IEEE STANDARDS ASSOCIATION IEEE

# 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
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1609.2™-2016
(Revision of
IEEE Std 1609.2-2013)

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

**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**

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

**This is a Redline Document produced by Techstreet, a business of Thomson Reuters.**

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fastpaced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.



Documents Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

## Redline Processing Notes:

1. ~~**Red Text**~~ - Red strikethrough text denotes deletions.

2. **Blue Text** - Blue underlined text denotes modifications and additions.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

**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.*

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

## 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.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

## 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.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

## 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.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

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

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

Nobumitsu Amachi
Lee Armstrong
William Byrd
Keith Chow
Sourav Dutta
Richard Edgar
Marc Emmelmann
Pedro Fernandes
Randall Groves
Gloria Gwynne
Ronald Hochnadel
Werner Hoelzl
David Hunter
Noriyuki Ikeuchi
Piotr Karocki
John Kenney
Stuart Kerry
Dmitri Khijniak
Thomas M. Kurihara
Paul Lambert
Jeremy Landt
Justin McNew
John Moring
Michael Newman
Alexandros Nikitas
Satoshi Oyama
Venkatesha Prasad
Alon Regev
Richard Roy
Bartien Sayogo
Kevin Smith
Rene Struik
Walter Struppler
Jasja Tijink
Steven Tilden
Thomas Tullia
Dmitri Varsanofiev
John Vergis
George Vlantis
Hung-Yu Wei
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
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Jianbin Fan
J. Travis Griffith
Gary Hoffman
Ronald W. Hotchkiss
Michael Janezic
Joseph L. Koepfinger*
Hung Ling
Kevin Lu
Annette D. Reilly
Gary Robinson
Mehmet Ulema
Yingli Wen
Howard Wolfman
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus


Copyright © 2016 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

## 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.


Copyright © 2016 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

## 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



Copyright © 2016 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

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


Copyright © 2016 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

# 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.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016

## 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.

## 1.3 Document organization

Clause 1 provides an overview of the document. Clause 2 contains the normative references. Clause 3 contains definitions and abbreviations. Clause 4 provides a general description of WAVE Security Services and their use. Clause 5 specifies validity of signed secured protocol data units (SPDUs), correctness of encrypted protocol data units (PDUs), and core cryptographic operations ~~how WAVE Security Services may be used by calling entities to execute specific security use cases~~. Clause 6 specifies the encoding and structure of messages generated and consumed by WAVE Security Services. Clause 7 provides a specification of certificate revocation lists, which are a mechanism used to distribute information about certificates that should not be trusted. Clause 8 specifies mechanisms for peer-to-peer certificate distribution. Clause 9 defines the primitives used to communicate between WAVE Security Services and other functional entities.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

Annex A provides a Protocol Implementation Conformance Statement (PICS) proforma. Annex B provides ASN.1 modules. Annex C provides a description of the IEEE 1609.2 security profile and a proforma that may be used by developers of applications (or other entities that invoke WAVE Security Services) to specify options for how those applications are to interact with WAVE Security Services. ~~Annex C provides an IEEE 1609.2 security profile for the Basic Safety Message (BSM) specified by the Society of Automotive Engineers (SAE).~~ Annex D provides examples, including examples of encoded ~~protocol data united (PDU)~~ datagrams and sample process flows, from the point of view of an entity invoking WAVE Security Services rather than from the point of view of WAVE Security Services. Annex E describes other considerations that impact the deployment of a secure communications system using the techniques of this standard ~~provides an informative rationale and FAQ. Annex F is a copyright statement covering the text from Clause 6 that was excerpted from other sources~~. Annex F provides an informative bibliography.

## 1.4 Document conventions

Unless otherwise stated, conventions follow those in IEEE Std 802.11™ [B11][1], including conventions for the ordering of information elements within data streams.

Numbers are decimal unless otherwise noted. Numbers preceded by 0x are to be read as hexadecimal, so that 0xFF is equivalent to "FF hexadecimal". Occasionally, this standard includes representations of octet strings in hexadecimal form; these strings are indicated as hexadecimal on a case-by-case basis.

Figures are used for illustration and are informative, unless otherwise noted.

[1] The numbers in brackets correspond to those of the bibliography in Annex F.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

## 1.5 Testing considerations

The services defined in this standard, with the exception of the peer-to-peer certificate distribution service specified in Clause 8, operate over internal interfaces that are not directly observable in normal operations. Conformance claims made about an implementation of this standard can only be fully tested by direct access to the specific interfaces of that implementation. This standard does not provide a normative interface specification, so an implementation of a test process is not guaranteed a standard interface that may be used to access the implementation under test.

## ~~1.5 Note to implementers~~

~~Future versions of this standard may differ significantly from the current version. In particular, international harmonization efforts, advances in cryptanalysis, and other considerations make it likely that future versions of this standard will not preserve backwards compatibility with the current version. Changes of data structures in future versions of the standards will be reflected by changes in the version numbers within those data structures.~~

## 2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard (SHS), Aug. 2015. Available from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf ~~October 2008~~.[2]

Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS), July 2013. Available from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES), Nov. 2001. Available from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

IEEE Std 1363™-2000, IEEE Standard Specifications for Public Key Cryptography. [3, 4]

IEEE Std 1363a™-2004, IEEE Standard Specifications for Public Key Cryptography—Amendment 1: Additional Techniques.

[2] FIPS publications are available from the National Technical Information Service (NTIS), U.S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (http://www.ntis.org/).

[3] IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08855-1331, USA (http://standards.ieee.org/).

[4] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

IEEE Std 1609.0™/D1.0, April 2011, Draft SIEEE Guide for Wireless Access in Vehicular Environments (WAVE)—Architecture.[5]

IEEE Std 1609.3 2010™, Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services.

