Frequently Asked Questions

Regarding the RSU 4.1 Specification

Compiled March 30, 2018

This document is intended to provide guidance to developers and deployers. Feedback on the specification and this document will be considered in future revisions to the RSU Specification. Please submit your feedback to USDOT through the Connected Vehicle Helpdesk (?).

Table of Contents

Message Forward

[redacted] There is ambiguity about how much of the packet to forward. Should it include the WSMP header? Security header? Payload only?

There have been differing opinions on this question. The header info is useful for some applications, while only the payload is useful for others. So the answer may be to make this configurable. But for now, we recommend to forward the payload + WSMP header as received.

Pg. 14, reference 9

[redacted] Requirements specify 802.3at 2009 . This standard is superseded now by the 802.3-2012 standard Section 2 Clause 33 Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI). I assume 2012 is the actual test standard? You do reference it in the list.

From our experience, section 33 in the 802.3at-2009 spec was directly incorporated into the 2012 version as Clause 33. Either version should be acceptable for the PoE since they should contain the same requirements.

RSU-MIB

[redacted] For the "rsuTxPower" (Page 94) under "rsuSysDescription OBJECT IDENTIFIER ::= { rsuMIB 17 }", does this represent the system wide TxPower setting for the antennas ?

rsuTxPower can be considered a default transmit power level to be used if a power level is not defined by an application.

[redacted] Since each of the applications - Immediate-Forward/Store-Repeat/ipv6-provider can transmit the packets at a configurable TxPower, Could you tell us how this "rsuTxPower" parameter should alter the behavior of the system ?

The power level defined by the application would take precedence

[redacted] In RSU 4.1 spec, SNMP MIB indicating 2 bytes for PSID. But, isn't it PSID can go up to 4 bytes as per WAVE standards?

Make the following changes:

DISPLAY-HINT ""4x"" SYNTAX OCTET STRING (SIZE(1..4))"

[redacted]\RSE\RSU41F~1.MIB(107) : Error 28 : Item "rsuSRMDsrcMsgId" in sequence "RsuSRMStatusEntry" has conflicting syntax specified

Definition of rsuSRMTxDsrcMsgId in RsuSRMStatusEntry should be changed to Integer32

[redacted]\RSE\RSU41F~1.MIB(109) : Error 28 : Item "rsuSRMTxChannel" in sequence "RsuSRMStatusEntry" has conflicting syntax specified

Definition of rsuSRMTxChannel in RsuSRMStatusEntry should be changed to Integer32

[redacted]\RSE\RSU41F~1.MIB(231) : Error 28 : Item "rsuIFMDsrcMsgId" in sequence "RsuIFMStatusEntry" has conflicting syntax specified

Definition of rsuIFMDsrcMsgId in RsuIFMStatusEntry should be changed to Integer32

[redacted]\RSE\RSU41F~1.MIB(232) : Error 28 : Item "rsuIFMTxMode" in sequence "RsuIFMStatusEntry" has conflicting syntax specified

Definition of rsuIFMTxMode in RsuIFMStatusEntry should be changed to INTEGER

[redacted]\RSE\RSU41F~1.MIB(233) : Error 28 : Item "rsuIFMTxChannel" in sequence "RsuIFMStatusEntry" has conflicting syntax specified

Definition of rsuIFMTxChannel in RsuIFMStatusEntry should be changed to Integer32

[redacted]\RSE\RSU41F~1.MIB(723) : Error 28 : Item "rsuWsaChannel" in sequence "RsuWsaServiceEntry" has conflicting syntax specified

Definition of rsuWsaChannel should be changed to Integer32

[redacted]I am trying to compile the RSU MIB using this product https://agentpp.com/tools/agenpro.html. I got so many errors and I contacted the author of the software …
I had compiled that file previously to use with an SNMP manager from this company http://www.mg-soft.si/mgMibBrowserPE.html?p1=products&p2=mgProductsNMA-SNMP and I had no problem, there were no errors.

