written document if there are any issues regarding technical aspects of the project, schedules, deliverables, performance, or costs.

1.3.1.3 The written document shall be transmitted (electronically and in hard copy) to the CITY by the CONTRACTOR **within 5 business days of the verbal discussion**.

1.3.1.4 The document shall clearly and concisely state what was discussed and shall clearly and concisely indicate any conclusions and all decisions made. The CITY shall review this document for accuracy.

1.3.1.5 The CITY shall have the right to make corrections to this document. Only the final CITY approved document shall be used for later reference.

1.3.1.6 If the CITY has not commented on or revised the document within 20 business days after receipt, it shall be assumed to be an accurate representation of the discussions as transmitted.

1.3.1.7 Following all meetings and teleconferences, the CONTRACTOR shall submit detailed minutes of the meeting/teleconference including any decisions, clarifications, changes and action items to the CITY for review. (Note: The CITY may make changes and adjustments to the meeting minutes and shall distribute the revised report to all parties.)

1.3.1.8 All action items shall clearly indicate the action, person responsible for the action, and the date the action is to be completed.

1.3.1.9 Only the final meeting minutes reviewed and approved by the CITY shall be used for later reference.

1.3.1.10 Meeting minutes shall be transmitted to the CITY within 5 business days of the meeting.

1.3.1.11 If the CITY has not commented on or revised the meeting minutes within 20 business days after receipt, they shall be assumed to be an accurate representation of the meeting as transmitted.

1.3.2 Contract Document Submittal

1.3.2.1 At the request of the City, the CONTRACTOR may be required to conduct periodic teleconferences and/or web conferences to review the status of design, construction, deliveries, testing, documentation, etc. if the City believes such periodic discussions are necessary. If such web conferences are requested [by the City or the contractor], the contractor shall be responsible for providing the appropriate web conference tool and teleconferencing service.

1.3.2.2 All fax transmittals shall be followed up with a [mailed] hard copy of the same document that must be received by the CITY within 5 business days. The CONTRACTOR shall not assume that faxed documents have been received intact; thus, a confirmation that a fax has been transmitted does not constitute proof that the intended party received the fax.

1.3.2.3 All documents received by the CITY shall be date stamped upon receipt. The date stamped on the received hard copy document shall be used for measuring all contract schedules and milestones.) The date the document is received and stamped or acknowledged by the CITY (and not the date sent by the CONTRACTOR) shall be used for measuring all contract schedules and milestones.

1.3.2.4 All documents transmitted by the CONTRACTOR (regardless of media used) shall be dated, numbered, and identified by the CONTRACTOR. Document numbers shall be sequential from the start of the project; no numbers shall be skipped.

1.3.2.5 The CONTRACTOR shall maintain on ongoing list of all documents transmitted; the list shall include the topic of the document, date of transmission, and person(s) to whom the document was sent on a secure web site.

1.3.2.6 The CONTRACTOR shall maintain a secure web site which shall contain electronic copies of all documents transmitted to the CITY.

1.3.2.7 The web site shall only be accessible by personnel authorized by NYCDOT.

1.3.2.8 The secure web site shall maintain a log of all persons accessing the web site; this log shall note the date, time, IP Address, and person logging in and shall be accessible to the CITY.

1.3.2.9 Documents may be transmitted to the CITY via email to expedite delivery; all such documents must be acknowledged by the City to be considered received. Note that the City may request that selected documents be delivered in hard copy versions in which case the hard copy of the same document that must be received by the CITY within 5 business days.

1.3.2.10 The CONTRACTOR shall not assume that emailed documents have been received intact; thus, a confirmation that an email has been received does not constitute proof that the intended party received the email. The City must acknowledge proper receipt by appropriate email.

1.3.2.11 The delivery of all items to the CITY including but not limited to submittals, documentation, software, subassemblies, training, RSUs, etc. shall include a memorandum of transmittal to *Mr. Mohamad Talas* identifying the specific deliverable enclosed and identifying what contract requirement is being addressed. Deliveries without such a memorandum of transmittal shall be considered informal in nature and shall not constitute completion with regard to project schedules [e.g. milestones], payments, or work items.

1.3.2.12 Each page of all multi-page documents transmitted to the CITY shall include the page number without skipping, total number of pages, and document number.

1.3.2.13 All contract documents shall be provided electronically in Adobe PDF and Microsoft Word 2010 format or as agreed by the City.

1.3.2.14 All contract documents may be shared with USDOT for their review. Documents shared with USDOT will not be made public except as required by a court or other legal action.

1.4 Software Source Code

1.4.1 RSU Software

1.4.1.1 The SOFTWARE source code shall be provided to the CITY prior to acceptance of the equipment. Acceptance is defined in section 1.6.7.

1.4.1.2 Acceptance of the equipment shall not occur if the SOFTWARE source code and all required documentation has not been provided and accepted by the CITY. Acceptance of the equipment and the start of any warranty shall be delayed until the source code and documentation has been reviewed, approved, and accepted by the CITY.

1.4.1.3 The provisions of this section shall apply to both the existing SOFTWARE if modified by the CONTRACTOR and to any new SOFTWARE developed or provided for this contract.

1.4.1.4 The CITY shall have the unrestricted and perpetual right to use and modify all SOFTWARE including embedded firmware for use within the jurisdictional boundaries of NY CITY.

1.4.1.5 The perpetual right to use and modify this SOFTWARE shall not depend upon the execution of any maintenance and/or support contracts with the CONTRACTOR or other product vendors.

1.4.1.6 It is understood that the SOFTWARE represents the intellectual property of the CONTRACTOR and the CITY shall maintain its confidentiality. However, the CITY shall have the right to hire independent contractors, other companies, or staff to develop and complete modifications to the SOFTWARE; such contractors and staff shall execute non-disclosure agreements with the CITY such that the SOFTWARE is used exclusively for the CITY of New York and is not provided to others in any form and is only available within the entity on a need to know basis.

1.4.1.7 If the CITY modifies or causes modifications to the RSU software by parties other than the original vendor, or if the CITY uses the software in an RSU unit which is not from the original equipment supplier, the CITY will indemnify the original vendor from all claims arising from the operation of the RSUs so modified (i.e. running the modified software). The CITY shall maintain accurate records of all such modifications.

1.4.1.8 All SOFTWARE source code shall be provided in electronic form suitable for use with the development environment provided by the CONTRACTOR.

1.4.2 Development and support environment

1.4.2.1 In order for the CITY to modify the SOFTWARE, the CONTRACTOR shall provide and set up a complete SOFTWARE development environment including computer and all necessary software to allow the CITY or its consultants to modify and deploy the software as described herein.

1.4.2.2 The development facility shall include all necessary media to allow the environment to be constructed (installed) on a commonly available virgin machine including operating system, development tools, libraries, make files, network interfaces, drivers, and all SOFTWARE. Installation of the development system support software requires that the software installation DVD/CD's be provided; the use of a simple backup-restore utility is not acceptable. Utilities shall be provided to allow the full use of all peripherals installed in or attached to the development system. In addition, the contractor shall also provide any cryptographic keys necessary to enable the City to install the software written or modified by the City.

1.4.2.3 The development environment shall include, but not be limited to, text editors, compilers, language pre-processors, libraries, source code, code management utilities, tool kits, operating systems, backup and restore utilities, partition utilities, anti-virus utilities, firewalls, network utilities, database software, and report generators necessary to support modifications to and deployment of the RSU SOFTWARE. All software shall be fully licensed for use by New York City on the development environment or subsequent replacement machines. Acceptance of the development station will require that the CONTRACTOR demonstrate that all installation media and vendor documentation has been provided, and that the source code for all RSU SOFTWARE as required herein is delivered.

1.4.2.4 The development environment shall fully support the ability to modify and deploy the RSU SOFTWARE, load the new SOFTWARE onto the RSU itself and to install an enrollment certificate provided by the SCMS.

1.4.2.5 The CONTRACTOR shall demonstrate that the source code is complete and accurate by building the complete SOFTWARE from the source code and development environment provided; the production version of the RSU generated by this process shall be the only SOFTWARE used for all acceptance testing.

1.4.2.6 If the CONTRACTOR has included and third party products as part of the RSU SOFTWARE, then such products shall be included in the source provided; the CITY will execute an appropriate software license with the third party that shall be paid for by the CONTRACTOR. If the source code for such third party software is not generally available, then only the object code for this software must be provided. All such instances shall be brought to the attention of the ENGINEER prior to use for approval and **shall be noted in the bid documents.**

1.4.2.7 It is the intent of these provisions that the CITY shall be able to modify the RSU functionality as necessary to support additional control functions, communications schemas, and applications. Further, the CITY shall be able to contract with third parties to port this SOFTWARE to future platforms or may make the SOFTWARE available to other parties for the supply of compatible equipment **exclusively for New York City DOT**.

1.4.2.8 The cost for the development shall be included in the ITEM labeled “Software Development Station”. Payment will be made for the SOFTWARE development environment when it is provided and demonstrated to the City. The development equipment shall be provided prior to site testing of the controllers.

1.4.2.9 The software development environment is optional. The City may elect to purchase this option at any time up to the final acceptance of equipment.

1.4.3 Software documentation

1.4.3.1 The CONTRACTOR shall provide SOFTWARE documentation to the CITY sufficient to enable an experienced programmer to modify the SOFTWARE. This shall include configuration information, *make* file description, code management documentation, and instructions in how to setup and install all software on a machine with an empty, formatted hard drive in such a way that secure boot is required and software updates are required to be signed. Documentation shall also identify the procedures for loading all SOFTWARE.

1.4.3.2 The CONTRACTOR shall include detailed database documentation for the source code used by the ASD. The CITY shall have the unrestricted right to use this documentation for its system development and for sharing with other contractors for the purpose of modifying or supplying controllers to the CITY (subject to the execution of a Non Disclosure Agreement).

1.4.3.3 The SOFTWARE documentation shall also include description of all function calls, classes, subclasses, database schema, application of COTS software, and object models.

1.4.3.4 All source code shall include in-line comments and documentation in the header files to identify the function being performed, variables, and algorithms, control strategies, errors, etc.

1.4.3.5 All error codes shall be clearly documented in a single manual for easy reference.

1.4.3.6 The CONTRACTOR shall provide detailed documentation regarding the SOFTWARE structure including object models, timing dependencies, linkages, and relationships between functions and procedures.

1.4.3.7 The SOFTWARE documentation shall be submitted to the CITY for review and approval for acceptable level of detail and thoroughness. The SOFTWARE documentation must be provided prior to acceptance of the equipment. T

1.4.3.8 If subsequent changes are required due to SOFTWARE defects or contracted changes, the provided documentation must be updated within 60 days of the SOFTWARE correction.

1.5 Supplemental Information Required with the Bid

1.5.1.1 As noted herein, the bidder is required to provide certain supplemental information with his/her bid. **This information shall be included as an attachment to the bid book**. The following checklist is provided to assist the bidder in ensuring that the necessary supplemental information has been included. Failure of the bidder to include this information may be grounds to reject the bid. All pages shall be numbered continuously showing the total number of pages attached (page X of Y) and shall contain the bidders name, the bid number and the date of the bid opening. All information provided shall clearly indicate the section of the specifications addressed and information being provided.

1.5.1.2 The bidder shall copy this check list (page) and include it with the bid documents.

SUPPLEMENTAL INFORMATION CHECKLIST			
✔		Required information	Specification Reference
	1	Project Schedule	
	2	Qualifications	
	3	Three Year supply history	
	4	Warranty Disclosure	
	5	Annual Cost to extend software warrantee	
	6	Source code license requirements	
	7	Details for any third party software	
	8	Listing of all custom electronic components and a price for the supply of such over the 15 year life after the expiration of the warranty.	
	9	Acknowledgement of receipt of all addendum and notices transmitted by NYCDOT	

Bidders name:

_____

Contact Person: _____

Bidders Address:

_____

_____

Telephone Number: _____

Fax Number: _____

Email Address: _____

1.6 Interchangeability and Compatibility of RSU Units

1.6.1.1 The RSU shall operate properly as specified herein without modifications at any location within the City.

1.6.1.2 The RSU shall operate properly with all ASDs purchased as part of this CVPD project or subsequent contracts as long as they conform the relevant standards and the procurement specifications (reference ASD procurement specifications for NYC CVPD).

1.6.2 Interchangeability Verification

1.6.2.1 The CONTRACTOR shall demonstrate the interchangeability as required above during the Prototype deployment.

1.6.2.2 The CONTRACTOR shall provide a complete submission detailing how compatibility and interchangeability are supported between the each suppliers ASD and the various locations for the RSU installation.

1.6.3 Testing and Product Qualification

1.6.3.1 This specification includes extensive requirements for design submittals, prototypes, prototype testing, design reviews, and evaluations.

1.6.3.2 The CONTRACTOR shall include a Factory Acceptance Testing, Site Acceptance Testing, and 60 day site burn-in.

1.6.3.3 The CONTRACTOR shall include all costs associated with the design, submittals, and testing including but not limited to Prototype Testing, Design Approval Testing, Factory Acceptance Testing, Site Acceptance Testing, and 60 day burn-in testing in the cost of the items supplied under this contract. (Note: No separate payment will be made for any submittals or testing as required herein.)

1.6.3.4 For all testing, the CONTRACTOR shall develop a test plan and test procedures and be responsible for implementing the complete test environment that shall be used to verify that the equipment including all software fully meet the requirements as specified herein.

1.6.3.5 The CONTRACTOR shall conduct a detailed design review with the City concurrent with their submittals for the design and operation of all hardware and software. This walk through of the design shall occur at the City offices (TBD) and shall be scheduled at least 14 days in advance. It is suggested that this design review occur early in the procurement process to avoid any necessary re-work.

1.6.4 Design Approval Testing

1.6.4.1 The contractor shall be responsible for conducting a design approval test at a facility provided by the contractor prior to or concurrent with the delivery of the prototypes.

1.6.4.2 The design approval test shall demonstrate that the RSU meets all of the requirements including operational, performance, and environmental requirements as stated herein.

1.6.4.3 The contractor shall submit the proposed design acceptance test at least 30 days prior to the planned execution of the tests.

1.6.4.4 The City and its representatives will review the proposed test plan and procedures and indicate necessary changes which shall be adopted by the contractor.

1.6.4.5 The contractor shall schedule the design approval tests such that they can be witnessed by the City and its representatives. The contractor may be required to shift the schedule up to 7 days to accommodate conflicting personnel schedules and travel costs.

1.6.4.6 The design approval tests shall be conducted on not less than 2 units concurrently; the failure of any unit may be cause for the suspension of further testing until the problem is repaired. In such cases, the City may require a restart of the total testing or continue the test program depending on the nature of the failure.

1.6.4.7 The contractor shall be responsible for all aspects of the test environment at no further cost to the City. This shall include but be limited to environmental testing equipment, simulation and measurements for processor loading and communications, and shall include both positive and negative testing.

1.6.4.8 The contractor shall be responsible for all monitoring and data collection during the testing and shall develop a detailed test report at the conclusion of the testing which shall be provided to the City for final approval within 5 days of the completion of the testing.

1.6.5 Factory Acceptance Testing

1.6.5.1 Factory acceptance testing shall verify that all inputs, outputs, sensors, and radios are operating within the required specifications.

1.6.5.2 All units shall be operated for a period of 1 week during which they shall be fully operational, continuously monitored for proper operation and subjected to temperature and voltage variations for the full range of operation.

1.6.5.3 The contractor shall develop a factory acceptance test plan for review and approval by the City.

1.6.6 Site Acceptance test

1.6.6.1 As each RSU is installed at the selected intersection/location [by the City or a separate installation contractor), it shall be activated such that it can download operating certificates and operated for a period of several minutes to verify that all interfaces and software is fully operational.

1.6.6.2 The contractor shall work with the City to develop an appropriate test environment for verifying that the RSU has been properly installed and is operating as specified herein. The City will provide the necessary test equipment, tools, for this initial part of the site acceptance test. However, such tools are expected to be simply additional ASDs or RSUs with a known radio communications pattern installed to communicate with the Unit under test.

1.6.6.3 Following the initial installation test, the operation of the unit will be monitored continuously and when it completed 60 days of fault free operation, the unit shall be declared to have passed the site acceptance test.

1.6.6.4 Any defect which is evident within this 60 day period shall either be corrected (software download), or replaced with a new unit and the defective unit will be returned to the contractor for analysis and repair.

1.6.6.5 Note that the City will attempt to retrieve the failing RSU as quickly as possible depending on staff availability and weather. Delays in retrieving the RSU shall not affect the contractor's obligation to repair this defective unit.

1.6.7 Final Acceptance

1.6.7.1 Once all of the Units have been installed at either the intersections or support locations and passed the 60 day site test, the 36 month warranty on the individual units shall commence.

1.6.7.2 The City will keep track of the date of installation, site acceptance, and start of warrantee.

1.6.7.3 During the warranty, the contractor shall be responsible for all repairs as stated herein. Software "corrections" and updates shall be coordinated with NYCDOT such that the City determines which updates to install in which fleets of vehicles.

1.6.7.4 Final acceptance of the equipment and software shall occur at the end of the 36 month warranty for each unit.

2 General Technical Requirements

2.1 Overview

2.1.1 General

2.1.1.1 This specification defines the minimum general technical requirements applicable to discrete electronic components, and the mechanical, electrical design, and construction of all assemblies and subassemblies. These requirements also describe the means and testing profiles by which the equipment as a whole and in parts shall be tested to determine compliance with these specifications. This specification identifies the ambient conditions within which the equipment must operate satisfactorily and reliably.

2.1.2 Conformance to Standards

2.1.2.1 Unless noted otherwise, the RSU shall meet the requirements set forth in the following standards:

a. Institute of Electrical and Electronics Engineers (IEEE) 802.11p
b. IEEE 1609 family
c. Society of Automotive Engineers (SAE) J2735
d. SAE J2945 family of standards
e. NEMA standards for Traffic Control Equipment (for environmental, including but not limited to shock, vibration, EDS, temperature, humidity, power interruption, and power input.

2.1.2.2 The equipment, materials, and installation shall conform to the applicable requirements of the following: Underwriters Laboratories Incorporated (UL), Electronic Industries Association (EIA), National Electrical Code (NEC), National Electrical Safety Council (NESC), American Society of Testing and Materials (ASTM), Insulated Power Cable Engineers Associates (IPCEA), American National Standards Institute (ANSI), National Electronic Manufacturers Association (NEMA). (Note: UL listing/certification of the complete RSU and cabinet is not a requirement.)

2.2 Clarifications and precedence

2.2.1 Conflict Resolution

2.2.1.1 Where there are conflicts between this specification and any other documents or standards listed above, the bidder shall bring such conflicts to the attention of the CITY for resolution at least 10 business days prior to the bid opening.

2.2.1.2 After award of the contract, the judgment of the CITY shall be considered final in all cases without further compensation to the CONTRACTOR.

2.2.1.3 The specific requirements of this specification shall take precedence over existing federal, state, and local standards or specifications unless otherwise noted.

2.2.1.4 Any conflicts within this specification must be brought to the attention of the CITY for resolution prior to construction.

2.3 Cooperative development

2.3.1.1 Not all aspects of the RSU requirements have been fully documented at this time; the contractor shall work cooperatively with the Connected Vehicle Program and with the City and its engineers during the design and development of the RSU to optimize its utility for the NY CVPD.

2.3.1.2 Such cooperation will include sharing documents with the USDOT, conducting design reviews with the project team, and review and comments on the submittals.

2.3.1.3 The contractor shall work closely with the City and its consultants to establish the operating parameters that can be modified for each of the applications where appropriate.

2.3.1.4 The contractor shall work closely with the City and its consultants to establish the OTA software and parameter update procedures and protocols.

2.3.1.5 The contractor shall work closely with the City and its consultants to establish the operation and operating parameters that can be modified for the data collection and logging applications.

2.3.1.6 The contractor shall work closely with the City and its consultants to establish the Security management approach and interfaces to the TMC and SCMS for the management of security credentials.

2.3.1.7 The contractor shall work with the ASD Suppliers to ensure interoperability and support for all of the features included in the ASD specification.

2.3.1.8 The contractor shall include provisions for this level of cooperation in their bid.

2.4 Definitions

2.4.1.1 Wherever used in these specifications the following interpretation shall apply:

- State - State of New York Department of Transportation (also NYS and NYSDOT)
- CITY – New York City DOT (also NYC and NYCDOT)/New York City Department of Citywide Administrative Services. (also NYC and NYCDCAS).
- ENGINEER – The CITY'S representative who shall be responsible for reviewing all documents; the ENGINEER shall be responsible for interpreting this specification. The CITY may hire a consultant to act as the ENGINEER for this project.
- CONTRACTOR – the CONTRACTOR is used interchangeably with the term VENDOR, SUPPLIER and MANUFACTURE in this document to refer to the single business entity that executes a contract with the CITY for the supply of the equipment and services described in this document.

2.5 Glossary of Terms

2.5.1.1 The following table defines selected project-specific terms used throughout this Concept of Operations document.

Table 2 Glossary of Terms

Term	Definition
Access Control	Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.
Administrator	These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.
Aggregation	The process of combining data elements of similar format into a single data element that is a statistical representation of the original elements.
Analysis	The process of studying a system by partitioning the system into parts (functions, components, or objects) and determining how the parts relate to each other.
Anonymity	Lacking individuality, distinction, and "recognizability" within message exchanges.
Anonymous Certificate	A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
APDU	Application Protocol Data Unit. This is a defined data structure that is transferred at a peer level between two applications.
Application	One or more pieces of software designed to perform some specific function; it is a configuration of interacting Engineering Objects. A computer software program with an interface, enabling people to use a computer as a tool to accomplish a specific task.
Application User	A user who interfaces with Application Layer software for a desired function or feature.
Assumption	A judgment about unknown factors and the future which is made in analyzing alternative courses of action.
Authenticate	The process of ensuring that an APDU originated from a source identified within the message
Authentication	The process of determining the identity of a user that is attempting to access a network.
Authenticate-ability	The ability of the receiver of information to authenticate the sender's identity or trustworthiness to send data within the domain. If required, this can be accomplished by verifying the incoming message has been digitally 'signed' by the sender.
Authenticity	The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source.
Authorization	The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.
Available	Ready or able to be used
Backup	The ability of one System Element replacing another System Element's functionality upon the failure of that System Element.
Bad Actor	A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope.
Boundaries	The area of management and control for a System or Object. It could be by latitude/longitude or by county or by regional jurisdictions.
Broadcast	A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog.

Cardinality	The characterization of the relationship between the number of sender(s) and receiver(s) of a data exchange. (e.g. broadcast (one-to-many) unicast (one to one))
Center	An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms “back office” and “center” are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of this ConOps Specification these are considered the same.
Concept of Operations (ConOps)	A user-oriented document that describes a system’s operational characteristics from the end user’s viewpoint.
Confidentiality	The property of being unable to read PDU contents by any listener that is not the intended receiver
Configurable Parameter	Non-static data that can be adjustable and updated when needed.
Configuration	Data that is used to customize the operational environment for a System Element or System User, or the System as a whole
Configure	The process of selecting from a set of option(s) or alternative values in order to create a specific operational environment.
Constraint	An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.
Contract	In project management, a legally binding document agreed upon by the customer and the hardware or software developer or supplier; includes the technical, organizational, cost, and/or scheduling requirements of a project.
Control	To exercise influence over.
Coverage Area	A geographic jurisdiction within which the System provides services.
Cyber Address	The cyber or network address of a Unified Implementation of the Reference Architecture object.
Data Consumer	1) A user or system that is receiving or using data from another user or system. 2) Any Unified Implementation of the Reference Architecture object that registers with and subsequently requests and receives delivery of data from a data warehouse.
Data Provider	1) Any Unified Implementation of the Reference Architecture object that registers with and subsequently deposits data into a data warehouse 2) A System User that is supplying or transmitting data to another user or system. A data provider is likely to be an aggregator of data.
Data Warehouse	A data storage facility that supports the input (deposit) and retrieval (delivery) of clearly defined data objects. This can be design and implemented in a variety of ways, including publish/subscribe and a traditional query based database.
Decrypt	To decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access. See Encryption.
Deployment Benefits	This term refers to the measures of effectiveness used by the NYCDOT and the Independent Evaluator on a periodic basis to assess the benefits realized from the utilization of connected vehicle technology and applications within the project’s deployment areas.

Digital Certificate or Signature	A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Note: From the SysAdmin, Audit, Network, Security Institute - www.sans.org website.
DNS (Domain Name System)	The internet protocol for mapping host names, domain names and aliases to IP addresses.
Encryption	Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.
End-User	The ultimate user of a product or service, especially of a computer system, application, or network.
Environment	The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system shall do or how it will do it.
Extensibility	The ability to add or modify functionality or features with little or no design changes.
Field	These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSU and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure.
Forwarding	The process of forward sending data onto another entity (system user) without modifying or storing the data for any substantial length of time.
Functionality	The capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product.
Geo-Fence	An electronic set of geo reference points that form a bounded geographic region.
Geo-Referencing	The process of scaling, rotating, translating and de-skewing the image to match a particular size and position. To define something in terms of its physical location in space.
Hardware	Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners.
Now (N)	Transient Data that is hyper current (relevant at the time of reporting for applications that require sub-second response).
Adjacent (A)	Data that is hyper local (relevant to a geographic area within ~1 minute travel distance)
Recent (R)	Transient Data that is current (relevant at the time of reporting for applications that do not require sub-second response).
Local (L)	Data that is local (relevant to a geographic area within 10 minute travel distance)
Historic (H)	Transient Data that is historical (relevant at the time of reporting for an indefinite interval).
Regional (R)	Data that is regional in scope (relevant to a geographic area greater than 10 minute travel distance).
National (N)	Data that is national in scope.
Continental (C)	Data that is continental in scope.
Static (S)	Data that is permanent (relevant at the time of reporting for an indefinite interval).

Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Immediate Forward Messages	Dynamic messages from ancillary devices connected to an RSU. An Example would be Signal Phase and Timing (SPaT). The RSU broadcast Immediate Forward messages only when the RSU receives them.
Integrity	1) To maintain a system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible. 2) The property of being certain that a message's contents are the same at the receiver as at the sender.
Interconnect	The communications link between two architectural objects.
Internet	An interconnected system of networks that connects computers around the world via the TCP/IP protocol.
IPv6	Internet Protocol version 6 (IPv6) is a protocol upgrade of for IPv4 (the current basis of the internet. IPv6 uses 128 bit addresses as opposed to the 32 bit IPv4 address. The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations, however network appliance (switches, routers, firewalls, etc.) shall specifically support IPv6.
Issuance	For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA). For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA). Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.
Jurisdictional Scope	The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.
Link	A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.
Hardware	Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners.
Now (N)	Transient Data that is hyper current (relevant at the time of reporting for applications that require sub-second response).
Adjacent (A)	Data that is hyper local (relevant to a geographic area within ~1 minute travel distance)
Recent (R)	Transient Data that is current (relevant at the time of reporting for applications that do not require sub-second response).
Local (L)	Data that is local (relevant to a geographic area within 10 minute travel distance)
Historic (H)	Transient Data that is historical (relevant at the time of reporting for an indefinite interval).
Regional (R)	Data that is regional in scope (relevant to a geographic area greater than 10 minute travel distance).
National (N)	Data that is national in scope.

Continental (C)	Data that is continental in scope.
Static (S)	Data that is permanent (relevant at the time of reporting for an indefinite interval).
Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Integrity	1) To maintain a system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible. 2) The property of being certain that a message's contents are the same at the receiver as at the sender.
Interconnect	The communications link between two architectural objects.
Internet	An interconnected system of networks that connects computers around the world via the TCP/IP protocol.
Issuance	For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA). For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA). Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.
Jurisdictional Scope	The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.
Link	A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.
Logical Security	Safeguards that include user identification and password access, authentication, access rights and authority levels.
Misbehaving User	A user who exhibits misbehavior.
Misbehavior	The act of providing false or misleading data, operating in such a fashion as to impede other users, or to operate outside of their authorized scope. This includes suspicions behavior as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages. etc.; either purposeful or unintended
Misbehavior Information	Includes Misbehavior Reports from System Users, as well as other improper System User acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages and other inappropriate System User behavior.
Misbehavior Report	Data from a System User identifying suspicious behavior from another System User that can be characterized as misbehavior.
Mobile	These are vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travelers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information
Non-repudiation	The property whereby a PDU is constructed in such a way that the PDU sender cannot effectively deny having been the sender of that PDU; and the PDU receiver cannot effectively deny having received a particular PDU.

On-Board Equipment (OBE)	Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment.
Operational Data Environment	The ODE consist of several different USDOT developed smart data routers brokering processed data between various data sources, including the Unified Implementation of the Reference Architecture, and a variety of data users (e.g. RDE, TMCs). As a smart data router, the ODE routes data from disparate data sources to software applications (including CV applications) that have placed data subscription requests to the ODE. The ODE also performs necessary security / credential checks and, as needed, data valuation, aggregation, integration and propagation functions.
Operators	These are the day-to-day users of the System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.
Permission	Authorization granted to do something. From the System's perspective, permissions are granted to System Users and Operators determining what actions they are allowed to take when interacting with the System.
Persistent Connection	A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received. This is opposite of Session-oriented Connection.
Physical Security	Safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information. This can range from simply a locked door to badge entry. with armed security guards
Priority	A rank order of status, activities, or tasks. Priority is particularly important when resources are limited.
Privacy	The ability of an individual to seclude information about themselves, and thereby reveal information about themselves selectively.
Process	A series of actions, changes, or functions bringing about a result.
Protocol Data Unit (PDU)	A defined data structure that is transferred at a peer level between corresponding software entities functioning at the same layer in the OSI standard model which are operating on different computing platforms that are interconnected via communications media .
Public Key	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).
Regional (R)	Data that is regional (relevant to a geographic area within ~30 minute travel distance)
Registry	A repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.
Reliability	Providing consistent and dependable system output or results.
Repackage Data	Data that is broken down for aggregation, parsing or sampling.
Requirement	(A) A condition or capability needed by a user to solve a problem or achieve an objective. (B) A condition or capability that shall be met or possessed by a system component to satisfy a contract, standard, specification, or other formally imposed document. (C) A documented representation of a condition or capability as in definition (A) or (B). (IEEE Std 610.12-1990)
Research Data Exchange	A web-based data resource provided by the USDOT ITS-JPO's Real-Time Data Capture and Management (DCM) program which collects, manages, and provides archived and real-time multi-source and multi-modal data to support the development and testing of ITS applications.

Roadside Equipment	Traffic Management equipment installed along the roadside to convey traffic or traveler information to passing drivers or to connected said management equipment to a Traffic Management Center or other back office services and applications.
Scalability	The capable of being easily grown, expanded or upgraded upon demand without requiring a redesign.
Scenario	A step-by-step description of a series of events that may occur concurrently or sequentially.
Secure Storage	Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off.
Secure Transmission	To protect the transfer of confidential or sensitive data usually by encryption, Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS) or similar secure communications.
Secure/Securely	Referring to storage, which consists of both logical and physical safeguards
Security Credential Management System	A Connected Vehicle Security Credential Management System (SCMS) provides DSRC devices with digital certificates that the devices use to sign (authenticate) and encrypt DSRC messages. The SCMS also revokes certificates, when warranted and provides a certificate revocation list (CRL) to remaining devices
Session-oriented Connection	A connection between two networked devices that is established intermittently and to handle few requests thereafter. The connection is meant to be temporary lasting for minutes, hours, but likely not more than a day before it is closed. This is opposite of Persistent Connection.
Software	Software is a general term that describes computer programs. Terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software.
States	A distinct system setting in which the same user input will produce different results than it would in other settings. The System as a whole is always in one state. A state is typically commanded or placed in that state by an operator. States are Installation, Operational, Maintenance, Training, and Standby.
Status	Anomalies, actions, intermittent and other conditions used to inform the System Operator for reparation or maintenance.
Store and Repeat Messages	Static messages that are loaded on RSUs for broadcast to passing vehicles. An Example would be a Curve Speed Warning (CSW) Message that contains the geometry of the subject curve and an advised speed in which to traverse the curve. These messages are loaded as individual text files that contain the broadcast strategy (how often the message is broadcast, what (DSRC) channel the messages is broadcast on, etc.) and the message payload.
Subsystem	An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
Synchronization	the act or results of occurrence or operating at the same time or rate
System	(A) A collection of interacting elements organized to accomplish a specified function or set of functions within a specified environment. Typically the System Elements within the System are operationally self-contained but are interconnected and collaborate to meet the needs of the System and its Users. (B) A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.

System Element	(A) A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment. (B) An object and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system element includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
System Need	A capability that is identified and supported within the System to accomplish a specific goal or solve a problem
System Performance	This term refers to the measures of effectiveness used by NYCDOT traffic management operations staff on a periodic basis to manage the on-going operation of the system.
System Personnel	This represents the staff that operates and maintains the System. In addition to network managers and operations personnel, System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployment teams, and Testers.
System Requirements Specification (SyRS)	A structured collection of information that embodies the requirements of the system.
System User	System Users refers to Mobile, Field, and Center Systems.
Testers	These users verify the System's operation when any changes are made to its operating hardware or software.
Time	A measurable period during which an action, process or condition occurs.
Time synchronization	Calibration adjustment of date, hour, minutes and seconds for keeping the same time within a system.
Time-of-Day	Current hours, minutes and seconds within a day.
Traceability	The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test.
Transition	A passage from one state, stage, subject, or place to another
Trust Credentials	A user's authentication information which determines permissions and/or allowed actions with a system and other users.
Unicast	The sending of a message to a single network destination identified by a unique address.
User	An individual who uses a computer, program, network, and related services of a hardware and/or software system, usually associated with granting that individual with an account and permissions.
User Need	A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system.
Valid	When data values within a message are acceptable and logical (e.g., numbers fall within a range, numeric data are all digits).
Validate	To establish or confirm the correctness of the structure, format and/or contents of a data object.

2.6 Acronym List

2.6.1.1 The following table defines selected project-specific acronyms used throughout this Concept of Operations document

Table 3. Acronym List

Acronym/ Abbreviation	Definition
AASHTO	American Association of State Highway and Transportation Officials
ACL	Access Control List
AIFS	Arbitration Interframe Space, See IEEE 802.11
ASD	Aftermarket Safety Device
BSM	Basic Safety Message
C	Celsius (Unit of Temperature)
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CCH	Control Channel
CFR	Code of Federal Regulations
CML	Communications Message Log
CRL	Certificate Revocation List
CSW	Curve Speed Warning
CW min	Contention Window Minimum Value
dBm	Decibel-milliwatts
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DSRC	Dedicated Short-Range Communication
EBR	Exception Based Reporting
EDCA	Enhanced Distributed Channel Access
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
GHz	Gigahertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers

IFM	Immediate Forward Messages
IPv6	Internet Protocol version 6
IETF	Internet Engineering Task Force
ITS	Intelligent Transportation Systems
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MB	Megabyte
MIB	Management Information Base
MHz	Megahertz
MPDUs	MAC Protocol Units
MTBF	Mean Time Between Failure
NEMA	National Electrical Manufacturers Assocation
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol
NTP	Network Time Protocol
OID	Object Identifier (SNMP MIB OID)
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PHY	Physical Layer, refers to a specific layer in the Open Systems Interconnection (OSI) reference model
PoE	Power-over-Ethernet
PSID	Provider Service Identifier
QoS	Quality of Service
RDE	Research Data Exchange
RF	Radio Frequency
RFID	Radio Frequency Identifier
RSU	Roadside Equipment Note that this term in interchangeable with RSU
RSU	Roadside Unit – this is the current designation for the Connected Vehicle support equipment located at the roadside broadcasting infrastructure information, receiving and processing various messages from the CV vehicle equipment, and portable pedestrian unit.

