



IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Certificate Management Interfaces for End Entities

Corrigendum 1

IEEE Vehicular Technology Society

Developed by the
Intelligent Transportation Systems Committee

IEEE Std 1609.2.1™-2022/Cor 1-2023
(Corrigendum to IEEE Std 1609.2.1-2022)

STANDARDS

IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Certificate Management Interfaces for End Entities

Corrigendum 1

Developed by the

Intelligent Transportation Systems Committee
of the
IEEE Vehicular Technology Society

Approved 5 June 2023

IEEE SA Standards Board

Abstract: This corrigendum provides corrections to references, figures, processes, tables, and ASN.1 modules from 1609.2.1-2022.

Keywords: authorization, certificate, end entity, enrollment, IEEE 1609™, IEEE 1609.2.1™, interface, Security Credential Management System (SCMS)

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

Copyright © 2023 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 26 September 2023. 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 979-8-8557-0017-6 STD26387

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/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 Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

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

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA 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 makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. 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 their 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: THE NEED TO PROCURE 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 balloting 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 is 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, nor 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 the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, 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 subcommittees of the IEEE SA Board of Governors 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 evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

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 constitute 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.

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html>.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

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, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, 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; <https://www.copyright.com/>. 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 10 years. When a document is more than 10 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 [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

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 <https://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.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users 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.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this draft standard was completed, the Wireless Access in Vehicular Environments (WAVE)—Security Services Working Group had the following membership:

Justin McNew, *Chair*
Kevin Smith, *Vice Chair*
William Whyte, *Vice Chair*

Adrian Buckley
Andras Edelmayer
Ron Hochnadel
Carl Kain
John Kenney
Malik Khan

Virendra Kumar
Thomas Kurihara
Tom Lusco
Julius Madey
Sean Maschue
Ira McDonald

Vincent Park
Randal Roebuck
Richard Roy
Jasja Tijink
Jimmy Upton
Drew Van Duren

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

William Byrd
Marco Hernandez
Werner Hoelzl
Ming Jiang
Piotr Karocki
John Kenney
Virendra Kumar
Thomas Kurihara

Hyeong Ho Lee
William Lee
Charles Lusco
Julius Madey
Justin McNew
Michael Montemurro
Rajesh Murthy
Satoshi Oyama
Brian Russell

Kevin Smith
Walter Struppler
Mark Sturza
Dmitri Varsanofiev
John Vergis
William Whyte
Scott Willy
Yu Yuan

When the IEEE SA Standards Board approved this standard on 5 June 2023, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Sara R. Biyabani
Doug Edwards
Ramy Ahmed Fathy
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick

Joseph S. Levy
Howard Li
Gui Lin
Johnny Daozhuang Lin
Xiaohui Liu
Kevin W. Lu
Daleep C. Mohla
Andrew Myles

Paul Nikolich
Annette D. Reilly
Robby Robson
Lei Wang
F. Keith Waters
Karl Weber
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1609.2.1-2022/Cor 1, IEEE Standard for Standard for Wireless Access in Vehicular Environments (WAVE)—Certificate Management Interfaces for End Entities—Corrigendum 1.

IEEE Std 1609.2.1-2022 was published on 30 June 2022. Since that time, there has been significant implementation activity that has uncovered various errors and unclarities in the base standard. This document addresses those issues.