We have been using SnmpB, but are transitioning to the MG-Soft package. The only errors that appear are with regard to inclusion in an OBJECT-GROUP. They aren't critical and haven't prevented the MIB from compiling. It seems that many of the other errors are related to the IPv6-MIB file, which the AgenPro software author points out has a problem. If the IPv6 module needs to be corrected, then we may reconsider using it in the RSU MIB.

[redacted] In the RSU MIB, rsuDsrcFwdDeliveryStart and rsuDsrcFwdDeliveryStop in table RsuDsrcForwardEntry are defined as OCTET STRING. Could you please elaborate on how the time is represented in the OCTET STRING?

This was first implemented in the 4.0 spec as the following (and did not change in the 4.1 spec):

YYYYMMDDhhmm

Where,
YYYY = 4-digit hex representation of year (e.g. 2018 = 0x07E2)
MM = 2-digit hex representation of month
DD = 2-digit hex representation of day
hh = 2-digit hex representation of hour
mm = 2-digit hex representation of minute

As an example, right now UTC time is 12:35 PM, March 13, 2018, which would be represented as 07E2030D0C23.

We have gotten several comments regarding this representation, and in a future version of the MIB, we would recommend that the date be represented as 'DisplayString' instead of 'OCTET STRING' for clarity.

[redacted] About the PSID, since it is defined as a variable length entry, do I assume that the PSID should be the p-encoded value and not just an integer?

Yes, please use the p-encoded value for PSID.

[redacted] rsuIFMStatusTable entries are labeled "read-only" in the MIB, but are labeled "read-create" in the Object Map

Access should be "read-create" to allow for row creation; change to "read-create" in the MIB.

[redacted] For the "rsuTxPower" (Page 94) under "rsuSysDescription OBJECT IDENTIFIER ::= { rsuMIB 17 }", does this represent the system wide TxPower setting for the antennas ?. Since each of the applications - Immediate-Forward/Store-Repeat/ipv6-provider can transmit the packets at a configurable TxPower, Could you tell us how this "rsuTxPower" parameter should alter the behaviour of the system ?

rsuTxPower can be considered a default transmit power level to be used if a power level is not defined by an application. The power level defined by the application would take precedence.

In RSU 4.1 a spec we have a "Notification" and a corresponding "Notification Object" but for Notification - "rsuGpsNmeaNotify" (15628.4.1.100.0.12) we have Notification Object - "rsuGpsNmeaNotifyInterval" (15628.4.1.100.1.12) which is a read-write parameter, which does not make sense as a SNMP TRAP, as the Notification Objects will contains the details of the TRAP that's being generated. Has "rsuGpsNmeaNotifyInterval" been wrongly placed here? In

page 96 of the RSU 4.1a spec as shown below the "rsuGpsOutputString" is being used as a NotificationObject. Is this an oversight?

The intent is to simply send the NMEA string as an snmp notification (trap), similar to the rsuGpsOutput object. We want to make the send interval for that notification configurable, which is the point of rsuGpsNmeaNotifyInterval. But there is not a dedicated notification object that holds the NMEA string. The notification should be the same as that held in rsuGpsOutputString.

[redacted] The GPS NMEA string is reported by two sources currently. Are two sources needed for sending the same information?

The notification was added to provide flexibility to the user and promote the use of SNMP. The notification can be disabled if not needed.

[redacted] rsuMessageCountsByPsidId has been defined as a "read-only" parameter.
rsuMessageCountsByPsidCounts has been defined as a "read-only" parameter.
rsuMessageCountsByPsidRowStatus has been defined as a "read-create" parameter.

How do we use it to query statistics for each PSID? As my understanding from what is expected by 4.1 Spec is that the user should define the PSIDs for which he wants to query statistics. The above definition does not do that. Is there any other way that we have to interpret?

Those parameters should be ‘read-create’ since the structure of the table will not be constant and new rows will need to be created as new messages are broadcast.

