INTERNATIONAL STANDARD

ISO/IEC/IEEE 8802-1AR

Second edition
2020-03

This document is a preview generated by EVS

Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks —

Part 1AR: Secure device identity

Télécommunications et échange entre systèmes informatiques — Exigences pour les réseaux locaux et métropolitains —

Partie 1AR: Identité de dispositif sécurisé

Reference number
ISO/IEC/IEEE 8802-1AR:2020(E)

© IEEE 2018

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© IEEE 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

© IEEE 2018 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted (see www.iso.org/directives).

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

ISO/IEC/IEEE 8802-1AR was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AR-2018) and drafted in accordance with its editorial rules. It was adopted, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This second edition cancels and replaces the first edition (ISO/IEC/IEEE 8802-1AR:2014), which has been technically revised.

A list of all parts in the ISO/IEC 8802 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This document is a preview generated by EVS

© IEEE 2018 – All rights reserved

This document is a preview generated by EVS

IEEE Std 802.1AR-2018
(Revision of
IEEE Std 802.1AR-2009)

This document is a preview generated by EVS

IEEE Standard for
Local and Metropolitan Area Networks—

Secure Device Identity

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 June 2018

IEEE-SA Standards Board

Abstract: A Secure Device Identifier (DevID) is cryptographically bound to a device and supports authentication of the device's identity. An Initial Device Identifier (IDevID) provide by the supplier of a device can be supplemented by Local Device Identifiers (LDevIDs) facilitating enrollment (provisioning of authentication and authorization credentials) by local network administrators.

Keywords: access control, authentication, authorization, certificate, IEEE 802.1AR, LANs, local area networks, MAC security, MANs, metropolitan area networks, PKI, port-based network access control, secure association, Secure Device Identifier, security, X.509

This document is a preview generated by EVS

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

Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 2 August 2018. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-5019-5 STD23186
Print: ISBN 978-1-5044-5020-1 STDPD23186

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.

Copyright © 2018 IEEE. All rights reserved.

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.

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

Translations

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

Official statements

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

Comments on standards

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

Comments on standards should be submitted to the following address:

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

Laws and regulations

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

Copyrights

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

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

Photocopies

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

Updating of IEEE Standards documents

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

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

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Xplore at http://ieeexplore.ieee.org/ 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.

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

Participants

At the time this standard was completed, the IEEE 802.1 working group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Mick Seaman, *Security Task Group Chair, Editor*

SeoYoung Baek
Shenghua Bao
Jens Bierschenk
Steinar Bjornstad
Christian Boiger
Paul Bottorff
David Chen
Feng Chen
Weiying Cheng
Rodney Cummings
János Farkas
Norman Finn
Geoffrey Garner
Eric W. Gray
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Patrick Heffernan
Marc Holness
Lu Huang
Tony Jeffree
Michael Johas Teener
Hal Keen
Stephan Kehrer
Philippe Klein
Jouni Korhonen
Yizhou Li
Christophe Mangin
Tom McBeath
James McIntosh
Tero Mustala
Hiroki Nakano
Bob Noseworthy
Donald R. Pannell
Walter Pienciak
Michael Potts
Karen Randall
Maximilian Riegel
Dan Romascanu
Jessy V. Rouyer
Eero Ryytty
Soheil Samii
Behcet Sarikaya
Frank Schewe
Johannes Specht
Wilfried Steiner
Patricia Thaler
Paul Unbehagen
Hao Wang
Karl Weber
Brian Weis
Jordon Woods
Nader Zein
Helge Zinner
Juan Carlos Zuniga