SAE	Society of Automotive Engineers
SCH	Service Channel
SCMS	Security Credential Management System
SNMP	Simple Network Management Protocol
SRM	Store and Repeat Messages
SSH	Secure Shell
SSP	Service Specific Permission
TLS	Transport Layer Security
TXOP	Transmission Opportunity Value
USDOT	United States Department of Transportation
UTC	Universal Time, Coordinated
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VSC3	Vehicle Safety Communications 3 (Consortium)
WAAS	Wide Area Augmentation System
WAVE	Wireless Access in Vehicular Environments
WiMAX	Worldwide Interoperability for Microwave Access
WSA	WAVE Service Announcement
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol

2.7 References

2.7.1.1 The following table lists the references used to develop the concepts in this document. As some of the base standards referred to in the list are currently evolving, their identifiers have been temporarily highlighted to indicate that the version may change.

Table 4. References

#	Document Name
1	USDOT DSRC Roadside Unit (RSU) Specification version 4.0 (2014)
2	IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
3	IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture (IEEE 1609.0-2013, or later)
4	Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages (IEEE 1609.2-2016 as modified by Guidance Note 5, or later)
5	Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services (IEEE 1609.3-2016, or later)
6	Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operations (IEEE 1609.4-2016, or later)
7	Standard for Wireless Access in Vehicular Environments (WAVE) – Identifier Allocations (IEEE 1609.12-2016, or later)
8	Dedicated Short Range Communications (DSRC) Message Set Dictionary (SAE J2735, 2016 or later)
9	Standard for Power over Ethernet (IEEE 802.3at, 2009)
10	NEMA Standard for Traffic Controller Assemblies with NTCIP Requirements (NEMA TS 2-2003 v02.06)
11	Military Standard for Environmental Engineering Considerations and Laboratory Tests (MIL-ST-810G)
12	AASHTO Standard Specifications for Structural Supports of Highway Signs, Luminaries, and Traffic Signals (AASHTO LTS-5-I2)
13	International Electrotechnical Commission Standard for Environmental Testing (IEC-60068-2-6)
14	International Electrotechnical Commission Standard for Classification of Environmental Conditions (IEC-60721-3-4)
15	Standard for Electromagnetic Compatibility Measurement Procedures and Limits for Components of Vehicles, Boats, and Machines (SAEJ1113, 2013)
16	International Electrotechnical Commission Standard for Electromagnetic Compatibility (IEC EN61000-3-2)
17	NEMA Standard for Enclosures for Electrical Equipment (NEMA 250-2008)
18	DARPA Internet Program Protocol Specification version 4 (IPv4)
19	DARPA Internet Program Protocol Specification version 6 (IPv6)
20	On-Board System Requirements for V2V Safety Communications (SAE J2945/1, 2016 or later)
21	USDOT Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1 or later
22	Federal Communications Commission (FCC) Code of Federal Regulations Title 47, Parts 0, 1, 2, 15, 90, and 95

23 USDOT DTFH61-12-D-00020 DSRC RSU v4.0 Test Plan

24 Federal Information Processing Standards (FIPS) Publication 140-2 – Security Requirements for Cryptographic Modules

25 Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)

26 Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254)

27 Simple Network Management Protocol Version 3 (SNMPv3) (as specified in IETF RFC 3411, IETF RFC 3412, IETF RFC 3413, IETF RFC 3414, IETF RFC 3415, IETF RFC 3416, IETF RFC 3417, and IETF RFC 3418)

2.8 General Requirements

2.8.1 Equipment and Accessories

2.8.1.1 The CONTRACTOR shall be responsible for all incidental accessories necessary to make the RSU and all of its elements complete and ready for operation, even if not particularly specified.

2.8.1.2 Such incidentals shall be furnished, delivered, and installed by the CONTRACTOR without additional compensation or expense to the CITY. Note that the City will be responsible for the actual field installation of the RSUs based on instructions from the vendor.

2.8.1.3 Minor details not usually shown or specified, but necessary for the proper installation and operation of the ASD shall be included in the work in the CONTRACTOR's bid price, the same as if herein specified. (Note: By the submittal of a bid, it is understood and agreed by the CONTRACTOR that the system description provided herein is complete and includes all equipment necessary for the proper functioning of the ASD and all equipment, even though every item may not be specifically mentioned.)

2.8.1.4 All equipment and components furnished shall be new, of the latest design and manufacture, and in an operable condition at the time of delivery.

2.8.1.5 All parts shall be of high quality workmanship without any part or attachment being substituted or applied contrary to the manufacturer's recommendations and standard practices.

2.8.1.6 The CONTRACTOR shall not use the following parts in the design of any RSU assembly/subassemblies provided under this contract.:

- Obsolete components
- Components no longer supported by the manufacturer
- Components not recommended for new designs
- Components which have been discontinued or which the CONTRACTOR should have reasonably been expected to know were discontinued,
- Components which the vendor has announced plans to discontinue at the time of the bid in the design of any assembly/subassemblies provided under this contract.

2.8.1.7 The apparent silence of the specifications as to any detail, or the apparent omission from them of a detailed description concerning any work to be done and materials to be furnished shall be regarded as meaning that only the best general practice is to prevail

and that only the best material and workmanship is to be used. Interpretation of these Specifications shall be made upon that basis.

2.8.2 Furnished Material

2.8.2.1 All adhesives used shall have a minimum of 20 years of expected life under adverse field conditions. The CONTRACTOR shall not use 'stick-on' retention devices for any purpose unless specifically authorized by the CITY. The CONTRACTOR shall be required to show proof of the life expectancy of the adhesives proposed backed by the manufacturer of the material.

2.8.2.2 Where the RSU includes panels which must 'open', 'drop-down' or otherwise be moved to provide access to connectors, devices, option jumpers, etc., these panels shall use ¼ turn winged metal fasteners or similar simple but reliable latching mechanisms and not screw-in nuts or 'PEM studs'.

2.8.3 Serial Number

2.8.3.1 All RSUs shall have a unique serial number, which is permanently affixed to the unit.

2.8.3.2 The serial numbers shall include an obviously readable date of manufacture, the vendor's ID, and the subassembly or assembly ID.

2.8.3.3 The CONTRACTOR shall work with the CITY to determine an acceptable numbering scheme and starting numbers for serial numbers. (Note: the CITY tracks the serial numbers by procurement contract; hence, the scheme used for serial numbers needs to identify the specific contract as well as the unique unit.)

2.8.3.4 The serial number of the unit shall be stored in non-volatile storage on the device in such a way that it cannot be accessed or modified without proper authorization. The TMC shall be provided with a cryptographic key or keys and certificate or certificates, or other authentication mechanism that allows it to verify the specific device serial number for the purposes of maintenance support and to change the serial number.

2.8.4 Warranty

2.8.4.1 The purchasing of the RSUs shall be for "turnkey" units – with all software, hardware, certifications, and 36-month warranty – delivered to NYCDOT ready for installation.

2.8.4.2 The warranty shall include all hardware and software supplied under this contract including installation kits.

2.8.4.3 The CONTRACTOR shall maintain a presence within the NY City jurisdiction for the repair, stocking, and testing/certification of the RSUs.

2.8.4.4 According to the warranty terms, the City will deliver the "defective" or suspect RSUs to a depot point within the City geographic boundary. The CONTRACTOR shall test, repair, or replace the unit at their discretion within 2 business days.

2.8.4.5 Software "bugs" discovered during the warranty period shall be reviewed by the contractor. The vendor shall then develop a solution and coordinate with the City for testing and then the downloading of the software update to all field units.

2.8.4.6 The CONTRACTOR shall address all software defects with a recommended correction within 30 days or less from the discovery date.

2.8.4.7 Note that the 36 month warranty shall start at the successful completion of the site acceptance test and the 60 day initial period of operation. Failures during the 60 day period shall cause the 60 day observation period to be restarted from the beginning or continue at the discretion of the City.

2.8.4.8 Software defects noted within the 60-day “end” of the warranty period shall extend the final acceptance and warranty duration until the software “correction” has been installed and demonstrated reliable and proper operation for 60 days.

3 System Overview and Hardware Requirements

3.1 Functional Description

3.1.1.1 Under this Specification, the Contractor shall furnish RSU devices to be mounted directly on a traffic pole or mast arm, or installed in an adjacent cabinet.

3.1.1.2 The RSU in the NYC CVPD shall be capable of both transmitting and receiving using dedicated short range communications (DSRC) radios at 5.9 Gigahertz (GHz) band approved by the Federal Communications Commission (FCC), and implement the appropriate Institute of Electrical and Electronics Engineers (IEEE) and Society of Automotive Engineers (SAE) standards (IEEE 802.11p, IEEE 1609 family, and SAE J2735).

3.1.1.3 To support Vehicle-to-Infrastructure (V2I) applications, DSRC will be integrated with existing traffic signal equipment, such as Signal Controllers and backhaul communications to the Traffic Management Centers (TMCs). The DSRC RSU is a carrier-grade device capable of acting as the infrastructure first point-of-contact for vehicles and other mobile devices.)

3.2 System Design

3.2.1.1 As part of NYC's CVPD, intersections in the pilot area will be instrumented with RSU's to communicate with vehicles equipped with ASDs.

3.2.1.2 The RSU shall monitor its communications with other ASDs in the connected vehicles and infrastructure to provide alerts to drivers/operators.

3.2.1.3 RSUs shall be installed at locations to support system management functions such as providing security credentials, managing application and parameter configurations, uploading logged information (mobility, operations, and event oriented data). (Note: these locations consist of fleet terminal facilities, airports, and river crossings (bridges and tunnels) where vehicles frequently travel.)

3.2.1.4 The RSU shall be integrated into the existing system elements shown in **Figure 1**.

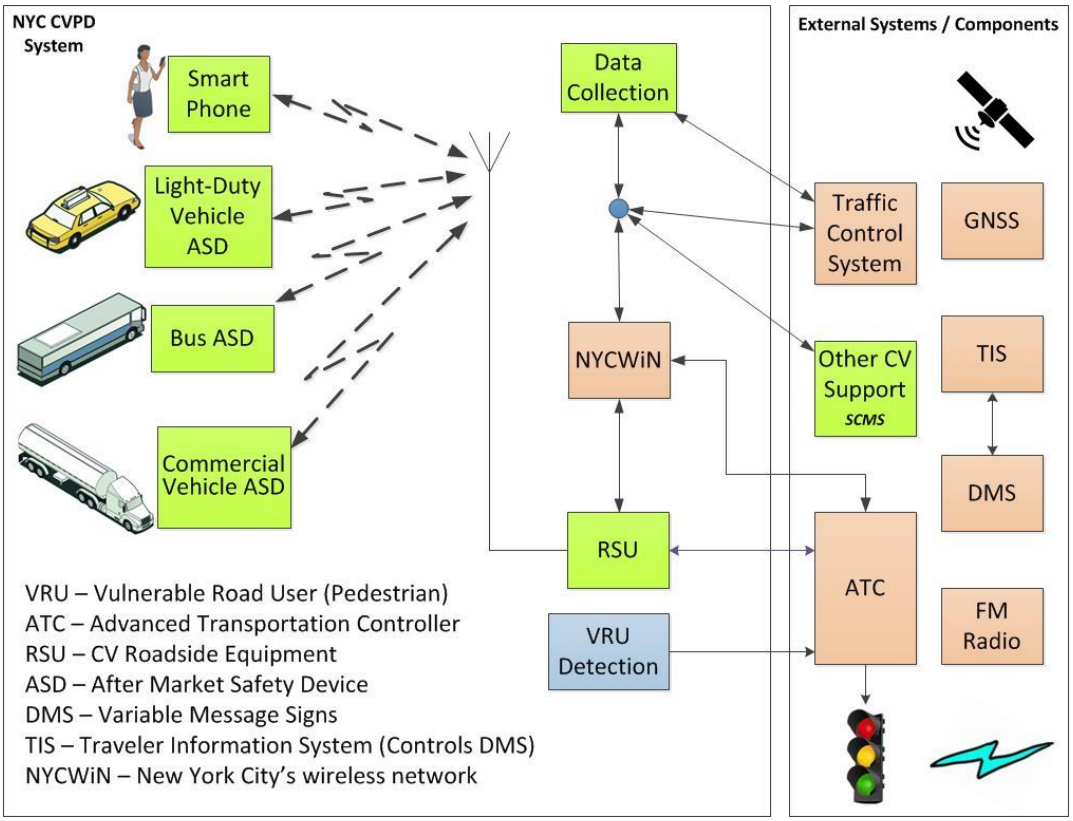

Figure 1 Envisioned NYC CVPD System

3.2.1.5 The RSU shall facilitate communication between transportation infrastructure and vehicles and other mobile devices by exchanging data over DSRC in compliance with industry standards, including but not limited to IEEE 802.11, IEEE 1609.x, SAE J2735, and SAE J2945/1.

3.2.1.6 The RSU shall be integrated with a backhaul system to enable remote management and provide vehicles and other mobile devices with services and applications delivered by back office service providers.

3.2.1.7 RSUs shall be incorporated with NYC's traffic control system to deliver enhance traffic management services to vehicles and other mobile devices.

3.2.1.8 The RSU shall act as a DSRC interface between NYC's traffic control system, the backhaul network, the ASDs, and the personal information devices (PID) as illustrated in the following high-level diagram Figure 2 below.

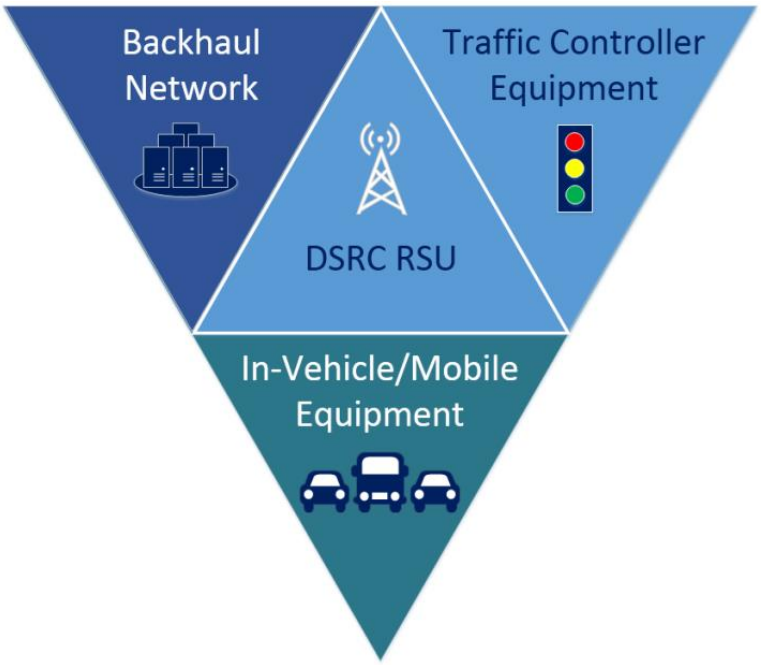

Figure 2 High Level Conceptual Diagram of the RSU

3.3 System Requirements

3.3.1 System Layout

3.3.1.1 Figure 3 - Figure 5 below depict the RSU deployment configurations. The red boxes in these diagrams highlight the system components that are covered by this specification, including the RSU device and antennas, excluding supporting hardware and infrastructure such as gantries or mast arms and traffic controller or electronics cabinets.

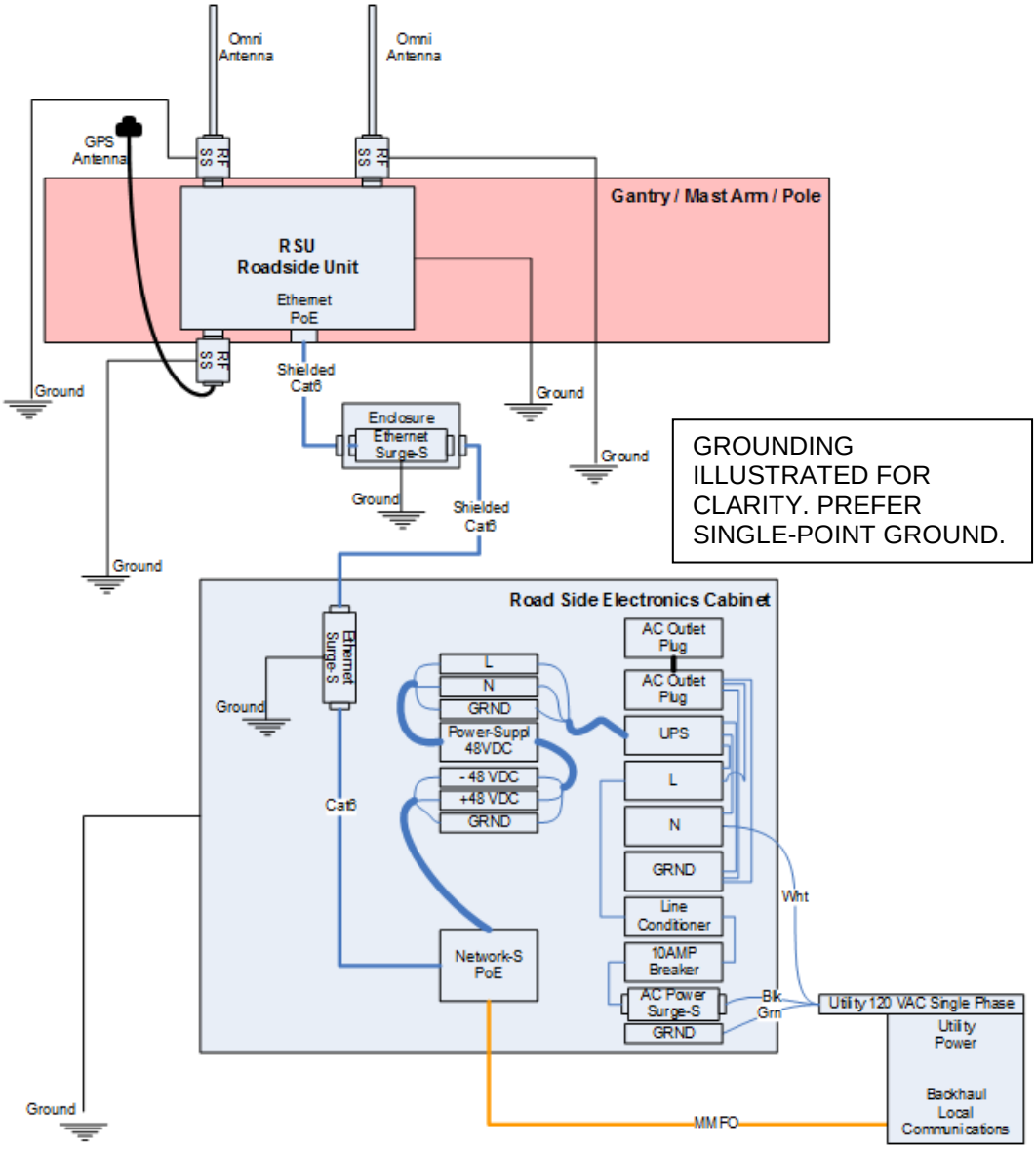

Figure 3. Configuration diagram of an RSU mounted on a Mast Arm

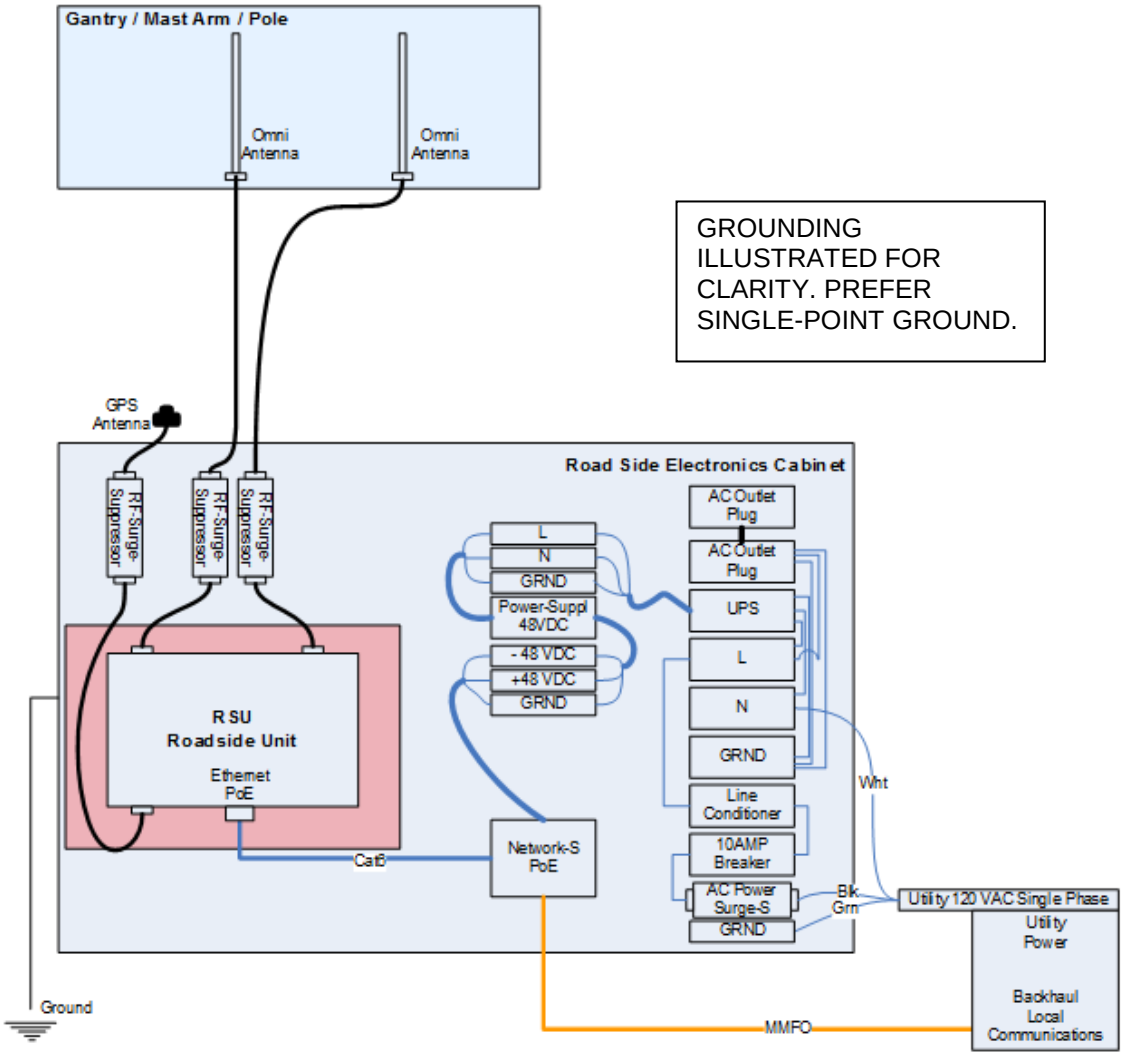

Figure 4. Configuration diagram of an RSU installed inside a roadside electronics cabinet

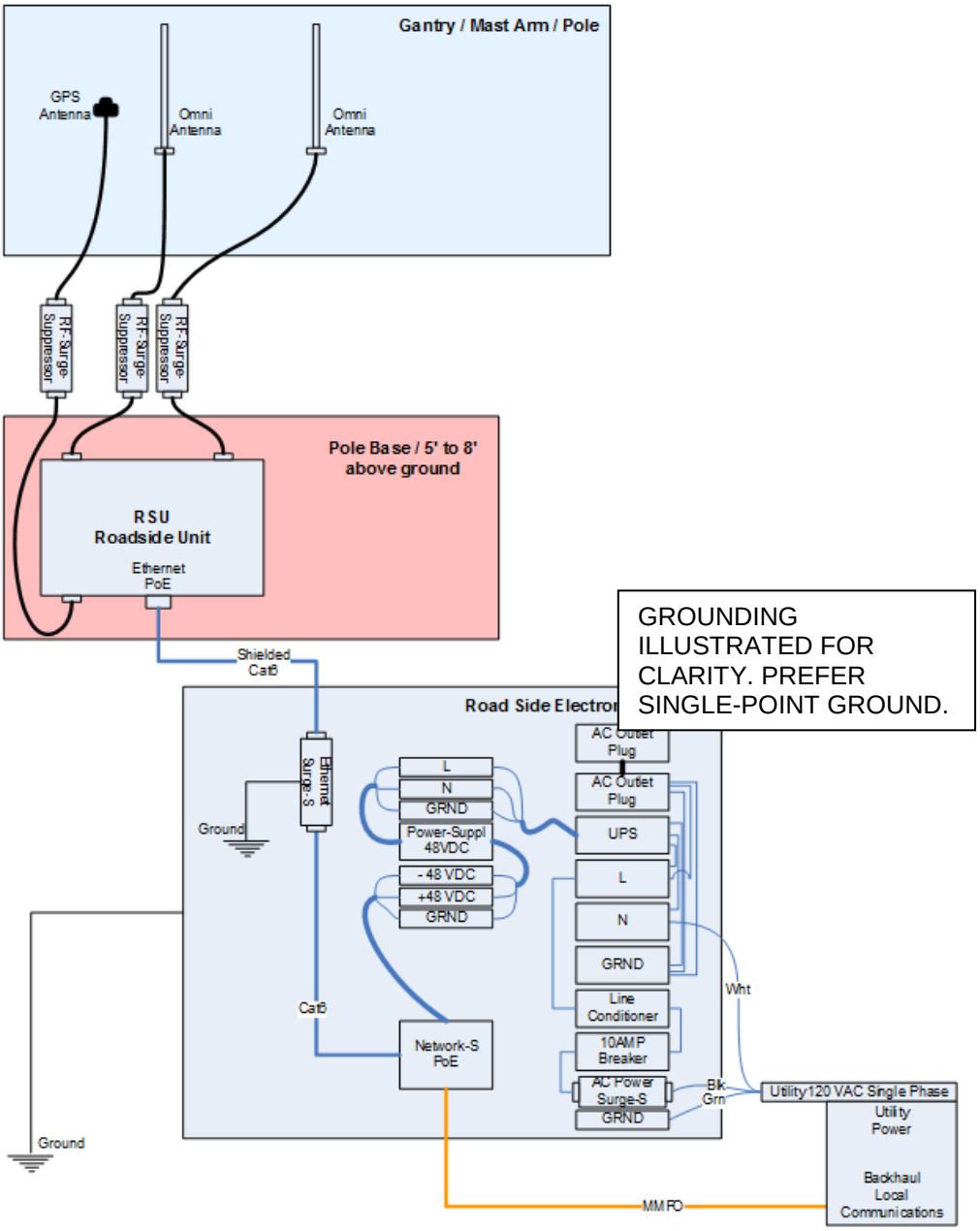

Figure 5. Configuration diagram of an RSU mounted on a roadside Pole Base, 5-8' off the ground.

3.3.1.2 The RSU shall be mounted directly on a traffic pole or mast arm or installed in an adjacent cabinet as shown in Figure 3Figure 5 to ensure reliable RF communication coverage and efficacy can be met.

3.3.1.3 Deployment locations that require the installation of multiple RSUs shall be referred to as an "RSU System," that function as a single unit and are connected to the supporting infrastructure through a single physical interface.

3.4 Basic Functionality

The Inputs and Outputs, Enablers and Controls, and Activities of an RSU are depicted in Figure 6.

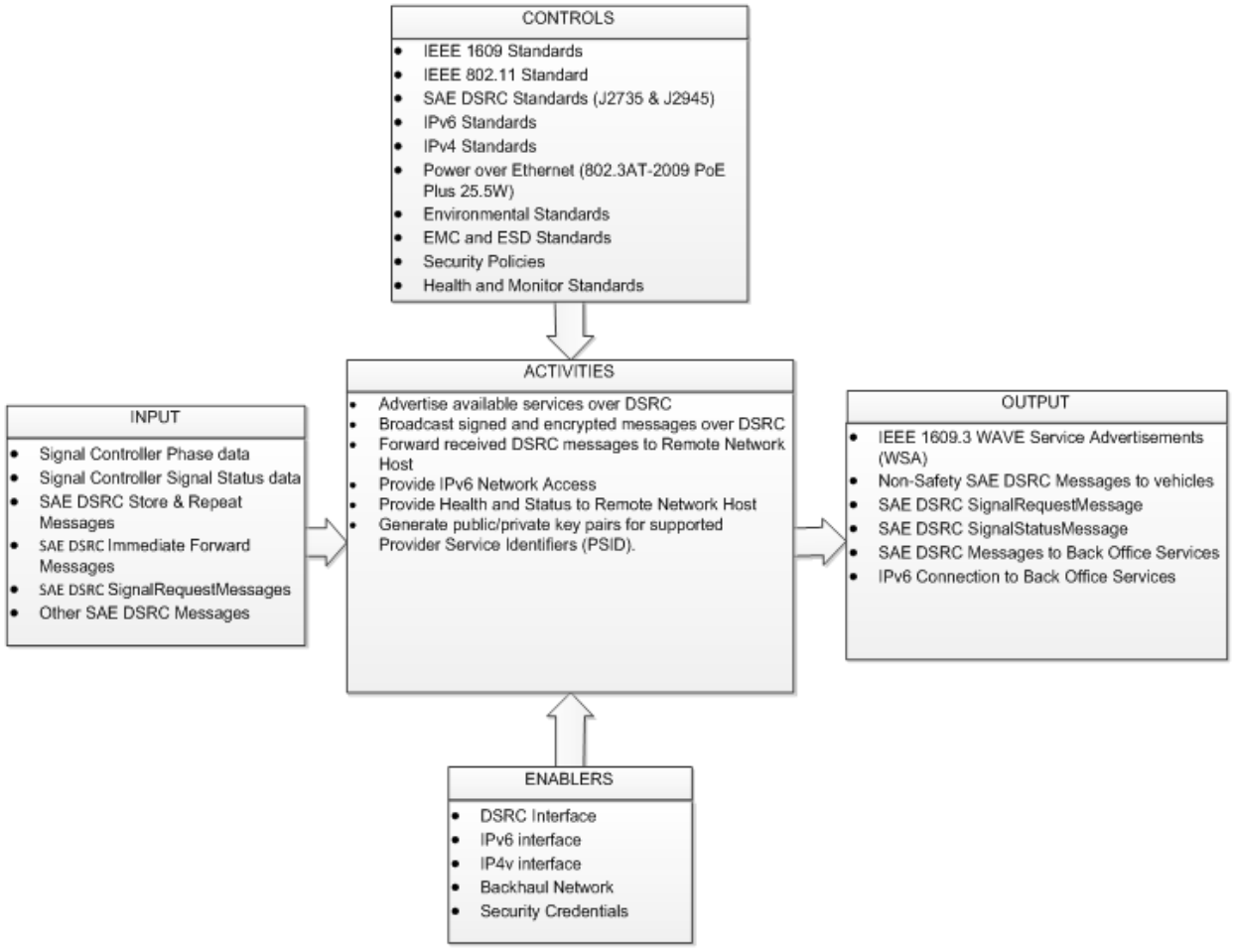

Figure 6. Context diagram of an RSU

3.4.1 IPv6 Access

3.4.1.1 The RSU shall provide DSRC-equipped mobile devices with access to Back Office services by way of IPv6.

3.4.1.2 The RSU shall provide DSRC-equipped mobile devices with access to Back Office services by way of IPv6. It shall support IPv6 tunneling on an IPv4 network (NYCWiN or other city-owned network); the vendor shall work with NYCDOT to identify the method and mechanisms to be used.

Note: This allows devices to take advantage of services such as the Situation Data Clearinghouse, Situation Data Warehouse, and Security Credential Management System (SCMS) as well as other public and private network services. In the case of the Situation Data Clearinghouse and Situation Data Warehouse, data related to traffic conditions (speed, volume, etc.) are sent from a vehicle over DSRC through an RSU to

the Situation Data Clearinghouse and Situation Data Warehouse utilizing the RSUs backhaul connection. In the case of the SCMS, a vehicle is able to request certificates through the RSU to the RA component of the SCMS.

3.4.1.3 However – all such services and/or access to all such services shall be governed by and managed by the CV back office support software located at the TMC in NYC. That is – all connections to any external network (outside NYCDOT) will be controlled by and managed by the NYC CV back office support software. At this point, it is not clear whether or under what circumstances the RSU may connect directly to any external service such as the SCMS, or the USDOT Situation Data Clearinghouse or Situation Data Warehouse.

3.4.2 Broadcast of Protocol Data Units (PDU)

3.4.2.1 The RSU broadcasts Protocol Data Units (PDU) (messages) formatted in accordance with SAE J2735 using either the Store and Repeat or the Immediate Forward mechanism.

3.4.2.2 Store and Repeat PDUs shall be downloaded from a back office service and stored on the RSU.

3.4.2.3 Broadcast Instructions are included with each PDU that defines how often the PDU should be broadcast, when the PDU should start being broadcast, when the PDU should stop being broadcast, the channel that should be used for the broadcast, the PSID the PDU is associated with, and whether the PDU should be signed and/or encrypted. These broadcast instructions shall be extracted from the stored message and written to the appropriate SNMPv3 OID. Once the PDU expires, it shall be removed from RSU storage and either the associated SNMPv3 OID should be set to indicate no broadcast, or a fresher version of the message should be broadcast.

3.4.2.4 The RSU broadcasts Immediate Forward PDUs as they are sent to the RSU. (Note: in addition, the RSU may create, sign, and transmit other messages (e.g. SPaT))

3.4.2.5 Broadcast instructions accompany PDUs, including the channel that should be used for the broadcast, the PSID the PDU is associated with, and whether the PDU should be signed and/or encrypted. These broadcast instructions should be extracted from the Immediate Forward message and written to the appropriate SNMPv3 OID. Once the Immediate Forward messages cease, the associated SNMPv3 OID should be set to indicate no broadcast.

3.4.2.6 The RSU shall obtain and manage digital certificates to sign messages that are indicated as to be signed.

3.4.2.7 For each type of message, the RSU shall offer the facility to be configured to sign or not sign it. For each message that is signed, the RSU shall offer the facility to be configured to attach the certificate once every t milliseconds or to every message, per the security profile for that message.

3.4.2.8 The RSU shall receive PDUs broadcast by a DSRC-equipped mobile device and forward them to a remote host.

3.4.2.9 PDUs are forwarded based on the PSID. The PSID of the PDU to be forwarded, the IP address and port number of the remote host, the transport protocol to use, the Receive

Signal Strength, the interval at which to forward, and the time period during which to forward are all configurable. The configurable parameters are stored in an appropriate SNMPv3 OID. This allows for capabilities such as traffic monitoring, health and status reporting, and certificate requests.

3.4.2.10 Under this contract, the RSU provider shall be required to develop the application level software which resides on the RSU for the purpose of collecting the BSM mobility data. ASD RF monitoring data, and collecting the data from all logs within the vehicle whenever it is so configured. As noted above, selected RSUs will be required to announce their ability to collect the data logged on the vehicles, and initiate uploading those log contents to the RSU and then forwarding them to the TMC.

3.4.2.11 The RSU shall also be responsible for managing and uploading software modifications to the ASDs within their range and for managing the parameter updates. The vendor shall work cooperatively with the City and the selected ASD vendor(s) to establish a reliable and secure protocol for managing such software and parameter updates for the ASDs.

3.4.3 General Software Requirements

3.4.3.1 The developer shall provide a distribution mechanism to the RSU and updates to the system based on the input from the City to meet the objectives of the NYC CVPD project.

3.4.3.2 The developer shall provide patches to remediate vulnerabilities in the RSU.

3.4.4 General Hardware Requirements

3.4.4.1 The RSU shall support Single Channel Continuous and dual Channel Alternating DSRC Channel Modes simultaneously

3.4.4.2 The RSU shall contain internal computer processing and permanent storage capability

3.4.4.3 The RSU shall contain an integrated high sensitivity GPS receiver for positioning and timing. The GPS receiver shall achieve lock when there is open sky above, even in the presence of urban canyons.