[redacted] Description for rsuSetRole is copy and paste from previous entry

Change description to: "The role of the RSU in a set (master or slave)"

[redacted] Description for rsuSetEnable is copy and paste from previous entry

Change description to: "The status of the RSU set. 0 is not operating in a set; 1 is operating in a set."

[redacted] Description for rsuSetSlaveTable is copy and paste from previous entry

Change description to: "Holds the configuration parameters for the slave RSUs."

[redacted] Description of rsuSetSlaveEntry is copy and paste from previous entry

Change description to: "A row describing the configuration of each slave RSU."

[redacted] In RSU 4.1 spec, rsuSRMTxInterval accepting values in the range of -2147483648 to 2147483647. Is in it TxInterval should be greater than 0. It should not accept values less than or equal to 0.

Agree, but already limited to positive values in the latest spec.

Integer32 (1..2147483647)

[redacted] rsuWsaProviderContext is only 4 bytes, which is short for a text field. Also, the dot3 MIB is 32 bytes.

Change length to 32 bytes

SYNTAX OCTET STRING (SIZE (0..32))

[redacted] As per 1609.3 MIB, WSM max payload range is from 1 to 2302. RSU 4.1 MIB limiting SRM payload to 1500 only…UMTRI created MAPs for some of the intersections and those payloads crossed current 1500 limit. Is it possible make 4.1 MIB in-line with 1609.3 MIB with respect to this?

The two OIDs describe slightly different characteristics of the packet, but if there are MAP payloads being developed that exceed the range given in the MIB then we will reconsider the range. For now, we would suggest using the same range (1..2302) as that given in the 1609.3 MIB.

[redacted] What are the units for “rsuSecCredAttachInterval”, is it number of packets? Or in units of 100msec?

This is the number of packets. So if you set it to 20, then every 20th message should have a cert attached. It may be valuable to also change the range to 0..100 where 0 indicates that no messages are signed. This will be considered for a future revision of the spec.

[redacted] Description for rsuWsaServiceTable has not been changed from the original

Changed description to: "Holds general configuration parameters for the RSU WAVE Service Advertisement."

[redacted] rsuSetRole only needs 2 values

Change rsuSetRole SYNTAX field to INTEGER {master(0), slave(1)}

[redacted] rsuSetEnable only needs 2 values

Change rsuSetEnable SYNTAX field to INTEGER {independent (0), set(1)}

USDOT_RSU-Req_278-v001

[redacted] Power supply requirements specify a voltage between 37 V and 57 V. This covers the input range of both Type 1 and Type 2 devices. We assume that it's up to the vendor to specify either a Type 1 OR Type 2 PoE PD in the implementation of the RSU in which case the operating voltage range is different according to Type. See Table 33-18 Page 662.

It is not the intent to specify Type 1 or Type 2, only compliance with 802.3at. To avoid confusion, the voltage range may be removed in a subsequent update to the spec.

[redacted] The PICS requirements at the end of the Clause 33 (33.8 Page 692-711) are large and detailed. No indication is given within the RSU 4.1 about which tests or subset of tests are required. Are only the electrical testing required for PD and PSE or the full protocol stack involving the Management functions, Data Link Layer for the PSE also included for the entire system?

The intent is to verify that the RSU itself complies with the 802.3at standard. It is not the intent to require testing of a COTS power injector that is already certified to comply with 802.3at.

[redacted] Is it the intent of the RSU 4.1 requirements to specify a Type1 or Type2 or either PoE powered device as the requirement?

It is not the intent to specify Type 1 or Type 2, only that the device comply with 802.3at.

[redacted] Is it the intent of the Verification Method column of the Power Requirements section 3.1 to require FULL PICS test reports on the PoE equipment? If not which tests? (Obviously either PD alone or PD + PSE if so required)

If the power injector is a COTS product that is already certified to comply with 802.3at, then there is no need to repeat the testing on the power injector.