Contents

2. Normative references.....	11
3. Definitions, acronyms, and abbreviations	12
3.1 Definitions	12
4. Architecture	12
4.1 Security Credential Management System (SCMS).....	12
4.3 System parameters	13
5. Secure session.....	14
5.3 Transport Layer Security (TLS)	14
5.4 ISO/TS 21177	14
6. Web API.....	14
6.3 SCMS REST API v3	14
7. Data structures—Abstract Syntax Notation 1 (ASN.1)	19
7.1 Presentation and encoding	19
7.2 Data structures from IEEE Std 1609.2.....	19
7.3 SCMS protocol data unit structures	25
7.4 Secured protocol data unit structures.....	27
7.5 Parameterized types	28
7.6 Certificate profiles	29
8. Data structures—files	35
8.2 Authorization certificate download files.....	35
8.3 Successor enrollment certificate download files.....	36
9. Cryptographic constructions.....	37
9.3 Butterfly key mechanism.....	37
9.5 Binary hash tree for ACPC activation codes	39
10. Validity conditions for particular SPDUs.....	40
10.1 Validity of SignedCertificateRequest	40
11. Extensions and modifications of IEEE Std 1609.2.....	41
Annex B (normative) ASN.1 modules.....	42
B.1 General.....	42
B.2 Ieee1609Dot2Dot1AcaEeInterface.asn	42
B.3 Ieee1609Dot2Dot1AcaLaInterface.asn	42
B.4 Ieee1609Dot2Dot1AcaMaInterface.asn	43
B.5 Ieee1609Dot2Dot1AcaRaInterface.asn.....	43
B.6 Ieee1609Dot2Dot1Acpc.asn	43
B.7 Ieee1609Dot2Dot1CamRaInterface.asn.....	43
B.8 Ieee1609Dot2Dot1CertManagement.asn	44
B.9 Ieee1609Dot2Dot1EcaEeInterface.asn	44
B.10 Ieee1609Dot2Dot1EeMaInterface.asn	44
B.11 Ieee1609Dot2Dot1EeRaInterface.asn	45
B.12 Ieee1609Dot2Dot1LaMaInterface.asn	45
B.13 Ieee1609Dot2Dot1LaRaInterface.asn	45

B.14 Ieee1609Dot2Dot1MaRaInterface.asn.....	45
B.15 Ieee1609Dot2Dot1Protocol.asn	46
B.16 Ieee1609Dot2Asn/Ieee1609Dot2.asn.....	46
B.17 Ieee1609Dot2Asn/Ieee1609Dot2BaseTypes.asn	46
B.18 Ieee1609Dot2Asn/Ieee1609Dot2Crl.asn.....	46
B.19 Ieee1609Dot2Asn/Ieee1609Dot2CrlBaseTypes.asn	47
B.20 Ieee1609Dot2Asn/Ieee1609Dot2HeaderInfoExtensionBase.asn	47
B.21 Ieee1609Dot2Asn/EtsiTs103097ExtensionModule.asn.....	47
Annex E (informative) Example encodings of certificate profiles	48
E.6 Enrollment certificate.....	48
E.9 Registration authority (RA) certificate.....	49
Annex H (informative) Certificate access manager (CAM)–registration authority (RA) interface.....	51
H.5 CamRaBatchResponse.....	51

IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Certificate Management Interfaces for End Entities

Corrigendum 1

NOTE—The editing instructions contained in this **corrigendum** define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strike through~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.

2. Normative references

Delete the following note in Clause 2:

NOTE—This list of normative references includes the “base standard” IEEE Std 1609.2-2016, and its amendments IEEE Std 1609.2a™-2017 and IEEE Std 1609.2b™-2019. Where the current document refers to “IEEE Std 1609.2”, this is shorthand for the combination of the base standard and its amendments.

Change the following reference in Clause 2:

IEEE Std 1609.2™-2016~~22~~, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages.

Delete the following references in Clause 2:

IEEE Std 1609.2a™-2017, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages—Amendment 1.

IEEE Std 1609.2b™-2019, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages—Amendment 2.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

Change the following definitions in 3.1:

certificate acceptance policy: A policy setting constraints on the digital certificates (ITU-T Recommendation X.509 or IEEE Std 1609.2 based) that may be used to authorize certain activities.

~~certificate acceptance policy:~~ A, for example, a statement of properties that a *Security Credential Management System (SCMS)* component certificate is required to have when it is used to authenticate that SCMS component in the context of a *Transport Layer Security (TLS)* session.

4. Architecture

4.1 Security Credential Management System (SCMS)

4.1.2 Supported interfaces

4.1.2.6 EE–RA interface

Change the following sentence in 4.1.2.6:

The EE–RA interface is used ~~as follows~~ for the following:

4.1.4 Assumed lifecycle and use cases

4.1.4.2 Initial enrollment certificate request/download

Change the following sentences and bullets in 4.1.4.2:

In this use case, an end entity that does not yet have an IEEE 1609.2 enrollment certificate requests and receives an enrollment certificate from the ECA, ~~as follows~~. This enrollment certificate may contain constraints on the permissions the end entity can request in the authorization certificates. The mechanism by which the ECA determines whether the end entity is entitled to the permissions requested for the enrollment certificate is outside the scope of this document. The mechanism by which the end entity is configured to know which ECA to apply to is also outside the scope of this document.