3.4.4.4 The RSU shall contain a Power-over-Ethernet capable interface that supports both IPv4 and IPv6 connectivity, and compliant with 802.3at

3.4.4.5 The RSU shall have a nominal operating voltage between 37 and 57 V DC, compliant with IEEE 802.3at.

3.4.4.6 The RSU shall support inbound power through a single, designated Ethernet port by Power-over-Ethernet (PoE) in compliance with IEEE 802.3at.

3.4.4.7 Any accompanying power injector shall be compliant with IEEE 802.3at.

3.4.4.8 The RSU shall have sufficient memory to support all of the following concurrently:

3.4.4.8.1 The RSU shall hold log data for 48 hours from a minimum of 25 ASDs before transmission to the TMC. This includes the event logs, mobility logs, RF propagation logs, RF sighting logs, and operation logs.

3.4.4.8.2 The RSU shall maintain a complete copy of all ASD software/firmware and parameters for immediate transmission to the ASDs when they are within range of the RSU

3.4.4.8.3 The RSU shall hold a 24 hour copy of the RF database captured by the RSU as described herein for the purpose of tracking RF operation.

3.4.4.8.4 The RSU shall hold a complete copy of all firmware and software and drivers used within the RSU such that new versions of each or all can be downloaded without affecting the immediate operation. It is expected that the RSU will verify all downloads of its software before committing it to operation.

3.4.4.9 Note that the RSU will be connected to a switched source of power. Thus, there may be intermittent power connections occurring at various rates at any time. The RSU shall always start, restart, or continue proper operation regardless of the repetition rate, time between interruptions, and time of occurrence whenever the power is within the defined operating voltages.

3.4.4.10 If the power applied is outside the nominal operating voltages, the unit shall be protected from damage including loss of memory, corruption of memory, electronic damage, and mechanical damage regardless of the duration of the power including transients and power interruptions of any type as described above.

3.4.5 Environmental and electrical

3.4.5.1 The RSU shall be designed to operate properly in the outdoor environment. (e.g. temperature, humidity, rain, fog, sun, snow, shock, vibration, TBD) {Ref augmented NEMA TS2-2003})

3.4.5.2 The RSU and all constituent equipment shall be designed to operate within the constraints of the environmental requirements described in this section. The term RSU shall be interpreted as meaning all constituent equipment provided by the contractor. This shall include the power injector, mounting brackets, connectors, cables, and surge protection equipment to be provided as part of the installation kit. Note that the existing traffic controller cabinets do not include a 48 VDC power supply which is necessary for the PoE inserter; hence, the requirements specified herein for the RSU shall apply to the 48 VDC supply to be provided as part of the installation kit.

3.4.5.3 The RSU shall function as intended within the temperature range of -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F) without adjustment.

3.4.5.4 The RSU shall function as intended under the rate of change in ambient temperature up to 17 degrees C (30 degrees F) per hour, throughout the required operational temperature range.

3.4.5.5 The RSU shall function as intended after storage at a temperature range of -45 degrees C (-50 degrees F) to +85 degrees C (+185 degrees F).

3.4.5.6 The RSU shall be capable of continuous operation under a relative humidity of 95% non-condensing over the temperature range of operate at a temperature range of +4.4 degrees C (+40.0 degrees F) to +43.3 degrees C (+110.0 degrees F).

3.4.5.7 The RSU shall be capable of continuous operation when moisture is caused to condense on the EQUIPMENT by allowing it to warm up to room temperature (from -40C) in an atmosphere having relative humidity of at least 40%.

3.4.5.8 The RSU shall pass the rain test with a rainfall rate of 1.7 mm/min (4in/hour), wind speed of 18 m/sec (40 mph) and 30 minutes on each surface of the device as called out in MIL-STD-810 G method 506.5 Procedure

3.4.5.9 The RSU shall pass the salt fog test with 5% saline exposure for 2 cycles x 48 hours (24 hours wet/24 hours dry) as called out in MIL-STD-810 G method 509.5.

3.4.5.10 The RSU mounting bracket shall be able to withstand winds up to 150 miles per hour per AASHTO Special Wind Regions Specification B19

3.4.5.11 The RSU shall comply with the United States Military Standard MIL-STD-810G.

3.4.5.12 The RSU shall pass environmental testing conducted in accordance with the procedures specified in IEC-60068 and IEC-60721.

3.4.5.13 The RSU shall comply with the United States Military Standard MIL-STD-810G, Test Method 514.6, Procedure I, Category 4. (Heavy truck profile) for packaging and shipping. (Note: this is intended to provide reasonable assurance that material can withstand transportation and handling including field installation, removal, and repair.)

3.4.5.14 The RSU shall be immune to radio frequency (RF)/Electromagnetic Interference (EMI) per SAE J1113.

3.4.5.15 The RSU shall be able to withstand electrostatic discharges from the air up to +/-15 kV and electrostatic discharges on contact up to +/-8 kV, in compliance with IEC EN61000-3-2.

3.4.6 Mechanical Requirements

3.4.6.1 The installation and removal of the RSU shall not damage the mounting location, e.g., traffic pole or mast arm.

3.4.6.2 The weight of the RSU, excluding antennas, mounting hardware and Power-over-Ethernet (PoE) Power Injector, shall NOT exceed fifteen (15) pounds

3.4.6.3 The RSU shall be contained in a dedicated NEMA 4X-rated enclosure.

3.4.6.4 The external Power-over-Ethernet (PoE) connector shall be compliant with the Outdoor IP66 rating.

3.4.6.5 The RSU shall support installation on a shelf, wall, or pole (horizontal or vertical).

3.4.6.6 The RSU shall include an LED to indicate the power status of the device in accordance with the following protocol:

- Off - No Power
- Solid Green - Device is powered on

3.4.6.7 The RSU shall include an LED to indicate the operational status of the device in accordance with the following protocol:

- Off - No Power
- Blinking Green - Device Start-Up
- Solid Green - Device Operational
- Amber - Firmware Update In Progress
- Red-Fault

3.4.6.8 The device shall provide tamper evidence to detect tampering of the device (e.g. opening of the case).

3.4.6.9 The device shall also report if there is evidence of tampering or if the device is opened including the date and time and location that the evidence became electrically visible. Note: this depends on the nature of the entry – and when the device is powered.

3.4.6.10 All unused media ports (e.g. USB) shall be sealed.

3.4.6.11 There shall be no removable media.

3.4.6.12 The RSU shall not subject a technician to any hazardous condition due to its operation while servicing.

3.4.7 Performance Characteristics

3.4.7.1 The RSU shall have a computed Mean Time Between Failure (MTBF) for an average of 100,000 hours.

3.4.7.2 The RSU shall meet the operational availability requirements of 99.9%. (Clarification: this does not include scheduled maintenance.)

3.4.7.3 The RSU shall receive DSRC messages throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions:

a. When receiving on an 802.11 Operating class 17 channel (even 10 MHz Service Channel, numbers 172 through 184).
b. When receiving Part 1 of the SAE J2735 defined Basic Safety Message (BSM)
c. With a BSM transmit rate of 10 Hz
d. With a Data Rate of 6 Mbps
e. With an RSU antenna centerline height of 8 meters
f. With a BSM transmit power of VRPMax, as defined in SAE J2945/1

3.4.7.4 The RSU shall transmit DSRC messages throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions

a. When transmitting on an 802.11Operating class 17 channel (even 10 MHz Service Channel, numbers 172 through 184).
b. When transmitting Wave Service Advertisements (WSA), as defined in IEEE 1609.3
c. With a WSA Transmission Rate of 10 Hz
d. With a Data Rate of 6 Mbps
e. With an RSU antenna centerline height of 8 meters
f. With a maximum WSA transmit EIRP
g. Using a Receiver conforming to SAE J2945/1 Section 6.4.2

3.4.7.5 If the RSU stops transmitting, for any reason it shall signal ‘device needs servicing’; the mechanism for such notification shall be developed jointly with the City.

3.4.7.6 The RSU shall include appropriate watchdog circuits and process control software such that program failure or device failures can be corrected with an automatic reset and reboot of the system without annoying the driver.

3.4.7.7 The RSU shall accept software updates over the backhaul to the TMC and shall be able to stop a specific application, load a new version of the application, and start the new application and have it automatically integrate into the normal operation of the RSU without rebooting the system.

3.4.7.8 Watchdog mechanisms shall include failsafe operation such that this process does not create false alerts, corruption of stored logs, erroneous log entries, damage to the existing firmware and operating parameters.

3.4.7.9 Each reboot shall be logged into the RSU operations log.

3.4.8 Performance Monitoring

3.4.8.1 The RF power level of all received messages shall be available as an attribute of the specific message and made available to the RF monitoring subsystem application operating on the RSU.

3.4.9 Adaptability

3.4.9.1 The NYC CVPD applications shall have modifiable algorithms and software parameters for tuning the system’s operation.

3.4.10 Software Installation

3.4.10.1 The RSU shall support installing and maintaining authorized software additions or modifications components by authorized entities over the Local Systems Interface (LSI).

3.4.10.2 It is expected that this port (Ethernet) will be used to load the fundamental RSU firmware, and even the initial versions of the applications. Thereafter, the software update mechanism shall be used for adding applications and for replacing/updating applications.

3.4.11 Software updates

3.4.11.1 The contractor is expected to deliver the initial prototypes with all software operational and ready for testing. However, it is recognized that during the initial deployment and testing as well as during the “silent” period during the ASD installation in the fleet vehicles, it may become necessary to update any and all firmware stored on the RSU.

3.4.11.2 The RSU software shall be designed such that it is possible to update any part or all of the RSU software from the TMC over the backhaul media without requiring operator intervention at the field device and without forcing a reboot unless necessary (new operating system or drivers). Note that the backhaul media supports only IPv4 and it is the responsibility of the RSU developed to work with the CV back office software developer to establish a mechanism to manage IPv6 communications to/from the ASDs over the IPv4 backhaul.

3.4.11.3 As noted above, the RSU shall include appropriate watchdog mechanisms that will monitor all software processes and alert the process monitor [on the RSU] when a process appears to be inoperative and initiate a message (TBD) to the TMC indicating this condition. When noted, the operating platform shall be able to reload and restart the failed process and shall make an entry in the operations log indicating that this action took place. Such actions shall include managed hysteresis that will avoid continuous retries for a failed process until it receives and update. In this case, the RSU shall include a notification in its status log that this has occurred.

3.4.11.4 This restart process shall be designed such that it does not cause the transmission of erroneous data (SPaT/MAP/RTCM, etc.), cause erroneous or corruption of any of the onboard logs, or erroneous alerts or alarms to the driver.

3.4.11.5 Once the RSU has been installed and verified as operational, it shall not be necessary to physically “touch” the unit again unless there is a hardware failure or required hardware/electrical repair/update. All updates of applications, operating systems, data collection software, etc. shall take place using a dialog with the TMC over the backhaul media.

3.4.11.6 All OTA updates shall use the same protocol for interoperability. While the firmware and/or parameters may be different, the fundamental mechanism for loading new applications and for updating applications and application parameters (including logging all event, RF, and operations parameters) shall be interoperable between vendors.

3.4.11.7 As noted above, it shall be possible to update and add individual applications to the RSU. In all cases, the RSU shall verify that the software update has been received properly (and signed) and is uncorrupted. It shall then stop the existing process that is being replaced, and start the new process.

3.4.11.8 The RSU supplier shall cooperate with the ASD supplier to develop the dialogs and messages for the updating and management of both applications and processes on the ASD as described in that procurement specification.

3.4.11.9 The RSU design shall enforce that all software updates of any type are signed.

3.4.12 Informative comments

3.4.12.1 The RSU shall sign SPaT messages.

3.4.12.2 Encrypted log data will be transmitted in encrypted form “through” the RSU for use by the TMC where it will be decrypted; in the case, the RSU is acting as a store and forward data handler to compensate for the differences in the capabilities of the backhaul and the DSRC.

3.4.12.3 Messages such as the MAP, BIM, TIM, and RTCM will be signed at their source or the TMC and passed to the RSU which will broadcast them to mobile devices.

3.4.12.4 The RSU shall collect (through an internal application) its RF data as described herein and for the development of the mobility data using the BSM messages – hence, the RSU is expected to be able to authenticate all messages it receives.

3.4.12.5 The RSU for NYC should consider the use of a hardware accelerator for cryptographic verification since it is anticipated that it could “see” well over 600 messages per second due to the density of the vehicles and the proximity of other RSUs.

3.4.12.6 The RSU vendor shall work closely with the City and its consultants during the design phase to insure interoperability with the ASDs, and adoption of the new and emerging standards that are essential for the support of the NYC applications.

4 Functional and Behavioral Requirements

4.1 Functional Requirements

4.1.1.1 All device configurations in the RSU shall use SNMPv3 protocol.

4.1.1.2 At installation locations that require multiple RSUs to provide the required DSRC coverage, all RSUs shall be configured to operate as a single functional unit.

4.1.1.3 One (1) RSU in the RSU Set shall be configured as the Set "Master" as the basis for the configuration of the other RSUs in the Set.

4.1.1.4 All non-Master RSUs in the RSU Set shall be automatically configured based on the configuration of the Set "Master" RSU.

4.1.1.5 The connections between all RSUs in an RSU “Set” shall be protected with at least 128 bits of cryptographic security. This requirements document does not put any additional design requirements on the security of those connections, but it is expected that the detailed specification for this communications security mechanism shall be made available for review by the CITY.

4.1.1.6 If the RSU Set has a backhaul connection, all data between the Back Office and the RSU Set shall route through a single device connecting the RSU Set Master to the other RSUs in the backhaul.

4.1.1.7 The RSU shall forward messages received on any DSRC interface, containing a specified PSID, to a specified network host, as configured in SNMPv3 MIB OID 1.0.15628.4.1.7 (See section 9).

4.1.1.8 The Message Forwarding SNMPv3 MIB Object contains the following information:

a. PSID
b. Dest_IP Address
c. Dest_Port
d. TransPort_Protocol
e. RSSL
f. MsgForwardInterval (RSU forwards every nth message received)
g. DeliveryStart
h. DeliveryStop
i. Payload

4.1.1.9 The RSU shall send the GPGGA NMEA String to a specified UDP port at a specified rate, upon acquisition of 3 or more Satellites, as configured in SNMPv3 MIB OID 1.0.15628.4.1.8 (See Appendix A), which contains the following data:

a. Destination IP Address
b. Port (default is 5115)-sample rate (default is once a second, with a valid range of 1-18000 seconds, in increments of 1 second)

4.1.1.10 The RSU shall maintain a system clock based on timing information from a local positioning system. (Note: GPS is intended to serve as the primary time source and

the NTP server is intended to be available as a secondary, backup time source in the event that the RSU loses GPS.)

4.1.1.11 The RSU shall conform to the Universal Time, Coordinated (UTC) standard for the system time standard.

4.1.1.12 The RSU shall indicate to an authorized user if an internal clock drift (skew rate) has exceeded a configurable tolerance.

4.1.1.13 The RSU shall indicate to an authorized user the loss of a time source if the time source input has been lost for a configurable period of time or has failed after a configurable number of query attempts (note: the time source itself shall also be indicated).

4.1.1.14 The RSU shall notify a remote host via SNMPv3 the following:

a. If a time source has been lost for a configurable period of time
b. If the value of a clock source deviates beyond a predefined skew rate
c. If the deviation between two or more time sources exceeds a predefined threshold

4.2 Positioning

4.2.1 Location Correction Mechanism

4.2.1.1 The RSU shall utilize a local subsystem to determine its position on the surface of the earth using a default sample rate of 1 Hz

4.2.1.2 The RSU shall write a CRITICAL entry to the System Log if it is not able to acquire a minimum of 3 Satellites within 20 seconds after entering the "Operate" state

4.2.1.3 The RSU shall utilize WAAS corrections, when available and broadcast the RTCM message.

4.2.1.4 The RSU shall store a reference set of GPS coordinates for itself

4.2.1.5 The RSU should evaluate GPS sub-frame data to indicate the legitimacy of the GPS data frame source and indicate to an authorized user suspicious GPS data.

4.2.1.6 The RSU shall notify a remote host via SNMPv3:

a. if its GPS position deviates from the stored reference by more than a configurable radius
b. if a suspicious GPS signal is detected
c. of its current NMEA GPGGA string at a configurable interval

4.2.2 Access Control

4.2.2.1 The RSU shall enforce clear associations between roles, services and the distinct authentication and authorizations required to access those services.

4.2.2.2 Access to sensitive services shall require an authenticated, authorized role.

4.2.2.3 Access to sensitive data shall require an authenticated, authorized role.

4.2.3 Authentication

4.2.3.1 The RSU shall be configurable to limit the number of repeated authentication attempts for services requiring authentication.

~~4.2.3.2 The RSU shall utilize certificate pinning to secure all TLS sessions with the SCMS Device Configuration Manager and other SCMS nodes to which it connects.~~

~~4.2.3.3 The RSU shall terminate a TLS session if the server public key certificate is not identical to the stored public key certificate.~~

4.2.3.4 The RSU shall terminate a TLS session if the server public key certificate signature verification fails during TLS session establishment.

4.2.3.5 The RSU shall re-authenticate authorized users when transitioning from "Standby" State.

4.2.3.6 The RSU should verify the IEEE 1609.2 digital signature on all messages previously signed by the TMC or other backhaul services prior to forwarding over the DSRC interface.

4.2.3.7 Services requiring role-based authentication shall meet the authentication requirements of FIPS 140-2, Section 4.3 Level 2 and any supporting FIPS 140-2 implementation guidance.

4.2.3.8 Services requiring authentication shall meet the single attempt and multiple attempt authentication strength requirements of FIPS 140-2, Section 4.3.

4.2.3.9 The RSU shall require SSH Version 2 or TLS Version 1.2 using mutual (two way) public key credential authentication for all authorized user sessions.

4.2.3.10 The RSU shall require HTTPS using mutual (two way) public key credential authentication for all HTTPS connections to the RSU.

4.2.3.11 All HTTPS administrative and data sessions to the RSU shall utilize TLS Version 1.2

4.2.3.12 The RSU shall be able to be configured whether to transmit application-specific messages signed with expired IEEE 1609.2 certificates.

4.2.4 Configuration

4.2.4.1 The RSU shall be configurable regarding the maximum frequency (number per second) or ratio (percentage) of DSRC message digital signatures to verify based on PSID.

4.2.4.2 The RSU shall be able to be configured whether to accept, drop, or respond to application-specific messages signed with expired certificates.

4.3 System Log Files

4.3.1 Typical Log files

4.3.1.1 The RSU shall generate system log file entries at the appropriate priority level depending on the system event.

4.3.1.2 Typical Linux operating system log files shall contain the following priority levels:

- EMERGENCY (Level 1) – The application has completely crashed and is no longer functioning. Normally, this shall generate a message on the console as well as all root terminals. This is the most serious error possible. This should not normally be used for applications outside of the system level (file systems, kernel, etc.). This usually means the entire system has crashed.
- ALERT (Level 2) – The application is unstable and a crash is imminent. This shall generate a message on the console and on root terminals. This should not normally be used for applications outside of the system level (file systems, kernel, etc.).
- CRITICAL (Level 3) – A serious error occurred during application execution. Someone (systems administrators and/or developers) should be notified and should take action to correct the issue.
- ERROR (Level 4) – An error occurred that should be logged, however it is not critical. The error may be transient by nature, but it should be logged to help debug future problems via error message trending. For example, if a connection to a remote server failed, but it shall be retried automatically and is fairly self-healing, it is not critical. But if it fails every night at 2AM, you can look through the logs to find the trend.
- WARNING (Level 5) – The application encountered a situation that it was not expecting, but it can continue. The application should log the unexpected condition and continue on.
- NOTICE (Level 6) – The application has detected a situation that it was aware of, it can continue, but the condition is possibly incorrect.
- INFO (Level 7) – For completely informational purposes, the application is simply logging what it is doing. This is useful when trying to find out where an error message is occurring during code execution.
- DEBUG (Level 8) – Detailed error messages describing the exact state of internal variables that may be helpful when debugging problems.

4.3.2 System Log File (Syslog)

4.3.2.1 The RSU shall log system events to a standard operating system Log (Syslog) File.

4.3.2.2 The Priority Level of events that are recorded in the RSU System Log file shall consist of all priorities available for the operating system

4.3.2.3 The RSU shall write an entry in the System Log file for INFO events and above, by default

4.3.2.4 The Priority Level of events that are recorded in the RSU System Log file shall be configurable by authorized users

4.3.2.5 The RSU shall close open System Log files once per week at a configurable time

4.3.2.6 Upon closing a System Log file, the RSU shall open a new System Log file.

4.3.2.7 At a configurable time and age, the RSU shall delete old system log files.

4.3.2.8 The RSU shall allow authorized users to view System Log Files stored in the System Log File directory on the device through an Ethernet interface.

4.3.2.9 The RSU shall write a WARNING entry to the System Log File when a non-DSRC network host connection changes state. The entry shall contain the following data:

a. Date and Time
b. Interface
c. New State (connected, not connected)

4.3.3 Interface Log Files

4.3.3.1 The RSU shall provide operators the ability to capture packets transmitted and received on any enabled communication interface for troubleshooting purposes. (Note: interface logs are not intended for long term data capturing.)

4.3.3.2 The RSU shall have the ability to log all transmitted and received packets across all enabled communication interfaces, while in the "Operate" State.

4.3.3.3 All Interface Log File configurations contained in SNMPv3 MIB OID 1.0.15628.4.1.9 (See Appendix A) shall have the following default values:

a. Generate = off
b. Max file size = 20 MB
c. Max Collection Time = 24 hr

4.3.3.4 An Interface Log File shall be generated for a RSU communication interface upon setting the “generate” flag in SNMPv3 MIB OID 1.0.15628.4.1.9 (See Appendix A) for that interface to "on". (Note: when set to "on" both transmitted and received packets are logged.)

4.3.3.5 An Interface Log File shall stop being generated for a RSU communication interface upon setting the “generate” flag in SNMPv3 MIB OID 1.0.15628.4.1.9 (See Appendix A) for that interface to "off".

4.3.3.6 A separate and independent Interface log file shall be generated for each direction (transmit and receive) of a RSU communication interface when the SNMPv3 MIB OIB 1.0.15628.4.1.9 (See Appendix A) for that interface is set to "on".

4.3.3.7 Interface Log File format: Each Interface Log File shall be generated in the industry standard packet capture (pcap) format and contain the following data:

a. Date and Time (in UTC, when the packet was logged)
b. RSSI (for Packets Received over DSRC)
c. TxPower (for Packets Transmitted over DSRC)
d. packet (complete transmitted or received packet)

4.3.3.8 The RSU shall close an active Interface Log File upon reaching the configured "Max file size" in SNMPv3 MIB OID 1.0.15628.4.1.9 (See Appendix A).

4.3.3.9 The RSU shall close all active Interface Log Files when transitioning to "standby" state.

4.3.3.10 The RSU shall close an active Interface Log File upon reaching the configured "Max collection time" in SNMPv3 MIB OID 1.0.15628.4.1.9 (See Appendix A).

4.3.3.11 The RSU shall generate a new Interface Log File upon closing a previously active Interface Log File when the configured "Max file size" in SNMPv3 MIB OID 1.0.15628.4.1.9 (See Appendix A) is reached.

4.3.3.12 Each RSU Interface Log File shall be named according to the following convention:

a. RSU ID (MIB OID 1.0.15628.4.1.17)
b. Interface ID
c. Transmit or Receive

d. Data and Time (UTC date and time when the file was created)

4.3.3.13 The RSU shall allow authorized users to view Interface Log Files stored in the Interface Log File directory on the device through an Ethernet interface.

4.3.4 Store and Repeat-Encoded Payload

4.3.4.1 The RSU shall broadcast DSRC messages based on Active Message text files loaded on the device. (Clarification: Store and Repeat is equivalent to Active Message.)

4.3.4.2 Each text file shall contain the broadcast instructions and encoded payload for one (1) DSRC message and include the following data elements:

a. Message Type/Description
b. Message PSID
c. Message Priority
d. Transmission Channel Mode
e. Transmission Channel
f. Transmission Broadcast Interval
g. Message Delivery (broadcast) start time
h. Message Delivery (broadcast) stop time
i. Signature
j. Encryption
k. Configuration Storage
l. Payload (including security fields)

4.3.4.3 The RSU shall begin broadcasting the payload of an Active Message text file over a DSRC interface, based on the broadcast instructions contained in the Active Message text file, on or after the start time specified in the broadcast instructions of the Active Message text file for each Active Message text file stored on the unit. (Note: see Appendix B containing the message format.)

4.3.4.4 The RSU shall stop broadcasting the payload of an Active Message text file as a DSRC message at end time specified in the broadcast instructions of the Active Message text file for each Active Message text file stored on the unit.

4.3.4.5 The RSU shall have the capability to store at least 100 Active Message text files in an Active Message directory.

4.3.4.6 The RSU shall allow authorized users to add/remove Active Message text files to/from the Active Message directory through SNMPv3 OID 1.0.15628.4.4.x.

4.3.4.7 The RSU shall allow authorized users to remove Messages from the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.

4.3.4.8 The RSU shall allow authorized users to view the contents of Active Messages in the Active Message directory through SNMPv3 1.0.15628.4.1.4.

4.3.4.9 The RSU shall allow authorized users to modify an Active Message through SNMPv3 1.0.15628.4.1.4.

4.3.4.10 The RSU shall write an INFO entry to the System Log File for each authorized access to an Active Message text file containing the following data:

a. Date and Time
b. File Name (name of Active Message text file as stored in the Active Message directory)
c. Successful operation (installation, removal, or modification)
d. User ID

4.3.4.11 The RSU shall write a WARNING entry to the System Log File for each failed access attempt to an Active Message text file containing the following data:

a. Date and Time
b. File Name (name of Active Message text file as stored in the Active Message directory)
c. Failed operation (install, remove, modify)
d. User ID

4.3.4.12 The RSU shall write a NOTICE entry to the System Log File when an Active Message changes broadcast status resulting from a user initiated device shut down, device boot up, message start time or message end time. Each entry shall contain the following data:

a. Date and Time
b. File Name (name of the Active Message text file as stored in the Active Message directory)
c. Broadcast Status (Start/Stop)

4.3.5 Store and Repeat-Raw Data Payload

4.3.5.1 The RSU shall broadcast DSRC messages based on configuration text files containing raw, un-encoded data, loaded on the device. Each text file shall contain the broadcast instructions and human readable data elements for 1 DSRC message and include the following data elements:

a. Message Type/Description
b. Message PSID
c. Message Priority
d. Transmission Channel Mode
e. Transmission Channel
f. Transmission Broadcast Interval
g. Message Delivery (broadcast) start time
h. Message Delivery (broadcast) stop time
i. Signature (security configuration information per the 1609.2 security profile)
j. Encryption
k. <list of raw data elements>

4.3.5.2 The RSU MAY store raw data text files for encoding into messages to be broadcast over a DSRC interface.

4.3.5.3 This is similar to the Store & Repeat-Encoded Payload functionality described with the exception that the file stored on the RSU would contain raw, un-encoded, data to be encoded prior to being broadcast over DSRC. For Example a human readable/configurable Map configuration file.

4.3.5.4 The RSU MAY encode raw data contained in a text file residing on the RSU into messages to be broadcast over a DSRC interface.

4.3.5.5 This is similar to the Store & Repeat-Encoded Payload functionality described with the exception that the RSU would encode the raw data contained in the stored file into a DSRC Payload of the appropriate format prior to broadcasting over DSRC. For Example a human readable/configurable Map configuration file.

4.3.6 Immediate Forward-Encoded Payload

4.3.6.1 The RSU shall broadcast DSRC messages based on information received from a network host.

4.3.6.2 Each Immediate Forward (IF) message received from a network host shall contain the broadcast instructions and payload for one (1) DSRC message and include the following data elements. (Note: Appendix B contains the format of the Immediate Forward Message.)

a. Message Type/Description
b. Message PSID
c. Message Priority
d. Transmission Channel Mode
e. Transmission Channel
f. Transmission Broadcast Interval (set to Null)
g. Message Delivery (broadcast) start time (set to Null)
h. Message Delivery (broadcast) stop time (set to Null)
i. Signature
j. Encryption
k. Payload

4.3.6.3 The RSU shall accept raw data over a non-DSRC Interface for encoding into messages to be broadcast over a DSRC interface.

4.3.6.4 The RSU shall receive raw, un-encoded, data from a network host that shall be encoded prior to being broadcast over DSRC. For example, raw SPaT data from a Signal Controller.

4.3.6.5 The RSU shall encode raw data received on a non-DSRC interface into messages to be broadcast over a DSRC interface.

4.3.6.5.1 The RSU shall encode the raw data into a DSRC Payload of the appropriate format prior to broadcasting over DSRC. For example, raw SPaT data from a Signal Controller.

4.4 System Security

4.4.1 Security Management and Operations

4.4.1.1 The Security Management and Operations Concept describes how the NYC CVPD shall be employing the SCMS for the applications and the applicable physical security requirements. The project shall use [interface to] the SCMS to obtain enrollment certificates for each RSU and each ASD.

4.4.1.2 As of this writing, there are no established certification requirements and test procedures for the use of the SCMS and for the installation of the enrollment certificate in the devices (RSU, ASD). Therefore, the Vendor shall certify that their devices conform to the applicable standards for the DSRC communications (IEEE 1609.x, and IEEE 802.11p) and that their message sets conform to the SAE J2735 and J2945/x for the BSM, SPaT, MAP, and location correction. Since these standards are still in development, the NYC CVPD shall require that the RSU and ASD conform to the standards as adopted by 12/31/2016.

4.4.1.3 The RSU shall support application certificates with different geographic validity region than the associated enrollment certificate.

4.4.1.4 The RSU shall support setting the certificate geographic region to be requested for application certificates.

4.4.1.5 The system administrators shall configure the RSU to request application certificates with only designated geographic locations.

4.4.1.6 The RSU supplier shall provide the serial number and its enrollment certificate for each RSU.

4.4.1.7 The system administrator shall request new certificates bound to the new location if the RSU moves from one location to another.

4.4.1.7.1 The RSU interface shall allow requesting a new RSU application certificate with a particular site.)

4.4.1.8 The RSU-SCMS interface shall allow the a new request application certificates with different contents from the current ones during the lifetime of the current ones.

4.4.1.9 The RSU shall delete old certificates upon location change.

4.4.1.10 The RSU shall request certificates for supporting roadside alert (RSA) if the NYC CVPD aims to support RSA in addition to SPaT and MAP messages.

4.4.1.10.1 The NYCDOT's existing policies and processes shall provide logical access to the installed RSU.

4.4.1.11 Note: if a device misbehaves, the SCMS shall blacklist the device and its enrollment certificates and prevent it from obtaining more authorization certificates.

4.4.1.12 The ASD shall obtain certificates via IPv6 connectivity through the RSU.

4.4.1.13 The RSU shall broadcast the WSA for certificate download on control channel 178 and indicate IPv6 connectivity and the IP address on a service channel other than channel 172 or 178.

4.4.1.14 The RSU shall implement a firewall blocking all IP access from devices to any IP address other than those approved for specific applications.

4.4.1.15 The RSUs shall support IPv6 tunneling over IPv4.

4.4.1.16 Communication between the RSU and the SCMS shall operate in an encrypted, end-to-end connection in accordance with the published SCMS interface.

4.4.1.16.1 The SCMS interface should not need any further security.)

4.4.1.17 The RSU shall report over a management interface if channel busy ratios go above a configurable threshold.

4.4.1.18 The RSU shall operate client-side transport layer security (TLS) and accept only TLS server certificates with specific URLs.

4.4.1.19 The RSU shall protect root certificates for client-side TLS against modification and provide other certificates in the chain, which shall not make a separate query to the internet to obtain the entire chain.

4.4.1.20 The RSU shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS.

4.4.1.21 The RSU shall support establishment of a standard TLS-based VPN with client authentication for communication to the TMC, with a long-term client cert and a single CA cert trusted to authorize connections from the TMC.

4.4.1.22 The RSU shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application.

4.4.1.23 The RSU shall store RF Monitoring log file entries encrypted with an encryption key belonging to the TMC.

4.4.1.24 The host processor on the RSU shall perform and pass integrity checks as specified in the following:

4.4.1.24.1 The integrity checks performed at boot shall use a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified.

4.4.1.24.2 Until all integrity checks on the software and firmware configuration of the host have passed, the device shall not allow a privileged application to sign a message.

4.4.1.24.3 If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any application to have access to stored private keys.

4.4.1.24.4 If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any privileged application to operate.

4.4.1.25 The OS on the RSU shall maintain an Access Control List (ACL) for which applications on the host may use each private key in the hardware security module (HSM).

4.4.1.26 The OS on the RSU shall not permit keys designated as private to be read from the HSM.

4.4.1.27 The validation of signed software shall require use of a verification key that is protected by local hardware to a level equivalent to FIPS 140-2 at the level appropriate for the device.

4.4.1.28 All cryptographic software and firmware for the HSM shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification.

4.4.1.29 The HSM 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.

4.4.1.30 The HSM operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

4.4.1.31 The certificate management service shall start requesting a new certificate or batch of pseudonym certificates a day before the expiry of the current certificate or batch.

4.4.1.32 When verifying, the device shall require that 1609.2 signed messages are signed by a certificate that is protected from modification by, or chains back to a certificate that is protected from modification by, the secure boot process.

4.4.1.33 The RSU shall not create or transmit messages for any usage scenario if the usage scenario requires it to use 1609.2 certificates and it does not currently have valid certificates for that usage scenario

4.4.1.34 The RSU shall verify a DSRC message when any of the following conditions is met:

a. A device identifies the message as containing a new DE_TemporaryID value.
b. The message results in the issuance of issue either advisory, warning, or alert.
c. Other potential threat situations such as infrastructure size restrictions, speed compliance, red light violations, and other safety applications.
d. Other situations as identified during the Phase 2 Design. Verification consists of meeting the IEEE 1609.2 requirements specified herein this document and the associated message's Security Profile (to be provided in Phase 2).

4.4.1.35 The RSU shall support a secure session protocol through VPN over TLS to the TMC for protecting the firmware download.

4.4.1.36 The RSU shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted.

4.4.2 Physical Security

4.4.2.1 The RSU shall be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 2 Physical Security Requirements.

4.4.2.2 The RSU should be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 3 Physical Security Requirements that require a tamper response mechanism, such as sending off an indicator to the backhaul network.

4.4.2.3 Communication between the RSU and the SCMS shall operate in an encrypted, end-to-end connection in accordance with the published SCMS interface. (Note: The SCMS interface should not need any further security.)

4.4.3 Authentication

4.4.3.1 The RSU shall be protected by a password compliant with either local operator security policies or a policy based on existing standards (e.g., FIPS 140- Level 3 and 4 in Section 4.3.3).

4.4.3.2 The RSU shall support multiple SNMPv3 users each with an individual password.

4.4.3.3 The RSU should support multi-factor authentication. (Bidders shall indicate if their proposed RSU provides this type of authentication.)

4.4.3.4 The RSU should enforce multi-factor authentication on all SSH Version 2 sessions and all TLS sessions to the RSU. (Bidders shall indicate if their proposed RSU provides this type of authentication.)

4.4.3.5 The RSU shall support password recovery for the RSU User Accounts that cannot be violated by physical access alone.