[redacted] Please define " …an accredited test facility" for 802.3 testing purposes.

This should be an industry-recognized facility that can certify that the device functions according to the specification to ensure interoperability.

USDOT_RSU-Req_312
USDOT_RSU-Req_313

[redacted] The temperature range described in 312, has a ramp up described in 313, but the doubt is how long this test should last. Starting from -34ºC to 74ºC at a rate of 17ºC/h would give a duration of 6.4h. Would say that this is the right approach? Another alternative would be ramp 17ºC in one hour; keep that temperature for another hour, and repeat the process until the maximum temperature is reached.

Please refer to the NEMA TS 2-2003 v02.06 standard section 2.2. This section includes a set of temperature tests that can be adapted to the RSU tests. Figure 2-1 shows a temperature profile beginning at ambient. The test operation would reduce to the minimum temp at 17 °C/h, soak the device at that temp, then raise to the maximum temp at 17 °C/h, soak the device at that temp, then return to ambient at 17 °C/h.
Since the procedure is geared for traffic signal control hardware, some details will need to be modified. For example, the RSU is powered by PoE rather than directly by AC. The important thing is that the unit is operating, except where the procedure calls for power to be removed.

[redacted] Is it possible to test to similar or fundamentally the same test specification and procedures as those given in the standards and still claim compliance. E.g. Temperature range is referred to in NEMA TS 2-2003 v02.06 as -34 to +74 but no test method specified in that document. Can we use an IEC 60068 series test and procedure or must it be a NEMA (or other US or int) based environmental test and procedure?

If the standard doesn't specify a test method, then please use an appropriate procedure to verify that it meets the spec. For the case you mentioned, there are some basic test procedures described in section 2.2 of NEMA TS 2-2003.

USDOT_RSU-Req_315-v001

[redacted] Standard environmental chambers have difficulty regulating the humidity below 10C. Should the test be run down to the required 4.4C at an unregulated humidity, or down to 10C at 95% humidity?

Defer to the testing company, which recommends to run the test down to 4.4C with unregulated humidity. Recommend referring to Table 2-1 in the NEMA TS 2-2003 standard referenced by this req.

[redacted] There are not many labs that can go through some of the test you have specified like blowing rain can we instead comply with IP66 or IP56 that tests many of the same effects of environmental solids and liquid effects.

The goal is for the device to operate through the conditions described in the test (e.g. blowing rain at 1.7 mm/min & 18 m/s). If you have an enclosure that's rated to a standard that meets the test requirements, then there's no need to repeat the tests.
(Perhaps a combination of analysis and testing would be effective. For example, for Req_318,

calculate the appropriate wind load on the device, then apply that force to the bracket for the test.)

[redacted] We have 3 different reference for vibration test in the document can we conduct only the one with the highest requirements or the most relevant one?

If the RSU passes a test from one standard that has higher requirements then it would satisfy the requirements of the standard with lower requirements. These is no need to repeat tests for the lower requirements.

[redacted] For the Climatic testing the test facility would only be able to test according to IEC 60068 or MIL-STD-810G. Is this acceptable?

Because many environmental requirements specify NEMA TS 2-2003 v02.06 it would be difficult to consider testing to other standards. If there are more appropriate tests, we would consider them in the next revision to the spec.

USDOT_RSU-Req_319-v001

[redacted] Looking at the some of the information in the MIL-STD you refer to is for jet aircraft in version G and for general use in version F, we are going to test base on version F.

Confusion stems from a reference in the MIL-STD-810F that wasn't updated to MIL-STD-810G. Instead of "514.5C-17 and 516.5", reference should be "514.6E-1 and 516.6" in MIL-STD 810G.

[redacted] 514.5C-17 refers to 810F NOT 810G – In 810G this is an aircraft vibration spec.

We are aware of this discrepancy. The correct figure in MIL-STD-810G is 514.6E-1.