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

Thomas Alexander
Johann Amsenga
Butch Anton
Stefan Aust
Christian Boiger
Paul Bottorff
Nancy Bravin
Vern Brethour
Demetrio Jr Bucaneg
William Byrd
Juan Carreon
Yesenia Cevallos
Keith Chow
Charles Cook
Sourav Dutta
Donald Eastlake, III
Janos Farkas
Andrew Fieldsend
Yukihiro Fujimoto
David Goodall
Eric W. Gray
Randall Groves
Michael Gundlach
Stephen Haddock
Marco Hernandez
Werner Hoelzl
Rita Horner
Russell Housley
Noriyuki Ikeuchi
Atsushi Ito
Raj Jain
SangKwon Jeong
Manabu Kagami
Piotr Karocki
Stuart Kerry
Yongbum Kim
Jeff Koftinoff
Hyeong Ho Lee
James Lepp
Jon Lewis
Michael Lynch
Elvis Maculuba
John Messenger
Michael Montemurro
Ronald Murias
Satoshi Obara
Thomas Palkert
Bansi Patel
Arumugam Paventhan
Clinton Powell
Karen Randall
R. K. Rannow
Alon Regev
James Reilly
Maximilian Riegel
Robert Robinson
Jessy Rouyer
Reinhard Schrage
Mick Seaman
Daniel Smith
Dorothy Stanley
Thomas Starai
Walter Struppler
Gerald Stueve
Mitsutoshi Sugawara
Bo Sun
Patrik Sundstrom
Mark-Rene Uchida
Dmitri Varsanofiev
George Vlantis
Khurram Waheed
Hao Wang
Lisa Ward
Karl Weber
Brian Weis
Andreas Wolf
Chun Yu Charles Wong
Dayin Xu
Yunsong Yang
Oren Yuen

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

When the IEEE-SA Standards Board approved this standard on 14 June 2018, it had the following membership:

Jean-Philippe Faure, *Chair*
Gary Hoffman, *Vice-Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Guido R. Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
Hung Ling
Dong Liu
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles
Paul Nikolich
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Mehmet Ulema
Phil Wennblom
Philip Winston
Howard Wolfman
Jingyi Zhou

*Member Emeritus

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

Introduction

This introduction is not part of IEEE Std 802.1AR-2018, IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity.

This standard specifies Secure Device Identifiers (DevIDs) for use with IEEE Std 802.1X™ [B1][1] and other industry standards and protocols that authenticate, provision, and authorize communicating devices.

Each DevID comprises an RFC 5280 conformant X.509 certificate that identifies the subject device and can include authorization information signed by the certificate's issuer, a secret private key that corresponds to the certificate's subject public key, and any certificate chain required to facilitate the certificate's use. A device's DevID module stores each of its DevID secrets securely and supports signing operations that prove possession of the secret (and thus that the device is the subject of the associated DevID certificate), while ensuring that the secret remains confidential so the device cannot be impersonated by others.

An Initial Device Identifier (IDevID) provided by a device's supplier can be supplemented by one or more Local Device Identifiers (LDevIDs), each using an existing or a freshly generated secret, facilitating enrollment (provisioning of authentication and authorization credentials to authenticated devices) by a local network administrator.

The first edition of IEEE Std 802.1AR was published in 2009. This revision added the ECDSA P-384/SHA-384 signature suite option; removed the RSA-2048/OPAQUE option (that permitted the use of an undisclosed hash function); restructured the document to enable future signature suite changes, for clarity (particularly in conformance statements and the PICS), and revised the MIB. A DevID module can now implement more than one signature suite (facilitating interoperability and the use of a device in different authentication environments) and additional service operations (that do not conflict with mandatory requirements) as long as these are disclosed (facilitating backwards compatibility and support of DevID functionality by other modules, e.g., TPM).

[1]Numbers in brackets correspond to entries in the Bibliography in Annex C.

Copyright © 2018 IEEE. All rights reserved.

This document is a preview generated by EVS

Contents

1. Overview ... 13

1.1 Scope ... 14
1.2 Purpose ... 14
1.3 Relationship to other standards ... 14

2. Normative references ... 15

3. Definitions ... 17

4. Acronyms and abbreviations ... 20

5. Conformance ... 22

5.1 Requirements terminology ... 22
5.2 Protocol Implementation Conformance Statement ... 22
5.3 Required capabilities ... 22
5.4 Optional capabilities ... 23
5.5 Supplier information ... 23

6. Secure Device Identifiers (DevIDs) and their use ... 25

6.1 DevID secrets ... 26
6.2 DevID certificates ... 26
6.3 DevID certificate chains ... 28
6.4 DevID Trust Model ... 28
6.5 Privacy considerations ... 30