IEEE Std 1609.12 2012™, Standard for Wireless Access in Vehicular Environments (WAVE)—Identifier Allocations.

IETF Request for Comments: 3629, UTF-8, A Transformation Format of ISO 10646.[5]

IETF Request for Comments: 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation.

ITU-T Recommendation X.680 (11/2008), Information Technology—Abstract Syntax Notation One (ASN.1): Specification of Basic Notation, 2008. Available from http://handle.itu.int/11.1002/1000/9604.

ITU-T Recommendation X.696 (08/2014), Information Technology—Specification of Octet Encoding Rules (OER), 2014. Available from http://www.itu.int/rec/T-REC-X.696-201408-I.

[5] This IEEE standards project was not approved by the IEEE SA Standards Board at the time this publication went to press. For information about obtaining a draft, contact the IEEE.

[5] IETF publications are available from http://www.ietf.org.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

NIMA Technical Report TR8350.2, "Department of Defense World Geodetic System 1984, Its Definition and Relationships with Local Geodetic Systems."~~7~~ Available from http://earth-info.nga.mil/GandG/ publications/tr8350.2/tr8350_2.html

NIST Special Publication SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. [6]

Standards for Efficient Cryptography Group, "SEC 1: Elliptic Curve Cryptography," Version 2.0, May 21, 2009.[7]

Standards for Efficient Cryptography Group, "SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)," ~~Working Draft~~ Version 1.0~~.97~~, ~~March 2011~~ Jan. 24, 2013.

United Nations Statistics Division, "Composition of Macro Geographical (Continental) Regions, Geographical Sub-Regions, and Selected Economic and Other Groupings," [referred to as "UN Region Codes"] revision of 31 Oct. 2013. Available from http://unstats.un.org/unsd/methods/m49/m49regin.htm.

[6] NIST special publications are available from http://csrc.nist.gov/publications/nistpubs/.

[7] SECG publications are available from http://www.secg.org.

~~7 This technical report is available from http://earth-info.nga.mil/GandG/tr8350/tr8350_2.html.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

United States Census, 2010 FIPS Codes for Counties and County Equivalent Entities. Available from http://www.census.gov/geo/reference/codes/cou.html.

# 3. Definitions, abbreviations, and acronyms

## 3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[8]

**advanced encryption standard (AES)**: Federal Information Processing Standard (FIPS) 197, ~~A U.S. government standard~~ specifying a symmetric block cipher; also, the block cipher specified in that standard.

**application:** A higher layer entity that may make use of WAVE communication facilities.

**Application** ~~**operational**~~ **permissions**: The actions a certificate holder is allowed to take as stated in their certificate. Expressed in this standard using Provider Service Identifiers (PSIDs).

**associated certificate** (of a private key): The certificate used to verify signatures generated by that private key.

[8]*IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**associated public key** (of a certificate): The public key that is used to verify signatures associated with a certificate.

**asymmetric cryptographic algorithm**: A cryptographic algorithm that uses two related keys, a public key and a private key, such that the public key is derived from the private key but, given only the public key, it is computationally infeasible to derive the private key.

**authenticated channel**: A logical communications channel such that the receiver has assurance that the sender is who they claim to be, and that modifications to the data can be detected. A channel may be authenticated by applying cryptographic mechanisms to the channel itself, or by checking the transmitted protocol data units (PDUs) by some out-of-band mechanism.

**authentication**: A cryptographic service that provides assurance that the sender of a ~~communication~~ protocol data unit (PDU) is who they claim to be.

**authorization**: A cryptographic service that provides assurance that the sender of a protocol data unit (PDU) is entitled to certain permissions.

**authorization certificate**: A certificate that is used to validate application protocol data units (PDUs) other than certificate requests.

**block cipher**: A symmetric encryption algorithm that processes data in blocks, typically of 8 or 16 octets.

**certificate**: *See* **digital certificate**.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

~~**Basic Safety Message (BSM)**: A message, described in SAE J2735, used to announce the status of an object such as a vehicle, pedestrian, or roadside worker.~~

~~**calling entity:** A functional entity that invokes WAVE Security Services.~~

**certificate authority (CA) certificate**: A certificate that is used to verify other certificates. ~~a type of *security management certificate.*~~

**certificate authority (CA)**: An entity that issues certificates~~. A correctly functioning certificate authority has procedures in place to ensure that certificates are only issued~~ to entities that are entitled to them.

**certificate chain**: An ordered ~~list~~ set of certificates such that each certificate ~~in the list~~ (except for the ~~first~~ top) was issued by the certificate ~~before~~ above it in the list. *See also*: ~~**full**~~ **complete certificate chain**; **partial certificate chain**.

**certificate holder**: The entity authorized to use a particular digital certificate to establish trust. The certificate holder can carry out operations using the private key corresponding to the certficate's public key. A certificate holder's certificate is referred to as a *locally held certificate.*

**certificate management information**: Information that allows the secure data service to determine the trustworthiness of certificates and received data.

**certificate revocation list (CRL ~~distribution center~~) distribution center**: ~~A networked~~ An entity that stores and distributes certificate revocation lists (CRLs).

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**certificate revocation list (CRL) series (CRL series)**: An integer used to assign different certificates issued by the same certificate authority (CA) to distinct sets, such that the certificates in different sets appear on different revocation lists if revoked.

**certificate revocation list (CRL)**: A list identifying certificates that have been revoked. *See*: **revocation**.

**certificate revocation list (CRL) signer**: An entity authorized to sign certificate revocation lists (CRLs).

**certificate signing request (CSR)**: A ~~communication~~ protocol data unit (PDU) sent from an entity to a certificate authority (CA), requesting that the ~~certificate authority issue~~ CA issues a certificate on behalf of the entity.