USDOT_RSU-Req_319-v001
USDOT_RSU-Req_320-v001
USDOT_RSU-Req_439-v001

[redacted] Vibration and shocking: The specifications of MIL-STD-810G, IEC-60068 and IEC 60721 are all very large and have multiple categories and vibration levels. Is it possible to choose a worst case scenario?

In this case, IEC 60068/60721 are preferred for operating shock and vibe (USDOT_RSU-Req_320-v001). MIL-STD-810G should be followed for transportation shock and vibe

(USDOT_RSU-Req_439-v001). If some tests satisfy multiple requirements then there is no need to repeat them.

[redacted] In every test, how shall the RSU show evidence that it is working correctly?

Many requirements are tested in the functional test plan released at the same time as the 4.1 spec. This includes examples of tests to verify many functional requirements. We have not designed a test to address every requirement.

[redacted] The NEMA standard specifies that the device should withstand power spikes of 300V, when the nominal voltage is 120V. In our case the devices are powered by POE (between 37V and 57V) the 300V limit is the same? Or should it be proportional?

You are correct, the NEMA requirement is for devices that run from nominal 120 VAC. The RSUs are powered according to 802.3at, so the test would have to be adjusted for those minimum and maximum voltage levels. Basically, we need to know that the device operates at its minimum and maximum supply voltage at the minimum and maximum rated temperature.

[redacted] The NEMA document describes the usage of test switches to determine that the device works correctly when certain conditions are imposed (for example, in low or high temperature). There are no test switches for the RSU....

The purpose of test switches is to be able to operate the device from outside of the test chamber. Since most functions of the RSU are operable through an Ethernet interface, physical test switches will typically not be required.

[redacted] Where can you find the IEC 60068/60721 document?

The IEC standards should be available for purchase here: webstore.iec.ch

USDOT_RSU-Req_325-v001

[redacted] For IP testing they'd use BS EN 60529:1992+A2:2013, IP 66 (similar, but not the same) >>>Is this acceptable?

The enclosure should meet or exceed IP 66 or NEMA 4X.

USDOT_RSU-Req_331-v001
USDOT_RSU-Req_359-v001

[redacted] About the LEDs on the RSU: only two LEDs are required, correct (one for power and another for status with 3 possible colors)?

2 LEDs would be acceptable

USDOT_RSU-Req_346-v002

[redacted] We have decided on having an additional user (e.g.: "super_user") which has the same set of rights as the "root" user (the current user that we support to login in into the RSU). The password for the super_user is not changeable. For password recovery the user has to login as "super_user" and change the password for the root user. Having an additional user for password recovery, is this approach fine?

Leaving an unchangeable password on the RSU opens up risk related to password compromise. Some thoughts:

1) Ideally, there would be multiple user accounts implemented on the RSU. The different accounts would be provisioned with varying access permissions with the root account only being used sparingly (and if on a Linux-based system sudo would be more appropriate than logging in as root).
2) If the super_user account has the same privileges as the root user, then compromise of the super_user account would leave the device completely compromised. RSU operators should have the ability to modify any passwords on a regular basis so that the risk of password compromise is mitigated somewhat.
3) Is the assumption that the super_user password would be shared / the same across all RSUs? This would open up significant risk and is very similar to the issue that drove the propagation of the recently widespread Mirai botnet.
4) There should be restrictions on the ability to log into the root (and super_user) account remotely.
5) Using the super_user account with the above security controls applied for password recovery purposes would likely be acceptable, however if you implemented less-privileged accounts then you could use root for the same purpose. One CONOPS is that the root account password is tracked out of band (offline in a safe for example) by the RSU managers and brought out when needed for a password recovery.

USDOT_RSU-Req_437-v005

[redacted] How is the RSSI value supposed to be used for this function?

The intent is to filter out messages from distant or unreliable sources. Only messages received above a certain RSSI should be forwarded. Messages below that level should not be forwarded.