4.4.3.6 If the RSU synchronizes it's system clock to a Network Time Protocol (NTP) service, the device shall authenticate messages received from the NTP service

4.4.4 Configuration

4.4.4.1 The RSU configuration files shall enforce digital signatures to prevent unauthorized modifications.

4.4.4.2 Network protocol Secure Shell version 2 (SSHv2) should be configured as follows (Bidders shall indicate if their proposed RSU provides this type of authentication.):

a. Root Login Disable root
b. Use certificate-based authentication,
c. Rate-limited (to slow down brute-force attempts)
d. Use FIPS 140-2-compliant cryptography

4.4.5 Access Control

4.4.5.1 The RSU shall restrict remote network access based on an IP Address Access Control List (ACL)

4.4.5.2 If so equipped, Web-Based access to the RSU shall only be through Hypertext Transfer Protocol Secure (HTTPS)

4.4.5.3 The RSU shall only be accessible through the following network protocols:

a. Secure Shell Version 2 (SSHv2)
b. SNMPv3
c. SCP

4.4.6 Interfaces

4.4.6.1 The RSU can only be accessed from the IP Addresses contain in the ACL.

4.4.6.2 Each RSU Ethernet interface shall be protected by a configurable firewall with a default to be closed.

4.4.6.3 The RSU should support NAT64 protocol

4.4.6.4 The RSU shall utilize TLS versions and cipher suites consistent with SCMS interface specifications.

4.4.6.5 Services and protocols shall be able to be inhibited according to physical interface, source/destination IP address and source/destination ports

4.4.7 Data Protection

4.4.7.1 The RSU local file system shall be encrypted;

4.4.7.2 The RSU shall synchronize its system clock to a Network Time Protocol (NTP) Service in the event that it loses GPS fix.

4.4.7.3 The RSU shall immediately apply integrity protections to the store-and-repeat message data following SNMP-secured download to the RSU.

4.4.7.4 All secret and private keys received shall be encrypted, integrity-protected, and authenticated using a FIPS 140-2 Approved cryptographic key transport mechanism.

4.4.7.5 All sensitive RSU system files and application files shall be digitally signed using a digital signature algorithm listed in FIPS 186-4.

4.4.7.6 The RSU shall successfully verify the digital signature on all sensitive RSU system and application files prior to exposing any services.

4.4.7.7 The RSU shall implement a secure mechanism in software to securely store and provide strict access controls to all sensitive security parameters, including:

a. TLS public and private keys (as used for HTTPS or other TLS tunneling, including with the SCMS)
b. SSH public and private keys
c. Passwords
d. SNMP keys and passphrases
e. Any sensitive security parameters not stored in a hardware secure storage mechanism

4.4.7.8 The RSU software secure storage shall perform the following for its data protection:

a. Prevent read-access to all stored security parameters
b. Maintain integrity of all security parameters, including associations of keys with entities and processes
c. Check the integrity of stored security parameters when accessing
d. Prevent unauthorized modification of security parameters, except by authorized users
e. Prevent unauthorized addition of security parameters, except by authorized users
f. Prevent unauthorized substitution of security parameters, except by authorized users
g. Encrypt all sensitive security parameters when not in use

4.4.7.9 The RSU shall store passwords in secure storage only after modifying via a one-way cryptographic function.

4.4.7.10 The RSU shall zero-ize all non-factory installed parameters, cryptographic keys, applications, data and configurations when undergoing a factory reset.

4.4.7.11 Upon sudden loss of external power, the RSU shall undergo a shutdown procedure that preserves file system integrity.

4.4.8 Notifications

4.4.8.1 The RSU shall indicate the following to authorized users:

a. Store-and-Repeat message integrity failures
b. Any expired IEEE 1609.2 public key credentials it has stored
c. Any expired X.509 public key credentials it has stored
d. Pending expirations of all public key credentials to a configurable warning time value

4.4.8.2 The RSU shall notify a remote host via SNMPv3:

a. If an Active Message fails an Integrity check
b. If a configurable number of consecutive authentication attempts have failed
c. If the signature of a signed DSRC message has failed verification
d. Of any access control errors and rejections

4.4.8.3 If secure storage is available, the RSU shall notify a remote host via SNMPv3 if the secure parameters stored in secure storage have failed an Integrity check.

4.4.8.4 If FIPS 140-2 level 3 is implemented, the RSU shall notify a remote host via SNMPv3 if the enclosure has been tampered with according to FIPS 140-2 Section 4.5 Level 3 tamper indication requirements.

4.4.9 Logging

4.4.9.1 The RSU shall log the following:

a. GPS location and time data on a configurable interval
b. metrics on packet integrity or transmission/reception errors
c. all authentication parameter modifications
d. authentication failures and successes, including exceeding the limit on number of failed attempts
e. attempts to perform a service allocated to a role(s) for which the entity is not authenticated
f. authorization failures when a role or identity attempts access services and data requiring authorization
g. input and output protocol violations, including encoding errors and invalid parameters
h. session management failures in each of the session-based network protocols it supports
i. time errors, including loss of time source(s), re-acquisition of time source(s), unexpected time changes, and time mismatches (between sources) that exceed a configurable threshold
j. application errors and system events
k. GPS location changes that exceed a configurable value

l. all application errors
m. modifications to store-and-forward messages, including all parameters that impact the timing of the messages
n. signature verification failures on received DSRC messages
o. TLS session errors
p. all additions, modifications and removal of secret, public and private cryptographic keys

4.4.9.2 The RSU shall log and indicate to an authorized user success or failure of digitally signing all sensitive RSU system and application files using a digital signature algorithm listed in FIPS 186-4.

4.4.10 Information Management

4.4.10.1 As noted above, the log data from the ASD will be encrypted on the ASD and passed through the RSU as a store and forward messaging task. The data will not be decrypted at the RSU.

4.4.10.2 Some of the data such as ASD application configuration, ASD process management and ASD software updates will be signed at the source, and held on the RSU for transmission to the ASD at the appropriate opportunity.

4.4.10.3 Some of the data will be collected on the RSU – which need not be encrypted but is transmitted to the TMC on request such as the RSU logs and configuration.

4.4.10.4 It is not clear if the firmware and parameter updates need to be encrypted at this time.

4.4.10.5 Note that the security keys for the ASD logged data will be different for each vehicle fleet. This is to ensure that in the event that an ASD is compromised, only the fleet owner has the key necessary to unlock the data. Such keys need to be changed periodically.

4.4.11 System Maintainability

4.4.11.1 Note: The TMC staff shall be able to monitor the NYC CVPD system-wide RSU malfunctions.

4.4.11.2 Note: The Parameter Control functional entity shall meet the highest security requirements for a device of the appropriate class. (Note: this shall be derived via the Confidentiality/Integrity/Availability (CIA) analysis once the application specification is developed in detail.)

4.4.11.3 Note: The Parameter Control functional entity shall update the parameter control message signatures daily.

4.4.11.4 All RSUs shall carry no more than two weeks' worth of operating certificates.

4.4.11.5 The day before the current week's certificates become invalid, the RSUs shall download the next week's worth of certificates.

4.4.11.6 The RSU with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages received.(Note: the only exception to this is a firmware update in which case it may be necessary to update

the software responsible for DSRC communications. In such cases, the delay shall be minimized as much as possible.

4.4.11.7 The RSU with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages transmitted.

4.4.11.8 The NYC CVPD performance monitoring subsystem shall measure the RF monitoring range of the RSU.

4.4.11.9 The RSU shall record the first BSM message it hears from each ASD along with the time and the RF level.

4.4.11.10 The static RSU shall record the last BSM message it hears from each ASD along with the time and the RF level.

4.4.11.11 Note that if the ASD ID changes as it is approaching the RSU, then that will appear as 2 different vehicles since there is no attempt to track the vehicles. The statistical data will be aggregated for each ASD and each RSU to be able to develop the useful communications envelope around each RSU.

4.4.11.12 The RSU shall upload the data to the back office system whenever its buffers are full or more than 60 minutes old.

4.4.11.13 Once the RF log data is received and acknowledged by the back office system, it shall be purged from the RSU.

4.4.11.14 The RSU shall authenticate all transactions to retrieve its RF logs.

4.4.11.15 The RSU shall allow recording of the RF signal level for any message received. (For example, when the RSU hears a BSM from any vehicle, it shall be able to measure and record the RF level of the received message.)

4.4.12 System Reliability

4.4.12.1 The RSU shall revert to a fail-safe mode as specified in Table 8 when unable to perform its normal operations.

4.4.12.2 An RSU attempting to install new firmware or parameters shall receive from the ASD a report of a self-diagnosed failure of itself or one of its software modules.

4.5 Policy and Regulation

4.5.1 Maintenance

4.5.1.1 The RSU shall meet the USDOT certification requirements as defined in TBD prior to December 31, 2016. (Note: this shall be detailed in the design phase.)

4.6 USDOT Situation Data Clearinghouse and Warehouse

4.6.1.1 If broadcasting Intersection Safety Awareness messages, the RSU shall deposit an Intersection Situation Data (ISD) Protocol Data Unit (PDU) (message) into the NYCDOT Situation Data Clearinghouse once every 2 seconds.

4.6.1.2 The ISD PDUs shall comprise of one (1) SAE SPaT message and one (1) SAE MAP message.

4.6.1.3 The RSU shall retrieve SAE Traveler Information Messages from the NYC Situation Data Warehouse that are relevant to the RSU's geographic location.

4.6.1.4 Note that all interactions with the USDOT Data Warehouse and Situation Data Clearinghouse will be managed by the TMC in coordination with the RSU. The RSU will not connect directly to any external systems except through the TMC which shall manage all such interactions.

4.7 Behavioral Requirements

4.7.1.1 The RSU shall update all properly authenticated and verified configuration parameters no more than 15 seconds after an authorized user issues an "updateconf" command.

4.7.1.2 The RSU shall update all properly authenticated and verified configuration parameters no more than 15 seconds after an authorized user makes changes to any of the writeable SNMPv3 MIB Objects

4.7.1.3 The RSU shall update all software within 15 seconds after receiving the downloaded software from the TMC providing the updated software passes the authentication and integrity checks.

4.7.1.4 The RSU shall acknowledge receipt, authentication, and verification of the parameter and software updates concurrent with their execution; if the parameters and software fail authentication or verification the RSU shall respond with a failure code indicative of the problem.

4.7.2 Antenna Output Power

4.7.2.1 The RSU transmit output power shall be configurable and shall correspond to the channel utilization and power restrictions identified in J2945/0.

4.7.3 Operational States

4.7.3.1 The RSU shall have a set of operational states as illustrated in Figure 7 and defined in Table 5 below.

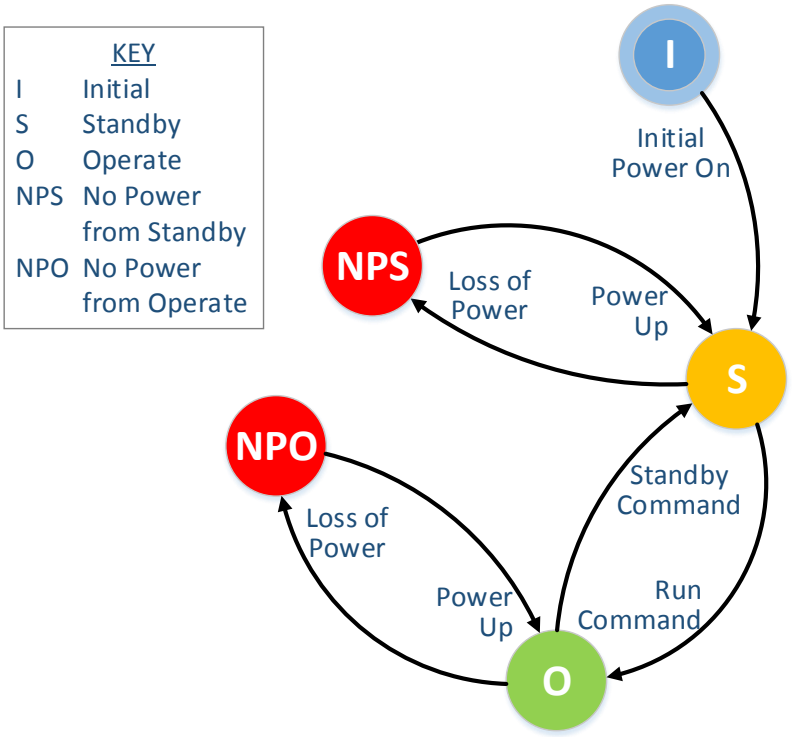

Figure 7. Roadside Unit State Diagram

Table 5. Operational States and State Transitions

State	Definition
Initial	This is the initial state of the device from the factory, with no specified requirements. The device shall revert to the “initial” state after a factory reset.
Standby	• Core Operating System is operational • DSRC radios are not operational/broadcasting • Interface logging is disabled; • Configuration changes are enabled
No Power Operate	This state results from a loss of power when the RSU is in the Operate State; this is **NOT** a graceful shutdown that would be enacted by a transition to Standby State prior to a transition to the No Power State.
No Power Standby	This state results from a loss of power when the RSU is in the Standby State. The unit should return to the Standby state upon power up.
Operate	• All DSRC radios are operational/broadcasting • System log is enabled • Configuration changes are disabled

4.7.3.2 State Transition – Initial to Standby

4.7.3.2.1 The RSU shall transition from the "Initial" state to the "Standby" state upon power on. (Note: transition from the "Initial" state to the "Standby" state only happens the first time the device is powered on after manufacturing or after factory reset.)

4.7.3.2.2 The RSU shall only return to the "Initial" state from "Standby" stateif a factory reset is initiated.

4.7.3.3 State Transition - Operate to Standby

4.7.3.3.1 The RSU shall transition from the "Operate" State to the "Standby" State no more than 5 seconds after an authorized user issues a "standby" command.

4.7.3.4 State Transition - Standby to Operate

4.7.3.4.1 The RSU shall transition from the "Standby" State to the "Operate" state no more than 10 seconds after an authorized user issues a "run" command.

4.7.3.5 State Transition - Current to No Power

4.7.3.5.1 The RSU shall transition from its current State to the "No Power" State upon loss of power or user initiated shut down without corrupting or damaging the file system or files contained on the unit.

4.7.3.6 State Transition - No Power to Previous State

4.7.3.6.1 When power is restored, the RSU shall transition from the “No Power” state to the State (“Standby” or “Operate”) the RSU was in when power was lost

4.7.3.7 Factory Reset

4.7.3.7.1 The RSU shall support a "Factory Reset" mechanism (command, button, etc.) for authenticated, authorized local users to remove all configuration parameters and operator installed files, returning the device to its original Factory Settings and “Initial” State.

4.7.4 Operational Modes

4.7.4.1 Operational Mode-Connected

4.7.4.1.1 The RSU shall operate with full functionality while connected to an operations center.

4.7.4.1.2 "Connected Mode" implies that the RSU is intended to continuously be connected to an operation center.

4.7.4.2 Operational Mode-“Standalone”

4.7.4.2.1 The RSU shall operate with full functionality while not connected to an operations center, until the device’s security credentials expire.

4.7.5 Operational Configuration – SNMPv3

4.7.5.1 The RSU Configuration, Management, and Status information shall be provided through SNMPv3. The RSU Management Information Base (MIB) is contained herein.

4.7.5.2 SMNPv3 MIB Configurations: The RSU shall operate based on parameters contained in the SNMPv3 MIB stored on the device.

4.7.5.3 SMNPv3 MIB Configuration Default Parameters: The RSU shall have default values for each configuration parameter in the SNMPv3 MIB.

4.7.5.4 SMNPv3 MIB Configuration Parameter Valid Range: The value of each SNMPv3 MIB Object shall be restricted to a valid range in which the RSU shall operate.

4.7.5.5 SNMPv3 MIB Walk: The RSU shall allow an authorized user to perform a MIB walk on the SNMPv3 MIB to produce a complete list of all supported MIBs and OIDs and the current setting for each Object.

4.7.5.6 SMNPv3 MIB Parameter Modification: The RSU shall allow an authorized user to modify the value of any writeable SNMPv3 MIB Object within its valid range.

4.7.5.7 SMNPv3 MIB Modification Validation-System Status Log File entry: The RSU shall write an INFO entry to the System Status Log File if the value of a writable SNMPv3 MIB Object is modified to an out of range value. The log entry shall contain the following data elements:

a. Date and Time
b. file name (name of the MIB file)
c. "MIB Object Value Out-of-Range: "
d. OID (of the Object whose value is out of range)
e. user ID
f. attempted value

4.7.5.8 SMNPv3 MIB Modification Validation-retain current value: The RSU shall retain the current value for a writable SNMPv3 MIB Object that is modified to an out of range value.

4.7.5.9 SNMPv3 MIB installation: The RSU shall allow authorized users to copy/move a SNMPv3 MIB from a network host to the SMNPv3 MIB directory on the device through an Ethernet Interface.

4.7.5.10 SNMPv3 MIB copy: The RSU shall allow authorized users to copy the SNMPv3 MIB from the SNMPv3 MIB directory to a network host through an Ethernet Interface.

4.7.5.11 SNMPv3 MIB Installation Validation-System Status Log File entry: The RSU shall write a CRITICAL entry in the System Status log file if a SNMPv3 MIB that contains out of range values for a writable Object is copied/moved into the SNMPv3 MIB directory. The log entry shall contain the following data elements:

a. Date and Time
b. file name (name of the MIB file)
c. "MIB Object Value Out-of-Range:"
d. OID (of the Object whose value is out of range)
e. user ID
f. offending value

4.7.6 Health and Status Monitoring

4.7.6.1 The RSU shall report the following items over SNMPv3:

a. Status of its memory (OID ucdavis.4)
b. Status of its CPU load
c. Status of its non-volatile storage
d. Standard system load average values
e. Time elapsed since it entered the “Operate” state
f. Time elapsed since it was first powered on
g. Last user to log in
h. Time the last user logged in
i. Source IP address of the last user to log in
j. Number of messages transmitted and received over DSRC, sorted by Alternating or Continuous, SCH or CCH, and Sent or Received
k. Number of messages transmitted over DSRC, sorted by PSID

4.7.6.2 The RSU should report over SNMPv3 its internal temperature

4.8 Interface Requirements

4.8.1 Backhaul Office

4.8.1.1 At installation locations that require multiple RSUs, the “master” RSU in the set shall be functional as the Ethernet interface between other non-master RSUs and the backhaul communication.

4.8.1.2 The RSU shall, at a minimum, include a 1x10/100 Base-T Ethernet (RJ45) port that supports 48V DC and is compliant with 802.3at Power-over-Ethernet (PoE), including IPv4 and IPv6.

4.8.1.3 The RSU shall support multiple, independent IPv4 and IPv6 networks.

4.8.1.4 If the RSU contains additional integrated wireless interfaces, such as 802.11b\g\n\a\ac\other Wi-Fi, Cellular 3G\4G, and others, those interfaces shall be inhibited or implement equivalent security access controls, authentication, integrity, and confidentiality to the services available over the wired PoE interface.

4.8.2 DSRC

4.8.2.1 FCC Regulation 47 CFR Compliance: The RSU shall comply with Federal Communications Commission (FCC) Code of Federal Regulations Title 47 Parts 0, 1, 2, 15, 90, and 95.

4.8.2.2 Each RSU shall include 2 radios capable of operating on all 7 channels of the DSRC spectrum and capable of having their output level modified for each channel and each message.

4.8.2.3 Nominally one channel will be 172 and shall monitor the BSM messages, and transmit the SPaT, MAP, and RTCM messages.

4.8.2.4 The second channel will be 178 and shall alternate or change between channels and modes for the support of IP communications and messages necessary for the CVPD support of software and parameter updates and log downloads to the TMC.

4.8.3 802.11

4.8.3.1 The RSU shall conform to IEEE Std. 802.11, as bounded by the general requirement to fully support the IEEE 802.11p specification and the IEEE 1609.x protocol specification set.

4.8.3.2 The RSU shall implement the Orthogonal frequency division multiplexing (OFDM) physical layer of the Open Systems Interconnection (OSI) model defined in Clause 18 of IEEE 802.11, unless otherwise indicated (including all data rates in 18.2.3.4).

4.8.3.3 The RSU shall use the default values defined in IEEE 802.11 unless otherwise indicated (including the coverage class in 18.3.8.7).

4.8.3.4 The RSU shall send 802.11 data frames using the Quality of Service (QoS) Data subtype.

4.8.3.5 The RSU shall configure an AIFS of a given access category with an integer value from 2 to X, where the value of X is based on the chip set used – as defined by the vendor.

4.8.3.6 Vendor should provide the limit for X, based on the chip set used

4.8.3.7 The Transmission Opportunity (TXOP) Value limit of a given AC shall be capable of being set to 0.

4.8.3.8 Contention Window Minimum Value: The CWmin of a given AC shall take any value of the form (2^k)-1, for k = 1 through Y.

4.8.3.9 Vendor should provide the limit for Y, based on the chip set used.

4.8.4 802.11p

4.8.4.1 The RSU shall send MAC Protocol data units (MPDUs) outside the context of a basic service set (BSS), i.e. with Management Information Base (MIB) variable dot11OCB Activated is set to "true".

4.8.4.2 The RSU shall support Operating class 17 (even 10 MHz channels in the range 172 to 184).

4.8.4.3 The RSU shall support Operating class 18 (odd 20 MHz channels in the range 175 to 181).

4.8.4.4 The RSU shall have a configurable EDCA parameter with a default as defined in IEEE 802.11.

4.8.5 IEEE 1609.2

4.8.5.1 The RSU shall conform to IEEE 1609.2

4.8.5.2 The RSU shall conform to the USDOT Security Credential Management System End Entity Requirements.

4.8.5.3 The RSU shall store all private keys in secure storage, such as that contained in a Hardware Security Module.

4.8.6 IEEE 1609.3

4.8.6.1 The RSU shall conform to IEEE 1609.3.

4.8.6.2 The RSU shall process both transmitted and received IPv6 packets.

4.8.6.2.1 At a minimum, IP based communications over DSRC shall be used for the exchange of data between the onboard equipment and the 1609.2 security credential management system.

4.8.6.3 The RSU shall process (both transmit and receive) WAVE Short Message Protocol (WSMP) messages.

4.8.6.4 The RSU shall assign a configurable PSID value (default to the value specified for the associated application area defined in IEEE 1609.12-2016, or later) and a configurable User Priority value (default to 2) to each data frame.

4.8.6.5 The following WSMP-N- header options shall be configured on the RSU:

a. Data Rate
b. Transmit Power Used

4.8.7 IEEE 1609.3 – WAVE Service Advertisements

4.8.7.1 The RSU shall conform to the WAVE Service Advertisement (WSA) Security Profile defined in IEEE 1609.3-2016 Annex H.1. (Note: Appendix E contains an example WSA for an RSU advertising intersection.)

4.8.7.2 The RSU shall broadcast WAVE Service Advertisements (WSA) on the Control Channel (CCH).

4.8.7.3 The RSU shall broadcast WAVE Service Advertisements (WSA) during Time Slot 0.

4.8.7.4 The RSU WAVE Service Advertisement (WSA) shall include DSRC Service Channel (SCH) Services from WSA MIB OID 1.0.15628.4.1.13.

4.8.7.5 The RSU WAVE Service Advertisement (WSA) shall include DSRC Service Channel (SCH) Services based on the Store and Repeat messages contained in MIB OID 1.0.15628.4.1.4.

4.8.7.6 The RSU WAVE Service Advertisement (WSA) shall include DSRC Service Channel (SCH) Services based on Immediate Forward messages received on non-DSRC interfaces as listed in MIB OID 1.0.15628.4.1.5.

4.8.7.7 Store & Repeat messages broadcast on the DSRC Control Channel (CCH), 178 shall NOT be included in the WAVE Service Advertisement.

4.8.7.8 Immediate Forward messages broadcast on the DSRC Control Channel (CCH), 178 shall NOT be included in the WAVE Service Advertisement.

4.8.8 IEEE 1609.4

4.8.8.1 Each DSRC radio contained in the RSU shall conform to IEEE 1609.4.

4.8.8.2 Each DSRC radio in the RSU shall be configurable to operate either in "Continuous" (operating continuously on a single Service Channel) or "Alternating" (switched between two Service Channels (or the Control Channel and a Service Channel)) Mode, as shown in Figure 9 of IEEE 1609.4-2016.

4.8.8.3 The RSU shall support Continuous Mode and Alternating Mode radio operations simultaneously

4.8.8.4 Each DSRC radio in the RSU shall be configurable to send messages either on Channel 178 during the Control Channel (CCH) interval or on any of the 10 MHz or 20 MHz channels with no time interval restrictions.

4.8.8.5 RSU DSRC Radios in Continuous Mode shall be configurable for operation on any 10 MHz or 20 MHz channel (default Channel 172) with no time interval restrictions.

4.8.8.6 RSU DSRC Radios in Alternating Mode shall broadcast WAVE Service Advertisements and Control Channel WAVE Short Messages on Channel 178 during the Control Channel (CCH) interval

4.8.8.7 RSU DSRC Radios in Alternating Mode shall be configurable to operate on any 10 MHz or 20 MHz channel during the Service Channel (SCH) Interval. Note: the service Channel configuration is part of the SNMPv3 MIB; see Appendix A.

4.8.8.8 Service Channel Interval: RSU DSRC Radios in Alternating Mode shall be capable of switching to the configured Service Channel every Service Channel interval with no time interval restrictions.

4.8.8.9 RSU Sets-Service Channel Alternating Mode: All non-master RSU DSRC radios in Alternating Mode within the same RSU set shall automatically operate on the same service channel(s) as the configuration of the “master” RSU.

4.8.8.10 RSU DSRC radios in Alternating Mode shall avoid the synchronized collision phenomenon described in Annex B of IEEE 1609.4 when broadcasting messages on during the Control Channel interval.

4.8.8.11 The RSU shall implement the readdressing option defined in IEEE 1609.4.

4.8.9 Configurable Latitude/Longitude/Elevation

4.8.9.1 The RSU shall include configurable location settings for Latitude, Longitude, and Elevation that can be SET by the TMC and used for transmission in the WSA message and used by the ASD or other on-board units to improve the accuracy and stability of the location determination mechanism/algorithms.

4.8.9.2 The RSU shall be configurable to use the Latitude, Longitude, & Elevation determined by the built-in GPS receiver or the TMC-configured Latitude/Longitude/Elevation.

4.8.9.3 The accuracy, resolution, shall be consistent with the needs of the WSA message.

4.8.9.4 The TMC shall be able to retrieve the Latitude, Longitude, & Elevation developed by the on-board GPS to confirm the approximate location of the RSU.

4.8.10 CAN Bus Interface/Mobile/RSU

4.8.10.1 The City wishes to install RSUs in one of the vehicles used for a mobile work crew (striping, sealing, etc.) but current FCC regulations prohibit the operation of an RSU while in motion. To support this type of operation, the following requirements have been added to the RSU specification.

4.8.10.2 The mobile RSU shall include an interface to the Vehicle CAN/J bus to be able to determine whether the vehicle it is connected to (mounted in) is in motion or in “park” and stationary. The vendor shall review the contents of the vehicle bus and determine how to accurately determine that the vehicle is stationary without special operator interaction.

4.8.10.3 The determination of mobile vs. stationary condition shall be subject to configurable hysteresis for time and location.

4.8.10.4 When the vehicle is stationary, the mobile RSU shall act as a normal RSU with communications to the back-office and perform normal data collection, which includes RF levels for received BSM Messages.

4.8.10.5 The support for “mobile” operation shall be configurable from the TMC.

4.9 Automatic Diagnostics

4.9.1.1 The CV system shall export RSU status to the traffic signal system for display on the traffic signal system map.

4.9.1.2 The CV system shall export RSU RF signal range information to the Traffic Management Center for processing where it may be placed on system displays and other applications to manage the hardware..

4.10 Safety Management Plan

4.10.1.1 The TMC staff shall be able to monitor the NYC CVPD system-wide RSU malfunctions.

4.10.1.2 The RSU shall broadcast the regulatory speed information to the ASD. (TIM, BIM)

4.10.1.3 The RSU shall broadcast the location of a curve and other details to support the CSPD-COMP application. (BIM)

4.10.1.4 The RSU shall broadcast the location of a static work zone to support the SPDCOMPWZ application. (BIM/TIM)

4.10.1.5 The RSU shall broadcast the location of a moving work zone to support the SPDCOMPWZ application.

4.10.1.6 The RSU shall broadcast the location of a school zone to support the SPDCOMPWZ application.

4.10.1.7 The RSU shall broadcast the location of a roadway's vehicle size restriction to support the OVC application.

4.10.1.8 The RSU shall not overload the power supplies provided. (During operation, turn off, turn on, etc. per NEMA TS2 environmental testing.)

4.10.1.9 Maximum power consumption is TBD. (Note: this shall be detailed in the design phase.)

4.10.1.10 The RSU shall allow the TMC to remotely perform a “reboot” of the RSU using SNMPv3.

4.10.1.11 The RSU shall resume normal operation within 2 minutes of application of power under all circumstances.

5 Application Requirements

5.1 Safety Applications

5.1.1.1 The RSU shall broadcast SPaT and MAP data to the vehicles deployed along the NYC CVPD corridors as per J2735.

5.1.1.1.1 The SPaT data shall be locally generated and signed per the SPaT security profile in Appendix D.

5.1.1.1.2 The MAP data shall be generated by the TMC and signed per the MAP security profile in Appendix D.

5.1.1.2 The RSU shall broadcast the roadway's clearance height and restrictions.

5.1.1.3 The RSU shall broadcast the roadway geometry for the speed zone, curve speed warning, and vehicle restrictions.

5.1.1.4 The RSU shall be able to receive the PSM from surrounding pedestrians and determine when pedestrians are in specific crosswalks. (future)

5.1.1.5 The RSU shall receive PSMs from the PIDs per J2945/9. (future)

5.1.1.6 The RSU shall transmit pedestrian detections in response to PSMs from the crosswalk (future)

5.1.1.7 The RSU shall decode pedestrians' request for crossing. (future)

5.1.1.8 The RSU shall indicate pedestrian presence in the roadway as measured by pedestrian detection devices.

5.2 Security Management Operating Concept

5.2.1.1 The RSU shall meet the USDOT certification requirements as defined in TBD prior to December 31, 2016. (Note: this will be detailed in the design phase.)

5.2.1.2 The RSU shall interface with signal controllers, NYCWiN, and DSRC messages from vehicles and pedestrians. (Note: this shall be expanded into multiple requirements for each interface.)

6 System Interfaces

6.1 Global Navigation Satellite System (GNSS)

6.1.1.1 Each DSRC device shall obtain its time and position from the GNSS per the requirements of J2945/1.

6.2 Wide Area Augmentation System (WAAS) [Location Correction]

6.2.1.1 Each RSU shall broadcast WAAS corrections per its Store and Repeat configuration.

6.3 Security Credential Management System (SCMS)

6.3.1.1 The device supplier shall provide devices provisioned with valid enrollment certificates with a lifetime of three years..

6.3.1.2 The device supplier shall provide devices that meet the interface requirements of the USDOT's certification program.

6.3.1.3 The RSU need not support CRLs. (Note: given the short timescale of the certificate renewal and storage process.).

6.3.1.4 The SCMS shall issue an operational certificate life span of one week. (Note: this shall be detailed in the design phase.).

6.3.1.5 The SCMS shall maintain the blacklist internally

6.3.1.6 Devices shall implement certificate download per the SCMS Interface (detailed requirements to be derived during Phase 2 as the final interface document is not yet published).

6.3.1.7 The device supplier shall sign the firmware images and manage the certificate management process for the firmware images.

6.3.1.8 The SCMS certificate shall have a lifespan of 3 years instead of weeks.

6.3.1.9 The SCMS signature scheme shall provide at least 128-bit security.

6.4 Object Registration and Discovery Service (ORDS)

6.4.1.1 This will be managed at the TMC

6.5 Data Distribution System (DDS)

6.5.1.1 This will be managed at the TMC

6.6 Research Data Exchange (RDE)

6.6.1.1 The interface for transferring performance measurement information to the USDOT Research Data Exchange shall be negotiated by the NYC CVPD project team and the USDOT RDE operators during the detailed design of the system in Phase 2.

6.7 Advanced Traffic Signal Controllers

6.7.1.1 The Advanced Traffic Signal Controllers (ATSC) shall provide data to the RSU over a secured link.

6.7.1.2 Advanced Traffic Signal Controllers shall maintain an authenticated NTP based time reference

6.7.1.3 ATSCs shall import (from the RSU) UTC time reference linked to the GPS signal.

6.7.1.4 SPaT messages shall be translated to UTC time [from line frequency based time] by the traffic controller prior to transmission to the RSU for development of the SPaT message.

6.7.1.5 Messages received from the traffic controller shall be signed following 1609.2 such that the RSU can authenticate the origin of the message and to defeat compromised information from rogue equipment attached to the Ethernet link.

6.7.1.6 The interface to the traffic controller shall utilize the updated NTCIP 1202 objects and the NTCIP 1103 Exception based reporting (EBR) mechanism to retrieve the necessary data from the traffic controller to construct the SPaT message.

6.7.1.7 As noted herein, the MAP message will be signed at the TMC (where it is developed) and the content of the MAP message will remain un-touched through its passage to the traffic controller and the RSU and finally to the DSRC broadcast of the MAP message.

6.7.1.8 It is expected that the SPaT message will be developed within the RSU based on the data received from the ASTC.

6.7.1.9 Because the Link between the traffic controller and the RSU is an “open” connection, it must be secured such that all exchanges to and from the ASTC are authenticated in both directions. The vendor shall use the security profile and security requirements and work with the ASTC vendor to ensure the integrity/security of this link.

7 Test Requirements

7.1.1.1 The vendor shall be responsible for conducting all tests at no cost to the City and shall develop the test procedures to confirm/verify conformance to the required standards and these project specifications.

7.1.1.2 The vendor shall be responsible for the providing the test environment and all test equipment and simulation equipment and for all “data takes” and records created during the testing.

7.1.1.3 The City or their designated personnel shall be provided the opportunity to witness and participate in all testing.

7.1.1.4 All test procedures including test cases, test steps, and the testing environment shall be submitted to the City for review prior to any testing.

7.1.1.5 The vendor shall provide a minimum of 10 business day advance notice of any testing to be performed such that the City can schedule participation if appropriate.

7.2 Radio Transmission

7.2.1.1 Based on the data collected, the DSRC-equipped vehicles (ASD) shall transmit messages in the form of BSMs to nearby RSUs, which shall then process them locally to collect the “probe data” and RF monitoring data.

8 Dedicated Short Range Communications (DSRC)

8.1 Requirements

8.1.1.1 The DSRC radio communications shall conform to 802.11p, IEEE 1609.2-1609.4, and to relevant portions of the SAE J2735 message set standards.

8.1.1.2 The RSU shall use DSRC wireless technology for the transmission of information to be exchanged between Vehicles-to-Infrastructure (V2I) and Vehicle-to-Pedestrian (V2P).