**chains to**: A digital certificate A *chains to* another certificate B if B is above A in the certificate chain (q.v.) from A to the root.

**complete** ~~**full**~~ **certificate chain**: A certificate chain in which the top certificate is a root certificate and the bottom certificate is an end-entity certificate.

**confidentiality**: A cryptographic service that provides assurance that only the intended recipients of a protocol data unit (PDU) can read it.

**consistency conditions**: Criteria for validity of a signed protocol data unit (PDU) that depend only on the contents of the signed secured protocol data unit (SPDU) and not on the state of the receiver.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

~~**communications certificate:** A certificate used to sign either secure data or a *WAVE Service Advertisement*.~~

~~**computationally infeasible:** An operation that requires an exceptionally large amount of computing power to complete. The threshold for computational infeasibility will rise over time as computing power at a given price point increases.~~

**counter mode with cipher block chaining message authentication code (CCM)**: A mode of operation of a block cipher ~~in which~~ where the data is encrypted with a keystream, which in turn is generated by encrypting an incrementing counter, and in turn authenticated with a message authentication code calculated using cipher block chaining mode.

**critical information field**: An information field necessary to establish the validity of a signed secured protocol data unit (SPDU).

**cryptographic type** (of a certificate): How a certificate transfers information about its associated public key (q.v.). Cryptographic types of certificate are: **implicit certificate**; **explicit certificate**.

**cryptographic verification**: The process of determining whether a signature on a signed ~~communication~~ secured protocol data unit (SPDU) is consistent with the ~~communication~~ SPDU and the private key.

**cryptographically secure hash function**: A function that maps an arbitrary-length input into a fixed-length output (the hash value) such that (a) it is computationally infeasible to find an input that maps to a specific hash value and (b) it is computationally infeasible to find two inputs that map to the same hash value. All hash functions used in this document are cryptographically secure hash functions.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**Cryptomaterial Handle**: A reference to a private key and the associated public key or certificate, used to indicate to the secure data service that the referenced key should be used in a particular operation ~~stored within the security processing services~~.

**cryptomaterial**: A private key, a public key, or a certificate.

**data plane:** A component of the abstract architecture containing entities that exchange user data.

**decode**: To convert an array of octets into a data structure. *Contrast*: **decrypt, encode.**

**decrypt**: To convert unreadable, encrypted data to readable, decrypted data using a decryption algorithm and a key. *Contrast*: **decode, encrypt.**

**decryption algorithm**: An algorithm that takes as input ciphertext and a key and (if the correct key is provided) produces the original plaintext.

**delta certificate revocation list (delta CRL)**: A certificate revocation list that carries information only about certificates that were revoked within a certain time period. *Contrast*: **full certificate revocation list**.

**(permitted) depth of chain** (in a certificate authority (CA) certificate's permissions): The length that a certificate chain is permitted to be, starting from the certificate with which the depth value is associated and ending with an end-entity certificate.

**digital certificate**: A digitally signed document binding a public key to an identity and/or a set of permissions.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**direct hashing**: Creating a hash of particular data by passing that data through a hash function without including any additional data or processing.

**dubious certificate**: A certificate for which the most recent certificate revocation list (CRL) is overdue, i.e., it is scheduled to be issued but has not yet been received.

**elliptic curve cryptography (ECC)**: A form of public-key cryptography based on the problem of finding discrete logarithms in a group defined over elliptic curves.

**Elliptic Curve Digital Signature Algorithm (ECDSA)**: A ~~specific~~ digital signature mechanism based on the elliptic curve discrete logarithm problem and standardized in Federal Information Processing Standard (FIPS) 186-4.

**Elliptic Curve Integrated Encryption Scheme (ECIES)**: A public-key encryption mechanism based on the elliptic curve discrete logarithm problem.

**encode**: To convert a data structure into an array of octets. *Contrast*: **decode, encrypt.**

**encrypt**: To convert readable data to unreadable, encrypted data using an encryption algorithm and a key. *Contrast*: **decrypt, encode.**

**encryption algorithm**: An algorithm that takes as input plaintext and a key and produces ciphertext.

**encryption certificate**: A certificate that contains an encryption key.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**end-entity certificate**: ~~Any~~ A certificate ~~other than one~~ used ~~by a CA for~~ to validate application PDUs or certificate ~~management operations~~ requests.

**enrolment certificate**: A certificate used to validate a ~~sign a Certificate Signing Request. A type of *security management*~~ certificate request (CSR). *Contrast*: ~~**operational**~~ **authorization certificate, certificate authority (CA) certificate**.

**explicit certificate**: A certificate that contains a public key and the certificate authority's signature.

**full certificate revocation list (full CRL)**: A certificate revocation list that carries information about certificates that were revoked and have not expired, ~~whenever~~ regardless of when the revocation took place. *Contrast*: **delta certificate revocation list**.

**global consistency conditions**: Consistency conditions (q.v.) which apply to all protocol data units (PDUs) regardless of the application area in which they are used.

**hash function**: *See*: **cryptographically secure hash function.**

**hash ID-based revocation**: Revocation (q.v.) which identifies certificates to be revoked via their cryptographic hash.

**hash value**: The output of a hash function.

**IEEE 1609.2™ security profile**: A ~~specification of the~~ means for specifying options and parameters that are provided to the 1609.2 security services by a particular consumer of those services. May be used as part of the specification of a *secure data exchange entity* (q.v.).

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**implicit certificate**: A digital certificate that ~~does not explicitly contain the certificate holder's public key, but instead~~ allows the associated public key to be reconstructed from a reconstruction value and the certificate authority's public key rather than directly providing the associated public key.

**inherited permissions**: Permissions within a subordinate certificate that are communicated by reference to the issuing certificate, rather than stated explicitly within the subordinate certificate.

