P1609.2b

Submitter Email: wwhyte@onboardsecurity.com
Type of Project: Modify Existing Approved PAR
PAR Request Date: 20-Sep-2018
PAR Approval Date: 30-Oct-2018
PAR Expiration Date: 31-Dec-2021
Status: Modification to a Previously Approved PAR for an Amendment
Root PAR: P1609.2b **Approved on:** 15-Jun-2017
Root Project: 1609.2-2016

1.1 Project Number: P1609.2b
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
Amendment 2: Protocol Data Unit (PDU) Functional Types and Encryption Key Management

Changes in title: Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages Amendment 2: Protocol Data Unit (PDU) Functional Types and Encryption Key Management

3.1 Working Group: Dedicated Short Range Communication Working Group (VT/ITS/1609_WG)
Contact Information for Working Group Chair
Name: Thomas Kurihara
Email Address: t.kurihara@ieee.org
Phone: 703 516 9650
Contact Information for Working Group Vice-Chair
Name: Kevin Smith
Email Address: kevin.s.smith@cox.net
Phone: 7604194506

3.2 Sponsoring Society and Committee: IEEE Vehicular Technology Society/Intelligent Transportation Systems (VT/ITS)
Contact Information for Sponsor Chair
Name: Thomas Kurihara
Email Address: t.kurihara@ieee.org
Phone: 703 516 9650
Contact Information for Standards Representative
Name: Thomas Kurihara
Email Address: t.kurihara@ieee.org
Phone: 703 516 9650

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 10/2018
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 02/2019

5.1 Approximate number of people expected to be actively involved in the development of this project: 25
5.2.a. Scope of the complete standard: This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

5.2.b. Scope of the project: This amendment extends the secure communications functionality of Std 1609.2-2016 and Std 1609.2a to provide one additional field in the signed data structure to support Secure Protocol Data Units (SPDUs) received by a functional entity other than an application.

Additionally, this project clarifies the use of the encryption primitives

Changes in scope of the project: ~~Scope~~ This amendment extends the secure communications functionality of Std 1609.2-2016 and Std 1609.2a to provide one additional ~~types~~field in the signed data structure to support Secure Protocol Data Units (SPDUs) received by a functional entity other than an application. Additionally, this project clarifies the use of ~~Service~~the ~~Specific~~encryption ~~Permissions;~~primitives ~~adds~~within ~~additional~~1609.2-2016,

within 1609.2-2016, explicitly allowing an ephemeral data encryption key to be exported from the encryption primitive for later reuse.

Finally, this project expands some elements of the Protocol Implementation Conformance Statement (PICS) proforma to provide better coverage of the approach to peer-to-peer certificate distribution favored by the European Telecommunications Standards Institute (ETSI).

~~informative~~explicitly ~~material;~~allowing ~~and~~an ~~corrects~~ephemeral ~~errors~~data ~~and~~encryption ~~ambiguities~~key ~~discovered~~to ~~since~~be exported from the ~~publication~~encryption primitive for later reuse. Finally, this project expands some elements of the ~~previous~~Protocol ~~amendment~~Implementation Conformance Statement (PICS) proforma to provide better coverage of the approach to peer-to-peer certificate distribution favored by the European Telecommunications Standards Institute (ETSI).

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: The safety-critical nature of many Wireless Access in Vehicular Environments (WAVE) applications makes it vital that services be specified that can be used to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay. Additionally, the fact that the wireless technology will be deployed in communication devices in personal vehicles as well as other portable devices, whose owners have an expectation of privacy, means that in as much as possible the security services must be designed to respect privacy and not leak personal, identifying, or linkable information to unauthorized parties. This standard describes security services for WAVE management messages and application messages designed to meet these goals.

5.5 Need for the Project: ISO TC 204 WG 18 has been developing standards that use IEEE 1609.2 mechanisms to protect secure sessions. In this process the ISO WG has identified that there are secured PDUs related to application activities that may be consumed by an entity other than the application itself. These functional entities include the TLS handshake engine and a security subsystem associated with the application process that manages access control decisions for the application. 1609.2 and 1609.2a currently provide no mechanism to indicate the functional entities intended to consume a payload. This means that there is a risk that a payload intended for one functional entity could be accidentally or maliciously directed to a different one, creating a security vulnerability. This project adds an additional field to the HeaderInfo structure in 1609.2 to distinguish the intended functional entity type to receive a PDU, removing that risk.

5.6 Stakeholders for the Standard: The stakeholders for the project are the U.S. Department of Transportation Joint Intelligent Transportation Systems Office, automobile manufacturers, State and local transportation officials, toll authorities and toll tag manufacturers, public safety officials, commercial vehicle manufacturers, public transit officials, and providers of certificate management services. In addition, users of ISO 21177 will make use of the additional functionality from this amendment.

Intellectual Property
6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No
6.1.b. Is the Sponsor aware of possible registration activity related to this project?: No

---

7.1 Are there other standards or projects with a similar scope?: No
7.2 Joint Development
Is it the intent to develop this document jointly with another organization?: No

---

8.1 Additional Explanatory Notes: Since the PAR was originally proposed, representatives from ETSI have requested that the encryption key management functionality be included in this amendment in order to facilitate European deployment