

IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages

IEEE Vehicular Technology Society

Sponsored by the
Intelligent Transportation Systems Committee

IEEE Std 1609.2™-2016

(Revision of
IEEE Std 1609.2-2013)

IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages

Sponsor

**Intelligent Transportation Systems Committee
of the
IEEE Vehicular Technology Society**

Approved 29 January 2016

IEEE-SA Standards Board

Abstract: 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.

Keywords: cryptography, IEEE 1609.2™, security, wireless access in vehicular environments (WAVE)

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1 March 2016. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-0767-0 STD20841
Print: ISBN 978-1-5044-0768-7 STDPD20841

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://ieeexplore.ieee.org/xpl/standards.jsp> or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Dedicated Short Range Communications Working Group had the following membership:

Thomas M. Kurihara, *Chair*
Justin McNew, John Moring, William Whyte, *Vice Chairs*

Mike Brown	Carl Kain	Richard Roy
Hanbyeog Cho	John Kenney	Kevin Smith
Hans-Joachim Fischer	Bill Lattin	Jasja Tijink
Ramez Gerges	Jules Madey	Michaela Vanderveen
Aleksandar Gogic	Sean Maschue	George Vlantis
Shubha Gopalakrishna	Jim Misener	Jason Wang
Gloria Gwynne	Frank Perry	Aaron Weinfield
Ronald Hochnadel	Randy Roebuck	

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Nobumitsu Amachi	Piotr Karocki	Alon Regev
Lee Armstrong	John Kenney	Richard Roy
William Byrd	Stuart Kerry	Bartien Sayogo
Keith Chow	Dmitri Khijniak	Kevin Smith
Sourav Dutta	Thomas M. Kurihara	Rene Struik
Richard Edgar	Paul Lambert	Walter Struppler
Marc Emmelmann	Jeremy Landt	Jasja Tijink
Pedro Fernandes	Justin McNew	Steven Tilden
Randall Groves	John Moring	Thomas Tullia
Gloria Gwynne	Michael Newman	Dmitri Varsanofiev
Ronald Hochnadel	Alexandros Nikitas	John Vergis
Werner Hoelzl	Satoshi Oyama	George Vlantis
David Hunter	Venkatesha Prasad	Hung-Yu Wei
Noriyuki Ikeuchi		William Whyte

When the IEEE-SA Standards Board approved this standard on 29 January 2016, it had the following membership:

Jean-Philippe Faure, *Chair*
Vacant, *Vice Chair*
John Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams	Ronald W. Hotchkiss	Gary Robinson
Masayuki Ariyoshi	Michael Janezic	Mehmet Ulema
Ted Burse	Joseph L. Koepfinger*	Yingli Wen
Stephen Dukes	Hung Ling	Howard Wolfman
Jianbin Fan	Kevin Lu	Don Wright
J. Travis Griffith	Annette D. Reilly	Yu Yuan
Gary Hoffman		Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1609.2™-2016, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages.

5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC/WAVE, hereafter simply WAVE), as specified in a range of standards including those generated by the IEEE P1609 working group, enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. This connectivity makes possible a range of applications that rely on communications between road users and road operators, including vehicle safety, public service, commercial fleet management, tolling, and other operations.

With improved communications come increased risks, and the safety-critical nature of many 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 personal vehicles, whose owners have a right to privacy, means that in as much as possible the security services should respect that right and not leak personal, identifying, or linkable information to unauthorized parties.

With this in mind, at the time that IEEE P1609 was established to develop the standards for the WAVE wireless networking protocols, the IEEE also established IEEE P1556 (later renumbered as IEEE Std 1609.2) to develop standards for the security techniques that will be used to protect the services that use these protocols. These applications face unique constraints. Many of them, particularly safety applications, are time-critical: the processing and bandwidth overhead due to security must be kept to a minimum, to improve responsiveness and decrease the likelihood of packet loss. For many applications, the potential audience consists of all vehicles on the road in North America; therefore, the mechanism used to authenticate messages must be as flexible and scalable as possible, and must accommodate the smooth removal of compromised WAVE devices from the system. Additionally, as mentioned above, the privacy of privately owned and operated vehicles, and potentially other personal devices within the WAVE system, must be respected as far as technically and administratively feasible.

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
1.3 Document organization	2
1.4 Document conventions	2
1.5 Testing considerations	2
2. Normative references	2
3. Definitions, abbreviations, and acronyms	4
3.1 Definitions	4
3.2 Abbreviations and acronyms	10
4. General description	12
4.1 WAVE protocol stack overview	12
4.2 Secure data service (SDS)	15
4.3 Security services management entity (SSME)	18
4.4 Behavior of SDEEs	20
5. Cryptographic operations and validity	20
5.1 Certificate validity	20
5.2 Signed SPDU validity	33
5.3 Cryptographic operations	41
6. Data structures	46
6.1 Presentation and encoding	46
6.2 Integer types	46
6.3 Secured protocol data units (SPDUs)	47
6.4 Certificates and other security management data structures	59
7. Certificate revocation lists (CRLs) and the CRL Verification Entity	74
7.1 General	74
7.2 CRL Verification Entity specification	74
7.3 Data structures	75
7.4 CRL: 1609.2 Security envelope	80
8. Peer-to-peer certificate distribution (P2PCD)	85
8.1 General	85
8.2 P2PCD operations	86
8.3 P2PCD Entity specification	96
8.4 Data structures	97
9. Service primitives and functions	98
9.1 General comments and conventions	98
9.2 Identifiers used in the interface specification	100
9.3 Sec SAP	106
9.4 SSME SAP	139
9.5 SSME-Sec SAP	162
Annex A (normative) Protocol Implementation Conformance Statement (PICS) proforma	167
A.1 Instructions for completing the PICS proforma	167

A.2 PICS proforma—IEEE Std 1609.2	169
Annex B (normative) ASN.1 modules	179
B.1 1609.2 security services	179
B.2 Certificate revocation list (CRL).....	189
B.3 Peer-to-peer certificate distribution (P2PCD).....	192
Annex C (informative) Specifying the use of IEEE Std 1609.2 by SDEEs.....	194
C.1 General.....	194
C.2 IEEE 1609.2 security profiles	194
C.3 IEEE 1609.2 security profile proforma	204
C.4 Service Specific Permissions (SSP).....	206
C.5 Assurance level.....	207
C.6 Recommendations on certificates	207
Annex D (informative) Examples and use cases	208
D.1 Guidance for SDEE specifiers and implementers.....	208
D.2 Processing CRLs.....	209
D.3 Constructing a certificate chain	210
D.4 Peer-to-peer certificate distribution	215
D.5 Example data structures	222
Annex E (informative) Deployment considerations	226
Annex F (informative) Bibliography	228

IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

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.

1.2 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.