**integrity**: A cryptographic service that provides assurance that any changes to a protocol data unit (PDU) made after it is validly created will be detected.

**issuing certificate**: ~~If the public key from~~ The certificate that issues a ~~A can be used to verify the signature on certificate B, then A is the *issuing certificate* for B. *Contrast:*~~ **subordinate certificate.**

**linkage-based revocation**: Revocation (q.v.) which identifies certificates to be revoked via a linkage value (q.v.) included in the certificate.

**linkage value**: A value included in a certificate that enables that certificate to be revoked via linkage-based revocation (q.v.).

**locally held certificate**: A certificate on a device such that WAVE Security Services on that device may generate a signature on a secured protocol data unit (SPDU) which verifies correctly with that certificate.

**management plane**: A component of the abstract architecture containing functions that manage the entities in the data plane.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**misbehavior**: Behavior that results in devices receiving information that could cause them to take incorrect actions.

**misbehavior authority**: A management component on the network with responsibility for determining which devices are responsible for misbehavior.

**misbehavior reporting**: The activity of providing information to some authority, known as the misbehavior authority, about misbehavior within a particular application area. The subsequent actions taken by the misbehavior authority may be application area specific.

**network byte order**: An ordering of the bytes of an integer such that the byte transmitted first is the byte containing the most significant bit, and the most significant bit is first in that byte.

**non-repudiation (of origin)**: A cryptographic service whereby the origin of a message can be demonstrated to a third party, preventing the sender from denying that they produced the message.

**off-cycle certificate revocation list (CRL)**: A certificate revocation list (CRL) that is issued before the "next CRL" time indicated in the previous CRL in the CRL series.

~~**Local Service Index for Security (LSI-S):** An identifier used to identify a secure communications entity to the security services.~~

~~**operational certificate:** Any certificate other than an enrolment certificate.~~

**partial certificate chain**: A certificate chain that is not a ~~full~~ complete certificate chain, i.e., the ~~first~~ top certificate is not a root certificate or the ~~last~~ bottom certificate is not an end-entity certificate.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**permitted depth of chain**: See: **depth of chain**.

**peer-to-peer certificate distribution**: A mechanism for allowing devices to learn certificates from peer devices.

**plaintext**: Unencrypted data.

**properly formed certificate**: A certificate that can be parsed correctly according to the data structures and encoding defined in this standard.

~~**provider:** Advertiser of a WAVE service. See also: **user; WAVE Service Advertisement**.~~

**Provider Service Identifier (PSID)**: An ~~octet string that identifies a service provided by a higher layer entity~~ identifier of an application area. (See IEEE Std 1609.12).

**Provider Service Identifier (PSID) derived from context**: A Provider Service Identifier (PSID) associated with a protocol data unit (PDU) received by a secure data exchange entity (SDEE), where the SDEE does not obtain the PSID from the PDU itself, but by some other means.

**pseudonym certificate**: An authorization certificate (q.v.) that indicates its holder's permissions but not its holder's identity.

**pseudonymity:** A property wherein an entity's permanent or long-lived identities, and its long-term patterns of behavior, cannot be deduced from its network traffic and are only observable by appropriately authorized parties.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**public-key digital signature**: A cryptographically secure checksum that is generated using a private key and verified using a public key.

**reconstruction value**: A value in an implicit certificate that allows the associated public key to be recovered.

**relevance conditions**: Criteria for validity of a signed secured protocol data unit (SPDU) that depend on the local state of the receiver.

**replay attack**: An attack in which an attacker retransmits, possibly with a delay, data that was originally validly transmitted.

**revocation**: The publication by a relevant authority of the information that a particular certificate is no longer to be trusted.

**root certificate**: A self-signed certificate that can be used as a trust anchor to verify other certificates.

**secure data service**: A subset of Wireless Access in Vehicular Environments (WAVE) Security Services providing services that allow secure data service entities to request communications security services to be applied to protocol data units (PDUs).

**secure data exchange entity (SDEE):** An ~~A secure communications~~ entity that uses IEEE 1609.2 services to secure any communications ~~other than *WAVE Service Advertisements*~~.

**secure data exchange entity (SDEE)-specific consistency checks**: Consistency checks (q.v.) which are specific to a SDEE (q.v.).

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**secure data exchange entity (SDEE)-verified relevance checks**: Relevance checks (q.v.) which cannot be verified within the security services.

**secured protocol data unit (SPDU)**: A protocol data unit which has been processed by WAVE Security Services before transmission.

**security envelope:** The additional data added to a protocol data unit by the security services when transforming it into a secured protocol data unit.

~~**Secure entity** : A functional entity that uses IEEE 1609.2 services to secure communications for any purpose other than security management.~~

~~**secure data exchange certificate:** A certificate that is used to verify the signature on data other than a *WAVE service advertisement*. *Contrast:* **WSA certificate, communications certificate**.~~

**security services** ~~**Certificate**~~ **management entity (SSME** ~~**CME**~~**)**: The management entity responsible for managing the certificate management information on a device.

**security management message**: A protocol data unit (PDU) used to manage certificates or information about certificates.

~~**secure provider service:** A higher layer entity that requests that its entry in a WAVE Service Advertisement be secured.~~

**security management**: Operations that support acquiring or establishing the validity of 1609.2 certificates.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**security profile policy**: For an *IEEE 1609.2 security profile* (q.v.), a set of entries in the security profile for which values used by different implementations should be coordinated and for which values may change over time.

**security service-verified relevance conditions**: Relevance conditions (q.v.) that can be tested within the security services.