USDOT_RSU-Req_453-v002

[redacted] Requirement USDOT_RSU-Req_453-v002 (page 36) mentions OID 1.0.15628.4.4.x.. When I compile the MIB file (after correcting the previous errors), I don't see any OID 1.0.15628.4.4.

This is a typo in the RSU spec. The referenced OID should be "1.0.15628.4.1.4.x".

USDOT_RSU-Req_454-v002 - USDOT_RSU-Req_456-v002

[redacted] The following three requirements specify the removal, viewing and modification of messages in the Active Message directory, shouldn't the removal, viewing and modification of an active message be done in the MIB via an SNMP agent since the implementation of message directories is left to the device manufacturer?

In this version of the spec, interaction with the RSU is primarily intended to be done by SNMP. However, we had several requests to maintain the current method of managing Store and Repeat messages, at least for the time being. So the intent is that changes to the active messages done over SNMP should be reflected in the active message folder. The spec doesn't specify the directory structure, so the RSU vendor can store the active messages in whichever location they think is best.

USDOT_RSU-Req_495-v002

[redacted] Can you please let us know few details about "USDOT_RSU-Req_495-v002" requirement:
- Like Test case for it as it's not available in "Bench Test Plan-April, 2017" document.

This requirement is intended to generate an indication that an attempt was made to load a MIB that contains errors to the RSU. We didn't develop a test for this in our functional test plan because we don't plan to do a test for that particular requirement.

[redacted] Is there or will there be an independent certifying authority to present test reports etc. to for certification?

Certification will be done by one of the three certification labs established by USDOT: 7 Layers, Danlaw, and OmniAir.

[redacted] Is compliance simply a self-certification like CE mark? What evidence is required to be shown/available to others to check?

One of the three certification labs will certify most core requirements. The rest will be self-certified, however, Leidos will test some requirements and provide feedback only, not certification.

[redacted] Please define “accredited test facility” Which accreditations?

The test facility should have an appropriate accreditation such as ISO/IEC 17025.

[redacted] Can you give some examples on how the payload is supposed to look like? The spec just says “Payload=<DSRC message payload>”. Our assumption currently is that it is a hex string of the UPER encoded payload.

Your assumption is correct, J2735 specifies UPER and it’s expected to be hex. We haven’t specified the encoding since that is dependent upon the standards. Unfortunately, we don’t have an example to share right now.

[redacted] What is the difference between “encoded” and “raw”? Could you provide an example of a raw message?

Encoded payload is as described above. Raw payload is unencoded with each element described in a human-readable format. This may be a list of fields in the payload, similar to the “message dispatch items” info in an active message file.

[redacted] For “TxChannel=SCH” the spec sais “SCH refers to the #operator configured DSRC Service Channel)”. How is it configured, which parameter/OID?

This may be done using the rsuDCMSCH object.

[redacted] One general note on the message processing interface: We believe that the current way of receiving plain text files via unsecured open UDP ports raises a security risk for RSUs. For future releases therefore we suggest to use an authenticated mechanism (e.g. TLS) only for such a functionality.

This is a good point, and the intent is to move away from using text files and toward SNMP. However, the operator should have the ability to close any open ports if that is a concern. We have that noted for the next release.

USDOT_RSU-Req_550-v002

[redacted] The only way we can interpret the original is to have the Operating and Shock tests the SAME as the Transport test. This seems quite extreme. Is this what the actual intent was of the drafters?

If one test can satisfy both requirements then there’s no need to repeat the test. The intent is to assure that the device will survive a reasonable level of shock and vibration during transport,

installation, and operation. In a future revision, we will consider removing this vibration requirement in favor of Req_320.

[redacted] The testing environments in 516.6 do not match the intended RSU mounting scenarios for operational testing in any way. Why is this called out?

Shock testing is required to guarantee operation of the RSU throughout its lifetime after being subjected to (reasonable) shock events during transit, installation, or operation. For example, the unit may be dropped during installation or hit with flying debris while mounted in the field.