8.1.1.3 Software parameters between the RSU and ASD and PID shall be uploaded via DSRC channels 174 and 176.

8.1.1.4 The RSU shall transmit the MAP message, on a different channel at a rate of approximately once or twice per second. (Channel TBD – currently 172)

8.1.1.5 Contents of the MAP message shall conform to SAE J2735.

8.1.1.6 The RSU shalll comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses, and can radiate radio frequency energy and shall be in accordance to avoid causing harmful interference to radio communications

- Standards Conformance: IEEE 802.11p technology, IEEE 1609 suite
- Frequency Bands: 5.9GHz
- Transmit Power: 5.9GHz; -10 to +23dBm
- Receive Sensitive: 5.9GHz; -97dBm
- Antenna: 5.9GHz only
- Bandwidth 10 MHz
- Low latency communication (<<50ms)
- High data transfer rates (3-27 Mbps)
- Line-of-sight up to 1000m and 360º
- Low power message reception (<-90dBm)

8.1.1.7 The RSU shall store up to eight (8) different MAP messages.

8.1.1.8 The RSU shall allow the TMC to configure the specific MAP message at any time.

8.1.1.9 The TMC shall be able to schedule the MAP message in the RSU at one-minute resolution.

8.1.1.10 The TMC shall be able to schedule the MAP message in the RSU by day of the week (M-F, Sa, Su) and time of day.

Appendix A. RSU Specific MIB Objects

9 RSU Specific MIB Objects

The MIB objects below are taken from the Current USDOT RSU specification (4.1) to reflect the functionality included in that document. The vendor shall extend the MIB with additional objects to manage and support the various data collection and OTA software management, and SCMS support as necessary. This shall include but not be limited to the encryption keys for the data collected by the RSU, and the RSU interface to the SCMS. For the NY project, the RSU is intended to be a smart device responsible for running applications indicated herein to collect operational data, manage its own SCMS interface and keep its certificates, and to switch channels to support both the upload and download functions on the service channels.

9.1.1.1 This section contains the RSU specific MIB OIDs

```
RSU-MIB DEFINITIONS ::= BEGIN

IMPORTS
      MODULE-IDENTITY, OBJECT-TYPE, Integer32,
      Counter32, NOTIFICATION-TYPE                  FROM SNMPv2-SMI
      TEXTUAL-CONVENTION, DateAndTime, RowStatus,
      PhysAddress, DisplayString, MacAddress        FROM SNMPv2-TC
      MODULE-COMPLIANCE, OBJECT-GROUP               FROM SNMPv2-CONF
      Ipv6Address                                   FROM IPV6-TC;

rsuMIB MODULE-IDENTITY
      LAST-UPDATED     "201608310230Z"
      ORGANIZATION     "US-DOT"
      CONTACT-INFO     "postal:   TBD
                              email:          TBD@TBD.com"
      DESCRIPTION      "Leidos implementation RSU 4.1 MIB
                              based on Savari and Cohda implementation of
RSU 4.0"
      REVISION         "201608310230Z"
      DESCRIPTION      "Second Draft for RSU 4.1 Spec."
      REVISION         "201608120230Z"
      DESCRIPTION      "First Draft for RSU 4.1 Spec."
      REVISION         "201606270245Z"
      DESCRIPTION      "Combining input from Vendors"
      REVISION         "201404150000Z"            -- 15 April 2014
midnight
      DESCRIPTION      "RSU MIB Definitions"
      ::= { iso std(0) rsu(15628) version(4) 1 }



RsuTableIndex ::= TEXTUAL-CONVENTION
      DISPLAY-HINT   "d"
      STATUS         current
      DESCRIPTION
            "A valid range of values for use in table indices"
      SYNTAX         Integer32 (1..2147483647)
```

```
RsuPsidTC ::= TEXTUAL-CONVENTION
      DISPLAY-HINT   "2x"
      STATUS         current
      DESCRIPTION
            "PSID associated with a DSRC message."
      SYNTAX         OCTET STRING (SIZE(1..2))


rsuContMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Represents an 802 MAC address of the DSRC Radio operating in
         Continuous Mode represented in the 'canonical' order defined by
         IEEE 802.1a, i.e., as if it were transmitted least significant
         bit first, even though 802.5 (in contrast to other 802.x
protocols)
         requires MAC addresses to be transmitted most significant bit
first"
    ::= { rsuMIB 1 }

-- add entries for multiple antennas

rsuAltMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents an 802 MAC address of the DSRC Radio operating in
         Alternating Mode represented in the 'canonical' order defined
         by IEEE 802.1a, i.e., as if it were transmitted least significant
         bit first, even though 802.5 (in contrast to other 802.x
protocols)
         requires MAC addresses to be transmitted most significant bit
first"
    ::= { rsuMIB 2 }


rsuGpsStatus OBJECT-TYPE
      SYNTAX       INTEGER (0..15)
      MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
      "Provides the number of GPS Satellites RSUxs internal GPS receiver
is
            tracking"
      ::= { rsuMIB 3 }


rsuSRMStatusTable OBJECT-TYPE
      SYNTAX SEQUENCE OF RsuSRMStatusEntry
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
    DESCRIPTION
            "Provides configuration information for each Store
            Repeat message broadcast by an RSU and x represents
            the number of Store and Repeat Messages being broadcast by
            the RSU, beginning with 0 (i.e. if the RSU is broadcasting
            3 Store and Repeat messages, the following objects will be
            provideds SRM0_Status, SRM1_Status, and SRM2_Status)."
      ::= { rsuMIB 4 }


rsuSRMStatusEntry OBJECT-TYPE
      SYNTAX RsuSRMStatusEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
                  "A row describing RSU Store and Repeat Message Status"
      INDEX   { rsuSRMIndex }
      ::= {rsuSRMStatusTable 1 }


RsuSRMStatusEntry ::= SEQUENCE {
        rsuSRMIndex             RsuTableIndex,
        rsuSRMPsid              RsuPsidTC,
        rsuSRMDsrcMsgId         INTEGER,
        rsuSRMTxMode            INTEGER,
        rsuSRMTxChannel         INTEGER,
        rsuSRMTxInterval        INTEGER,
        rsuSRMDeliveryStart     OCTET STRING,
        rsuSRMDeliveryStop      OCTET STRING,
        rsuSRMPayload           OCTET STRING,
        rsuSRMEnable            INTEGER,
        rsuSRMStatus            RowStatus
    }

rsuSRMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message Index "
    ::= { rsuSRMStatusEntry 1 }

rsuSRMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message PSID"
    ::= { rsuSRMStatusEntry 2 }

rsuSRMDsrcMsgId OBJECT-TYPE
    SYNTAX       Integer32
    MAX-ACCESS   read-create
```

```
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message DSRC Message ID"
    ::= { rsuSRMStatusEntry 3 }

rsuSRMTxMode OBJECT-TYPE
      SYNTAX       INTEGER { cont(0), alt(1) }
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "DSRC mode set for Store and Repeat Message transmit,
             Continuous or Alternating"
      ::= { rsuSRMStatusEntry 4 }

rsuSRMTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC channel set for Store and Repeat Message transmit"
    ::= { rsuSRMStatusEntry 5 }

rsuSRMTxInterval OBJECT-TYPE
    SYNTAX       Integer32
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Time interval between two Store and Repeat Message"
    ::= { rsuSRMStatusEntry 6 }

rsuSRMDeliveryStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message delivery start time"
    ::= { rsuSRMStatusEntry 7 }

rsuSRMDeliveryStop OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message delivery stop time"
      ::= { rsuSRMStatusEntry 8 }

rsuSRMPayload OBJECT-TYPE
      SYNTAX       OCTET STRING (SIZE(0..1400))
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "Payload of Store and Repeat message.
            Length limit derived from UDP size limit."
      ::= { rsuSRMStatusEntry 9 }
```

```
rsuSRMEnable OBJECT-TYPE
      SYNTAX       INTEGER { off(0), on(1) }
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "Set this bit to enable transmission of the message
             0=off, 1=on"
      ::= { rsuSRMStatusEntry 10 }

rsuSRMStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "create and destroy row entry"
      ::= { rsuSRMStatusEntry 11 }


rsuIFMStatusTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuIFMStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides configuration parameters for each Immediate
        Forward message broadcast by an RSU x represents the number of
        Immediate Forward Messages being broadcast by the RSU,
        beginning with 0 (i.e. if the RSU is broadcasting 3
        Immediate Forward messages, the following objects will be
provideds
        IFM0_Status, IFM0_Status, and IFM1_Status2)."
    ::= { rsuMIB 5 }

rsuIFMStatusEntry OBJECT-TYPE
    SYNTAX       RsuIFMStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Immediate Forward Message Status"
    INDEX   { rsuIFMIndex }
    ::= {rsuIFMStatusTable 1 }

RsuIFMStatusEntry ::= SEQUENCE {
    rsuIFMIndex             RsuTableIndex,
    rsuIFMPsid              RsuPsidTC,
    rsuIFMDsrcMsgId         INTEGER,
      rsuIFMTxMode            Integer32,
    rsuIFMTxChannel         INTEGER,
      rsuIFMEnable            INTEGER,
      rsuIFMStatus           RowStatus
    }


rsuIFMIndex OBJECT-TYPE
```

```
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message Index "
    ::= { rsuIFMStatusEntry 1 }


rsuIFMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message PSID"
    ::= { rsuIFMStatusEntry 2}


rsuIFMDsrcMsgId OBJECT-TYPE
    SYNTAX       Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message DSRC Message ID"
    ::= { rsuIFMStatusEntry 3 }

rsuIFMTxMode OBJECT-TYPE
      SYNTAX       INTEGER { cont(0), alt(1) }
      MAX-ACCESS   read-only
      STATUS       current
      DESCRIPTION
            "Immediate Forward Message Transmit Mode
             Alternating or Continuous"
      ::= { rsuIFMStatusEntry 4 }

rsuIFMTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "DSRC channel set for Immediate Forward Message transmit"
    ::= { rsuIFMStatusEntry 5 }

rsuIFMEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Set this bit to enable transmission of the message
            0=off, 1=on"
    ::= { rsuIFMStatusEntry 6 }

rsuIFMStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
```

```
      STATUS       current
      DESCRIPTION
            "create and destroy row entry"
      ::= { rsuIFMStatusEntry 7}


rsuSysObjectID OBJECT-TYPE
    SYNTAX       OBJECT IDENTIFIER
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
       "The vendor's authoritative identification of the network
        management subsystem contained in the entity. This value
        is allocated within the DSRC subtree (1.0.15628.4) and
        provides an easy and unambiguous means for determining
        `what kind of box' is being managed. 1.0.15628.4.1.6.0
        indicates an RSU"
    ::= { rsuMIB 6 }


rsuDsrcForwardTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuDsrcForwardEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "contains the DSRC PSID being forwarded to a network host,
        the IP Address and port number of the destination host, as
        well as other configuration parameters as defined."
    ::= { rsuMIB 7}


rsuDsrcForwardEntry OBJECT-TYPE
    SYNTAX       RsuDsrcForwardEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Message Forwarding"
    INDEX   { rsuDsrcFwdIndex }
    ::= {rsuDsrcForwardTable 1 }


RsuDsrcForwardEntry ::= SEQUENCE {
      rsuDsrcFwdIndex              RsuTableIndex,
      rsuDsrcFwdPsid               RsuPsidTC,
      rsuDsrcFwdDestIpAddr         Ipv6Address,
      rsuDsrcFwdDestPort           INTEGER,
      rsuDsrcFwdProtocol           INTEGER,
      rsuDsrcFwdRssi               INTEGER,
      rsuDsrcFwdMsgInterval        INTEGER,
      rsuDsrcFwdDeliveryStart      OCTET STRING,
      rsuDsrcFwdDeliveryStop       OCTET STRING,
      rsuDsrcFwdEnable             INTEGER,
      rsuDsrcFwdStatus             RowStatus
}
```

```
rsuDsrcFwdIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Message Forward Message Index "
    ::= { rsuDsrcForwardEntry 1 }

rsuDsrcFwdPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward PSID"
    ::= { rsuDsrcForwardEntry 2 }


rsuDsrcFwdDestIpAddr OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Destination Server IP address"
    ::= { rsuDsrcForwardEntry 3 }


rsuDsrcFwdDestPort OBJECT-TYPE
    SYNTAX       INTEGER (1024 .. 65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Destination Server Port Number"
    ::= { rsuDsrcForwardEntry 4 }

rsuDsrcFwdProtocol OBJECT-TYPE
    SYNTAX       INTEGER { tcp(1), udp(2) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Transport Protocol between RSU and Server"
    ::= { rsuDsrcForwardEntry 5 }

rsuDsrcFwdRssi OBJECT-TYPE
    SYNTAX       INTEGER (-100 .. -60)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Minimum Received Signal Strengh Level of DSRC Messages should be
        Forwarded to server"
    ::= { rsuDsrcForwardEntry 6 }

rsuDsrcFwdMsgInterval OBJECT-TYPE
    SYNTAX       INTEGER (1 .. 9)
```

```
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Interval with which RSU forwards DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 7 }

rsuDsrcFwdDeliveryStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Start time for RSU to start forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 8 }


rsuDsrcFwdDeliveryStop OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Stop time for RSU to stop forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 9 }

rsuDsrcFwdEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Stop time for RSU to stop forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 10 }

rsuDsrcFwdStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "create and destroy row entry "
    ::= { rsuDsrcForwardEntry 11 }


rsuGpsOutput OBJECT IDENTIFIER ::= { rsuMIB 8 }

rsuGpsOutputPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "GPS Out External Server Port Number"
      ::= { rsuGpsOutput 1 }

rsuGpsOutputAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
      MAX-ACCESS   read-write
      STATUS       current
```

```
      DESCRIPTION
            "Remote host IPv6 address to which to send the GPS string"
      ::= { rsuGpsOutput 2 }

rsuGpsOutputInterface OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Local interface on which to output the GPS string"
      ::= { rsuGpsOutput 3 }

rsuGpsOutputInterval OBJECT-TYPE
      SYNTAX       Integer32 (1 .. 18000)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Interval at which to send the GPS GPGGA NMEA String
        to external Server"
      ::= { rsuGpsOutput 4 }

rsuGpsOutputString OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..100))
      MAX-ACCESS   read-only
      STATUS       current
      DESCRIPTION
            "Contains GPS NMEA GPGGA output string"
      ::= { rsuGpsOutput 5 }

rsuGpsRefLat OBJECT-TYPE
      SYNTAX       Integer32
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the actual GPS latitude for validation of
             reported GPS latitude."
      ::= { rsuGpsOutput 6 }

rsuGpsRefLon OBJECT-TYPE
      SYNTAX       Integer32
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the actual GPS longitude for validation of
             reported GPS longitude."
      ::= { rsuGpsOutput 7 }

rsuGpsRefElv OBJECT-TYPE
      SYNTAX       Integer32
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the actual GPS elevation for validation of
             reported GPS elevation."
```

```
      ::= { rsuGpsOutput 8 }

rsuGpsMaxDeviation OBJECT-TYPE
      SYNTAX       Integer32
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the maximum allowable deviation (radius in meters)
             for comparison between the reported GPS coordinates and the
             static GPS coordinates."
      ::= { rsuGpsOutput 9 }


rsuInterfaceLogTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Provides configuration information for capturing log files
        for each communication Interface x represents the
        interface for which these configurations will apply"
    ::= { rsuMIB 9 }

rsuInterfaceLogEntry OBJECT-TYPE
    SYNTAX       RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Interface Log"
    INDEX   { rsuIfaceLogIndex }
    ::= {rsuInterfaceLogTable 1 }

RsuInterfaceLogEntry ::= SEQUENCE {
        rsuIfaceLogIndex             RsuTableIndex,
        rsuIfaceGenerate             INTEGER,
        rsuIfaceMaxFileSize          INTEGER,
        rsuIfaceMaxFileTime    INTEGER
   }

rsuIfaceLogIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Interface Logging Index "
    ::= { rsuInterfaceLogEntry 1 }


rsuIfaceGenerate OBJECT-TYPE
    SYNTAX INTEGER { off(0),
                     on(1) }
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
```

```
        "Enable / Disable interface logging. '0x00 = OFF' and
        '0x01 = ON'"
    ::= { rsuInterfaceLogEntry 2 }


rsuIfaceMaxFileSize OBJECT-TYPE
    SYNTAX INTEGER (5..40)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Maximum Interface Log File Size in Mega Bytes unit"
    ::= { rsuInterfaceLogEntry 3 }


rsuIfaceMaxFileTime OBJECT-TYPE
    SYNTAX INTEGER (1..48)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Maximum Collection time for Interface Logging in hrs unit"
    ::= { rsuInterfaceLogEntry 4 }


rsuSecCredReq OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE (1))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
      "rovides configuration parameters for when an RSU should
        request new 1609.2 security credentials in days before
        existing credentials expire"
    ::= { rsuMIB 10 }


rsuSecCredAttachInterval OBJECT-TYPE
    SYNTAX INTEGER (1..100)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Provides configuration parameters for when an RSU will attach
        1609.2 security credentials to a WAVE Short Message Protocol
        (WSMP) Message"
    ::= { rsuMIB 11 }


rsuDsrcChannelModeTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuDsrcChannelModeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
      "Provides Continuous and Alternating Channel Mode
        configurations for each DSRC interface.
        x represents the interface for which these
        configurations will apply"
```

```
    ::= { rsuMIB 12  }

rsuDsrcChannelModeEntry OBJECT-TYPE
    SYNTAX RsuDsrcChannelModeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing RSU Interface Log"
    INDEX   { rsuDCMIndex }
    ::= {rsuDsrcChannelModeTable 1 }

RsuDsrcChannelModeEntry ::= SEQUENCE {
      rsuDCMIndex       RsuTableIndex,
      rsuDCMRadio       DisplayString,
      rsuDCMMode        INTEGER,
    rsuDCMCCH         INTEGER,
    rsuDCMSCH         INTEGER
    }

rsuDCMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Radio Interface Channel Mode Index "
    ::= { rsuDsrcChannelModeEntry 1 }

rsuDCMRadio OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   read-only
      STATUS       current
      DESCRIPTION
            "Name of the radio that the configuration relates to."
      ::= { rsuDsrcChannelModeEntry 2 }

rsuDCMMode OBJECT-TYPE
    SYNTAX       INTEGER { cont(0), alt(1) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
           "DSRC Channel Mode. '0x00 = Continuous Mode'
         and, '0x01 = Alternating Mode'"
    ::= { rsuDsrcChannelModeEntry 3 }

rsuDCMCCH OBJECT-TYPE
    SYNTAX       INTEGER (172..184)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Control Channel number to use - applies in Alternating Mode"
    ::= { rsuDsrcChannelModeEntry 4 }

rsuDCMSCH OBJECT-TYPE
    SYNTAX       INTEGER (172..184)
```

```
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Service Channel number to use"
    ::= { rsuDsrcChannelModeEntry 5 }


rsuWsaServiceTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuWsaServiceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
             "Provides general configuration parameters for the RSU WAVE
        Service Advertisement.
        x represents the number of the service being advertised
        in the WSA, beginning with 0 (i.e. if the WSA
        advertises 2 services, the following objects will be
        provideds WSA_Service_0_Configuration and"
    ::= { rsuMIB 13 }

rsuWsaServiceEntry OBJECT-TYPE
    SYNTAX RsuWsaServiceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing RSU WSA Service "
    INDEX   { rsuWsaIndex }
    ::= {rsuWsaServiceTable 1 }

RsuWsaServiceEntry ::= SEQUENCE {
        rsuWsaIndex                 RsuTableIndex,
        rsuWsaPsid                  RsuPsidTC,
        rsuWsaPriority              INTEGER,
        rsuWsaProviderContext       OCTET STRING,
        rsuWsaIpAddress             Ipv6Address,
        rsuWsaPort                  INTEGER,
           rsuWsaChannel               Integer32,
         rsuWsaStatus                RowStatus
    }

rsuWsaIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " WSA Service Index "
    ::= { rsuWsaServiceEntry 1 }

rsuWsaPsid OBJECT-TYPE
      SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "WSA Service PSID"
```

```
    ::= { rsuWsaServiceEntry 2 }

rsuWsaPriority OBJECT-TYPE
    SYNTAX       INTEGER (0 .. 63)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Priority of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 3 }

rsuWsaProviderContext OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE (4))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "WSA Service Specific Provider Context "
    ::= { rsuWsaServiceEntry 4 }

rsuWsaIpAddress OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "IPv6 address of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 5 }

rsuWsaPort OBJECT-TYPE
    SYNTAX       INTEGER (1024 .. 65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Port Number of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 6 }

rsuWsaChannel OBJECT-TYPE
      SYNTAX       INTEGER (172..184)
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "The number of the channel on which the advertised service is
provided."
      ::= { rsuWsaServiceEntry 7 }

rsuWsaStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "create or destroy rows"
      ::= { rsuWsaServiceEntry 8 }


rsuWraConfiguration OBJECT IDENTIFIER ::= { rsuMIB 14 }
```

```
rsuWraIpPrefix OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address prefix of WRA Service Advertised "
    ::= { rsuWraConfiguration 1 }

rsuWraIpPrefixLength OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(1))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Length of IPv6 address prefix of WRA Service Advertised "
    ::= { rsuWraConfiguration 2 }

rsuWraGateway OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address of Gateway of WRA Service Advertised "
    ::= { rsuWraConfiguration 3 }

rsuWraPrimaryDns OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address of Primary DNS Server of WRA Service Advertised "
    ::= { rsuWraConfiguration 4 }


rsuMessageStats OBJECT IDENTIFIER ::= { rsuMIB 15 }

rsuAltSchMsgSent OBJECT-TYPE
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Alternating Service Channel since
            start of service."
    ::= { rsuMessageStats 1 }

rsuAltSchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Alternating Service Channel since
            start of service."
    ::= { rsuMessageStats 2 }

rsuAltCchMsgSent OBJECT-TYPE
```

```
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Alternating Control Channel since
            start of service."
    ::= { rsuMessageStats 3 }

rsuAltCchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Alternating Control Channel since
            start of service."
    ::= { rsuMessageStats 4 }

rsuContSchMsgSent OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Service Channel since
            start of service."
    ::= { rsuMessageStats 5 }

rsuContSchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Continuous Service Channel since
            start of service."
    ::= { rsuMessageStats 6 }

rsuContCchMsgSent OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Control Channel since
            start of service."
    ::= { rsuMessageStats 7 }

rsuContCchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Control Channel since
            start of service."
    ::= { rsuMessageStats 8 }

rsuMessageCountsByPsidTable OBJECT-TYPE
```

```
    SYNTAX SEQUENCE OF RsuMessageCountsByPsidEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides a count of transmitted messages sorted by PSID.
            Each row is a different PSID."
    ::= { rsuMessageStats 9 }

rsuMessageCountsByPsidEntry OBJECT-TYPE
    SYNTAX RsuMessageCountsByPsidEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing the number of messages transmitted "
    INDEX   { rsuMessageCountsByPsidIndex }
    ::= { rsuMessageCountsByPsidTable 1 }

RsuMessageCountsByPsidEntry ::= SEQUENCE {
      rsuMessageCountsByPsidIndex        RsuTableIndex,
      rsuMessageCountsByPsidId           RsuPsidTC,
      rsuMessageCountsByPsidCounts       Counter32,
      rsuMessageCountsByPsidRowStatus    RowStatus
      }

rsuMessageCountsByPsidIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " WSA Service Index "
    ::= { rsuMessageCountsByPsidEntry 1 }

rsuMessageCountsByPsidId OBJECT-TYPE
      SYNTAX       RsuPsidTC
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
            since the RSU was last powered on."
    ::= { rsuMessageCountsByPsidEntry 2 }

rsuMessageCountsByPsidCounts OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
            since the RSU was last powered on."
    ::= { rsuMessageCountsByPsidEntry 3 }

rsuMessageCountsByPsidRowStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
```

```
      DESCRIPTION
            "create or destroy rows"
      ::= { rsuMessageCountsByPsidEntry 4 }


rsuSystemStats OBJECT IDENTIFIER ::= { rsuMIB 16 }

rsuTimeSincePowerOn OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
            since the RSU was last powered on."
    ::= { rsuSystemStats 1 }

rsuTotalRunTime OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
            since the RSU was first powered on."
    ::= { rsuSystemStats 2 }

rsuLastLoginTime OBJECT-TYPE
      SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the time when the last user logged in."
    ::= { rsuSystemStats 3 }

rsuLastLoginUser OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the name of the last user to log in."
    ::= { rsuSystemStats 4 }

rsuLastLoginSource OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains name or address of the remote host from which
            the last user logged in."
    ::= { rsuSystemStats 5 }

rsuLastRestartTime OBJECT-TYPE
      SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
```

```
    DESCRIPTION
        "Contains the time when the RSU process was last started."
    ::= { rsuSystemStats 6 }

rsuIntTemp OBJECT-TYPE
      SYNTAX       INTEGER (-100..100)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the internal temperature of the RSU in degrees Celsius."
    ::= { rsuSystemStats 7 }

rsuSysDescription OBJECT IDENTIFIER ::= { rsuMIB 17 }

rsuMibVersion OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the version of this MIB."
    ::= { rsuSysDescription 1 }

rsuFirmwareVersion OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the version of firmware running on this RSU."
    ::= { rsuSysDescription 2 }

rsuLocationDesc OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..140))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains a description of the installation location of this RSU."
    ::= { rsuSysDescription 3 }

rsuID OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the ID given to this RSU."
    ::= { rsuSysDescription 4 }

rsuManufacturer OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the manufacturer of this RSU."
    ::= { rsuSysDescription 5 }
```

```
rsuSysSettings OBJECT IDENTIFIER ::= { rsuMIB 18 }

rsuTxPower OBJECT-TYPE
      SYNTAX       Integer32 (0..100)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Sets the output power of the RSU antennas
            as a percentage of full strength.  Default is 100%."
    ::= { rsuSysSettings 1 }

rsuNotifyIpAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IP address of the SNMP Manager that will
            receive the SNMP Notifications."
    ::= { rsuSysSettings 2 }

rsuNotifyPort OBJECT-TYPE
      SYNTAX       Integer32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port number of the SNMP Manager that will
            receive the SNMP Notifications.  Default is 162."
    ::= { rsuSysSettings 3 }

rsuSysLogCloseDay OBJECT-TYPE
      SYNTAX       INTEGER {      monday(1), tuesday(2), wednesday(3),
                                thursday(4), friday(5), saturday(6),
                                sunday(7) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the day of the week on which to close the system
            log file Default is Sunday."
    ::= { rsuSysSettings 4 }

rsuSysLogCloseTime OBJECT-TYPE
      SYNTAX       OCTET STRING (SIZE(3))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the time of day at which to close the system
            log file.  Default is 23:59:00 UTC."
    ::= { rsuSysSettings 5 }

rsuSysLogDeleteDay OBJECT-TYPE
      SYNTAX       INTEGER {      monday(1), tuesday(2), wednesday(3),
                                thursday(4), friday(5), saturday(6),
                                sunday(7) }
    MAX-ACCESS   read-write
```

```
    STATUS       current
    DESCRIPTION
        "Contains the day of the week on which to close the system
            log file Default is Sunday."
    ::= { rsuSysSettings 6 }

rsuSysLogDeleteAge OBJECT-TYPE
      SYNTAX       Integer32
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the age at which to delete old log files.
            Default is 30 days."
    ::= { rsuSysSettings 7 }



-- System Status

rsuSystemStatus OBJECT IDENTIFIER ::= { rsuMIB 19}

rsuChanStatus OBJECT-TYPE
      SYNTAX INTEGER {
        bothOp (0), --both Continuous and Alternating modes are
operational
        altOp (1),  --Alternating mode is operational, Continuous mode is
not operational
        contOp (2), --Continuous mode is operational, Alternating mode is
not operational
        noneOp (3)  --neither Continuous nor Alternating mode is
operational
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
           "Indicates which channel modes are operating.
            Note: Operating means the device is functioning
            as designed, configured, and intended"
    ::= { rsuSystemStatus 1 }



-- Situation Data

rsuSitData OBJECT IDENTIFIER ::= { rsuMIB 20 }

rsuSdcDestIpAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of the Situation Data Clearinghouse."
    ::= { rsuSitData 1 }
```

```
rsuSdcDestPort OBJECT-TYPE
      SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Clearinghouse
            will receive data."
    ::= { rsuSitData 2 }

rsuSdcInterval OBJECT-TYPE
      SYNTAX       Integer32 (1..18000)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the interval in seconds at which the RSU will send
            data to the Situation Data Clearinghouse."
    ::= { rsuSitData 3 }

rsuSdwIpAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of the Situation Data Warehouse."
    ::= { rsuSitData 4 }

rsuSdwPort OBJECT-TYPE
      SYNTAX       Integer32
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Warehouse
            will receive requrests from the RSU."
    ::= { rsuSitData 5 }


-- RSU Set

rsuSet OBJECT IDENTIFIER ::= { rsuMIB 21 }

rsuSetRole OBJECT-TYPE
      SYNTAX       Integer32
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Warehouse
            will receive requrests from the RSU."
    ::= { rsuSet 1 }

rsuSetEnable OBJECT-TYPE
      SYNTAX       Integer32
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
```

```
        "Contains the port on which the Situation Data Warehouse
            will receive requrests from the RSU."
    ::= { rsuSet 2 }

rsuSetSlaveTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuSetSlaveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides a count of transmitted messages sorted by PSID.
            Each row is a different PSID."
    ::= { rsuSet 3 }

rsuSetSlaveEntry OBJECT-TYPE
    SYNTAX RsuSetSlaveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing the number of messages transmitted "
    INDEX   { rsuSetSlaveIndex }
    ::= { rsuSetSlaveTable 1 }

RsuSetSlaveEntry ::= SEQUENCE {
      rsuSetSlaveIndex             RsuTableIndex,
      rsuSetSlaveIpAddress         Ipv6Address,
      rsuSetSlaveRowStatus         RowStatus
}

rsuSetSlaveIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Slave RSU index "
    ::= { rsuSetSlaveEntry 1 }

rsuSetSlaveIpAddress OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of each slave RSU.  One
            slave per row."
    ::= { rsuSetSlaveEntry 2 }

rsuSetSlaveRowStatus OBJECT-TYPE
      SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "create or destroy rows"
    ::= { rsuSetSlaveEntry 3 }
```

```
-- RSU Mode

rsuMode OBJECT-TYPE
    SYNTAX      INTEGER {
                        standby  (2),
                        operate  (4),
                        off      (16)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Specifies the current mode of operation of the RSU."
    ::= { rsuMIB 99 }


-- Asynchronous Messages
rsuAsync OBJECT IDENTIFIER ::= { rsuMIB 100 }

-- Notifications

rsuNotifications OBJECT IDENTIFIER ::= { rsuAsync 0 }


messageFileIntegrityError NOTIFICATION-TYPE
      OBJECTS      { rsuMsgFileIntegrityMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 1 }

rsuSecStorageIntegrityError NOTIFICATION-TYPE
      OBJECTS      { rsuSecStorageIntegrityMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 2 }

rsuTamperAlert NOTIFICATION-TYPE
      OBJECTS      { rsuTamperAlertMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 3 }

rsuAuthError NOTIFICATION-TYPE
      OBJECTS      { rsuAuthMsg }
      STATUS       current
      DESCRIPTION
```

```
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 4 }

rsuSignatureVerifyError NOTIFICATION-TYPE
      OBJECTS      { rsuSignatureVerifyMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 5 }

rsuAccessError NOTIFICATION-TYPE
      OBJECTS      { rsuAccessMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 6 }

rsuTimeSourceLost NOTIFICATION-TYPE
      OBJECTS      { rsuTimeSourceLostMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 7 }

rsuClockSkewError NOTIFICATION-TYPE
      OBJECTS      { rsuClockSkewMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 8 }

rsuTimeSourceMismatch NOTIFICATION-TYPE
      OBJECTS      { rsuTimeSourceMismatchMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 9 }

rsuGpsAnomaly NOTIFICATION-TYPE
      OBJECTS      { rsuGpsAnomalyMsg }
      STATUS       current
      DESCRIPTION
```

```
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 10 }

rsuGpsDeviationError NOTIFICATION-TYPE
      OBJECTS      { rsuGpsDeviationMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 11 }

rsuGpsNmeaNotify NOTIFICATION-TYPE
      OBJECTS      { rsuGpsOutputString }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report the NMEA string at the
configured
             interval."
      ::= { rsuNotifications 12 }


rsuNotificationObjects OBJECT IDENTIFIER ::= { rsuAsync 1 }

-- Notification Objects
rsuMsgFileIntegrityMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an Active Message
             Integrity error "
      ::= { rsuNotificationObjects 1 }

rsuSecStorageIntegrityMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing a secure storage
             Integrity error "
      ::= { rsuNotificationObjects 2 }

rsuTamperAlertMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an enclosure
             tampering error "
      ::= { rsuNotificationObjects 3 }
```

```
rsuAuthMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an authorization
              error "
      ::= { rsuNotificationObjects 4 }

rsuSignatureVerifyMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing a signature verification
             error "
      ::= { rsuNotificationObjects 5 }

rsuAccessMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an error or rejection
             due to Access Control List rules "
      ::= { rsuNotificationObjects 6 }

rsuTimeSourceLostMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message indicating a time source
             was lost"
      ::= { rsuNotificationObjects 7 }

rsuClockSkewMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing that a vendor-defined
             clock skew rate was exceeded "
      ::= { rsuNotificationObjects 8 }

rsuTimeSourceMismatchMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing a deviation between two
time sources that exceeds a vendor-defined threshold "
      ::= { rsuNotificationObjects 9 }
```

```
rsuGpsAnomalyMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an anomaly that was
             detected in the GPS signal "
      ::= { rsuNotificationObjects 10 }

rsuGpsDeviationMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message indicating that the reported GPS
             position differs from the reference by more than the
             allowed deviation "
      ::= { rsuNotificationObjects 11 }

rsuGpsNmeaNotifyInterval OBJECT-TYPE
      SYNTAX       Integer32 (0..18000)
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Sets the repeat interval in seconds for the Notification
             containing the GPS NMEA GPGGA string.
             Default is 0 (disabled)."
      ::= { rsuNotificationObjects 12 }

END
```

Appendix B. General MIB Objects

10 General MIB Objects

10.1.1.1 This section contains a list of MIB Objects for a typical Linux device. The RSU is expected to, at a minimum, support these, or similar Objects with corresponding Object Identifiers.