~~**security management certificate:** A certificate used to authenticate security management protocol data units. *Enrolment certificates* and *certificate authority certificates* are security management certificates. *Contrast:* **communications.**~~

**self-signed certificate**: A certificate whose signature can be verified with the public key in the certificate.

**Service Specific Permissions (SSP)**: A field that ~~encodes~~ indicates the permissions ~~relevant to~~ of a particular certificate holder with respect to a particular application area.

~~**ServiceInfo:** A field in an IEEE Std 1609.3 *WAVE service advertisement* (WSA) that announces the availability of a service. A WSA may contain multiple ServiceInfo fields.~~

**signature**: *See:* **public key digital signature**.

**subordinate certificate**: The certificate that was issued by an *issuing certificate*.

~~**store:** A collection of data objects (typically certificates and certificate revocation lists in this standard) such that each object stays in the store until it expires, is superseded, or is revoked.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**symmetric cryptographic algorithm**: A cryptographic algorithm that uses a single key. Knowledge of a symmetric encryption key allows both encryption and decryption. Knowledge of a symmetric authentication key allows generation and verification of message authentication codes.

**Symmetric Cryptomaterial Handle**: A reference to a symmetric key, used to indicate to the secure data service that the referenced key should be used in a particular operation.

**symmetric key**: The key for a ~~*See*~~ *symmetric cryptographic algorithm*~~.~~ (q.v.).

**Transport Layer Security (TLS)**: An Internet Engineering Task Force (IETF) ~~standard~~ protocol, specified in Request for Comments (RFC) 5246 [B13], providing for secure communications over Transmission Control Protocol/Internet Protocol (TCP/IP).

**trigger secure data exchange entity (trigger SDEE)**: A secure data exchange entity that sends a secured protocol data unit (SPDU) that triggers peer-to-peer certificate distribution.

**trigger secured protocol data unit (trigger SPDU)**: A secured protocol data unit (SPDU) that triggers peer-to-peer certificate distribution.

**trust anchor**: A certificate whose validity does not depend on the validity of other certificates.

~~**user:** Consumer of a WAVE service. See also: **provider; WAVE Service Advertisement**.~~

**valid certificate**: A certificate that is correctly formed, that has not been revoked or expired, and for which a certificate chain to a trust anchor can be constructed.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**verification type** (of a signed secured protocol data unit (SPDU)): An indication of whether a signed SPDU is to be verified with a public key associated with a certificate, or a public key included in the protocol data unit (PDU) payload. Takes the values *certificate* or *self-signed*.

~~**vehicle-to-infrastructure:** Wireless communication between vehicles and roadside units in either direction~~

**Wireless Access in Vehicular Environments (WAVE) device**: A device that is compliant to IEEE Std 1609.3™, IEEE Std 1609.4™, and IEEE Std 802.11™~~, operating~~ communicating outside the context of a basic service set ~~(BSS)~~. ~~(See IEEE Std 802.11 specification of "STA transmission of data frames outside the context of a BSS.")~~

~~**Wireless Access in Vehicular Environments (WAVE) Management Entity (WME):** A set of management functions, defined in IEEE Std 1609.3, required to provide WAVE Networking Services.~~

~~**Wireless Access in Vehicular Environments (WAVE) Service Advertisement (WSA):** A collection of data indicating the services that a given WAVE device is offering.~~

~~**Wireless Access in Vehicular Environments (WAVE) Service Advertisement (WSA) certificate:** A certificate used to verify a wireless access in *WAVE Service Advertisement*.~~

**Wireless Access in Vehicular Environments (WAVE) Short Message (WSM)**: A packet consisting of a~~ data payload and a~~ WAVE Short ~~*Message Protocol*~~MessagePprotocol (WSMP) header and WSM data.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

**Wireless Access in Vehicular Environments (WAVE) Short Message Protocol (WSMP)**: A ~~low~~ protocol specified in IEEE Std 1609.3 that minimizes communications overhead ~~protocol for exchange of messages in a rapidly varying radio frequency environment where low latency is also an important objective~~.

## 3.2 Abbreviations and acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| APDU | application protocol data unit |
| ASN.1 | Abstract Syntax Notation 1 |
| ~~**BSM**~~ | ~~Basic Safety Message~~ |
| CA | certificate authority |
| CCM | counter mode with cipher block chaining message authentication code |
| ~~**CME**~~ | ~~Certificate Management Entity~~ |
| CMH | Cryptomaterial Handle |

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

| | |
|---|---|
| COER | Canonical Octet Encoding Rules |
| CRACA | Certificate Revocation Authorizing Certificate Authority |
| CRL | certificate revocation list |
| CSR | certificate signing request |
| DSRC | dedicated short range communications |
| ECC | elliptic curve cryptography |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECIES | Elliptic Curve Integrated Encryption Scheme |
| EDCA | enhanced distributed channel access |
| FIPS | Federal Information Processing Standard |
| GNSS | Global Navigation Satellite System |
| GPS | Global Positioning System |

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

| | |
|---|---|
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IPv6 | Internet Protocol version 6 |
| ~~**LSI-S**~~ | ~~Local Service Index for Security~~ |
| ITS | intelligent transportation systems |
| MAC | medium access control, or message authentication code |
| NIST | National Institute for Standards and Technology |
| OBU | on-board unit |
| P2PCD | peer-to-peer certificate distribution |
| ~~**PDF**~~ | ~~probability distribution function~~ |
| PDU | protocol data unit |
| PHY | physical layer |

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

| | |
|---|---|
| ~~**PSC**~~ | ~~Provider Service Context~~ |
| PSID | Provider Service Identifier |
| ~~**PSSME**~~ | ~~Provider Service Security Management Entity~~ |
| RSU | roadside unit |
| RFC | Request for Comments |
| SAE | Society of Automotive Engineers |
| SAP | Service Access Point |
| SCMH | Symmetric Cryptomaterial Handle |
| SDEE | secure data exchange entity |
| SDS | secure data service |
| SSME | security services management entity |
| SP | special publication |

