|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_567- v001 | Physical Security: The roadside unit SHALL be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 2 Physical Security Requirements | FIPS 140-2 |
|  |  | USDOT\_RSU-  Req\_585- v001 | Physical Security: The roadside unit 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. | FIPS 140-2 |
|  |  | USDOT\_RSU-  Req\_344- v002 | Authentication: The roadside unit 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) | FIPS 140-2 Section  4.3.3 |
|  |  | USDOT\_RSU-  Req\_467- v001 | Authentication: The roadside unit SHALL support multiple SNMPv3 users each with an individual password |  |
|  |  | USDOT\_RSU-  Req\_345- v001 | Authentication: The roadside unit SHOULD support multi-factor authentication. |  |
|  |  |  |  | Secure Shell (SSH) |
|  |  | Version 2 (as |
|  |  | specified in IETF |
| USDOT\_RSU-  Req\_632- v002 | Authentication: The roadside unit SHOULD enforce multi-factor authentication on all SSH Version 2 sessions, and, if supported, all TLS- based remote access sessions to the roadside | RFC 4251, IETF  RFC 4252, IETF  RFC 4253, and  IETF RFC 4254) |
|  | unit. | Transport Layer |
|  |  | Security (TLS) |
|  |  | Protocol Version |
|  |  | 1.2 |
|  |  | USDOT\_RSU-  Req\_346- v002 | Authentication: The roadside unit SHALL support password recovery for the RSU User Accounts that cannot be violated by physical access alone. |  |
|  |  | USDOT\_RSU-  Req\_347- v002 | Configuration: The roadside unit configuration files SHOULD enforce digital signatures to prevent unauthorized modifications. | FIPS 186-4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_348- v001 | Access Control: The roadside unit SHALL restrict remote network access based on an IP Address Access Control List (ACL)  Note: The RSU can only be accessed from the IP Addresses contain in the ACL. |  |
|  |  | USDOT\_RSU-  Req\_350- v001 | Data Protection: The roadside unit local file system SHOULD be encrypted |  |
|  |  | USDOT\_RSU-  Req\_351- v002 | Interfaces: Each roadside unit Ethernet interface SHALL be protected by a configurable firewall with a default to be closed. |  |
|  |  | USDOT\_RSU-  Req\_440- v002 | Access Control: If so equipped, Web-Based access to the roadside unit SHALL only be through Hypertext Transfer Protocol Secure (HTTPS) |  |
|  |  | USDOT\_RSU-  Req\_442- v002 | Data Protection: the roadside unit SHOULD synchronize its system clock to a Network Time Protocol (NTP) Service in the event that it loses GPS fix. |  |
|  |  | USDOT\_RSU-  Req\_355- v001 | Authentication: If the roadside unit synchronizes it's system clock to a Network Time Protocol (NTP) service, the device SHALL authenticate messages received from the NTP service | Req\_442 |
|  |  | USDOT\_RSU-  Req\_356- v003 | Access Control: The roadside unit SHALL only be accessible through the following network protocols:   * Secure Shell version 2 (SSHv2) * SNMPv3 * SCP * TLS (HTTPS) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_583- v001 | Configuration: network protocol Secure Shell version 2 SHOULD be configured as follows:   * Root Login Disable root * Use certificate-based authentication, * rate-limited (to slow down brute-force attempts) * use FIPS 140-2-compliant cryptography | FIPS 140-2 |
|  |  | USDOT\_RSU-  Req\_606- v001 | Data Protection: The roadside unit SHALL immediately apply integrity protections to the store-and-repeat message data following SNMP- secured download to the roadsideunit. | Section 3.4.4,Section 3.4.5, Req\_607 |
|  |  | USDOT\_RSU-  Req\_607- v001 | 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. | Section 3.4.4 and  Section 3.4.5 |
|  |  | 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. | Section 3.4.4 and  Section 3.4.5 |
|  |  | USDOT\_RSU-  Req\_615- v001 | Notification: The roadside unit SHALL notify a remote host via SNMPv3:   * if an Active Message fails an Integrity check * if a configurable number of consecutive authentication attempts have failed * if the signature of a signed DSRC message has failed verification |  |
|  |  | USDOT\_RSU-  Req\_616- v001 | Notification: If secure storage is available, the roadside unit SHALL notify a remote host via SNMPv3 if the secure parameters stored in secure storage have failed an Integrity check. | Req\_579 |
|  |  | USDOT\_RSU-  Req\_617- v001 | Notification: If FIPS 140-2 level 3 is implemented, the roadside unit 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. | FIPS 140-2 Section  4.5 Level 3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_619- v001 | Access Control: The roadside unit SHALL enforce clear associations between roles, services and the distinct authentication and authorizations required to access those services. |  |
|  |  | USDOT\_RSU-  Req\_620- v001 | Access Control: Access to sensitive services SHALL require an authenticated, authorized role. |  |
|  |  | USDOT\_RSU-  Req\_621- v001 | Access Control: Access to sensitive data SHALL require an authenticated, authorized role. |  |
|  |  | USDOT\_RSU-  Req\_622- v001 | Authentication: The roadside unit SHALL be configurable to limit the number of repeated authentication attempts for services requiring authentication. |  |
|  |  | USDOT\_RSU-  Req\_623- v002 | Authentication: The roadside unit SHOULD utilize certificate pinning to secure all TLS sessions with the SCMS Device Configuration Manager and other SCMS nodes to which it connects. | Transport Layer Security (TLS) Protocol Version  1.2 (IETF RFC 5246 and IETF RFC 7469) with cipher suites pinned to USDOT Security Credential Management System Design: Security Credential Management System Proof– of–Concept Implementation EE  Requirements and |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_625- v001 | Authentication: The roadside unit SHALL terminate a TLS session if the server public key certificate signature verification fails during TLS session establishment. | Transport Layer Security (TLS) Protocol Version 1.2  (IETF RFC 5246, |
|  |  | 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. |  |