sysDescr OBJECT-TYPE	1.3.6.1.2.1.1.1
sysObjectID OBJECT-TYPE	1.3.6.1.2.1.1.2
sysUpTime OBJECT-TYPE	1.3.6.1.2.1.1.3
sysContact OBJECT-TYPE	1.3.6.1.2.1.1.4
sysName OBJECT-TYPE	1.3.6.1.2.1.1.5
sysLocation OBJECT-TYPE	1.3.6.1.2.1.1.6
sysServices OBJECT-TYPE	1.3.6.1.2.1.1.7
ifNumber OBJECT-TYPE	1.3.6.1.2.1.2.1
ifTable OBJECT-TYPE	1.3.6.1.2.1.2.2
ifEntry OBJECT-TYPE	1.3.6.1.2.1.2.2.1
ifIndex OBJECT-TYPE	1.3.6.1.2.1.2.2.1.1
ifDescr OBJECT-TYPE	1.3.6.1.2.1.2.2.1.2
ifType OBJECT-TYPE	1.3.6.1.2.1.2.2.1.3
ifMtu OBJECT-TYPE	1.3.6.1.2.1.2.2.1.4
ifSpeed OBJECT-TYPE	1.3.6.1.2.1.2.2.1.5
ifPhysAddress OBJECT-TYPE	1.3.6.1.2.1.2.2.1.6
ifAdminStatus OBJECT-TYPE	1.3.6.1.2.1.2.2.1.7
ifOperStatus OBJECT-TYPE	1.3.6.1.2.1.2.2.1.8
ifLastChange OBJECT-TYPE	1.3.6.1.2.1.2.2.1.9
ifInOctets OBJECT-TYPE	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts OBJECT-TYPE	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts OBJECT-TYPE	1.3.6.1.2.1.2.2.1.12
ifInDiscards OBJECT-TYPE	1.3.6.1.2.1.2.2.1.13
ifInErrors OBJECT-TYPE	1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos OBJECT-TYPE	1.3.6.1.2.1.2.2.1.15
ifOutOctets OBJECT-TYPE	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts OBJECT-TYPE	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts OBJECT-TYPE	1.3.6.1.2.1.2.2.1.18
ifOutDiscards OBJECT-TYPE	1.3.6.1.2.1.2.2.1.19
ifOutErrors OBJECT-TYPE	1.3.6.1.2.1.2.2.1.20
ifOutQLen OBJECT-TYPE	1.3.6.1.2.1.2.2.1.21
ifSpecific OBJECT-TYPE	1.3.6.1.2.1.2.2.1.22
atTable OBJECT-TYPE	1.3.6.1.2.1.3.1
atEntry OBJECT-TYPE	1.3.6.1.2.1.3.1.1
atIfIndex OBJECT-TYPE	1.3.6.1.2.1.3.1.1.1

```
atPhysAddress OBJECT-TYPE                1.3.6.1.2.1.3.1.1.2
atNetAddress OBJECT-TYPE                 1.3.6.1.2.1.3.1.1.3
ipForwarding OBJECT-TYPE                 1.3.6.1.2.1.4.1
ipDefaultTTL OBJECT-TYPE                 1.3.6.1.2.1.4.2
ipInReceives OBJECT-TYPE                 1.3.6.1.2.1.4.3
ipInHdrErrors OBJECT-TYPE                1.3.6.1.2.1.4.4
ipInAddrErrors OBJECT-TYPE               1.3.6.1.2.1.4.5
ipForwDatagrams OBJECT-TYPE              1.3.6.1.2.1.4.6
ipInUnknownProtos OBJECT-TYPE            1.3.6.1.2.1.4.7
ipInDiscards OBJECT-TYPE                 1.3.6.1.2.1.4.8
ipInDelivers OBJECT-TYPE                 1.3.6.1.2.1.4.9
ipOutRequests OBJECT-TYPE                1.3.6.1.2.1.4.10
ipOutDiscards OBJECT-TYPE                1.3.6.1.2.1.4.11
ipOutNoRoutes OBJECT-TYPE                1.3.6.1.2.1.4.12
ipReasmTimeout OBJECT-TYPE               1.3.6.1.2.1.4.13
ipReasmReqds OBJECT-TYPE                 1.3.6.1.2.1.4.14
ipReasmOKs OBJECT-TYPE                   1.3.6.1.2.1.4.15
ipReasmFails OBJECT-TYPE                 1.3.6.1.2.1.4.16
ipFragOKs OBJECT-TYPE                    1.3.6.1.2.1.4.18
ipFragFails OBJECT-TYPE                  1.3.6.1.2.1.4.18
ipFragCreates OBJECT-TYPE                1.3.6.1.2.1.4.19
ipAddrTable OBJECT-TYPE                  1.3.6.1.2.1.4.20
ipAddrEntry OBJECT-TYPE                  1.3.6.1.2.1.4.20.1
ipAdEntAddr OBJECT-TYPE                  1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex OBJECT-TYPE               1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask OBJECT-TYPE               1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr OBJECT-TYPE             1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize OBJECT-TYPE          1.3.6.1.2.1.4.20.1.5
ipRouteTable OBJECT-TYPE                 1.3.6.1.2.1.4.21
ipRouteEntry OBJECT-TYPE                 1.3.6.1.2.1.4.21.1
ipRouteDest OBJECT-TYPE                  1.3.6.1.2.1.4.21.1.1
ipRouteIfIndex OBJECT-TYPE               1.3.6.1.2.1.4.21.1.2
ipRouteMetric1 OBJECT-TYPE               1.3.6.1.2.1.4.21.1.3
ipRouteMetric2 OBJECT-TYPE               1.3.6.1.2.1.4.21.1.4
ipRouteMetric3 OBJECT-TYPE               1.3.6.1.2.1.4.21.1.5
ipRouteMetric4 OBJECT-TYPE               1.3.6.1.2.1.4.21.1.6
ipRouteNextHop OBJECT-TYPE               1.3.6.1.2.1.4.21.1.7
ipRouteType OBJECT-TYPE                  1.3.6.1.2.1.4.21.1.8
ipRouteProto OBJECT-TYPE                 1.3.6.1.2.1.4.21.1.9
ipRouteAge OBJECT-TYPE                   1.3.6.1.2.1.4.21.1.10
ipRouteMask OBJECT-TYPE                  1.3.6.1.2.1.4.21.1.11
ipRouteMetric5 OBJECT-TYPE               1.3.6.1.2.1.4.21.1.12
ipRouteInfo OBJECT-TYPE                  1.3.6.1.2.1.4.21.1.13
```

```
ipNetToMediaTable OBJECT-TYPE           1.3.6.1.2.1.4.22
ipNetToMediaEntry OBJECT-TYPE           1.3.6.1.2.1.4.22.1
ipNetToMediaIfIndex OBJECT-TYPE         1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress OBJECT-TYPE     1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress OBJECT-TYPE      1.3.6.1.2.1.4.22.1.3
ipNetToMediaType OBJECT-TYPE            1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards OBJECT-TYPE           1.3.6.1.2.1.4.23
icmpInMsgs OBJECT-TYPE                  1.3.6.1.2.1.5.1
icmpInErrors OBJECT-TYPE                1.3.6.1.2.1.5.2
icmpInDestUnreachs OBJECT-TYPE          1.3.6.1.2.1.5.3
icmpInTimeExcds OBJECT-TYPE             1.3.6.1.2.1.5.4
icmpInParmProbs OBJECT-TYPE             1.3.6.1.2.1.5.5
icmpInSrcQuenchs OBJECT-TYPE            1.3.6.1.2.1.5.6
icmpInRedirects OBJECT-TYPE             1.3.6.1.2.1.5.7
icmpInEchos OBJECT-TYPE                 1.3.6.1.2.1.5.8
icmpInEchoReps OBJECT-TYPE              1.3.6.1.2.1.5.9
icmpInTimestamps OBJECT-TYPE            1.3.6.1.2.1.5.10
icmpInTimestampReps OBJECT-TYPE         1.3.6.1.2.1.5.11
icmpInAddrMasks OBJECT-TYPE             1.3.6.1.2.1.5.12
icmpInAddrMaskReps OBJECT-TYPE          1.3.6.1.2.1.5.13
icmpOutMsgs OBJECT-TYPE                 1.3.6.1.2.1.5.14
icmpOutErrors OBJECT-TYPE               1.3.6.1.2.1.5.15
icmpOutDestUnreachs OBJECT-TYPE         1.3.6.1.2.1.5.16
icmpOutTimeExcds OBJECT-TYPE            1.3.6.1.2.1.5.17
icmpOutParmProbs OBJECT-TYPE            1.3.6.1.2.1.5.18
icmpOutSrcQuenchs OBJECT-TYPE           1.3.6.1.2.1.5.19
icmpOutRedirects OBJECT-TYPE            1.3.6.1.2.1.5.20
icmpOutEchos OBJECT-TYPE                1.3.6.1.2.1.5.21
icmpOutEchoReps OBJECT-TYPE             1.3.6.1.2.1.5.22
icmpOutTimestamps OBJECT-TYPE           1.3.6.1.2.1.5.23
icmpOutTimestampReps OBJECT-TYPE        1.3.6.1.2.1.5.24
icmpOutAddrMasks OBJECT-TYPE            1.3.6.1.2.1.5.25
icmpOutAddrMaskReps OBJECT-TYPE         1.3.6.1.2.1.5.26
tcpRtoAlgorithm OBJECT-TYPE             1.3.6.1.2.1.6.1
tcpRtoMin OBJECT-TYPE                   1.3.6.1.2.1.6.2
tcpRtoMax OBJECT-TYPE                   1.3.6.1.2.1.6.3
tcpMaxConn OBJECT-TYPE                  1.3.6.1.2.1.6.4
tcpActiveOpens OBJECT-TYPE              1.3.6.1.2.1.6.5
tcpPassiveOpens OBJECT-TYPE             1.3.6.1.2.1.6.6
tcpAttemptFails OBJECT-TYPE             1.3.6.1.2.1.6.7
tcpEstabResets OBJECT-TYPE              1.3.6.1.2.1.6.8
tcpCurrEstab OBJECT-TYPE                1.3.6.1.2.1.6.9
tcpInSegs OBJECT-TYPE                   1.3.6.1.2.1.6.10
```

```
tcpOutSegs OBJECT-TYPE                  1.3.6.1.2.1.6.11
tcpRetransSegs OBJECT-TYPE              1.3.6.1.2.1.6.12
the TCP Connection table                1.3.6.1.2.1.6.13
tcpConnEntry OBJECT-TYPE                1.3.6.1.2.1.6.13.1
tcpConnState OBJECT-TYPE                1.3.6.1.2.1.6.13.1.1
tcpConnLocalAddress OBJECT-TYPE         1.3.6.1.2.1.6.13.1.2
tcpConnLocalPort OBJECT-TYPE            1.3.6.1.2.1.6.13.1.3
tcpConnRemAddress OBJECT-TYPE           1.3.6.1.2.1.6.13.1.4
tcpConnRemPort OBJECT-TYPE              1.3.6.1.2.1.6.13.1.5
tcpInErrs OBJECT-TYPE                   1.3.6.1.2.1.6.14
tcpOutRsts OBJECT-TYPE                  1.3.6.1.2.1.6.15
udpInDatagrams OBJECT-TYPE              1.3.6.1.2.1.7.1
udpNoPorts OBJECT-TYPE                  1.3.6.1.2.1.7.2
udpInErrors OBJECT-TYPE                 1.3.6.1.2.1.7.3
udpOutDatagrams OBJECT-TYPE             1.3.6.1.2.1.7.4
udpTable OBJECT-TYPE                    1.3.6.1.2.1.7.5
udpEntry OBJECT-TYPE                    1.3.6.1.2.1.7.5.1
udpLocalAddress OBJECT-TYPE             1.3.6.1.2.1.7.5.1.1
udpLocalPort OBJECT-TYPE                1.3.6.1.2.1.7.5.1.2
egpInMsgs OBJECT-TYPE                   1.3.6.1.2.1.8.1
egpInErrors OBJECT-TYPE                 1.3.6.1.2.1.8.2
egpOutMsgs OBJECT-TYPE                  1.3.6.1.2.1.8.3
egpOutErrors OBJECT-TYPE                1.3.6.1.2.1.8.4
egpNeighTable OBJECT-TYPE               1.3.6.1.2.1.8.5
egpNeighEntry OBJECT-TYPE               1.3.6.1.2.1.8.5.1
egpNeighState OBJECT-TYPE               1.3.6.1.2.1.8.5.1.1
egpNeighAddr OBJECT-TYPE                1.3.6.1.2.1.8.5.1.2
egpNeighAs OBJECT-TYPE                  1.3.6.1.2.1.8.5.1.3
egpNeighInMsgs OBJECT-TYPE              1.3.6.1.2.1.8.5.1.4
egpNeighInErrs OBJECT-TYPE              1.3.6.1.2.1.8.5.1.5
egpNeighOutMsgs OBJECT-TYPE             1.3.6.1.2.1.8.5.1.6
egpNeighOutErrs OBJECT-TYPE             1.3.6.1.2.1.8.5.1.7
egpNeighInErrMsgs OBJECT-TYPE           1.3.6.1.2.1.8.5.1.8
egpNeighOutErrMsgs OBJECT-TYPE          1.3.6.1.2.1.8.5.1.9
egpNeighStateUps OBJECT-TYPE            1.3.6.1.2.1.8.5.1.10
egpNeighStateDowns OBJECT-TYPE          1.3.6.1.2.1.8.5.1.11
egpNeighIntervalHello OBJECT-TYPE       1.3.6.1.2.1.8.5.1.12
egpNeighIntervalPoll OBJECT-TYPE        1.3.6.1.2.1.8.5.1.13
egpNeighMode OBJECT-TYPE                1.3.6.1.2.1.8.5.1.14
egpNeighEventTrigger OBJECT-TYPE        1.3.6.1.2.1.8.5.1.15
egpAs OBJECT-TYPE                       1.3.6.1.2.1.8.6
the Transmission group                  1.3.6.1.2.1.10
the SNMP group                          1.3.6.1.2.1.11
```

```
snmpInPkts OBJECT-TYPE                  1.3.6.1.2.1.11.1
snmpOutPkts OBJECT-TYPE                 1.3.6.1.2.1.11.2
snmpInBadVersions OBJECT-TYPE           1.3.6.1.2.1.11.3
snmpInBadCommunityNames OBJECT-TYPE     1.3.6.1.2.1.11.4
snmpInBadCommunityUses OBJECT-TYPE      1.3.6.1.2.1.11.5
snmpInASNParseErrs OBJECT-TYPE          1.3.6.1.2.1.11.6
snmpInTooBigs OBJECT-TYPE               1.3.6.1.2.1.11.8
snmpInNoSuchNames OBJECT-TYPE           1.3.6.1.2.1.11.9
snmpInBadValues OBJECT-TYPE             1.3.6.1.2.1.11.10
snmpInReadOnlys OBJECT-TYPE             1.3.6.1.2.1.11.11
snmpInGenErrs OBJECT-TYPE               1.3.6.1.2.1.11.12
snmpInTotalReqVars OBJECT-TYPE          1.3.6.1.2.1.11.13
snmpInTotalSetVars OBJECT-TYPE          1.3.6.1.2.1.11.14
snmpInGetRequests OBJECT-TYPE           1.3.6.1.2.1.11.15
snmpInGetNexts OBJECT-TYPE              1.3.6.1.2.1.11.16
snmpInSetRequests OBJECT-TYPE           1.3.6.1.2.1.11.17
snmpInGetResponses OBJECT-TYPE          1.3.6.1.2.1.11.18
snmpInTraps OBJECT-TYPE                 1.3.6.1.2.1.11.19
snmpOutTooBigs OBJECT-TYPE              1.3.6.1.2.1.11.20
snmpOutNoSuchNames OBJECT-TYPE          1.3.6.1.2.1.11.21
snmpOutBadValues OBJECT-TYPE            1.3.6.1.2.1.11.22
snmpOutGenErrs OBJECT-TYPE              1.3.6.1.2.1.11.24
snmpOutGetRequests OBJECT-TYPE          1.3.6.1.2.1.11.25
snmpOutGetNexts OBJECT-TYPE             1.3.6.1.2.1.11.26
snmpOutSetRequests OBJECT-TYPE          1.3.6.1.2.1.11.27
snmpOutGetResponses OBJECT-TYPE         1.3.6.1.2.1.11.28
snmpOutTraps OBJECT-TYPE                1.3.6.1.2.1.11.29
snmpEnableAuthenTraps OBJECT-TYPE       1.3.6.1.2.1.11.30
```

Appendix C. IPv6 MIB Objects

11 IPv6 MIB Objects

11.1.1.1 This section contains a list of IPv6 MIB Objects for a typical Linux device. The RSU is expected to, at a minimum, support these, or similar Objects with corresponding Object Identities.

ipv6Forwarding OBJECT-TYPE	1.3.6.1.2.1.55.1.1.0
ipv6DefaultHopLimit OBJECT-TYPE	1.3.6.1.2.1.55.1.2.0
ipv6Interfaces OBJECT-TYPE	1.3.6.1.2.1.55.1.3.0
ipv6IfTableLastChange OBJECT-TYPE	1.3.6.1.2.1.55.1.4.0
ipv6IfTable OBJECT-TYPE	1.3.6.1.2.1.55.1.5
ipv6IfEntry OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1
ipv6IfIndex OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.1
ipv6IfDescr OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.2
ipv6IfLowerLayer OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.3
ipv6IfEffectiveMtu OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.4
ipv6IfReasmMaxSize OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.5
ipv6IfIdentifier OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.6
ipv6IfIdentifierLength OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.7
ipv6IfPhysicalAddress OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.8
ipv6IfAdminStatus OBJECT-TYPE	1.3.6.1.2.1.55.1.5.1.9
ipv6IfOperStatus OBJECT-TYPE	1.3.6.1.2.1.55.1.10
ipv6IfLastChange OBJECT-TYPE	1.3.6.1.2.1.55.1.5.11
ipv6IfStatsTable OBJECT-TYPE	1.3.6.1.2.1.55.1.6
ipv6IfStatsEntry OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1
ipv6IfStatsInReceives OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.1
ipv6IfStatsInHdrErrors OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.2
ipv6IfStatsInTooBigErrors OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.3
ipv6IfStatsInNoRoutes OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.4
ipv6IfStatsInAddrErrors OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.5
ipv6IfStatsInUnknownProtos OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.6
ipv6IfStatsInTruncatedPkts OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.7
ipv6IfStatsInDiscards OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.8
ipv6IfStatsInDelivers OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.9
ipv6IfStatsOutForwDatagrams OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.10
ipv6IfStatsOutRequests OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.11
ipv6IfStatsOutDiscards OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.12
ipv6IfStatsOutFragOKs OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.13
ipv6IfStatsOutFragFails OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.14
ipv6IfStatsOutFragCreates OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.15
ipv6IfStatsReasmReqds OBJECT-TYPE	1.3.6.1.2.1.55.1.6.1.16

```
ipv6IfStatsReasmOKs OBJECT-TYPE                    1.3.6.1.2.1.55.1.6.1.17
ipv6IfStatsReasmFails OBJECT-TYPE                  1.3.6.1.2.1.55.1.6.1.18
ipv6IfStatsInMcastPkts OBJECT-TYPE                 1.3.6.1.2.1.55.1.6.1.19
ipv6IfStatsOutMcastPkts OBJECT-TYPE                1.3.6.1.2.1.55.1.6.1.20
ipv6AddrPrefixTable OBJECT-TYPE                    1.3.6.1.2.1.55.1.7.0.0
ipv6AddrPrefixEntry OBJECT-TYPE                    1.3.6.1.2.1.55.1.7.1
ipv6AddrPrefix OBJECT-TYPE                         1.3.6.1.2.1.55.1.7.1.1
ipv6AddrPrefixLength OBJECT-TYPE                   1.3.6.1.2.1.55.1.7.1.2
ipv6AddrPrefixOnLinkFlag OBJECT-TYPE               1.3.6.1.2.1.55.1.7.1.3
ipv6AddrPrefixAutonomousFlag OBJECT-TYPE           1.3.6.1.2.1.55.1.7.1.4
ipv6AddrPrefixAdvPreferredLifetime OBJECT-TYPE     1.3.6.1.2.1.55.1.7.1.5
ipv6AddrPrefixAdvValidLifetime OBJECT-TYPE         1.3.6.1.2.1.55.1.7.1.6
ipv6AddrTable OBJECT-TYPE                          1.3.6.1.2.1.55.1.8
ipv6AddrEntry OBJECT-TYPE                          1.3.6.1.2.1.55.1.8.1
ipv6AddrAddress OBJECT-TYPE                        1.3.6.1.2.1.55.1.8.1.1
ipv6AddrPfxLength OBJECT-TYPE                      1.3.6.1.2.1.55.1.8.1.2
ipv6AddrType OBJECT-TYPE                           1.3.6.1.2.1.55.1.8.1.3
ipv6AddrAnycastFlag OBJECT-TYPE                    1.3.6.1.2.1.55.1.8.1.4
ipv6AddrStatus OBJECT-TYPE                         1.3.6.1.2.1.55.1.8.1.5
ipv6RouteNumber OBJECT-TYPE                        1.3.6.1.2.1.55.1.9.0
ipv6DiscardedRoutes OBJECT-TYPE                    1.3.6.1.2.1.55.1.10.0
ipv6RouteTable OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.0
ipv6RouteEntry OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.1.0
ipv6RouteDest OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.1.1
ipv6RoutePfxLength OBJECT-TYPE                     1.3.6.1.2.1.55.1.11.1.2
ipv6RouteIndex OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.1.3
ipv6RouteIfIndex OBJECT-TYPE                       1.3.6.1.2.1.55.1.11.1.4
ipv6RouteNextHop OBJECT-TYPE                       1.3.6.1.2.1.55.1.11.1.5
ipv6RouteType OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.1.6
ipv6RouteProtocol OBJECT-TYPE                      1.3.6.1.2.1.55.1.11.1.7
ipv6RoutePolicy OBJECT-TYPE                        1.3.6.1.2.1.55.1.11.1.8
ipv6RouteAge OBJECT-TYPE                           1.3.6.1.2.1.55.1.11.1.9
ipv6RouteNextHopRDI OBJECT-TYPE                    1.3.6.1.2.1.55.1.11.1.10
ipv6RouteMetric OBJECT-TYPE                        1.3.6.1.2.1.55.1.11.1.11
ipv6RouteWeight OBJECT-TYPE                        1.3.6.1.2.1.55.1.11.1.12
ipv6RouteInfo OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.1.13
ipv6RouteValid OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.1.14
ipv6NetToMediaTable OBJECT-TYPE                    1.3.6.1.2.1.55.1.12.0
ipv6NetToMediaEntry OBJECT-TYPE                    1.3.6.1.2.1.55.1.12.1.0
ipv6NetToMediaNetAddress OBJECT-TYPE               1.3.6.1.2.1.55.1.12.1.1
ipv6NetToMediaPhysAddress OBJECT-TYPE              1.3.6.1.2.1.55.1.12.1.2
ipv6NetToMediaType OBJECT-TYPE                     1.3.6.1.2.1.55.1.12.1.3
ipv6IfNetToMediaState OBJECT-TYPE                  1.3.6.1.2.1.55.1.12.1.4
```

```
ipv6IfNetToMediaLastUpdated OBJECT-TYPE          1.3.6.1.2.1.55.1.12.1.5
ipv6NetToMediaValid OBJECT-TYPE                  1.3.6.1.2.1.55.1.12.1.6
ipv6Notifications      OBJECT IDENTIFIER         1.3.6.1.2.1.55.2
ipv6NotificationPrefix OBJECT IDENTIFIER         1.3.6.1.2.1.55.2.0
ipv6IfStateChange NOTIFICATION-TYPE              1.3.6.1.2.1.55.2.0.1
ipv6Conformance OBJECT IDENTIFIER                1.3.6.1.2.1.55.3
ipv6Compliances OBJECT IDENTIFIER                1.3.6.1.2.1.55.3.1
ipv6Groups      OBJECT IDENTIFIER                1.3.6.1.2.1.55.3.2
ipv6Compliance MODULE-COMPLIANCE                 1.3.6.1.2.1.55.3.2.1
```

Appendix D. Active Message file format

12 Active Message file format

The format for both encoded Store & Repeat Messages and encoded Immediate Forward messages is contained below

# Message File Format
# Modified Date: 04/10/2014
# Version: 0.7
Version=0.7
#
Message Dispatch Items
#
All line beginning with # shall be removed in file sent to radio
#
# Message Type
# Values: SPAT, MAP, TIM, (other message types)
Type=<Type>
#
# Message PSID as a 2 Byte Hex value (e.g. 0x8003)
PSID=<PSID>
#
# Message Priority in the range of 0 (lowest) through 7
Priority=<priority>
#
# Transmission Channel Mode
# Allowed values: CONT, ALT
TxMode=<txmode>

Allowed values: 172, CCH, SCH (note: “CCH” refers to DSRC Channel 178 and SCH refers to the
#operator configured DSRC Service Channel)
TxChannel=<channel>
#
# Transmission Broadcast Interval in Seconds
# Allowed values: 0 for Immediate-Forwarding, 1 to 5 for Store-and-Repeat
TxInterval=<txinterval>
#
Message Delivery (broadcast) start time (UTC date and time) in the form:
# "mm/dd/yyyy, hh:mm”
# Leave value blank if Immediate Forward mode
DeliveryStart=<mm/dd/yyyy, hh:mm>
#
Message Delivery (broadcast) stop time (UTC date and time) in the form:
# "mm/dd/yyyy, hh:mm”
# Leave value blank if Immediate Forward mode
DeliveryStop=<mm/dd/yyyy, hh:mm>
#
# Message Signature/Encryption
Signature=<True\False>
Encryption=<True\False>
#
# Message Payload (encoded according to J2735 or other definition)
Payload=<DSRC message payload>

Appendix E. Example WAVE Service Advertisement (WSA)

13 Example WAVE Service Advertisement (WSA)

13.1 Context

13.1.1.1 Figure 8 indicates the context for the example WSA format, as indicated in IEEE 1609.3-2010.

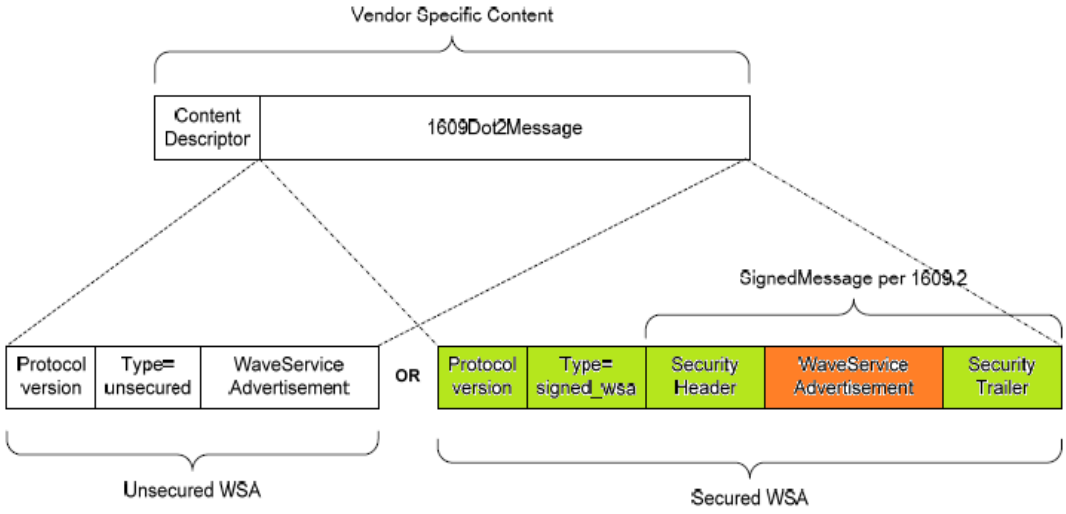

Figure 8. Context for Example WSA Format

13.2 Bytes (Hex)

```
d0 00 00 00 ff ff ff ff ff ff 00 ac 75 af 1f 10 ff ff ff ff ff ff e0 50 7f 00 50
c2 4a 43 01 02 0b 04 53 03 04 01 42 07 67 16 e8 a5 6d 3c 01 00 01 16 20 1f 00 23
1f 00 80 03 1f 00 bf e0 1f 00 bf e1 1f 00 bf f0 1f 00 04 10 97 c0 de 0f 0c 3e de
00 00 00 01 02 99 73 a4 82 47 e3 a9 10 f9 c0 c4 1d 67 3f cb 96 45 af 28 4c cf 1d
cf 7c 5a c7 c6 cd 88 8e 78 5a 01 02 0e 80 81 04 04 01 14 06 0f 11 8d e1 0c c5 38
5a 62 08 fc 66 ff ff ff ff 07 05 55 53 44 4f 54 01 23 1f 01 08 04 53 43 4d 53 09
10 20 01 18 90 11 0e a7 77 00 00 00 00 00 00 00 03 0a 02 3e dc 02 11 b6 00 0c 14
15 01 01 03 07 08 20 01 04 70 e0 fb 99 99 00 00 00 00 00 00 00 00 40 20 01 04 70
e0 fb 99 99 00 00 00 00 00 00 00 01 20 01 04 70 e0 fb 99 99 00 00 00 00 00 00 00
01 0e 06 00 e0 6a 00 9b 30 00 00 ed 21 52 92 c0 ba 00 00 00 ed 21 54 5c 87 69 11
8d e1 0c c5 38 5a 62 08 fc 03 6d 28 65 4e 6a 64 17 25 18 0b 1d c7 c1 6e cd 13 c4
20 61 95 b6 55 ad 28 56 26 aa 17 0e 2c 61 6d 08 38 5b 02 3c ec 41 35 b1 65 f6 21
73 d9 15 b7 3d 65 15 0e 97 58 0c b5 fd 09 b0 9c ee 37 71 a2
```

Note that the lengths provided for the fields in the table are for the example values that are populated and many of the fields are variable length. Values in **green** are taken from the configuration file of a specific installation. Values in **orange** are taken from measurements or circumstances at a specific location. This is from an older version of IEEE 1609.2; the RSU shall conform to the latest version of the IEEE 1609.2 standard (2017).

13.3 Breakdown per IEEE 1609.2

Field name						Length (octets)	Value (hex)	Description
802.11	*Frame Control*					2	D0 00	
	Duration ID					2	00 00	
	Destination MAC Address					6	ff ff ff ff ff ff	
	Source MAC Address					6	00 ac 75 af 1f 10	Device MAC Address
	SSID					6	ff ff ff ff ff ff	
	Sequence Number					2	e0 50	
	Category Code					1	7f	
	OUI					3	00 50 c2	
	Vendor					2	4a 43	
	1609.3	*Content Descriptor*				1	01	
		1609.2	*Protocol version*			1	02	16092Dot2Data Version 2
			Content Type			1	0b	16092DotData 0x0b (11) - signed_wsa
			Security Header	*Signer Type*		1	04	SignerIdentiferType 0x04 – certificate_chain
				Certificate	*Certificate Chain Length*	1	53	
					Version and Type	1	03	Certificate 0x03 – implicit ertificates
					Subject Type	1	04	ToBeSignedCertificate 0x04 - wsa
					Certificate Content Flags	1	01	CertificateContentFlags 0x01 – use_start_validity
					Signer_id	8	42 07 67 16 e8 a5 6d 3c	CertId8 signer id
					Signature_alg	1	01	PKAlgorithm 0x01 - ecdsa_nistp256_with_sha_256
					Scope subject name length	1	00	WsaScope 0x00 – empty name
					Permission type	1	01	ArrayType 0x01 - specified
					Permission length	1	16	
					Permissions list PSID	1	23	PsidPrioritySsp 0x23 – PSID (SCMS)

Permissions list Priority	1	1f	PsidPrioritySsp 0x1f – maximum priority
Service specific permission	1	00	0x00 – zero-length SSP
Permissions list PSID	2	80 03	PsidPrioritySsp 0x80 0x03 – PSID (TIM)
Permissions list Priority	1	1f	PsidPrioritySsp 0x1f – maximum priority
Service specific permission	1	00	0x00 – zero-length SSP
Permissions list PSID	2	bf e0	PsidPrioritySsp 0xbf 0xe0 – PSID (SPaT)
Permissions list Priority	1	1f	PsidPrioritySsp 0x1f – maximum priority
Service specific permission	1	00	0x00 – zero-length SSP
Permissions list PSID	2	bf e1	PsidPrioritySsp 0xbf 0xe1 – PSID (General IP)
Permissions list Priority	1	1f	PsidPrioritySsp 0x1f – maximum priority
Service specific permission	1	00	0x00 – zero-length SSP
Permissions list PSID	2	bf f0	PsidPrioritySsp 0xbf 0xe1 – PSID (MAP)
Permissions list Priority	1	1f	PsidPrioritySsp 0x1f – maximum priority
Service specific permission	1	00	0x00 – zero-length SSP
Region type	1	04	RegionType 0x04 - none
Expiration time	4	10 97 c0 de	Time32 - 0x10 0x97 0xc0 0xde = 00:00:00 27 Oct 2012 UTC
Start validity	4	0f 0c 3e de	Time32 – 0x0f 0x0c 0x3e 0xde = 00:00:00 01 Jan 2012 UTC
CRL series	4	00 00 00 01	CrlSeries
EccPublicKey type	1	02	EccPublicKeyType 0x02 – compressed_lsb_y_0
x	32	99 73 a4 82 47 e3 a9 10 f9 c0 c4 1d 67 3f cb 96 45 af 28 4c cf 1d cf 7c 5a c7 c6 cd 88 8e 78 5a	
Permission Indices length	1	01	
Permission indices	2	01	SSP of services 0x01 defined in Permissions matrix are applicable (in this case PSID 23; SCMS

				TbsDataFlags	1	0e	TbsDataFlags 0x0e – use_generation_time, expires, and use-location
				WSA data length	2	80 81	0x80 0x81 = 129 bytes
				WSA data		See below	

Field name					Length (octets)	Value (hex)	Description
802.11	1609.2	Security Trailer	*Generation time*		8	00 00 ed 21 52 92 c0 ba	Time64WithConfidece -
			Confidence		1	00	0x00 – full confidence
			Expiration time		8	00 00 ed 21 54 5c 87 69	Time64-
			Generation Location latitude		4	11 8d e1 0c	
			Longitude		4	c5 38 5a 62	
			Elev.		2	08 fc	
			Signature	EccPublicKey type	1	03	EccPublicKey 0x03 Compressed_lsb_y_1
				x	32	6d 28 65 4e 6a 64 17 25 18 0b 1d c7 c1 6e cd 13 c4 20 61 95 b6 55 ad 28 56 26 aa 17 0e 2c 61 6d	
				s	32	08 38 5b 02 3c ec 41 35 b1 65 f6 21 73 d9 15 b7 3d 65 15 0e 97 58 0c b5 fd 09 b0 9c ee 37 71 a2	
		CRC					

13.4 Breakdown per IEEE 1609.3

Field name			Length (octets)	Value (hex)	Description
WSA Header	*WAVE Version/Change Count*		1	04	WAVE Version = 1 (6 bits) Change Count = 0 (2 bits) 0x04 = 0b(000001)(00) Note: Rules for
	WSA Header extension fields *(Optional and for information purposes only)*	*Transmit Power Used*	3	04 01 14	WAVE Element ID = 4 Length = 1 20 dBm Note: Power level for WSA set to achieve desired range.
		3DLocationAndConfidence	17	06 0f 11 8d e1 0c c5 38 5a 62 08 fc 66 ff ff ff ff	WAVE Element ID = 6 Length = 15 latitude (4 octets): +29.451086 ° longitude (4 octets): -98.616259 ° elevation (2 octets): +230m position confidence (4 bits): 6 = 10 m elevation confidence (4 bits): 6 = 10 m positional accuracy (4 octets): 'unavailable' Note: Set with information from the RSU's GPS receiver.
		Advertiser Identifier	7	07 05 55 53 44 4f 54	WAVE Element ID = 7 Length = 5 ASCII content: '**USDOT**' Note: Above is an example. Device makers can use their own character strings at their discretion.