USDOT_RSU-Req_552-v002
USDOT_RSU-Req_321-v001

[redacted] What tests under J1113 2013 are required? This is normally a vehicle based standard so I fail to see how, say, J1113-11 (automotive conducted transients on power line) is relevant to a PoE+ powered device.

This requirement will be reconsidered in the next revision of the spec. IEC EN61000-4-6 has been recommended and would seem the most appropriate.

USDOT_RSU-Req_553- v002

[redacted] Is compliance simply a self-certification like CE mark? What evidence is required to be shown/available to others to check?

One of the three certification labs will certify most core requirements. The rest will be self-certified, however, Leidos will test some requirements and provide feedback.

[redacted] Please define “accredited test facility” Which accreditations?

The test facility should have an appropriate accreditation such as ISO/IEC 17025.

USDOT_RSU-Req_572-v001

[redacted] a. According to my understanding “Immediate Forward” is a “one-shot” function, meaning that the message is being sent out by the RSU just once as received by via SNMP. If that is true, how is the WSA mechanism for this supposed to work? Shall the RSU just send out one WSA prior to the message broadcast for that specific Immediate Forward message?

The RSU could recognize that an immediate forward message is being sent with some periodicity and send the WSA to advertise that service. When the IF message stops for some number of periods, then the WSA would stop advertising that service.

USDOT_RSU-Req_618-v002 and RSU MIB

[redacted] The SNMP OID for the "configurable period of time" for rsuTimeSourceLost NOTIFICATION-TYPE is not seen in the Spec. Could you please throw some light on the same.

This may be configurable by the vendor rather than by SNMP. If there is a need for this to be configured by SNMP, an OID may be added in the future. Otherwise, the term "configurable" may be changed to "vendor-defined".

[redacted] The RSU 4.1 Spec lacks info on the value of the configurable tolerance. What value can we have?

This value should be defined by the vendor. In the future, an OID may be added to make this configurable by SNMP. For now another means of setting the maximum clock skew would be acceptable. An example of the tolerance would be 100 us, but a more optimal number could be determined by the circumstances.

[redacted] For the rsuClockSkewError SNMP TRAP, our understanding is that, a reference clock is needed to check the skew rate for the system clock. In this case we need an additional time source as reference clock to check the skew rate. Is this understanding correct?

The intent is to give an indication of an incorrect or degraded clock or a potential security threat. This is important if there is a high skew rate in the system clock and the external (e.g. GPS) sources are not available. The skew rate would only be reported when the RSU does have those external sources. Every time the clock is updated, the RSU would do a compare of the internal clock and the update value it's being changed to. If that rate is beyond a configurable value, then it means that your internal clock is awful and the loss of a time source can be a big problem. So this is an additional indicator to the operator of the severity of a time source loss. Also, consider a bad actor on the roadside who broadcasts a false GPS signal with a false time. A jump in time resulting from the false signal would trigger a notice of large clock skew.

USDOT_RSU-Req_619-v001

[redacted] What are the mandatory roles that should be supported by the RSU?

This requires additional analysis, however to start we would recommend administrator, audit, and user.

[redacted] What kind of services can be accessed by these mandatory roles?

This also requires additional analysis, however a good breakdown would be:

- Administrator has access to all administrative functions with the exception of the ability to alter the security audit log. This role includes security-sensitive functions such as being able to load trust stores, load key material, and update users/groups/privileges.
- Audit supports the maintenance and review of the audit log on a regular basis. This includes the ability to rotate audit logs off-device to free up disk space.
- User has access to start /stop non-critical services. Ideally, you would remotely access a device using this role and elevate to one of the other more privileged roles once access is gained.
- You could also make a case for having a distinct security administrator role."