7. DevID Modules ... 31

7.1 DevID module functionality ... 31
7.2 DevID Service Interface ... 33
7.3 DevID Management Interface ... 37

8. DevID certificate fields and extensions ... 38

8.1 version ... 39
8.2 serialNumber ... 39
8.3 signature ... 39
8.4 issuer ... 39
8.5 validity ... 39
8.6 subject ... 40
8.7 subjectPublicKeyInfo ... 40
8.8 signatureAlgorithm ... 40
8.9 signatureValue ... 40
8.10 extensions ... 40

9. DevID signature suites ... 42

9.1 RSA-2048/SHA-256 ... 43
9.2 ECDSA P-256/SHA-256 ... 44
9.3 ECDSA P-384/SHA-384 ... 45

10. DevID MIB ... 46

10.1 Internet-Standard Management Framework ... 46
10.2 Relationship to other MIB modules ... 46
10.3 Structure of the MIB module ... 46
10.4 Security considerations ... 47

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

10.5 Definitions for Secure Device Identifier MIB 48

Annex A (normative) PICS proforma 60

A.1 Introduction 60
A.2 Abbreviations and special symbols 60
A.3 Instructions for completing the PICS proforma 61
A.4 PICS proforma for IEEE 802.1AR 63
A.5 Major capabilities and options 64
A.6 DevID Service Interface 65
A.7 DevID Random number generation 65
A.9 DevID Supplier Information 66
A.8 DevID Certificate fields and extensions 66
A.10 RSA-2048/SHA-256 Signature Suite 67
A.11 ECDSA P-256/SHA-256 Signature Suite 67
A.12 ECDSA P-384/SHA-384 Signature Suite 67

Annex B (informative) Scenarios for DevID 68

B.1 DevID use in EAP-TLS 68
B.2 DevID uses in consumer devices 69
B.3 DevID uses in enterprise devices 70

Annex C (informative) Bibliography 71

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

Figures

Figure 6-1 DevID trust hierarchy 28
Figure 7-1 DevID functionality 31
Figure B-1 Example EAP-TLS exchange 69

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

Tables

Table 7-1 DevID storage examples 32
Table 8-1 DevID certificate and intermediate certificate fields 38
Table 8-2 DevID certificate and intermediate certificate extensions 38
Table 10-1 DevID managed objects 48

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

This document is a preview generated by EVS

IEEE Standard for
Local and Metropolitan Area Networks—

Secure Device Identity

1. Overview

IEEE 802® Local Area Networks (LANs) are often deployed in networks that provide publicly accessible service access or that cannot be completely physically secured. The protocols that configure, manage, and regulate access to these networks and network-based services and applications typically run over the networks themselves. Secure and predictable operation of such networks depends on authenticating each device attached to and participating in the network, so that the degree of trust and authorization to be accorded to that device by its communicating peers can be determined.

Authentication of a human user, through a credential known to or possessed by that user, is often used to authenticate users of devices such as laptop personal computers. However many of the devices that compose a network are designed for unattended autonomous operation and might not support user authentication. These include the routers and bridges that interconnect and provide access to the LANs. Moreover, failure to provide devices that access the network with the mutual guarantee that they are connected to legitimate network access points allows malicious devices to interpose themselves between the network and its authenticated and authorized users, and effectively make use of the credentials of the latter. For these reasons a secure device identifier, i.e., one that embodies an authentication credential that cannot be easily removed or copied for use in a device under the control of someone who wishes to gain unauthorized access to or attack the operation of a network, is highly desirable.

Protocols for configuring, managing and regulating access to a network depend on the existence of a device identifier or human authentication of initial access to associate a device with an authentication credential. This can result in a “chicken-and-egg” scenario, wherein these credentials must be installed during an expensive “pre-provisioning” process before actual deployment. Even when device credentials are deployed in-place, the process is often interactive, involving a physically secured connection to the device being deployed and a knowledgeable system administrator.

Secure Device Identifiers (DevIDs) are designed to be used as interoperable secure device authentication credentials with Extensible Authentication Protocol (EAP [B4]) and other industry standard authentication and provisioning protocols.[1] A standardized device identity facilitates interoperable secure device authentication that helps simplify and standardize secure deployment and management of devices. A device is any entity in an IEEE 802 LAN that seeks to obtain services from the network or provide services on the network.