Service Info					
	Service Info WAVE element ID		1	01	per Annex E
	Provider Service Identifier		1	23	PSID: **0x23**
	ServicePriority		1	1f	priority: **31**
	Channel Index		1	01	1st set
		Provider Service Context	6	08 04 53 43 4d 53	WAVE Element ID = 8 Length = 4 ASCII content: '**SCMS**'

	Service Info extension fields	*IPv6 Address*	18	09 10 20 01 18 90 11 0e a7 77 00 00 00 00 00 00 00 03	WAVE Element ID = 9 Length = 16 SCMS server IP address 2001:1890:110e:a777::3
		Service Port	4	0a 02 3e dc	WAVE Element ID = 10 Length=2 port=16092
Channel Info	*Channel Info WAVE element ID*		1	02	per Annex E
	Operating Class		1	11	Operating Class: 17
	Channel Number		1	b6	channel: 182
	Adaptable		1	00	0: fixed
	DataRate		1	0c	Data Rate: 6 Mb/s
	Transmit Power Level		1	14	20 dBm Note: Power level for Service Channel transmissions set to achieve range goal.
	Channel Info extension fields	*Channel access*	3	15 01 01	WAVE Element ID = 21 Length = 1 1: alternating access

WAVE Routing Advertisement	*WRA WAVE element ID*		1	03	per Annex F
	Router Lifetime		2	07 08	1800 s
	IpPrefix		16	20 01 04 70 e0 fb 99 99 00 00 00 00 00 00 00 00	2001:0470:e0fb:9999::0000
	Prefix Length		1	40	64 bits
	Default Gateway		16	20 01 04 70 e0 fb 99 99 00 00 00 00 00 00 00 01	RSU IP address 2001:0470:e0fb:9999:: 1
	Primary DNS		16	20 01 04 70 e0 fb 99 99 00 00 00 00 00 00 00 01	2001:0470:e0fb:9999:: 1
	WRA Extension Fields	*Gateway MAC Address*	8	0e 06 00 e0 6a 00 9b 30	WAVE Element ID = 14 Length = 6 00:e0:6a:00:9b:30

Appendix F. Definitions

14 Definitions

14.1.1.1 Table 6 below lists the definitions of key terms in the system requirements.

Table 6. Definitions

ReqID	Term	Description
8.1.1.10	Time of day	NYC CVPD system operating hours
4.4.1.34 5.1.1.3	Warning	Notification from the ASD to the driver once the ASD determines that the application threshold has been exceeded and violation or crash is imminent.
3.2.1.2 3.4.12.4 4.4.1.34	Alert	Trigger generated by the once the ASD determines that the application threshold has been exceeded. Once the alert is triggered, the ASD generates the corresponding warning to the driver.
3.4.3.9	Time period	Amount of time needed by the RSU to forward the PDU based on its PSID.
4,4,1,34	Advise, advisory	Initial notification from the ASD to the driver once the ASD determines that the application threshold will exceed and violation or crash is likely to occur.
4.10.1.4 - 4.10.1.6 5.1.1.3	Zone	Pre-defined radius around a point of interest (e.g. bus stop) stored in the MAP message.
Appendix I, Section l3.3	Rotating 5 minute log of raw data	• The event log entries are expected to be recorded at the frequency of the available data or 10 Hz, whichever is less. • For Example, SPaT messages may occur at 10 Hz while MAP messages may occur at 2 Hz, thus the number of each type will vary. • Clarification: Measurements shall be recorded whenever they change or at 1 second intervals, whichever is shorter. Each message received (BSM, SPaT, MAP, TIM, RTCM) shall be recorded regardless of whether the data changes or not and replace the oldest data as new data is acquired.
4.7.5.7 4.7.5.11	Log entry	Collection of stored event logs in the ASDs
Appendix I, Section l3.3	Event record	Collection of BSMs generated by the ASDs before and after the alert is triggered.

Appendix G. DSRC Devices

15 DSRC Devices

15.1.1.1 Table 7 below identifies the details of each DSRC channel to be used in the NYC CVPD system infrastructure. The output level for all channels and messages shall be configurable by message type and channel.

Table 7. DSRC Channel Assignment

DSRC Channel	Purpose	Dominant Direction of exchanges
172	For transmission of the SPaT, MAP, BSM, and RTCM messages	V to V
174	Service channel for WAVE Short Message Protocols (WSMP) that indicate OTA software updates and application parameter changes and provide SCMS access Also IPv6	I to V
176	Service channel for WAVE Short Message Protocols (WSMP) that indicate OTA uploading of event and operations log information - access Also IPv6	V to I
178	Control channel for WAVE Service Advertisements that announce the device supports specific additional services for PED applications, parameter changes, OTA software updates, credential acquisition, and uploading of log files collected	I to V
180	Service channel for WAVE Short Message Protocols (WSMP) that indicate OTA uploading of event and operations log information - access Also IPv6	V to I
182	Service channel for WAVE Short Message Protocols (WSMP) that indicate OTA software updates and application parameter changes and provide SCMS access Also IPv6	I to V
184	Not Used for the Current NY Project; however, the radios shall be able to use this channel in the future for additional ASD applications such as emergency vehicle warnings.	V to V/I

15.1.1.2 Table 8 below describes the potential device fail modes in the NYC CVPD system.

Table 8. Device Fail Modes (Preliminary)

Fail Mode	Description
Mechanical	Corrosion, shock
Electrical	Electrostatic discharge, short circuit
Location Accuracy Loss	Device's location accuracy estimates exceeds the minimum performance ranges established by standards.
Certificates Unavailable	The device has been refused additional operational certificates.

Appendix H. Software Image Download Mechanisms for NYC CVPD

H.1 Introduction

1 New York City is working with its consultants to develop a generalized approach for secure over-the-air software updates that preserves the device anonymity. The following is a preliminary design; it is the intent of NYCDOT to work with the selected vendors to ensure interoperable operation while preserving the authenticity of the individual vendor's product software and the integrity of their ASD.

2 One of the issues with the NYC project is the need to retain the ability to update the firmware and to modify or tune the applications to meet the needs of the dense urban environment while continuing to install the field devices. This will require that the vendor establish and verify a stable and reliable in-vehicle "platform" which can be reliably modified as the City and the vendor gain experience with the nature of the driver interface, accuracy of the location, and utility of the various safety applications. The following mechanism is incomplete at this writing, but will be updated as we work with the vendor during the early phases of the design.

3 This current version is identified as draft 0.1, 2017/1/7)

H.2 General Flow

1. The supplier provides IDs for the devices that are globally unique.
   a. If necessary this is done by having NYC provide each supplier with a supplier ID that prefixes the device ID.
2. The supplier creates a firmware image for installation.
   a. The image must be suitable for a system where download and installation happen separately, i.e. authentication and other validation of the image must be able to be carried out without any two-way communications with the image provider.
      i. Any authentication of the image must be provided as part of the file
      ii. The supplier may encrypt the image for its devices, but this must be carried out as part of the production of the image.
      iii. The image may be encrypted for a subset of devices, for example to ensure that firmware images aren't provided to. In this case the supplier should use some approach to minimize the overhead due to encryption for this subset, such as Fiat-Naor broadcast encryption techniques; the approach used is however out of scope for this specification.
3. The supplier provides the image to the TMC (NYC) using a secure connection.
4. The TMC provides the image to the RSUs that support software update
5. The RSUs create a WAVE Service Advertisement (WSA) that indicates that software update services are available on a specified service channel.
6. The distribution protocol outlined in the next section is carried out. At a high level:
   a. The WSA indicates that software update is available on a specified service channel by the inclusion of the New York City Pilot Deployment Software Update PSID in a ServiceInfo. The Provider Service Context (PSC) field is not used.
   b. ASDs channel-switch their non-safety channel radio to the service channel.
   c. Firmware updates are broadcast on the service channel, using network coding to minimize the expected wait times for any device to obtain the full update image no matter when it starts listening or which packets it misses.
      i. Some updates are broadcast all the time; some are broadcast only if requested

ii. In addition to the update image packets, the RSU broadcasts a control packet indicating which update images are available, allowing devices to determine if there is an update for one of their images and, if so, whether they need to request it or just listen.
iii. Requests are not authenticated. This raises the possibility of denial of service attacks but this risk is considered to be low in this version of the system.

d. Devices for which the firmware update is applicable receive the network-coded packets and reassemble them into the original (authenticated and possibly encrypted) image.

7. Having reassembled the image, the device then uses a supplier-determined mechanism to validate and install them.

H.3 Future details to be developed and/or provided

Full details of the protocol will follow. This will include:

- PSID value for the WSA
- Packet format for the control packet and for the image network-coded packet
- Identification of the default network coding technique to use along with specification of any relevant parameters

Appendix I. BSM Related Data Collection

I.1 Introduction

1 The following summarizes the current approach to data collection which the NY team has developed and included the ConOps and requirement documents (Both are available on-line) – and shall be integrated into these RSU and ASD procurement documents. The data collection is divided into 3 general functions: 1) Operations and Maintenance (O&M) data; 2) Mobility data; and 3) Evaluation data collected to support the evaluation of the effectiveness of the CV technology with respect to safety applications – crash prevention and/or reduction in crash severity.

2 The intent of this appendix is to further clarify the data collection scheme and rationale for each such that the ASD and RSU providers can include the necessary software in their production products.

I.2 Existing Conditions and Constraints:

3 There are ~12,300 signalized intersections connected to the TMC via a cellular wireless/wireline network (NYCWiN) that provides real time data to the TMC; the system uses dynamically configured exception based reporting (NTCIP 1103) and polled data retrieval.

4 Past mechanisms for the physical collection of CV data (i.e. removable storage) are not practical due to the fleet size and costs. All data must be collected through “casual” OTA communications.

5 All infrastructure ↔ vehicle communications (V2I/I2V) will use DSRC (5.9 GHz); the system shall use one or more service channels to upload all data collected on the vehicles and download applications and operating parameters.

6 The backhaul bandwidth is limited – whether it is on NYCWiN (New York City’s private shared cellular network) or common carrier (3G/4G/LTE); we have a dense collection of field devices and are planning for a relatively dense collection of interacting vehicles. There are variable latencies and bandwidth limitations – as well as the fact that this is a shared media with other users (i.e. police and fire), including video. Thus, there are latencies and delays on the order of 200-750 ms on average, with significant deviations under “busy” conditions for all backhaul exchanges.

7 All of our pilot project vehicles are “fleet” owned – and hence return to a “barn” typically once per day – sometimes several times per day (taxi shift change). Note that we estimate the average vehicle runtime (ignition on, engine running) is between 13-14 hours per day due to the nature of the fleet operations.

8 Our fleet is expected to grow from an initial 8,000 vehicles to - - - ? The system will start with ~370 RSUs and we may add additional RSUs in the future for other services.

9 There are traffic operational restrictions [in the City] including the 25 mph speed limit (most all surface streets) and right-turn-on-red (RTOR) prohibition which are not common in other parts of the US and may impact the driver behavior, especially for individuals not familiar with the NYC environment and traffic laws.

10 NYC is a litigious place – and data collected can and will be subpoenaed and subject to Freedom of Information Act (FOIA) requests for all sorts of tort cases and "investigations" and hence, it must be aggregated, normalized, and obfuscated before it is stored in any location within NYC – except for NYU, where access is very limited and is protected by an IRB. It is important to note that time and location data (BSM) has the potential to become personally identifiable information (PII) if it can be tied to other records such as police reports and used in legal, disciplinary, and insurance proceedings, hence, all such data will be immediately processed as noted.

I.3 Data Needs and approaches:

I.3.1 O & M Data

1 **RSU**: The system needs to be able to determine the range (i.e. distance) over which RSUs are transmitting to, and receiving data from vehicles in an automated fashion. The monitoring process needs to alert maintenance personnel when there is suspect equipment such as the following examples:

- When the apparent range of valid communications is substantially different from the established norm [for the specific location].
- When the TMC is unable to establish communications with the RSU
- When the TMC receives operations log information from the RSU that indicates [software] process or equipment failure.

2 Note that this is the same approach used with the traffic signals: the system monitors field operation; it tries to "repair" selected problems by re-initializing communications, and sends alerts to the system operators when the failure either persists (e.g. communications failure) or is of a "dangerous" type (fault flash, "stuck signal").

3 **Collecting data on the ASD**: the first time an ASD receives [and authenticates] a SPaT message from a specific RSU, the ASD records its own BSM contents (location, time, speed, etc.), the SPaT message content [from the subject RSU], and the RF power level of the received signals into a "first" and "last" entry of an "ASD encounter record". It continues to receive and replace the "last" entry until a configurable timeout occurs in which case it adds this "ASD encounter record" to the RF "ASD sighting RSU log".

4 The ASD will also record the first and last MAP message it receives from each RSU in a similar fashion (recording the content of the MAP message and its own BSM message) and continue to replace the "last" entry until a configurable timeout occurs in which case it adds this "encounter record" to the RF "ASD sighting RSU log".

5 The ASD performs this same action for each separate [new] RSU encountered, for both the SPaT and MAP messages so that we can develop an effective communications radius for the RSU for each message type – as determined by the ASD.

6 **Uploading the data:** Whenever the ASD encounters an RSU that collects the "ASD sighting RSU log" using a properly signed WSA, it uploads the data on the identified service channel to the RSU where it is forwarded to the TMC when backhaul bandwidth is available. Once the data is received and authenticated at the TMC, the TMC will initiate an acknowledgement to the ASD (through the RSU) which then purges the data. Note that the ASD must continue to record (log) this data – which must be buffered so that no data is lost and only complete records are transmitted; note that the "ASD

encounter record" is not considered complete for each encounter until the timeout has occurred. The software must cover the various race conditions so that no data is corrupted or lost and data collection is continuous.

7 Comment: We expect to retrieve this data at selected "support" locations – but have the ability (through our OTA update process) to activate this data collection capability at any RSU.

8 All ASDs will include this feature – but it can be configured as indicated above and it can also be activated and de-activated and the software can be loaded and/or updated using the OTA configuration management. Note that the ASD produced "ASD sighting RSU log" must contain the serial number of the ASD in the header such that it can be analyzed and correlated with other O&M data. Therefore, the "ASD sighting RSU log" will be encrypted on the ASD when stored and transmitted in encrypted fashion to the TMC where it will be decrypted and "consumed" to perform the O&M analysis after which it will be destroyed.

9 The BSM data recorded in the vehicle includes the temporary vehicle ID which will be used to match the data received by the RSU as identified below.

10 The exact mechanism to retrieve the log data is still under development and a preliminary approach is presented in the previous appendix.

11 **ASD**: We need to be able to determine if the ASDs are transmitting and receiving data within a minimum range of the device in an automated fashion. The monitoring process needs to alert maintenance personnel when there is suspect equipment.

12 **Collecting data on the RSU:** The RSU collects the first and last BSM it receives and authenticates (along with the RF level) from each "new" & unique vehicle it sees. The logging is similar to the RSU discussion above; however, in this case the RSU includes the BSM contents and the time stamp along with the RF level of the BSM received. The central system can then match the temporary Vehicle Identification (VID) contained in the recorded BSM and match it with a BSM from a vehicle's "ASD sighting RSU log" (time will not be identical – but likely close, however the vehicle ID will match). Thus by matching up these two data flows (not in real time), the TMC can confirm the RF communications pattern around each vehicle and RSU – with sufficient statistical data to determine if the RSU is operating within accepted criteria and if the ASD/Vehicle system is operating within accepted criteria. We should also be able to construct a history and look for significant changes to alert the TMC operators to the need for proactive maintenance (e.g. foliage, obstructions). This file is the RF "RSU Sighting ASD Log" and each record is an "RSU Encounter Record".

13 These log file entries contain only the temporary vehicle ID and only for initial and final contact – and cannot really be used for any tracking or monitoring of the actual vehicle; however, we are planning to encrypt the data at the RSU such that the file contents when transmitted over-the-air or over the network it is not visible to anyone. Once the data has been analyzed, it is destroyed.

14 **V2V Encounters**: We wanted to determine if and where equipped vehicles encounter each other wherever they happen to be. We feel this will provide interesting information as to the number of encounters outside the instrumented areas since the taxis can go

anywhere within the City and sometimes the other fleets dispatch vehicles to other locations within the City.

15 Our Approach: Each ASD will keep a log of the other vehicle's BSM and its own BSM at their closest point of encounter. The time-out for "new encounters" will be configurable – but the desire is to simply see where they seem to encounter each other during the life of the project. We do not know if this is statistically interesting – and we recognize conditions such as vehicles paralleling each other that could cause confusing data for some situations – hence, it is only for determining the breadth of their dispersion and coverage. The host vehicle's ASD serial number is only included in the uploaded log header which must be encrypted prior to transmission and can only be requested with the proper authorization keys. This is classified as the "V2V Encounter Log" and each record will contain 2 BSMs (host vehicle and target vehicle) for each unique encounter. We also note that when the vehicles change ID's this will appear as a new encounter [for both vehicles] in the log entry, but because the logs contain the serial number of the ASD, such duplicates can be detected in the post processing.

16 This is called the "V2V Encounter Log" and each record is a "V2V Encounter Record".

17 In addition, to the data listed above, each ASD includes a "failure" or "anomaly" log for any and all "exception" conditions encountered by the software.

18 Our Approach: This data is collected in a separate "ASD Operations Log" by the software platform within the ASD and will be uploaded when the ASD receives a WSA from the RSU to provide this log data. This is expected to be supported only at the "barn" entry or "service" point RSUs so that we can determine if there are issues with the application or operating (Platform) software.

19 We expect this log to be continuous and overwrite the oldest entries if or when it becomes full. The number of entries is undetermined but needs to cover anomalies for at least one month. This will also include each "trip" start and end [time]: trip start is when the ignition switch is turned on and the trip end occurs when the ignition switch is turned off.

20 Note that when uploading logs, the ASD must not change its address until this exchange is complete or times out. In addition, the unit serial number will be included in this log – so we can determine the specific vehicle needing repairs. Hence, this log will be transmitted in an encrypted manner and will be decrypted at the TMC where it will be processed to determine operating statistics and maintenance issues and destroyed once analysis is complete.

21 The exact records to be stored in this log are still under development but are expected to include software "exceptions" or errors, detected hardware errors, GPS acquisition and loss of GPS lock, authentication errors, memory errors, alert failures (audio input does not match audio output), start and end trip times, certificate updates, software updates, application parameter changes, when the ASD can no longer transmit BSMs due to either time or location accuracy, etc... Each log entry will include a time stamp and, where appropriate, a location entry (latitude, longitude, elevation).

I.3.2 Mobility Data

1 The hardware (ASD & RSU) shall collect 3 types of mobility data using BSM message content. The first type is "bread crumb" data that will be collected by the RSU and is

intended for local use (at the intersection/RSU) and will not be transmitted to the TMC due to bandwidth limitations and hence is not available for use by others; this data may be used for future I-SIG enhancements – but will be disabled for the pilot project.

2 The second type is “bread crumb” data that shall be collected by the ASD and will be used for selected mobility measurements for project evaluation.

3 The third type of data will be collected to support travel time computations for the traffic control system; in this instance, the data collected (by the RSU) will be limited and used to develop link travel times to compare the Connected Vehicle (CV) data with the data currently being collected by the RFID toll tag readers strategically placed for the Mid-town in motion (MIM) adaptive control area.

4 All three data collection operations are described below.

5 **ASD Data** – ”bread crumb” data collection: The procurement specifications for the ASD require this feature – and it will be controlled and configured OTA for mobility evaluation purposes and for future use in I-SIG applications which are not part of the current CV Pilot project. The data collection intervals shall be configurable and may use the PDM/PVD messages to configure and collect this data (this will be discussed with the vendor and we may use the PDM to configure the collection parameters – but it will need to be modified to manage all of the various logs). The alternative is to use the OTA software download and parameter update to establish a specific data collection scheme and configure the interval and distance traveled (or both) record criteria for each entry. This is not intended to be 10 Hz data and the data collection interval will be configurable based on distance traveled or time traveled or both - whichever occurs first. This is the “Probe data log” and each entry will consist of the vehicle location (scaled for NYC), heading, speed, and path history.

6 Whenever the “event” mechanism (see ASD Procurement Specification for NYC CVPD) is triggered, all BSM data collected during the previous XX configurable minutes will be purged to avoid the possibility of compromising PII. We may not require the implementation of the PVD and PDM messages due to the wide range of possible configuration options, but that is still under consideration and will be discussed with the vendors. This BSM data will be encrypted in the vehicle and incorporate the ASD serial number in the log header; it will be sent to the RSU when it [the ASD] receives the appropriate authenticated WSA with directions as to which channel, etc. and where to send this data. The target for this data may be the RSU itself (an analysis application) or the TMC. If it is the TMC, the RSU will be handling this communications in a store and forward fashion due to the potential size of this file and the latencies and limitations of NYCWiN.

7 The data recording will be buffered and continuous on the ASD so that no data is lost by the infrequent transmissions. Note that in the CV instrumented section of the City, this data will be relatively short, but because the instrumented infrastructure is a very small part of the vehicle range, we must be prepared to receive relatively large files from vehicles that have traveled outside the instrumented area.

8 The data shall include configurable portions of the BSM data and the temporary vehicle ID and “rotating” certificates; the only rule is that the vehicle cannot change its ID during its exchange until it receives the request to purge the data (or times out). Techniques will be employed (sequence numbers and time-outs) to manage overlaps and anomalies

without loss of data where possible. This data may be used at the TMC for the purpose of measuring segment travel times where there is no instrumentation. Any data received at the TMC will be purged upon processing. Thus the data cannot be used to link the vehicle segments together; this data will not be passed to the RDE or the SDC/SDW.

9 Note that in the future, this data may be used at the local intersection to determine queue lengths, and other traffic mobility measures, but that is beyond the current scope and budget.

10 **RSU – "bread crumb" non real time data:** This requirement will be included in the RSU specification although this real-time data collection ***will not be used for the current CV project,*** however, it is described here as it will be included in the ASD specification for future use by the City. For this application, the RSU will be receiving BSM data from the vehicles [around the RSU] in real time and transferring selected BSMs received [i.e. within selected ranges] to the TMC at configurable intervals (near real time) as a snapshot of the traffic condition. The frequency of the BSM data collection will be configurable (seconds), and the "packaging" period will be configurable. This data will not be encrypted.

11 **RSU Data - travel time data**: For this application, the RSU will transmit selected vehicle sightings (BSMs) to the TMC where they can be used to develop link travel time information (statistical) even if the certificates and IDs change. This information allows the TMC to "match" vehicle IDs and compute the travel times between RSUs. The data collected using the CV data will be compared with the data collected from the toll tag readers to determine whether the CV data is sufficient so that the City can expand their data collection using CV infrastructure instead of the E-ZPass Toll tag [RFID] readers.

12 For this application, the system does not need to collect every BSM from every vehicle the RSU can hear; it only needs a single BSM for each vehicle it "hears" at the point closest to the center point of the intersection as the vehicle "passes through" the intersection (using the location information in the BSM); since the BSM includes the vehicle location (resolved to an exact location within NYC), heading, speed, and path history, it can provide sufficient information to compute the travel time and identify possible "issues" with the data. Some of the details as to the algorithm to be used to determine which BSM to be used still need to be worked out, but essentially only a single BSM is needed for each vehicle which can be sent in real-time to the TMC for matching to compute the travel times. This potentially reduces the number of possible BSMs for transmission [to the TMC] from 144K Bytes/vehicle to 80 bytes/vehicle. The tuning process will determine a location (or "region") within the intersection that provides the most accurate result based on vehicle speed and intersection geometry; the relative location needs to be consistent such that resolution and accuracy of the calculations are acceptable.

I.3.3 Evaluation Data

1 The New York Project is handling safety oriented "event" data in a very different manner.

2 The ASD contains a continuous, rotating log wherein it temporarily records: its own BSM on a 10 Hz basis, all BSMs for remote vehicles within a configurable distance, all SPaT and MAP messages heard from the nearest RSU (nearest 2 if more than one) and the time stamp. This is a five minute rotating buffer that replaces the oldest data as new data is acquired.

3 When a configured “event” is detected, the data collected immediately prior to the event (for a configurable amount of time) is copied from this temporary log to the “event record” and the data collected during and after the event for a configurable amount of time is added to the record. The record is then closed and encrypted and stored in the “Vehicle event log” which will be uploaded with the device serial number [in the header] when it encounters an RSU which broadcasts a properly authorized request [WSA] for this data. Once the RSU has uploaded the data, it forwards it to the TMC where it can be authenticated, decrypted, and used for the evaluation software – after which it is normalized, obfuscated, serial number stripped, and becomes available for others. Note that once the data has been properly received at the TMC, the TMC will notify the ASD to purge the log data.

4 Note that a configured “event” can be an alert, a silent alert (i.e. for a vehicle that is not notifying the driver because it is a control group or because of system testing), or it can be a specific change in one of the internal monitors such as the CAN bus (e.g. “hard” turn, sudden break, yaw rate).

5 Techniques shall be employed (sequence numbers and time-outs) to manage overlaps and anomalies without loss of data where possible.

6 Note: We are still in the design phase of specifying the ASD and RSU applications and operation, but the above captures the nature of the data we are collecting from our vehicles and the infrastructure.

7 This data is sufficient to evaluate the communications perimeter for the RSU and ASDs and to collect segment travel times for the mobility data – which is in our concept of operations document.

8 This approach will provide data about the occurrence of events of all types experienced by the vehicles based on configured parameters or alerts whether silent or audible to the driver

Appendix J. Detailed RSU Security Requirements

16 Detailed RSU Security Requirements

16.1 Introduction

The following table has been incorporated into this specification to document all of the security requirements included in the NY CVPD requirements document. It is recognized that this may be more complete than the text and that there may be conflicts between this section and the text above. The bidder shall bring such conflicts or issues to the attention of the City for clarification as required for questions.

ReqTitle	Requirement Text	Justification for the Requirement	Source for Justification
Roadside Unit: platform security	RSUs that are used for any identified usage scenario other than generating alerts for pedestrians crossing against the signal in Pedestrian in Signalized Intersection Warning shall conform to the physical, OS and software security requirements identified in this requirements list by “Device security classes: class 2”	Need to protect the system against devices being hacked	Security Management Operating Concept section 4.15
Roadside Unit: platform security	RSUs that are used to generate alerts for pedestrians crossing against the signal in Pedestrian in Signalized Intersection Warning shall conform to the physical, OS and software security requirements identified in this requirements list by “Device security classes: class 3”. These RSUs may be used for any other usage scenario in the ConOps.	Need to protect the system against devices being hacked	Security Management Operating Concept section 4.15
RSU: Management and configuration	RSUs shall support acting as an SNMPv3 Agent with SNMP messages protected by being sent over TLS per the requirements identified in this requirements list by “SNMP: Agent”	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.3
RSU: Management and configuration	An RSU will be provisioned at manufacturing time with an X.509 certificate with subjectAltName of the form rse-XXXX.cvpd.dot.nyc.gov, where XXXX is a four-hex digit serial number for the RSU, and a lifetime of five years	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.3, 5.2.5, 7.3
RSU: Management and Configuration	The X.509 certificate shall contain a verification key for ECDSA over the NIST p256 curve.	Ensure that devices can be securely managed	

RSU: Management and Configuration	The X.509 certificate may be self-signed or signed by a CA	Ensure that devices can be securely managed	
RSU: Management and configuration	The RSU supplier shall provide the RSU's X.509 certificate along with the RSU.	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.3, 5.2.5, 7.3
RSU: VPN	The RSU shall support establishment of a standard TLS-based VPN with client authentication for communication to the TMC	Ensure end-to-end security for bulk data upload	Security Management Operating Concept section 5.2.4
RSU: VPN	The RSU VPN client shall support the requirements identified in this list by "TLS: Client"	Ensure end-to-end security for bulk data upload	Security Management Operating Concept section 5.2.4
RSU: VPN	All bulk data upload from the RSU to the TMC to support usage scenarios in the ConOps shall be carried out over the VPN	Ensure end-to-end security for bulk data upload	Security Management Operating Concept section 5.2.4
RSU: VPN	The RSU VPN client shall support being provided with an IP address by the server	Ensure end-to-end security for bulk data upload	Security Management Operating Concept section 5.2.4
SNMP: Agent	An SNMPv3 Agent shall support the TLS Transport Model over TCP per RFC 5953		
SNMP: Agent	An SNMPv3 Agent shall support authenticating itself over TLS with an X.509 client certificate and shall support the requirements identified in this requirements list by "TLS: Client".	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.3
SNMP: Agent	An SNMPv3 Agent shall support installation of an X.509 client certificate and private key at initial provisioning time	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.3
SNMP: Agent	An SNMPv3 Agent shall support installation of a whitelist of trustworthy CAs such that only Cas on the whitelist will be trusted.	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.3
SNMP: Agent	An SNMPv3 Agent shall only allow the list of trustworthy Cas to be updated as part of a device reset.	Ensure that devices can be securely managed	Security Management Operating Concept 5.2.3
SNMP: Agent	An SNMPv3 Agent shall only accept tmc.cvpd.dot.nyc.gov as the tmSecurityName	Ensure that devices can be securely managed	
TLS: Client	A TLS Client shall support the requirements identified in this requirements list by "TLS: Common requirements"	Enable secure communications via TLS	Security Management Operating Concept section 5.2.5
TLS: Client	A TLS Client shall support client certificate authentication		

TLS: Client	A TLS Client shall support session renegotiation and shall require the mechanisms specified in RFC 5746 to prevent session renegotiation attacks.		
TLS: Client	A TLS Client shall only carry out client certificate authentication within the context of renegotiating an established session	The client shall not provide its certificate within an initial TLS handshake as that certificate would be provided in the clear and would compromise privacy. Instead the client shall establish a server-authenticated session, and then the server will initiate a renegotiation into a client-authenticated session. NOTE: this is not as necessary for RSUs as for ASDs but enforcing this requirement on both RSUs and ASDs makes server-side operations easier to manage	
TLS: Client	A TLS Client shall support TLS session resumption, configurable timeout to include the following range: 1 hour to 1 week		
TLS: Client	The TLS session resumption timeout value shall be configurable via SNMP and shall support at least the following range: 1 hour to 1 week		
TLS: Client	A TLS Client shall support authenticating itself over TLS with an X.509 client certificate	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.5
TLS: Client	A TLS Client shall support installation of an X.509 client certificate and private key at initial provisioning time	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.5
TLS: Client	A TLS Client shall support installation of a whitelist of trustworthy CAs such that only certificates signed by CAs on the whitelist will be trusted.	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.5
TLS: Client	A TLS Client shall support management of the list of trustworthy CAs via SNMP.	Ensure that devices can be securely managed	Security Management Operating Concept section 5.2.5
RSU: Red Light Violation Warning	The RSU shall support the requirements identified in this requirements list by “RSU: SPaT”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.3

RSU: Red Light Violation Warning	The RSU shall support the requirements identified in this requirements list by “RSU: MAP”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.3
RSU: Red Light Violation Warning	The RSU shall verify received BSMs per IEEE 1609.2 and per the BSM Security Profile of J2945/1 before using them for Red Light Violation Warning. This verification shall meet the requirements identified in this requirements list by “1609.2 verification”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.3
RSU: Red Light Violation Warning	If the RSU detects potential red light violations and stores them it shall strip the identifying data from the relevant BSMs	Protect privacy of drivers	Security Management Operating Concept section 5.3.3
RSU: Red Light Violation Warning	If the RSU detects potential red light violations and stores them it shall store the data encrypted with an encryption key belonging to the TMC per the requirements identified in this requirements list by “Encryption for TMC: Encryption”.	Protect privacy of drivers	Security Management Operating Concept section 5.3.3
RSU: Red Light Violation Warning	A RSU used in Red Light Violation Warning shall support the requirements identified in this requirements list by “Device Security Classes: Class 2”.	Protect receivers from false messages	Security Management Operating Concept 4.3.3
RSU: Speed Compliance	The RSU shall support the requirements identified in this requirements list by “RSU: MAP”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.4
RSU: Speed Compliance	An RSU used in Speed Compliance shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect receivers from false messages	Security Management Operating Concept section 4.4.3
RSU: Oversize Vehicle Compliance	The RSU shall support the requirements identified in this requirements list by “RSU: MAP”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.5
RSU: Oversize Vehicle Compliance	An RSU used in Oversize Vehicle Compliance shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect receivers from false messages	Security Management Operating Concept section 4.5.3
RSU: Emergency Communications and Evacuation Information	The RSU shall support the requirements identified in this requirements list by “RSU: TIM”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.6

RSU: Emergency Communications and Evacuation Information	The RSU shall create WSAs containing the PSID for TIM.	Protect receivers from false messages	Security Management Operating Concept section 5.3.6
RSU: Emergency Communications and Evacuation Information	The RSU shall support the requirements identified in this requirements list by “RSU: WSA”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.6
RSU: Emergency Communications and Evacuation Information	An RSU used in Emergency Communications and Evacuation Information shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect receivers from false messages	Security Management Operating Concept section 4.6.3
RSU: Pedestrian in Signalized Intersection Warning	The RSU shall support the requirements identified in this requirements list by “RSU: SPaT”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.7
RSU: Pedestrian in Signalized Intersection Warning	The RSU shall use SNMPv3 over TLS to receive signed MAP messages for use in Pedestrian in Signalized Intersection Warning from the TMC	Protect receivers from false messages	Security Management Operating Concept section 5.3.7
RSU: Pedestrian in Signalized Intersection Warning	The RSU shall support the requirements identified in this requirements list by “SNMP: Client”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.7
RSU: Pedestrian in Signalized Intersection Warning	The RSU shall verify received BSMs per IEEE 1609.2 and per the BSM Security Profile of J2945/1 before using them for Pedestrian in Signalized Intersection Warning. This verification shall support the requirements identified in this requirements list by “1609.2 verification”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.7
RSU: Pedestrian in Signalized Intersection Warning	RSUs shall verify received PSMs per IEEE 1609.2 and per the PSM Security Profile (to be provided in Phase 2) before using them for Pedestrian in Signalized Intersection Warning. This verification shall meet the requirements identified in this requirements list by “1609.2 verification”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.7

RSU: Pedestrian in Signalized Intersection Warning	If the RSU detects potential pedestrian / vehicle encounters and stores them it shall strip the identifying data from the relevant BSMs	Protect privacy of drivers	Security Management Operating Concept section 5.3.7
RSU: Pedestrian in Signalized Intersection Warning	If the RSU detects potential pedestrian / vehicle encounters and stores them it shall store the data encrypted with an encryption key belonging to the TMC per the requirements identified in this requirements list by "Encryption for TMC: Encryption".	Protect privacy of drivers	Security Management Operating Concept section 5.3.7
RSU: Pedestrian in Signalized Intersection Warning	A RSU used in Pedestrian in Signalized Intersection Warning to send warnings of pedestrians crossing with the signal shall support the requirements identified in this requirements list by "Device Security Classes: Class 2".	Protect receivers from false messages	Security Management Operating Concept section 4.7.3
RSU: Pedestrian in Signalized Intersection Warning	A RSU used in Pedestrian in Signalized Intersection Warning to send warnings of pedestrians crossing against the signal shall support the requirements identified in this requirements list by "Device Security Classes: Class 3".	Protect receivers from false messages	Security Management Operating Concept section 4.7.3
RSU: Mobile Accessible PED-SIG	The RSU shall support the requirements identified in this requirements list by "RSU: SPaT".	Protect receivers from false messages	Security Management Operating Concept section 5.3.8
RSU: Mobile Accessible PED-SIG	The TMC shall support the requirements identified in this requirements list by "RSU: SSM".	Protect receivers from false messages	Security Management Operating Concept section 5.3.8
RSU: Mobile Accessible PED-SIG	The RSU shall use SNMPv3 over TLS to receive signed MAP messages for use in Mobile Accessible PED-SIG from the TMC	Protect receivers from false messages	Security Management Operating Concept section 5.3.8
RSU: Mobile Accessible PED-SIG	The RSU shall support the requirements identified in this requirements list by "SNMP: Client".	Protect receivers from false messages	Security Management Operating Concept section 5.3.8
RSU: Mobile Accessible PED-SIG	RSUs shall verify received SRMs per IEEE 1609.2 and per the SRM Security Profile (to be provided in Phase 2) before using them for Mobile Accessible PED-SIG. This verification shall meet the requirements identified in this requirements list by "1609.2 verification".	Protect receivers from false messages	Security Management Operating Concept section 5.3.8
RSU: Mobile Accessible PED-SIG	If the RSU detects potential pedestrian / vehicle encounters and stores them it shall store the data encrypted with an encryption key belonging to the TMC per the requirements identified in this requirements list by "Encryption for TMC: Encryption".	Protect privacy of drivers	Security Management Operating Concept section 5.3.8

RSU: Mobile Accessible PED-SIG	A RSU used in Mobile Accessible PED-SIG to send warnings of pedestrians crossing with the signal shall support the requirements identified in this requirements list by “Device Security Classes: Class 2”.	Protect receivers from false messages	Security Management Operating Concept section 4.8.3
RSU: ASD Configuration and Update	The RSU shall create WSAs for use in ASD Configuration and Update that advertise a PSID for configuration and update.	Protect receivers from false messages	Security Management Operating Concept section 5.3.9
RSU: ASD Configuration and Update	The RSU shall support the requirements identified in this requirements list by “RSU: WSA”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.9
RSU: ASD Configuration and Update	The RSU shall use SNMPv3 over TLS to receive from the TMC information about new firmware updates or application configuration changes	Protect receivers from false messages	Security Management Operating Concept section 5.3.9
RSU: ASD Configuration and Update	The RSU shall support the requirements identified in this requirements list by “SNMP: Client”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.9
RSU: ASD Configuration and Update	The RSU shall support acting as an IPv6 router to transport IPv6 datagrams from the TMC to the ASD and from the ASD to the TMC.	Enable usage scenario operation	Security Management Operating Concept section 5.3.9
RSU: RSU Configuration and Update	An RSU used in RSU Configuration and Update shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect receivers from false messages	Security Management Operating Concept section 4.9.3
RSU: RSU Configuration and Update	The RSU shall support a secure firmware update method	Preserve security of RSU	Security Management Operating Concept section 5.3.10
RSU: RSU Configuration and Update	The secure firmware update method supported by the RSU shall not require live communication with the supplier, i.e. it shall support a process flow where updated firmware images are provided by the supplier to the TMC and then from the TMC to the RSU.	Preserve security of RSU	Security Management Operating Concept section 5.3.10
RSU: RSU Configuration and Update	The secure firmware update method supported by the RSU shall use cryptographic mechanisms that provide at least 128 bits of security.	Preserve security of RSU	Security Management Operating Concept section 5.3.10
RSU: RSU Configuration and Update	Firmware updates provided from the supplier to the TMC shall not be encrypted.	Preserve transparency as to what is being installed	Security Management Operating Concept section 5.3.10
RSU: RSU Configuratio	The RSU shall use SNMPv3 over TLS to receive from the TMC information about new firmware updates or	Protect receivers from false messages	Security Management Operating Concept section 5.3.10

n and Update	application configuration changes, and to allow the TMC to query it about its configuration status.		
RSU: RSU Configuration and Update	The RSU shall support the requirements identified in this requirements list by “SNMP: Client”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.10
RSU: RSU Configuration and Update	The RSU shall establish a VPN connection to the TMC to download new firmware images.	Protect receivers from false messages	Security Management Operating Concept section 5.3.10
RSU: RSU Configuration and Update	The RSU shall support the requirements identified in this requirements list by “RSU: VPN”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.10
RSU: RSU Configuration and Update	An RSU used in RSU Configuration and Update shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect receivers from false messages	Security Management Operating Concept section 4.10.3
RSU: RSU RF Monitoring	The RSU shall establish a VPN connection to the TMC to upload RSU RF Monitoring data	Ensure data is appropriately authentic and confidential	Security Management Operating Concept section 5.3.11
RSU: RSU RF Monitoring	The RSU shall support the requirements identified in this requirements list by “RSU: VPN”.	Ensure data is appropriately authentic and confidential	Security Management Operating Concept section 5.3.11
RSU: RSU RF Monitoring	An RSU shall be configurable to verify (per 1609.2) all, some or none of the received BSMs used for RSU RF Monitoring.	Protect receivers from false messages	Security Management Operating Concept section 5.3.11
RSU: RSU RF Monitoring	When the RSU verifies received BSMs, it shall verify them per IEEE 1609.2 and per the BSM Security Profile of J2945/1. This verification shall support the requirements identified in this requirements list by “1609.2 verification”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.11
RSU: RSU RF Monitoring	An RSU shall support the requirements identified in this requirements list by “1609.2 verification”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.11
RSU: RSU RF Monitoring	An RSU used in RSU RF Monitoring shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect integrity of data	Security Management Operating Concept section 4.11.3
RSU: RSU RF Monitoring	The RSU shall strip the identifying data from the relevant BSMs	Protect privacy of drivers	Security Management Operating Concept section 5.3.11
RSU: RSU RF Monitoring	The RSU shall store RF Monitoring data encrypted with an encryption key belonging to the TMC per the requirements identified in this requirements list by “Encryption for TMC: Encryption”.	Protect privacy of drivers	Security Management Operating Concept section 5.3.11

RSU: ASD RF Monitoring	An RSU whose SPaT messages are used in ASD RF Monitoring shall sign those SPaT messages with a 1609.2 application certificate containing the PSID for SPaT signing.	Protect receivers from false messages	Security Management Operating Concept section 5.3.12
RSU: ASD RF Monitoring	An RSU whose SPaT messages are used in ASD RF Monitoring shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect receivers from false messages	Security Management Operating Concept 4.12.3
RSU: ASD Event Data Upload	The RSU shall create WSAs for use in ASD Event Data Upload that advertise a PSID for data upload.	Protect receivers from false messages	Security Management Operating Concept section 5.3.13
RSU: ASD Event Data Upload	The RSU shall support the requirements identified in this requirements list by “RSU: WSA”.	Protect receivers from false messages	Security Management Operating Concept section 5.3.13
RSU: ASD Event Data Upload	The RSU shall establish a VPN connection to the TMC to upload ASD Event Data Upload data	Ensure data is appropriately authentic and confidential	Security Management Operating Concept section 5.3.13
RSU: ASD Event Data Upload	The RSU shall support the requirements identified in this requirements list by “RSU: VPN”.	Ensure data is appropriately authentic and confidential	Security Management Operating Concept section 5.3.13
RSU: ASD Event Data Upload	An RSU used in ASD Event Data Upload shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Protect integrity of data	Security Management Operating Concept section 4.13.3
Device security classes: class 1	A class 1 security device shall be compliant with FIPS 140-2 Level 2 physical security requirements.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3.1.1
Device security classes: class 1	A class 1 security device shall not allow remote configuration or login other than via SNMPv3 over TLS.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3.1.2
Device security classes: class 1	A class 1 security device shall support the requirements identified in this requirements list by “Device security classes: common requirements”	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3
Device security classes: class 2	A class 2 security device shall be compliant with FIPS 140-2 Level 2 physical security requirements.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3.2.1
Device security classes: class 2	A class 2 security device shall not allow remote configuration or login other than via SNMPv3 over TLS.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3.2.2
Device security classes: class 2	A class 2 security device shall support the requirements identified in this requirements list by “Device security classes: common requirements”	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3

Device security classes: class 3	A class 3 security device shall be compliant with FIPS 140-2 Level 3 physical security requirements.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3.3.1
Device security classes: class 3	A class 3 security device shall not allow remote configuration or login other than via SNMPv3 over TLS.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3.3.2
Device security classes: class 3	A class 3 security device shall support the requirements identified in this requirements list by “Device security classes: common requirements”	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.3
Device security classes: common requirements	A device may support a manufacturing state in which it does not meet all the security requirements below. In this case it shall support the requirements identified in this requirements list by “Device security classes: manufacturing state”.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.1
Device security classes: manufacturing state	A device shall provide functionality allowing an observer to easily determine whether it is in the operational or manufacturing state.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.1
Device security classes: manufacturing state	If the device allows a transition from operational to manufacturing state, it shall wipe all privileged applications (as defined in Security Management Operating Concept section 6.1.1) when that transition occurs.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.1
Device security classes: manufacturing state	If the device allows a transition from operational to manufacturing state, it shall wipe all keys from the HSM (as defined in Security Management Operating Concept section 6.1.1) when that transition occurs.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.1
Device security classes: manufacturing state	If the device allows a transition from operational to manufacturing state, it shall wipe all keys from the HSM (as defined in Security Management Operating Concept section 6.1.1) when that transition occurs.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.1
Device security classes: manufacturing state	If the device allows a user to cause a transition from operational to manufacturing state without any logical authentication of the user, it shall require that the user is physically present.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.1
Device security classes: common	The host processor on the device shall perform integrity checks on boot to ensure that it is in a known good software state.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.2

requirements			
Device security classes: common requirements	The integrity checks performed at boot shall require the use of a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.2
Device security classes: common requirements	Until all integrity checks on the software and firmware configuration of the host have passed, the device shall not allow a privileged application (as defined in Security Management Operating Concept section 6.1.1) to sign a message.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.2
Device security classes: common requirements	If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any application to have access to stored private keys.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.2
Device security classes: common requirements	If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any privileged application (as defined in Security Management Operating Concept section 6.1.1) to operate.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.2
Device security classes: common requirements	The OS on the device shall maintain an Access Control List (ACL) for which applications on the host may use each private key in the HSM	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device shall maintain an Access Control List (ACL) for which applications on the host may use each private key in the HSM.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device shall maintain an ACL for which applications can modify plaintext data stored in different locations on the device.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device shall maintain an ACL for which applications can read plaintext data stored in different locations on the device.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3

Device security classes: common requirements	The OS on the device shall maintain an ACL for which applications can enter cryptographic keys on the HSM.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device shall maintain an ACL for which applications can modify cryptographic keys on the HSM.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device shall allow privileged applications to operate without explicit user authentication	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device shall allow applications that update private key material within the HSM to operate without explicit user authentication	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS on the device, if it allows processes that modify or inspect executing processes in operational mode, shall require that those processes have explicit user authentication.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	The OS shall not permit keys designated as private to be read from the HSM.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.3
Device security classes: common requirements	When requested to install software, the host processor OS shall ensures that the software is signed by an authority with appropriate permissions and shall reject the installation if the signature or any of the validity checks on the software or its signing certificate fail.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.4
Device security classes: common requirements	The validation of signed software shall require use of a verification key that is protected by local hardware to a level equivalent to FIPS 140-2 at the level appropriate for the device	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.4

Device security classes: common requirements	The update mechanism shall prevent updates from being rolled back.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.3.4
Device security classes: common requirements	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 as noted below.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	All cryptographic software and firmware for the HSM shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	A cryptographic mechanism using a FIPS 140-2 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.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	A message authentication code shall only be used to verify the integrity of the HSM software/firmware if one of the following hods: § 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.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	All cryptographic software and firmware, cryptographic keys, and control and status information on the HSM 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.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1

Device security classes: common requirements	The HSM operating system shall implement role-based access control for the following activities: · Execute stored cryptographic software and firmware. · 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. · R read the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), and plaintext data. · Enter cryptographic keys.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	The HSM operating system 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 6.1.2. 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 6.1.2.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	The HSM operating system shall allow an unauthenticated role to create a new cryptographic key by combining an existing key with new input.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	The HSM operating system 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.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	The HSM 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	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1

	system processes (i.e., operator-initiated), cryptographic or not		
Device security classes: common requirements	The HSM operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	If the device has the HSM and the host processor communicate via a connection which can be accessed directly by other processors, 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.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.1.4.1
Device security classes: common requirements	The device shall provide tamper evidence to detect tampering of the device (e.g. opening of the case).	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.2
Device security classes: common requirements	All unused media ports (e.g. USB) shall be sealed.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.2
Device security classes: common requirements	There shall be no removable media.	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.2
Device security classes: common requirements	Device suppliers shall provide written evidence demonstrating how the devices meet these security requirements	Ensure appropriate level of security for operations	Security Management Operating Concept section 6.5
RSU: 1609.2 security management	RSUs shall support the requirements identified in this requirements list by “1609.2 security management: Application certificates common requirements”.	Protect receivers from false messages	
RSU: 1609.2 security management	The RSU shall be provided from the supplier already provisioned with an enrolment certificate for SPaT.	Protect receivers from false messages	Security Management Operating Concept section 7.2.4

RSU: 1609.2 security management	The RSU shall be provided from the supplier already provisioned with an enrolment certificate for WSA.	Protect receivers from false messages	Security Management Operating Concept section 7.2.4
RSU: 1609.2 security management	The RSU shall be provided from the supplier already provisioned with an enrolment certificate for SSM.	Protect receivers from false messages	Security Management Operating Concept section 7.2.4
RSU: 1609.2 security management	The RSU supplier shall provide a database of enrolment certificates cross-referenced to an appropriate physical ID for the RSU, e.g. the serial number.	Protect receivers from false messages	Security Management Operating Concept section 7.2.4, 7.2.6
RSU: 1609.2 security management	The RSU enrolment certificate shall have a geographic region that covers the entire Pilot Deployment site. The exact specification of this region will be provided in Phase 2.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.1
RSU: 1609.2 security management	The RSU enrolment certificate shall have a lifetime of at least three years, final choice to be made during Phase 2.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.1
RSU: 1609.2 security management	The RSU supplier shall provide a database of enrolment certificates cross-referenced to an appropriate physical ID for the RSU, e.g. the serial number.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.1
RSU: 1609.2 security management	The RSU certificate management service shall support requesting application certificates with geographic validity regions that are different from, but entirely contained within, the geographic validity region in the enrolment certificate	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.2, 8.1.2
RSU: 1609.2 security management	The RSU certificate management service shall read the region to be requested from a MIB which the TMC shall update via SNMP v3 per the requirements identified in this requirements list by “SNMP: Agent”	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.2, 8.1.2
RSU: 1609.2 security management	The RSU certificate management service shall request application certificates with a CrlSeries value of 0.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: 1609.2 security management	The RSU certificate management service shall start requesting a new application certificate a day before the expiry of the current one.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: 1609.2 security management	The RSU shall request new application certificates periodically once it has started requesting them, with a period to be determined in Phase 2, until it	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3

	receives the new application certificates.		
RSU: 1609.2 security management	The RSU certificate management service shall support requesting an application certificate before the normal certificate refresh time if so instructed by the TMC via SNMP, per the requirements identified in this requirements list by “SNMP: Agent”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.2, 8.1.2
RSU: 1609.2 security management	The RSU certificate management service shall support deleting an application certificate before the normal certificate refresh time if so instructed by the TMC via SNMP, per the requirements identified in this requirements list by “SNMP: Agent”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.1
RSU: 1609.2 security management	If the RSU is informed by the SCMS that its enrolment certificate is invalid, it shall store that information in a MIB entry and make it available to the TMC via SNMP per the requirements identified in this requirements list by “SNMP: Agent”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: 1609.2 security management	The RSU supplier shall provide a database of enrolment certificates cross-referenced to an appropriate physical ID for the RSU, e.g. the serial number.	Protect receivers from false messages	Security Management Operating Concept section 7.2.4, 7.2.6
1609.2 verification	When verifying, the device shall require that 1609.2 signed messages are signed by a certificate that is protected from modification by, or chains back to a certificate that is protected from modification by, the secure boot process.	Protect receivers from false messages	Security Management Operating Concept section 5.2.2.2, 6.1.3.2
1609.2 verification	The 1609.2 revocation check shall not include a check for the revocation status of end-entity certificates, as these have a CrlSeries value of 0, but shall include a check for the revocation status of CA certificates	Protect receivers from false messages	Security Management Operating Concept section 7.2.8
1609.2 verification	Revocation status of CA certificates shall be distributed during the certificate update process per the SCMS Interface document.	Protect receivers from false messages	Security Management Operating Concept section 7.2.8
RSU: ASD Certificate Update	The RSU shall create WSAs for use in ASD Certificate Update that advertise a PSID for data upload.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: ASD Certificate Update	The WSA created for use in ASD Certificate Update shall contain a WAVE Routing Advertisement with the	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6

	IP address of the DNS resolver provided by the TMC.		
RSU: ASD Certificate Update	The RSU shall receive the IP address of the DNS resolver for inclusion in the WSA from the TMC via SNMPv3 over TLS.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: ASD Certificate Update	The RSU shall support the requirements identified in this requirements list by “RSU: WSA”.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: ASD Certificate Update	The RSU shall support the requirements identified in this requirements list by “RSU: SNMP”.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: RSU Certificate Update	The RSU shall receive the IP address of the DNS resolver from the TMC via SNMPv3 over TLS.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: RSU Certificate Update	The RSU shall support the requirements identified in this requirements list by “RSU: SNMP”.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: RSU Certificate Update	An RSU shall implement certificate download per the CAMP SCMS Interface (detailed requirements to be derived during Phase 2 as the final interface document is not yet published)	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: RSU Certificate Update	The RSU shall support the requirements identified in this requirements list by “Device Security Classes: Class 1”.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.6
RSU: IPv6 Connectivity	The RSU shall provide IPv6 connectivity for use by devices connecting over the 5.9 interface.	Enable secure, reliable credential update	Security Management Operating Concept section 7.2.10
RSU: IPv6 Connectivity	The RSU shall implement a firewall blocking all IP access from mobile devices to any IP address other than those approved by the TMC.	Protect against DoS attacks	Security Management Operating Concept section 7.2.10
RSU: IPv6 Connectivity	The RSU shall update the list of permitted IP addresses as instructed by the TMC using SNMPv3 over TLS.	Protect against DoS attacks	Security Management Operating Concept section 7.2.10
RSU: IPv6 Connectivity	The RSU shall support the requirements identified in this requirements list by “SNMP: Agent”	Protect against DoS attacks	Security Management Operating Concept section 7.2.10
RSU: IPv6 Connectivity	The RSU shall maintain a log of security management related connections, anonymized so identifying information is removed from it.	Protect against DoS attacks	Security Management Operating Concept section 7.2.10, 8.1.3
RSU: IPv6 Connectivity	The RSU shall make the security management connections log available to the TMC via SNMPv3 over TLS.	Protect against DoS attacks	Security Management Operating Concept section 7.2.10, 8.1.3

Encryption for TMC: Encryption	Devices that encrypt for the TMC shall encrypt using IEEE 1609.2 encryption, exact details to be specified in Phase 2.	Prevent unauthorized disclosure of information	Security Management Operating Concept section 8.4.1
Encryption for TMC: Encryption	Devices that encrypt for the TMC shall encrypt using an ECIES key provided for that purpose by the TMC.	Prevent unauthorized disclosure of information	Security Management Operating Concept section 8.4.1
Encryption for TMC: Encryption	Devices that encrypt for the TMC shall support updating the key via SNMPv3 per the requirements identified in this requirements list by “SNMP: Agent”.	Prevent unauthorized disclosure of information	Security Management Operating Concept section 8.4.1
Encryption for TMC: Encryption	Devices that encrypt for the TMC shall not update the encryption with a new one unless the new one has a more recent generation time.	Prevent unauthorized disclosure of information	Security Management Operating Concept section 8.4.1
RSU: SPaT	The RSU shall sign SPaT messages with a 1609.2 application certificate containing one PSID, for SPaT signing.	Protect receivers from false messages	Security Management Operating Concept section 7.2.3
RSU: SPaT	The RSU shall not create or distribute SPaT messages if it does not have a currently valid signing certificate.	Protect receivers from false messages	Security Management Operating Concept section 7.2.3, 8.1.1.3
RSU: SPaT	The RSU shall support the requirements identified in this requirements list by “RSU: 1609.2 security management”.	Protect receivers from false messages	Security Management Operating Concept section 8.1
RSU: SPaT	The information that the RSU receives from the ITS-RE to support modifying SPaT messages shall be protected with TLS	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: SPaT	The RSU shall support the requirements identified in this requirements list by “RSU: RSU <-> ITS-RE Communications”	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: MAP	The RSU shall use SNMPv3 over TLS to receive signed MAP messages from the TMC	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: MAP	The RSU shall verify MAP messages per the MAP security profile (to be provided in Phase 2)		
RSU: MAP	The RSU shall verify MAP messages prior to starting to send them, rather than at the time they are received from the TMC		
RSU: MAP	The RSU shall support the requirements identified in this requirements list by “SNMP: Client”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: TIM	The RSU shall use SNMPv3 over TLS to receive signed TIM messages from the TMC	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: TIM	The RSU shall support the requirements identified in this requirements list by “SNMP: Client”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3

RSU: SSM	The RSU shall sign SSM messages with a 1609.2 application certificate containing one PSID, for SSM signing.	Protect receivers from false messages	Security Management Operating Concept section 7.2.3
RSU: SSM	The RSU shall not create or distribute SSM messages if it does not have a currently valid signing certificate.	Protect receivers from false messages	Security Management Operating Concept section 7.2.3, 8.1.1.3
RSU: SSM	The RSU shall support the requirements identified in this requirements list by “RSU: 1609.2 security management”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: WSA	The RSU shall sign WSAs with a 1609.2 application certificate containing one PSID, for WSA signing.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: WSA	The RSU shall support the requirements identified in this requirements list by “RSU: 1609.2 security management”.	Protect receivers from false messages	Security Management Operating Concept section 8.1.1.3
RSU: RSU <-> ITS-RE Communications	The RSU shall support the requirements identified in this requirements list by “RSU: Management and Configuration”.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2
RSU: RSU <-> ITS-RE Communications	The RSU shall support the requirements identified in this requirements list by “TLS: Client”.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2
RSU: RSU <-> ITS-RE Communications	The RSU shall support whitelisting individual client certificates.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2
RSU: RSU <-> ITS-RE Communications	The RSU shall support updating the whitelist of client certificates.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2
RSU: RSU <-> ITS-RE Communications	The RSU shall support being placed in a state where it accepts incoming TLS connections.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2
RSU: RSU <-> ITS-RE Communications	The RSU shall support being placed in a state where it does not accept incoming TLS connections.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2
RSU: RSU <-> ITS-RE Communications	The RSU shall support being placed in a state where all data exchanged with an indicated IP address associated with a TLS session is sent via that TLS session.	Protect messages from modification or disclosure	Security Management Operating Concept section 10.2

Appendix K. SPaT application Security Profiles

17 Introduction

17.1 SPaT Description and Security Needs

Signal phase and timing messages in the NYC pilot will be sent from supported intersection RSU at a rate equivalent to that of vehicle BSMs, namely 10Hz. SPaT messages are described as follows (CVRIA):

Current signal phase and timing information for all lanes at a signalized intersection. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable.[1]

The security concerns this security profile should address include the following:

Table 9: Application-specific Security Concerns

Application-Specific Security Concerns	Mitigations Supported by Security Profile
Replay	Receiving security application shall support detection of replay attacks
RSU transmitting outside of assigned area	Receiving security applications needs to check the declared message origin to determine if it is transmitting within a prescribed geo-fence indicated by the certificate's geographic restriction. Note: This is a 1609.2 'consistency check' in terms of the application security processing.
RSU not authorized to transmit for given intersection	The RSU should only be transmitting SPaT for intersection(s) for which it has authority
Strong association to correct intersection description	SPaT messages must be tightly indexed to the intersection in question so that ASD applications that receive MAP messages provide the correct information to the drivers. Note: This is a 1609.2 'relevance check' in terms of the application processing.
Revoked RSU transmitting	End entities should have reasonably fresh CRL information with respect to the validity period of the RSU certificate (~2 months)
Message spoofing	SPaT messages need to be signed. There is no need to encrypt.

17.2 IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the SPaT application security profile.

[1] http://local.iteris.com/cvria/html/applications/app67.html#tab-3

Table 10: SPaT Application Security Profile Identification

Name	Type	Recommended values	Description
Name	Text string	"SPAT_SecurityProfile"	The name to be used to refer to the profile. This should be unique among names used by security profiles that reference a particular PSID.
PSIDs	List of PSIDs	0x82	The PSIDs to be used by SDEEs that use this profile.
Other considerations	Text string	This SPAT security profile is designated for the NYC Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

17.3 Sending

The following table provides the security profile for message sending within the SPaT PSID.

Table 11: SPaT Application Security Profile for Sending Messages

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all SPaT messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - *tbsData.payload.extDataHash*
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	Needed to determine if message lies within the validity period of the signing credential
Set Generation Location in Security Headers	Boolean	True	Needed for credential and SPDU consistency checks
Set Expiry Time in Security Headers	Boolean	False	
Signed SPDU Lifetime	Time interval	N/A	Short-lived messages, no lifetime
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	1 second	Comment: Default setting from 1609.2 SDEE Specifiers guidance seems reasonable. Also, SPAT is typically sent out at 10Hz so at least every 5 messages would get the cert vs. the cert hash as the signer identifier.
Simple Signer Identifier Policy: Exceptions	Boolean	False	
Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length	Integer or enumerated	1	Will use the RSUs EE certificate only within the message. We will assume full pre-distribution of CA certs to the fleets.
Text Signer Identifier Policy	Text	N/A	

Name	Type	Recommended values	Notes
Sign With Fast Verification	enumerated	Yes-Compressed	
EC Point Format	Enumerated	Compressed	
p2pcd_useInteractive-Form	Boolean	N/A	
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	False	Each SPaT PDU transmitted must be uniquely signed
Time Between Signing	Time or n/a	N/A	
Encrypt Data	enumerated	No	SPaT messages are in plaintext

17.4 Receiving

The following table provides the message reception security features for the SPaT application security profile.

Table 12: SPaT Application Security Profile for Receiving Messages

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with SPAT messages
Verify Data	Enumerated	True	Verify all SPaT messages
Maximum Certificate Chain Length	Integer	4	Implementations are not required to support receiving a cert chain length > 4
Relevance: Replay	Boolean	False	SPaTs have generation time within them, so application behavior to detect replay is needed. Delayed SPaT messages need to be detected by the application.
Relevance: Generation Time in Past	Boolean	True	
Validity Period	Time interval	1 Minute	Within a one minute period, the application logic handles message latency issues. Beyond that, the security services will discard. This threshold is an important item for which 1609.2 can help provide guidance.
Relevance: Generation Time in Future	Boolean	True	
Acceptable Future Data Period	Time	N/A	
Generation Time Source	Enumerated	Security Header	

Name	Type	Value	Notes
Relevance: Expiry Time	Boolean	False	
Expiry Time Source	Enumerated	N/A	
Consistency: Generation Location	Boolean	True	The ASDs need to carry out consistency checks based on the SPAT's generation location.
Relevance: Generation Location Distance	Boolean or "Text"	True	
Validity Distance	Distance in meters or "Variable"	1000m	Security services will reject if more than 1000m
Generation Location Source	Enumerated	Payload	
Overdue CRL Tolerance	Time period or text	8 weeks	
Relevance: Certificate Expiry	Boolean	True	Assume that certs won't be on the CRL for long. Either way, check for cert. expiration.
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plaintext

17.5 Security management

The following table provides the security management features for the SPaT application security profile.

Table 13: SPaT Application Security Management Security Profile

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	10Hz messages consume more bandwidth
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	All	The type of geographic region supported for conformant certificates. Country and subregions defined in dictionary
Maximum Certificate Chain Length	Integer	8	
Use Individual Linkage ID	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

17.6 Specific Permission (SSP) Expression and Syntax

The IEEE 1609.2 SSP construct will be used to apply certificate permissions for specific activities in the SPaT application message. The SSP for SPaT messages will be composed as follows:

- SSP Max length is 31 Octets (per ETSI TS 103 097)
- SSP first octet is SSP Version (Version=0x01)

Syntactically populating the SSP first requires establishing a list of PSID-centric activities for which authorizations need to apply. In the case of SPAT messages, they and the respective SSP bit positions and values are included in the following table**:**

Table 14: PSID Activity or Activity Option and Permissions (consistent with J2735 dictionary)

SPaT Application Activity	SPaT Application Data Item	Octet	Bit Pos.	Bit Value
Provide SPaT information for one or multiple intersections	RSU Location	1	0	0: Certificate only authorized only for operation in a single location 1: Certificate authorized for SPaT messages at multiple intersections
Provide information about intersection state absent any advisory speeds or movement assist information	SPAT.intersections.IntersectionState.*	1	1	0: Certificate not allowed to sign 1: Certificate allowed to sign
Provide general status of the traffic controller for the signalized intersection(s) addressed by this SPaT	SPAT.intersections.IntersectionState.status	1	2	0: Certificate not allowed to sign 1: Certificate allowed to sign
Provide advisory speeds	SPAT.intersections.IntersectionState.states.MovementState.state-time-speed.MovementEvent.speeds.AdvisorySpeed	1	3	0: Certificate not allowed to sign 1: Certificate allowed to sign
Provide maneuver assist and movement state information	SPAT.intersections.IntersectionState.MovementList[] SPAT.intersections.IntersectionState.ManeuverAssistList[]	1	4	0: Certificate not allowed to sign 1: Certificate allowed to sign
Reserved	***	2-31	All	All bits 0

Appendix L. MAP Application Security Profiles

18 MAP Application Security Profile for the NYC Connected Vehicle Pilot

18.1 MAP Description and Security Needs

Signal phase and timing messages in the NYC pilot will be sent from supported intersection Roadside Equipment (RSU) at a rate of approximately once per second per intersection. MAP messages provide intersection geometry pertinent to driver applications that rely on detailed messaging regarding intersection state (e.g., Signal Phase and Timing [SPaT]).

While the RSU digitally signs SPaT messages, MAP messages are more static in nature and are to be 'centrally signed,' i.e., signed by the Traffic Management Center (TMC).

The security concerns this security profile should address include the following:

Table 15: Application-specific Security Concerns

Application-Specific Security Concerns	Mitigations Supported by Security Profile
Replay	Receiving security application shall support detection of replay attack. In addition, replay is a concern if the replayed message indicates an old intersection MAP configuration that is still within the validity period of the signing certificate. For that reason, the MAP messages should contain a reasonable expiration time (assuming the TMC's authorization cert has a long validity period).
Integrity errors	The sending application needs to digitally sign the messages. False intersection geometry descriptions could severely impact V2I applications.
Message spoofing	MAP messages need to be digitally signed by the TMC to ensure data origin and non-repudiation. There is no need to encrypt.
Signing certificate not authorized to provision MAP data for a given intersection or intersections within a given region.	The TMC should only be transmitting MAP messages for intersection(s) for which it has authority. The signing certificate needs to indicate a geographic restriction that definitively contains/overlaps the geographic constraint of the intersection(s).
Revoked RSU transmitting	End entities should have reasonably fresh CRL information with respect to the validity period of the RSU certificate (~2 months)
Incorrect entity signs message	Only the 0TMC should be able to digitally sign MAP messages.

18.2 IEEE 1609.2 Security Profile Identification

The following table provides the identification features for the MAP application security profile.

Table 16: MAP Application Security Profile Identification

Name	Type	Recommended values	Description
Name	Text string	"MAP_SecurityProfile"	
PSIDs	List of PSIDs	0x82	The PSIDs to be used by SDEEs that use this profile.
Other considerations	Text string	This MAP security profile is designated for the NYC Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

18.3 Sending

The following table provides the security profile for message sending within the MAP PSID.

Table 17: MAP Application Security Profile for Sending Messages

Name	Type	Recommended values	Notes
Sign Data	enumerated	True	Sign all MAP messages for data origin authentication and non-repudiation
Signed Data in Payload	Boolean	True	
External Data	Boolean	False	Otherwise we need to populate - *tbsData.payload.extDataHash*
External Data Source	Text	N/A	
External Data Hash Algorithm	enumerated	N/A	
Set Generation Time in Security Headers	Boolean	True	Needed to determine if message lies within the validity period of the signing credential (message's generation time only resolves to the minute)
Set Generation Location in Security Headers	Boolean	False	Centrally signed messages (TMC) do not need to indicate generation location. The signing certificate will indicate 'authority to sign' for a given region.
Set Expiry Time in Security Headers	Boolean	True	Lane closures or other intersection impediments may be somewhat dynamic, requiring multiple MAP message updates within the TMC authorization certificate's validity period.
Signed SPDU Lifetime	Time interval	Text	TMC signing application needs to set the time interval for this SPDU lifetime.
Signer Identifier Policy Type	Enumerated	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Time interval (for example, "one second")	Always	All MAP messages will contain the signing public key certificate.
Simple Signer Identifier Policy: Exceptions	Boolean	False	
Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length	Integer or enumerated	1	Will use the TMC's authorization certificate only within the message. We will assume full pre-distribution of CA certs to the fleets.

Name	Type	Recommended values	Notes
Text Signer Identifier Policy	Text	N/A	
Sign With Fast Verification	enumerated	Yes-Compressed	
EC Point Format	Enumerated	Compressed	
p2pcd_useInteractive-Form	Boolean	N/A	
p2pcd_max-ResponseBackoff	Time or n/a	N/A	
p2pcd_response-ActiveTimeout	Time or n/a	N/A	
p2pcd_request-ActiveTimeout	Time or n/a	N/A	
p2pcd_observed-RequestTimeout	Time or n/a	N/A	
p2pcd_currentlyUsed-TriggerCertificateTime	Time or n/a	N/A	
p2pcd_response-CountThreshold	Integer or n/a	N/A	
Repeat Signed SPDUs	Boolean	True	Following the initial, transmitted MAP PDU, each following one may be a re-transmit of the first so long as they are within the validity period of the message (as set by the signing application).
Time Between Signing	Time or n/a	Set to Message lifetime	
Encrypt Data	enumerated	No	MAP messages are in plaintext

18.4 Receiving

The following table provides the message reception security features for the MAP application security profile.

Table 18: MAP Application Security Profile for Receiving Messages

Name	Type	Value	Notes
Use Preprocessing	Enumerated	True	The full cert chain will not be sent with MAP messages
Verify Data	Enumerated	True	Verify all MAP messages
Maximum Certificate Chain Length	Integer	4	
Relevance: Replay	Boolean	False	
Relevance: Generation Time in Past	Boolean	False	Security services won't take control. The app must decide.
Validity Period	Time interval	N/A	
Relevance: Generation Time in Future	Boolean	False	This allows a TMC to set future expectations for a given intersection (e.g., a planned lane closure) even if the message doesn't reflect the current intersection state.
Acceptable Future Data Period	Time	24 hours	Vehicles should not accept anticipated intersections that are more than 24 hours in the future

Name	Type	Value	Notes
Generation Time Source	Enumerated	Payload	Contained in the MAP message Timestamp field
Relevance: Expiry Time	Boolean	N/A	
Expiry Time Source	Enumerated	N/A	
Consistency: Generation Location	Boolean	False	
Relevance: Generation Location Distance	Boolean or "Text"	N/A	
Validity Distance	Distance in meters or "Variable"	N/A	
Generation Location Source	Enumerated	N/A	
Overdue CRL Tolerance	Time period or text	8 weeks	Set at the duration of the certs.
Relevance: Certificate Expiry	Boolean	True	
Accept Encrypted Data	Enumerated or text	No	This entire message should be in plaintext

18.5 Security management

The following table provides the security management features for the MAP application security profile.

Table 19: MAP Application Security Management Security Profile

Name	Type	Value	Notes
Signing Key Algorithm	Enumerated	ecdsaNistP256withSha256	
Encryption Algorithm	Enumerated	N/A	
Implicit or Explicit Certificates	Enumerated	Implicit	What is supported by SCMS
EC Point Format	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages
SupportedGeographic Regions	Array of enumerated	An array of entries, each of which is one of: All	The type of geographic region supported for conformant certificates.
Maximum Certificate Chain Length	Integer	8	
Use Individual Linkage ID	Boolean	N/A	
Use Group Linkage ID	Boolean	N/A	
Signature Algorithms in Chain or CRL	Sequence of Enumerated	ecdsaNistP256withSha256	

18.6 Specific Permission (SSP) Expression and Syntax

The IEEE 1609.2 SSP construct will be used to apply certificate permissions for specific activities in the MAP application message. The SSP for MAP messages will be composed as follows:

- SSP Max length is 31 Octets
- SSP first octet (Octet 0) is the SSP Version (Version=0x01)

Syntactically populating the SSP first requires establishing a list of PSID-centric activities for which authorizations need to apply. In the case of MAP messages, they and the respective SSP bit positions and values are included in the following table**:**

Table 20: PSID Activity or Activity Option and Permissions (consistent with J2735 dictionary)

MAP Application Activity	MAP Application Data Item or Feature	Octet	Bit Pos.	Bit Value
Provide MAP information for intersection controlled by a traffic signal controller	TBD	1	0	0: Certificate not allowed to sign 1: Certificate allowed to sign
Provide MAP information for intersection NOT controlled by a traffic signal controller	TBD	1	1	0: Certificate not allowed to sign 1: Certificate allowed to sign
Provide speed limits in the road and lane topology	TBD	1	2	0: Certificate not allowed to sign 1: Certificate allowed to sign
Reserved	***	2-31	All	All bits 0