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

| | |
|---|---|
| SPDU | secured protocol data unit |
| SSP | Service Specific Permissions |
| TLS | Transport Layer Security |
| TAI | International Atomic Time |
| TTP | trusted third party |
| UTC | Coordinated Universal Time |
| UTF | Unicode Transformation Format |
| V2I | vehicle-to-infrastructure |
| V2V | vehicle-to-vehicle |
| WAVE | Wireless Access in Vehicular Environments |
| WGS | World Geodetic System |
| WME | WAVE Management Entity |

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

| | |
|---|---|
| ~~WSA~~ | ~~WAVE Service Advertisement~~ |
| WSM | WAVE Short Message |
| WSMP | WAVE Short Message Protocol |

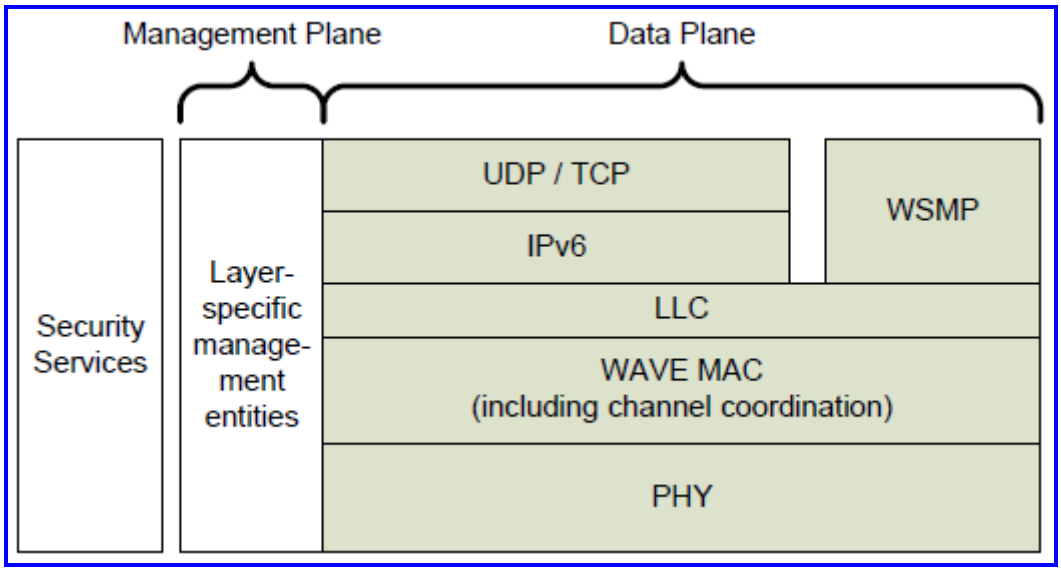
# 4. General description

## 4.1 WAVE protocol stack overview

Wireless Access in Vehicular Environments (WAVE) provides a communication protocol stack optimized for the vehicular environment, employing both customized and general-purpose elements as shown in Figure 1. ~~See IEEE P1609.0[11] for an overview of the WAVE architecture and services, including a description of the use of the security services described in this document~~ WAVE supports both IP- and non–IP-based data transfers, although individual devices might support only one networking stack. Non–IP-based data transfers are supported through the WAVE Short Message Protocol (WSMP) specified in IEEE Std 1609.3. Channel coordination is a collection of extensions to the IEEE 802.11 medium access control (MAC) specified in IEEE Std 1609.4 [B12]. The WAVE Management Entity (WME) and corresponding network services are specified in IEEE Std 1609.3. WAVE Security Services are specified in this standard. IEEE Std 1609.0 provides a description of the WAVE system architecture and operations.

~~[11] Information on references can be found in Clause 2.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

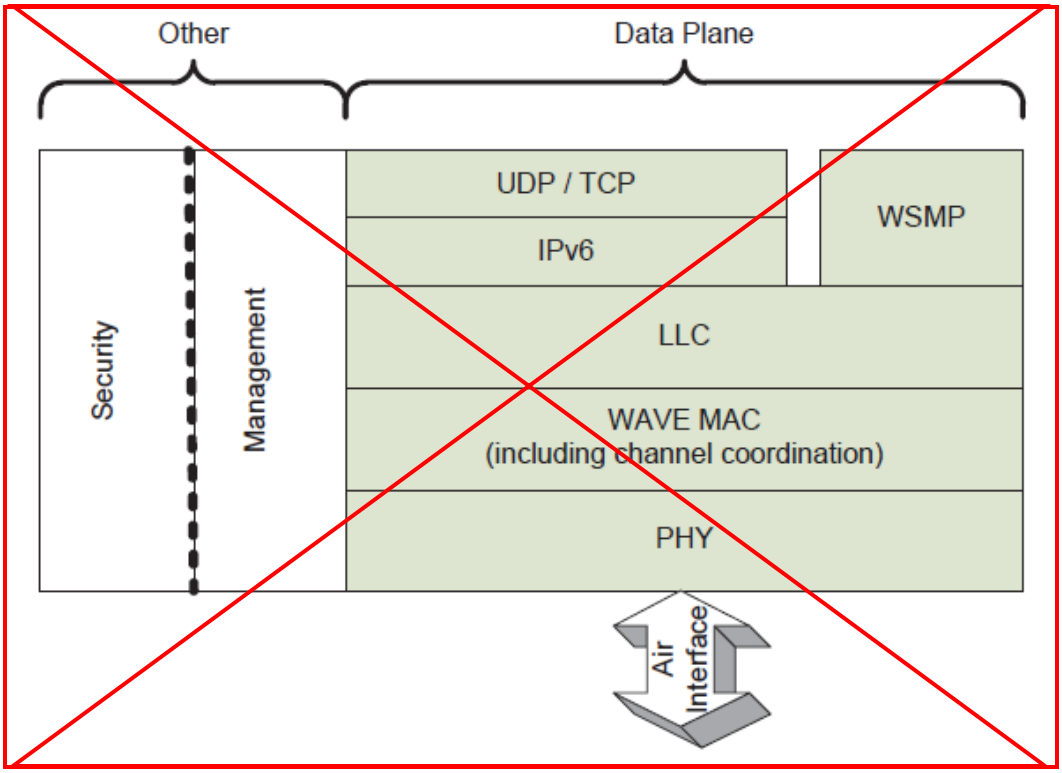



(New)