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

Copyright © 2018 IEEE. All rights reserved.

A device with DevID capability incorporates a globally unique manufacturer provided Initial Device Identifier (IDevID), stored in a way that protects it from modification. The device may support the creation of Locally Significant Device Identifiers (LDevIDs) by a network administrator. Each LDevID is bound to the device in a way that makes it infeasible for it to be forged or transferred to a device with a different IDevID without knowledge of the private key used to effect the cryptographic binding. LDevIDs can incorporate, and fully protect, additional information specified by the network administrator to support local authorization conventions. LDevIDs can also be used as the sole identifier (by disabling the IDevID) to assure the privacy of the user of a DevID and the equipment in which it is installed.

Multiple logical or physical devices, each with its own unique DevID can be contained within an aggregate device. The selection of a DevID for the aggregate device can depend on the context in which it is to be identified. This standard assumes that any such selection has been made and addresses device requirements independent of their simple or aggregate nature.

1.1 Scope

This standard specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device to its identifiers, the relationship between an initially installed identity and subsequent locally significant identities, and interfaces and methods for use of DevIDs with existing and new provisioning and authentication protocols.

1.2 Purpose

This standard defines a standard identifier for IEEE 802 devices that is cryptographically bound to that device, and defines a standard mechanism to authenticate a device's identity. This facilitates secure device provisioning.

1.3 Relationship to other standards

This standard specifies an identifier that is generally useful across IEEE 802 networks. It draws on and is informed by other standards that have been developed elsewhere for different purposes. Where possible, it attempts compatibility with the following:

a) Trusted Platform Module (TPM)

NOTE—TPM Keys for Platform Identity [B13] describes how TPM 1.2 can be used to provide DevID functionality, superseding IEEE Std 802.1AR-2009 Annex B.

b) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS [B6])

IETF RFC 7030 [B9] (Enrollment over Secure Transport) describes a certificate management protocol for Public Key Infrastructure (PKI) clients that need to acquire client certificates and associated Certification Authority (CA) certificates. A client can use an IDevID, as defined by this standard, to participate in the enrollment protocol which supports both client generated and CA generated public/private key pairs (LDevIDs).

This document is a preview generated by EVS

Copyright © 2018 IEEE. All rights reserved.

2. Normative references

The following referenced documents are indispensable for the application of this standard (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.

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.[2, 3]

ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).[4]

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 (SMIv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.[5]

IETF RFC 2579, STD 58, Textual Conventions for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Polk, W., Housley, R., Bassham, L., April 2002.

IETF RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., November 2003.

IETF RFC 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Schaad, J., Kaliski, B., Housley, R., June 2005.

IETF RFC 4108, Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages, R. Housley, August 2005.

IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W., May 2008.

IETF RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), Rescorla, E., August 2008.

IETF RFC 5480, Elliptic Curve Cryptography Subject Public Key Information, Turner, S., Brown, D., Yiu, K., Housley, R., Polk, T., March 2009.

IETF RFC 6353, Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), Hardaker, W., July 2011.

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

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

[4]ANSI publications are available from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[5]IETF RFCs are available from the Internet Engineering Task Force Web site at http://www.ietf.org/rfc.html.

Copyright © 2018 IEEE. All rights reserved.

This document is a preview generated by EVS

IETF RFC 6933, Entity MIB (Version 4), Bierman, A., Romascanu, D., Quittek, J., Chandramouli, M., May 2013.

IETF RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2, Moriarty, K., Kaliski, B., Jonnson, J., Rusch, A., November 2016.

ISO/IEC 8825-1 Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).[6]

NIST FIPS 180-4, Secure Hash Standard (SHS), August 2015.[7]

NIST FIPS 186-4, Digital Signature Standard (DSS), July 2013.

NIST Special Publication 800-90A, Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, E. Barker, J. Kelsey, June 2015.

This document is a preview generated by EVS

[6]ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112, USA (http://global.ihs.com/).

[7]NIST publications are available from the National Institute of Standards and Technology, NIST Public Inquiries, NIST, 100 Bureau Drive, Stop 3460, Gaithersburg, MD, 20899-3460, USA (www.nist.gov).

Copyright © 2018 IEEE. All rights reserved.