|  |  | USDOT\_RSU-  Req\_628- v002 | Authentication: Services requiring role- or identity-based authentication SHALL meet the authentication requirements of FIPS 140-2, Section 4.3 Level 2 and any supporting FIPS 140-  2 implementation guidance. | FIPS 140-2, Section  4.3 Level 2 and Level 3 |
|  |  | USDOT\_RSU-  Req\_629- v001 | Authentication: Services requiring authentication SHALL meet the single attempt and multiple attempt authentication strength requirements of FIPS 140-2, Section 4.3. | FIPS 140-2, Section  4.3 |
|  |  | USDOT\_RSU-  Req\_630- v001 | Authentication: The roadside unit SHALL require SSH Version 2 or TLS Version 1.2 using mutual (two way) public key credential authentication for all authorized user sessions. | Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF  RFC 4252, IETF  RFC 4253, and  IETF RFC 4254)  Transport Layer Security (TLS) Protocol Version 1.2 |
|  |  | USDOT\_RSU-  Req\_631- v001 | Authentication: The roadside unit SHALL require HTTPS using mutual (two way) public key credential authentication for all HTTPS connections to the roadside unit. |  |
|  |  | USDOT\_RSU-  Req\_635- v001 | Configuration: The roadside unit SHALL be configurable regarding the maximum frequency (number per second) or ratio (percentage) of DSRC message digital signatures to verify based on PSID. | Section 3.4.4 and  Section 3.4.5 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_636- v001 | Configuration: The roadside unit SHALL be able to be configured whether to accept, drop, or respond to application-specific messages signed with expired certificates. | Section 3.4.4 and  Section 3.4.5 |
|  |  | USDOT\_RSU-  Req\_638- v001 | Data Protection: The roadside unit SHALL cryptographically protect the integrity of all configuration information provided by the SCMS Device Configuration Manager (DCM). |  |
|  |  | USDOT\_RSU-  Req\_639- v002 | Data Protection: All cryptographic keys SHALL be established or generated using a FIPS Approved and allowed key generation and key establishment mechanisms. | FIPS 140-2 Annex A  and Annex D |
|  |  | USDOT\_RSU-  Req\_640- v001 | Data Protection: All sensitive roadside unit system files and application files SHALL be digitally signed using a digital signature algorithm listed in FIPS 186-4. | FIPS 186-4 |
|  |  | USDOT\_RSU-  Req\_641- v001 | Data Protection: The roadside unit SHALL successfully verify the digital signature on all sensitive roadside unit system and application files prior to exposing any services. |  |
|  |  | USDOT\_RSU-  Req\_642- v001 | Data Protection: The roadside unit SHALL implement a secure mechanism in software to securely store and provide strict access controls to all sensitive security parameters, including:  -TLS public and private keys (as used for HTTPS or other TLS tunneling, including with the SCMS)  -SSH public and private keys  -Passwords  -SNMP keys and passphrases  -Any sensitive security parameters not stored in a hardware secure storage mechanism | Req\_579 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_643- v001 | Data Protection: Software secure storage SHALL:  -prevent read-access to all stored security parameters,  -maintain integrity of all security parameters, including associations of keys with entities and processes  -check the integrity of stored security parameters when accessing  -prevent unauthorized modification of security parameters, except by authorized users  -prevent unauthorized addition of security parameters, except by authorized users  -prevent unauthorized substitution of security parameters, except by authorized users  -encrypt all sensitive security parameters when not in use | Req\_579 |
|  |  | USDOT\_RSU-  Req\_644- v001 | Data Protection: The roadside unit SHALL store passwords in secure storage only after modifying via a one-way cryptographic function. | Req\_579 |
|  |  | USDOT\_RSU-  Req\_645- v001 | Data Protection: The roadside unit SHALL zeroize all non-factory installed parameters, cryptographic keys, applications, data and configurations when undergoing a factory reset. | Req\_568 |
|  |  | USDOT\_RSU-  Req\_646- v001 | Data Protection: Upon sudden loss of external power, the roadside unit SHALL undergo a shutdown procedure that preserves file system integrity. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_647- v001 | Interfaces: The roadside unit SHALL utilize TLS versions and cipher suites consistent with SCMS interface specifications. | USDOT Security Credential Management System Design: Security Credential Management System Proof– of–Concept Implementation EE  Requirements and Specifications Supporting |
|  |  | USDOT\_RSU-  Req\_648- v001 | Interfaces: Services and protocols SHALL be able to be inhibited according to physical interface, source/destination IP address and source/destination ports |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yes** | **No** | **ReqID** | **Description** | **Reference** |
|  |  | USDOT\_RSU-  Req\_649- v002 | Logging: The roadside unit SHALL write the following entries to the System Log File:   * GPS location and time data on a configurable interval * metrics on packet integrity or transmission/reception errors * all authentication parameter modifications * attempts to perform a service allocated to a role(s) for which the entity is not authenticated * authorization failures when a role or identity attempts access services and data requiring authorization * input and output protocol violations, including encoding errors and invalid parameters * session management failures in each of the session-based network protocols it supports * all additions, modifications and removal of secret, public and private cryptographic keys * success or failure of digitally signing all sensitive roadside unit system and application files using a digital signature algorithm listed in FIPS 186-4 * any expired IEEE 1609.2 public key credentials it has stored * any expired X.509 public key credentials it has stored * pending expirations of all public key | FIPS 186-4 |