[redacted] In case of "Distinct Authentication and Authorization" - Does it mean multiple level of Authentication and Authorization is to be

This also requires additional design considerations be taking into account and is based heavily on the threat profile of the device itself. Ideally, there would be the ability to require multi-factor authentication to gain access to the elevated privilege (administrator, audit, security?) roles.

USDOT_RSU-Req_620-v001

[redacted] What are categorized as sensitive services? Can you give some examples of the same?

Some examples:

- Turning on/off the network interface card
- Loading private keys
- Loading trust anchors
- Viewing audit logs
- Removing audit logs (to rotate off)
- Starting/stopping services (e.g,. logging, ssh, etc)
- Starting /stopping web interface
- Starting/stopping network time protocol (NTP)

- Starting /stopping any custom scripts that may be loaded…
- Adding/deleting users
- Modifying privileges

USDOT_RSU-Req_621-v001

[redacted] What are categorized as sensitive data? Can you give some examples of the same?

Some examples:

- Audit log(s)
- User account database
- Password database
- Key material
- Any transaction logs that contain identifying information of some sort

USDOT_RSU-Req_622-v001

[redacted] What should be the behavior if the maximum number of attempts has been reached?

Ideally, a lockout timer should start that locks out the account for a minimum of 30 minutes.

USDOT_RSU-Req_635-v001
USDOT_RSU-Req_636-v001
USDOT_RSU-Req_615-v001

[redacted] There is no verification that is done by the RSU. What needs to be verified here (What OTA messages are to be verified?)

RSU should be verifying the IEEE 1609.2 signature applied to the OTA messages. See requirements below for additional verification that shall/should be conducted by the RSU as well.

USDOT_RSU-Req_607-v001 for example: "Data Protection: The roadside unit SHALL verify the integrity of the store-and-repeat message data prior to generating and transmitting IEEE 1609.2 secured messages that are derived from the message data.
USDOT_RSU-Req_609-v001: Data Protection: The roadside unit SHALL inhibit construction and transmission of an IEEE 1609.2-secured message derived from an integrity-failed store and repeat message.

USDOT_RSU_req_627-v001: Authentication: The roadside unit 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.

Application Layer PDU section pg. 11

[redacted] The specification says that the transmit parameters have to be part of the message itself and are then the OIDs are set by the RSU accordingly. On the other hand the test case specifies that the transmit parameters are set via SNMP first and the RSU shall then send a SPaT (with or without transmit parameters included?) based on these parameters without changing the OID. Is that understanding correct? Could you clarify how the functionality is really supposed to work?

The user should configure the Immediate Forward settings (PSID, Message ID, Mode, Channel, enable) using SNMP. Only the Immediate Forward messages sent to the appropriate port (default 1516) that match those preconfigured should be forwarded. All others should be ignored. This is reflected in the test plans correctly.

Active Message Files

[redacted] Can you give some examples on how the payload is supposed to look like? The spec just says "Payload=<DSRC message payload>". Our assumption currently is that it is a hex string of the UPER encoded payload.

Your assumption is correct, J2735 specifies UPER and it's expected to be hex. We haven't specified the encoding since that is dependent upon the standards. Unfortunately, we don't have an example to share right now.

[redacted] What is the difference between "encoded" and "raw"? Could you provide an example of a raw message?

Encoded payload is as described above. Raw payload is unencoded with each element described in a human-readable format. This may be a list of fields in the payload, similar to the "message dispatch items" info in an active message file.

[redacted] For "TxChannel=SCH" the spec sais "SCH refers to the #operator configured DSRC Service Channel)". How is that configured, which parameter/OID?

This may be done using the rsuDCMSCH object.

[redacted] We believe that the current way of receiving plain text files via unsecured open UDP ports raises a security risk for RSUs. For future releases therefore we suggest to use an authenticated mechanism (e.g. TLS) only for such a functionality.

This is a good point, and the intent is to move away from using text files and toward SNMP. However, the operator should have the ability to close any open ports if that is a concern. We have that noted for the next release.