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1609.2-2016




~~(Deleted)~~

**Figure 1—WAVE ~~Protocol Stack~~ reference model**

This standard specifies a ~~set~~ collection of ~~management plane~~ WAVE Security Services available to ~~applications and~~ processes running ~~in the various layers of the~~ on platforms including, but not limited to, WAVE ~~protocol stack as shown in Figure 2~~ devices. The WAVE Security Services are shown in Figure 2 and consist of WAVE Internal Security Services and WAVE Higher Layer Security Services.

WAVE Internal Security Services are:

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

— *Secure data service* (SDS): Transforming unsecured protocol data units (PDUs) into secured protocol data units (SPDUs) to be transferred between entities ~~using data-plane operations~~, and processing SPDUs on reception, including transforming SPDUs into unsecured PDUs. The additional data added to a PDU when it is transformed into a SPDU is referred to as the *security envelope*. An entity that uses the secure data service is referred to as a *secure data exchange entity* (SDEE) ~~These processes together are referred to as "Secure data exchange." The security services specified in this document support the signing and/or encryption of PDUs prior to their transmission, and the decryption and verification (as appropriate) of PDUs on reception~~.

— *Security management*: Managing information about certificates as specified in 4.3.

WAVE Higher Layer Security Services are:

— *Certificate revocation list (CRL) verification entity (CRLVE)*: Validates incoming CRLs and passes the related revocation information to the SSME for storage as specified in 5.1.3 and Clause 7.

— *Peer-to-peer certificate distribution (P2PCD) entity (P2PCDE)*: Enables peer-to-peer certificate distribution as specified in Clause 8.

~~— *security processing services:*~~

~~— provide processing that is performed to enable *secure communications that comprise* secure data and secure WAVE Service Advertisements (WSAs); and~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

— ~~*security management services:*~~

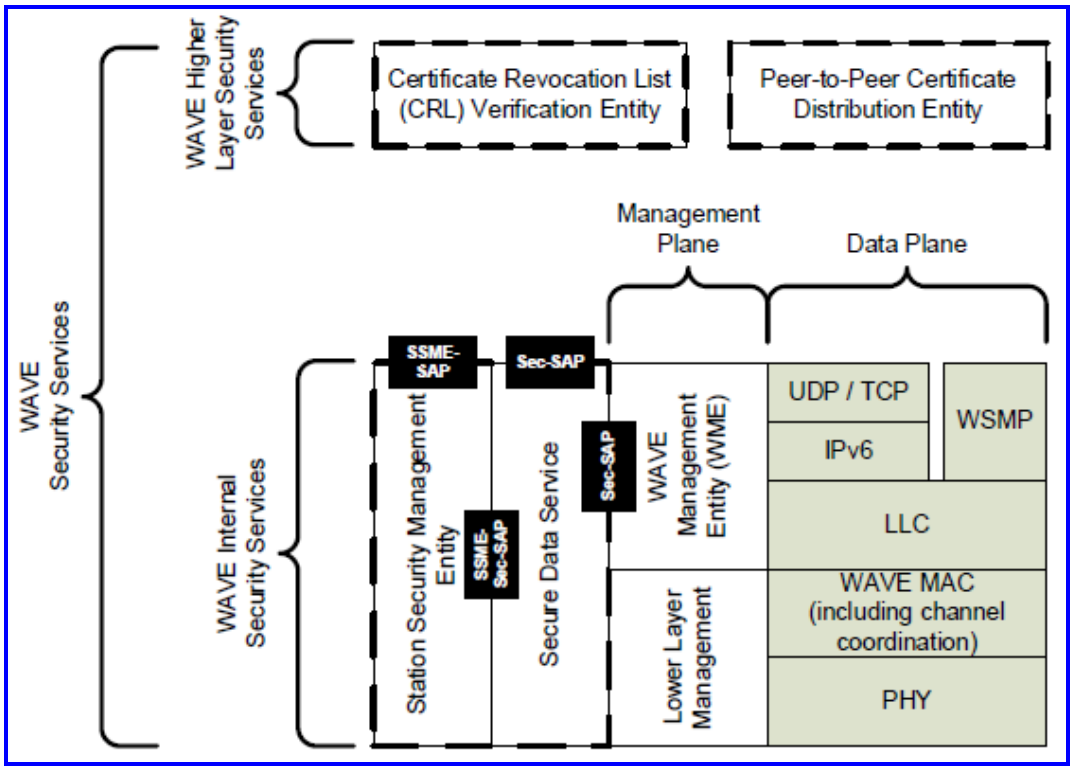
  — ~~provice certificate management services that are provided by the Certificate Management Entity (CME) and that manage information related to the validity of all certificates; and~~

  — ~~provide service security management services that are provided by the Provider Service Security Management Entity (PSSME) and that manage information related to certificates and private keys that are used to send secured WSAs.~~

The services and entities within the WAVE Security Services are shown in Figure 2, which also shows Service Access Points (SAPs) that support communications between WAVE Security Services entities and other entities. This standard specifies ~~the~~ information flows to support security processing via primitives defined at these SAPs. The Sec-SAP is used by higher layer entities and by the WME. Additionally, the certain SDS operations involve invoking certain primitives across the SSME-SAP as specified in 4.3 ~~Horizontal boundaries within the WAVE Security Services in Figure 2 are abstract and do not correspond to horizontal boundaries within the Data Plane~~.

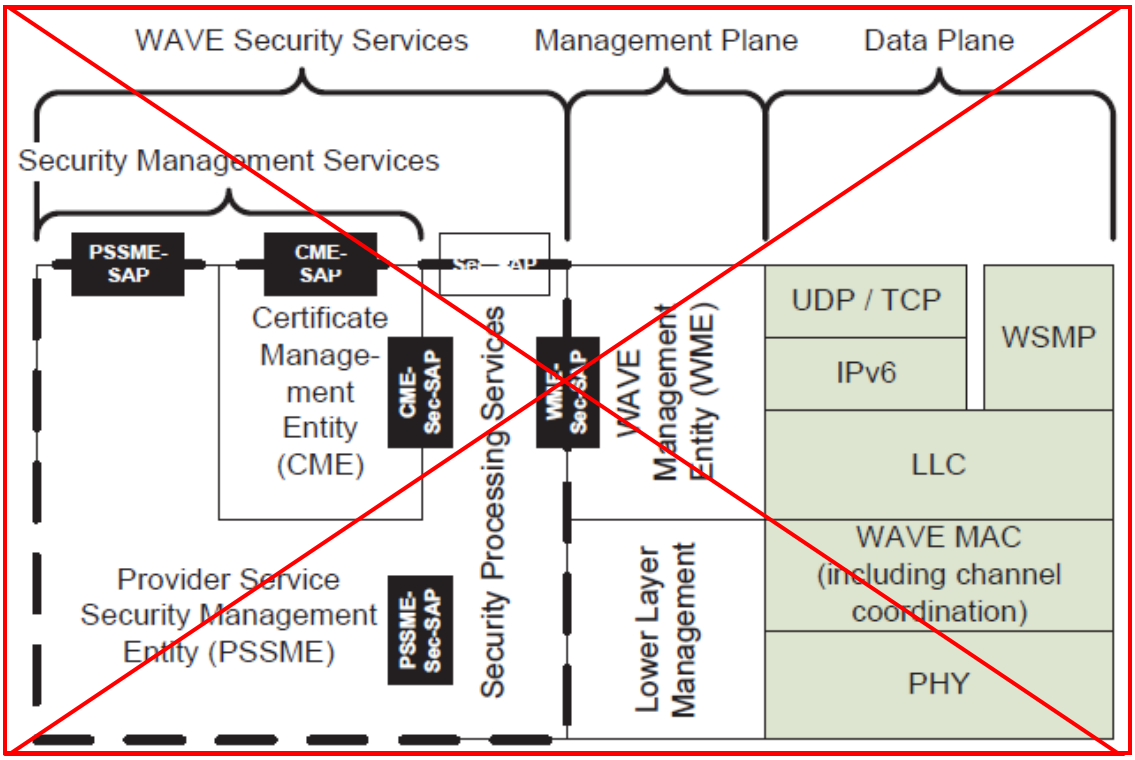
Information elements ~~Data~~ passed across the SAPs in this standard ~~is~~ are assumed to be secure and trustworthy. This standard does not provide mechanisms to ensure the trustworthiness of ~~this data~~ these information elements.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016




(New)

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016




~~(Deleted)~~

**Figure 2 —WAVE protocol stack showing detail of**

**WAVE ~~the~~ Security Services**

## ~~4.2 Generic security services~~

~~IEEE 1609 provides WAVE Security Services that in turn support the following generic security services:~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

- Confidentiality: Supported by the security processing services *Generate encrypted data* and *Decrypt encrypted data*.

- Authentication: Supported by the security processing services *Generate signed data* and *Verify signed data*.

- Authorization: Supported by the security processing services *Generate signed data* and *Verify signed data*.

- Integrity: Supported by the security processing services *Generate signed data* and *Verify signed data*.

## 4.3 Security processing services

### 4.3.1 General

The security processing services accept input requests from calling entities. The security processing services respond to each input request with a corresponding output confirmation containing the results of the request.

The security processing services consist of the following:

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

- Generating secured WSAs and processing signed WSAs on reception (hereafter, "Signed WSAs"). WSAs are defined in IEEE Std 1609.3. They originate at the WAVE Mangement Entity (WME) in the transmitting device, and are consumed by the WME in the receiving device. The WME is also defined in IEEE Std 1609.3. The security services specified in this document support the signing of WSAs prior to their transmission and the verification of WSAs on reception.

- Security processing for security management: ensuring access to cryptomaterial (private keys, public keys and certificates) as described in 4.4; generating certificate requests and processing responses; and validating Certificate Revocation Lists (CRLs).

- Storing private keys and their associated certificates.

An implementation of WAVE security services shall include at least one of the following security processing services:

- Generate signed data (see 5.3.2)

- Generate encrypted data (see 5.3.3)

- Verify signed data (see 5.3.6)

- Decrypt encrypted data (see 5.3.5)

- Generate signed WSA (see 5.4.1)

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016

— Verify signed WSA on reception (see 5.4.2)

— Generate certificate request (see 5.6.1)

— Verify response to certificate request (see 5.6.2)

— Verify certificate revocation list (see 5.6.4)

### 4.3.2 Secure data exchange

The secure data exchange operations are:

— Generate signed data (see 5.3.2)

— Generate encrypted data (see 5.3.3)

— Verify signed data (see 5.3.6)

— Decrypt encrypted data (see 5.3.5)

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 20:19:37 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1609.2-2016