- a) ~~This enrollment certificate may contain the following constraints on the permissions the end entity can request in the toBeSigned.certRequestPermissions field:~~
 - 1) ~~The mechanism by which the ECA determines whether the end entity is entitled to the permissions requested for the enrollment certificate is outside the scope of this document.~~
 - 2) ~~The mechanism by which the end entity is configured to know which ECA to apply to is outside the scope of this document.~~

- b) ~~The end entity is assigned at least one RA, as follows, to manage authorization certificate requests:~~
- 1) ~~The end entity may be assigned different RAs for different sets of applications.~~
 - 2) ~~The RA certificate is provided to the end entity.~~
 - 3) ~~The mechanism by which the end entity is configured with this information is outside the scope of this document.~~

4.1.4.3 Use cases authenticated with the enrollment certificate

4.1.4.3.1 General—Enrollment certificate registration and blocking—Relationship between EE and RA

Change the following sentences in 4.1.4.3.1:

~~If an EE is determined to be misbehaving, or otherwise to need certificate privileges to be withdrawn, the RA may be instructed to “block” that EE by marking the EE’s enrollment certificate as blocked. If an EE is determined by the MA to be misbehaving as described in 4.1.1, or otherwise to need certificate privileges to be withdrawn, the MA may instruct the RA to “block” that EE by marking the EE’s enrollment certificate as blocked.~~

Insert the following note at the end of 4.1.4.3.1:

NOTE—How an EE is determined to be misbehaving and who instructs the RA to block the EE are out of scope for this document.

4.3 System parameters

4.3.2 Time period parameters

4.3.2.4 Approaches for smooth transition

4.3.2.4.3 Overlap approach illustration for a subset of certificates

Change the following bullet in 4.3.2.4.3:

- time-baseCertNumber: 2022

5. Secure session

5.3 Transport Layer Security (TLS)

5.3.1 Prerequisites

5.3.1.2 SCMS component certificate and certificate acceptance policy

Change the following bullets in 5.3.1.2:

- a) There is an *ITU-T X.509 certificate acceptance policy* applied by each end entity to each SCMS component it communicates with. The policy applied by the end entity is specific to that end entity and known to the SCMS component~~that is known to both the SCMS component and the end entity:~~
 - 1) The certificate acceptance policy ~~for the end entity~~ specifies a pattern (or exact value) that the `subjectAltName` field in an SCMS component X.509 certificate is required to match in order for the certificate to be accepted as coming from an SCMS component of the correct type:

5.4 ISO/TS 21177

5.4.4 Client authentication with an enrollment certificate

Change the following sentence in 5.4.4:

If a client (i.e., an end entity) authenticates with an enrollment certificate within an ISO/TS 21177 handshake, the `Ieee1609Dot2Content` within the `CertificateVerify` message shall be signed with the PSID value `SecurityMgmtPsid`. The enrollment certificate shall conform to the enrollment certificate profile provided in ~~7.6.3.6~~7.6.3.7.

6. Web API

6.3 SCMS REST API v3

6.3.1 General

6.3.1.3 Protocol parameters

Change the following bullet in 6.3.1.3:

- c) `scmsV3-options` = list of HTTP ~~options~~ headers supported

6.3.1.4 HTTP headers

Change the subclause heading in 6.3.1.4:

Custom HTTP headers

6.3.1.6 HTTP options

Change the subclause heading in 6.3.1.6:

Common HTTP ~~options~~ headers

Change the following sentences in 6.3.1.6:

This document does not specify common HTTP ~~options~~ headers like If-Unmodified-Since (as specified in IETF RFC 7232) and Range (as specified in IETF RFC 7233).

For example, for the authorization certificate download (see 6.3.5.3.2), the HTTP response body is dependent on the ~~option~~ header Range as follows:

6.3.5 EE–RA interface

6.3.5.2 Authorization certificate request

6.3.5.2.3 SCMS component authentication

Change Table 10 to the following: