

BS ISO/IEC/IEEE 8802-1AR:2014



BSI Standards Publication

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks

Part 1AR: Secure device identity

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC/IEEE 8802-1AR:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/6, Data communications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 86408 7

ICS 35.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2014.

Amendments issued since publication

Date	Text affected
------	---------------

INTERNATIONAL
STANDARD

ISO/IEC/
IEEE
8802-1AR

First edition
2014-02-15

**Information technology —
Telecommunications and information
exchange between systems — Local and
metropolitan area networks —**

**Part 1AR:
Secure device identity**

*Technologies de l'information — Télécommunications et échange
d'information entre systèmes — Réseaux locaux et métropolitains —
Partie 1AR*



Reference number
ISO/IEC/IEEE 8802-1AR:2014(E)

AVA Documents
Document Sharing Hub
© IEEE 2009

© IEEE 2009

All rights reserved. Unless otherwise specified, 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 permission in writing from ISO, IEC or IEEE at the respective address below.

ISO copyright office
Case postale 56
CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
E-mail inmail@iec.ch
Web www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York
NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web www.ieee.org

Published in Switzerland

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, 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 ISO or the IEEE Standards Association.

ISO/IEC/IEEE 8802-1AR was prepared by the LAN/MAN Standards Committee of the IEEE Computer Society (as IEEE Std 802.1AR-2009). It was adopted by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

ISO/IEC/IEEE 8802 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks*:

- *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*
- *Part 1X: Port-based network access control*
- *Part 1AB: Station and media access control connectivity discovery*
- *Part 1AE: Media access control (MAC) security*
- *Part 1AR: Secure device identity*
- *Part 1AS: Timing and synchronization for time-sensitive applications in bridged local area networks*

- *Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)*



IEEE Standard for Local and metropolitan area networks— Secure Device Identity

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

22 December 2009

IEEE Std 802.1AR™-2009

Abstract: A secure device identifier (DevID) is cryptographically bound to a device and supports authentication of the device's identity. Locally significant identities can be securely associated with an initial manufacturer-provisioned DevID and used in provisioning and authentication protocols to allow a network administrator to establish the trustworthiness of a device and select appropriate policies for transmission and reception of data and control protocols to and from the device.

Keywords: access control, authentication, authorization, certificate, LANs, local area networks, MAC security, MANs, metropolitan area networks, PKI, port-based network access control, secure association, secure device identifier, security, X.509

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

Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 22 December 2009. 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 978-0-7381-6141-9 STD96035
Print: ISBN 978-0-7381-6142-6 STDPD96035

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.

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 or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "AS IS."

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. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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 publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her 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.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the 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, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, 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.

Introduction

This introduction is not part of IEEE Std 802.1AR-2009, IEEE Standard for Local and metropolitan area networks—Secure Device Identity.

A secure device identifier (DevID) is a cryptographic identity bound to a device used for assertion of the device's identity. IEEE Std 802.1AR specifies

- globally unique per-device identifiers 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.

IEEE Std 802.1AR can be used in conjunction with IEEE Std 802.1X™ [B2] and other IEEE and industry standards that require a secure identifier or credential as part of authentication and provisioning processes that establish trust in a device.¹

This is the first edition of IEEE Std 802.1AR.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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

This document is copyrighted by the IEEE. It is made available 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 this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards 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. 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 Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

¹The numbers in brackets correspond to those of the bibliography in Annex D.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

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 with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these 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. Other Essential Patent Claims may exist for which a statement 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.

Contents

1.	Overview	1
1.1	Scope.....	2
1.2	Purpose.....	2
1.3	Relationship to other standards.....	2
2.	Normative references	3
3.	Definitions	5
4.	Acronyms and abbreviations	7
5.	Conformance	9
5.1	Requirements terminology.....	9
5.2	Protocol Implementation Conformance Statement.....	9
5.3	Required capabilities.....	9
5.4	Optional capabilities	10
5.5	Recommended capabilities	10
6.	Secure Device Identifier Module	11
6.1	What is a device?	11
6.2	Components of a DevID module	11
6.3	DevID Service Interface	14
6.4	DevID Management Interface	20
6.5	PKI hierarchy requirements	22
6.6	Trust Model.....	24
7.	DevID Credential details	27
7.1	DevID hierarchy credential fields.....	27
7.2	DevID credential fields.....	27
7.3	Cryptographic Primitives.....	31
8.	Management Information Base	33
8.1	Internet-Standard Management Framework	33
8.2	Relationship to other MIB modules.....	33
8.3	Structure of the MIB	33
8.4	Security considerations	35
8.5	Definitions for Secure Device Identifier MIB	36
Annex A	(normative) PICS Proforma	47
A.1	Introduction.....	47
A.2	Abbreviations and special symbols.....	47
A.3	Instructions for completing the PICS proforma.....	48
A.4	PICS proforma for IEEE 802.1AR	50
A.5	Major capabilities and options.....	51
A.6	DevID Service Interface	51
A.7	DevID Management Interface	52
A.8	DevID Supplied Information	52
Annex B	(normative) Implementing a DevID with a TPM	53
B.1	DevID goals	53
B.2	DevID requirements.....	54

Annex C (informative) Scenarios for DevID	59
C.1 DevID use in EAP-TLS	59
C.2 DevID uses in consumer devices	60
C.3 DevID uses in enterprise devices	60
Annex D (informative) Bibliography	63
Annex E (informative) List of participants	66

IEEE Standard for Local and metropolitan area networks— Secure Device Identity

IMPORTANT NOTICE: *This standard is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

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

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. Further, the previously common assumption that network access controls were to provide protection of the network against abuse through unauthenticated and unauthorized access, while offering no protection to the accessing devices, is now known not only to expose those devices but also the network itself. 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 results in a “chicken-and-egg” scenario, wherein these credentials often 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) and other industry standard authentication and provisioning protocols. A standardized device identity facilitates interoperable secure device authentication that helps simplify and standardize secure deployment and management of devices. This standard will be of benefit to manufacturers of conformant LAN equipment, their customers, and users of LANs or LAN services that are based on such equipment.

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 may 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.

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. A verifiable unique device identity allows establishment of the trustworthiness of devices. This facilitates secure device provisioning.

1.3 Relationship to other standards

The present work has been undertaken to provide 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, this work attempts compatibility with the following standards:

- a) Trusted Platform Module (TPM)
- b) Worldwide Interoperability for Microwave Access (WiMAX)
- c) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

For other standards that have influenced the development of this standard or are of general interest see the bibliography (Annex D).

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.

ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).²

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 1999.³

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 2986, PKCS #10: Certification Request Syntax Specification Version 1.7, Nystrom, M., Kaliski, B., November 2000.

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 3410, Introduction and Applicability Statements for Internet Standard Management Framework, Case, J., Mundy, R., Partain, D., Stewart, B., December 2002.

IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Jonsson, J., Kaliski, B., February 2003.

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 4086, Randomness Requirements for Security, Eastlake 3rd, D., Schiller, J., Crocker, S., June 2005.

IETF RFC 4133, Entity MIB (Version 3), Bierman, A., McCloghrie, K., August 2005.

IETF RFC 4492, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., Moeller, B., May 2006.

IETF RFC 4949, Internet Security Glossary, Version 2, Shirey, R., August 2007.

IETF RFC 5008, Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME), Housley, R., Solinas, J., September 2007.

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.

²ANSI 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/>).

³IETF RFCs are available from the Internet Engineering Task Force Web site at <http://www.ietf.org/rfc.html>.

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

ISO/IEC 15802-1:1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.⁴

NIST FIPS 140-2, Annex C: Approved Random Number Generators.⁵

NIST FIPS 180-3, Secure Hash Standard (SHS), October 2008.

NIST FIPS 186-3, Digital Signature Standards (DSS), June 2009.

Standards for Efficient Cryptography (SEC), “SEC 1: Elliptic Curve Cryptography,” Certicom Research, 2000.⁶

⁴ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, 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, Colorado 80112, USA (<http://global.ihs.com/>). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

⁵NIST 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).

⁶This document is available at http://www.secg.org/collateral/sec1_final.pdf.

3. Definitions

For the purposes of this document, the following terms and definitions apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* should be referenced for terms not defined in this clause.⁷

aggregate device: A device containing multiple logical or physical devices.

authentication: The process of verifying an identity claimed by or for a system entity. Defined in RFC 4949.⁸

authentication exchange: The two-party conversation between systems performing an authentication process.

NOTE—Examples of authentication exchange methods are Extensible Authentication Protocol (EAP) and Simple Authentication and Security Layer (SASL).⁹

authentication process: The cryptographic operations and supporting data frames that perform the actual authentication.

Authenticator: An entity that facilitates authentication of other entities attached to the same LAN.

binding: *See:* **cryptographic binding**.

certificate revocation list (CRL): A signed list of revoked certificates. Defined in RFC 5280.

certificate signing request (CSR): A signed message from the device to the Certification Authority (CA) requesting a certificate be issued. This is a variant of the RFC 2986 defined *CertificateRequest* with additional specifications to enable the use of Elliptic Curve Cryptography (ECC).

cipher suite: A set of one or more algorithms, designed to provide any number of the following: data confidentiality, data authenticity, data integrity, replay protection.

client: The protocol entity that makes use of a service.

credential: A data object that provides authentication information such as a public key along with other identity fields. The entity identified by a credential normally possesses a secret or private key that can be used to prove its identity.

cryptographic binding: A data object constructed using cryptographic operations to combine a secret with other arbitrary data objects such that it may be proven that the result could only be created by an entity having knowledge of the secret.

cryptographic key: A parameter that determines the operation of a cryptographic function such as the following:

- a) The transformation from plain text to cipher text and vice versa
- b) Synchronized generation of keying material
- c) Digital signature computation or validation¹⁰

⁷The *IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.

⁸Information on references can be found in Clause 2.

⁹Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

¹⁰This and other definitions in this clause have been drawn from ASC X9 TR1, Technical Report for ABA ASC/X9 Standards Definitions, Acronyms, and Symbols, 2002.

device: A device is any entity that has a single IDevID credential.

IEEE 802 Local Area Network (LAN): IEEE 802 LANs are LAN technologies that provide a MAC Service equivalent to the MAC Service defined in ISO/IEC 15802-1:1995. IEEE 802 LANs include IEEE 802.3™ (CSMA/CD), IEEE 802.11™ (wireless), and IEEE 802.17™ (resilient packet ring).

NOTE—In this standard, also referred to simply as *LANs*.

Initial Secure Device Identifier (IDevID): The Secure Device Identifier installed on the device by the manufacturer.

key: *See:* cryptographic key.

Locally Significant Secure Device Identifiers (LDevIDs): A Secure Device Identifier credential that is unique in the local administrative domain in which the device is used.

Secure Device Identifier (DevID): A device identifier that is cryptographically bound to the device and is composed of the Secure Device Identifier Secret and the Secure Device Identifier Credential.

Secure Device Identifier Credential (DevID Credential), Secure Device Identifier Certificate (DevID Certificate): Synonym for a data object constructed using cryptographic operations to bind the DevID Name and other data to the cryptographic keying material possessed by the device.

Secure Device Identifier Module (DevID Module): A logical security component that will securely store and operate on one or more DevID Secret(s) and associated DevID Credentials.

Secure Device Identifier Root Credential Store: The database of root credentials for IDevID and LDevID credentials that are stored and used by a DevID compliant solution. This is equivalent to the common Web browser root store and may be shipped with the solution.

Secure Device Identifier Secret (DevID Secret): The private key portion of a public-private key pair bound to a DevID Credential.

zeroization: A method of erasing electronically stored data, cryptographic keys, and critical stored parameters by altering or deleting the contents of the data storage to prevent recovery of the data.

NOTE—Adapted from NIST Special Publication 800-57 [B32].¹¹

¹¹The numbers in brackets correspond to those of the bibliography in Annex D.

4. Acronyms and abbreviations

CA Certification Authority

NOTE—CA is also an abbreviation for secure Connectivity Association in IEEE Std 802.1AE™ and IEEE Std 802.1X™.

CPS Certification Practices Statement

CRL Certificate Revocation List

CSR Certificate Signing Request

EAP Extensible Authentication Protocol

EAP-TLS EAP Transport Layer Security

EC Elliptic Curve

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

FIPS Federal Information Processing Standard

IP Internet Protocol

LAN IEEE 802 Local Area Network

LMI Layer Management Interface

MAC Media Access Control

MIB Management Information Base

NIST National Institute of Standards and Technology

PICS Protocol Implementation Conformance Statement

PKCS Public-Key Cryptography Standards

RADIUS Remote Authentication Dial In User Service

RFC IETF Request for Comments

RNG random number generator

RSA Ron Rivest, Adi Shamir, and Leonard Adleman cryptography algorithm

SASL Simple Authentication and Security Layer

SHA Secure Hash Algorithm

SNMP Simple Network Management Protocol

SMI Structure of Management Information

TLS Transport Layer Security

TPM Trusted Platform Module

WiMAX Worldwide Interoperability for Microwave Access

5. Conformance

A claim of conformance to this standard is a claim that the behavior of an implementation of a Secure Device Identifier (IDeVID and LDeVID) meets the requirements of this standard as they apply to the format of the identifier, secure storage of it, and management of the identifier. Example uses of the DevID are provided but are not limited to the discussions in this standard.

Conformance to this standard does not ensure that a system implementing the standard is secure, nor does it ensure that the operation of protocols relying upon capabilities from this standard are immune to breaches by an attacker.

5.1 Requirements terminology

For consistency with existing IEEE standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

- a) *shall* is used for mandatory requirements
- b) *may* is used to describe implementation or administrative choices (may means is permitted to, and hence, may and may not mean precisely the same thing)
- c) *should* is used for recommended choices (the behaviors described by should and should not are both permissible but not equally desirable choices)

The PICS proforma (see Annex A) reflects the occurrences of the words shall, may, and should within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using *is*, *is not*, *are*, and *are not* for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementer or administrator, or whose conformance requirement is detailed elsewhere, is described by *can*. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by *can not*. The word *allow* is used as a replacement for the cliché “support the ability to...,” and the word *capability* means “is configurable such that...”

5.2 Protocol Implementation Conformance Statement

The supplier of an implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A and shall provide the information necessary to identify both the supplier and the implementation.

5.3 Required capabilities

A device for which conformance to this standard is claimed shall:

- a) Contain an IDeVID as specified in 6.2.1 (DevID credentials).
- b) Contain the credential chain as specified in 6.2.1 (DevID credentials).
- c) Support an RSA or ECDSA key as specified in 6.2.2 (Asymmetric cryptography).
- d) Generate random numbers as specified in 6.2.4 (Random number generator).
- e) Store an IDeVID secret as specified in 6.2.5 (Storage).
- f) Support the mandatory operations as specified in 6.3 (DevID Service Interface).
- g) Support the DevID credential format as specified in Clause 7 (DevID Credential details).

A device supporting Simple Network Management Protocol (SNMP) to manage the capabilities of DevIDs for which conformance to this standard is claimed shall:

- h) Restrict access to SNMP version 3 and higher, and only in privacy/authentication mode as specified in 6.3.12 (LDevID Credential insert).
- i) Implement the MIB Management Interface as specified in 6.4 (DevID Management Interface).

5.4 Optional capabilities

A device for which conformance to this standard is claimed may:

- a) Support LDevID credentials as specified in 6.2 (Components of a DevID module).
- b) Store DevID secrets externally to the DevID module as specified in 6.2.5 (Storage).
- c) Support the optional operations specified in 6.3 (DevID Service Interface).
- d) Share an LDevID key pair among multiple LDevID credentials as specified in 6.3.12 (LDevID Credential insert).
- e) Externally generate the IDevID secret as specified in 6.5.1 (Creation of DevID secret).
- f) Share the IDevID secret with LDevID credentials as specified in 6.5.1 (Creation of DevID secret).

5.5 Recommended capabilities

A device for which conformance to this standard is claimed should:

- a) Include Public Key Infrastructure (PKI) hierarchy root credentials in an easily discovered location as specified in 6.2.1 (DevID credentials).
- b) Support at least one LDevID credential as specified in 6.2.1 (DevID credentials).
- c) Encrypt externally stored secrets as specified in 6.2.5 (Storage).
- d) Support the recommended operations as specified in 6.3 (DevID Service Interface).
- e) Confirm that inserted LDevID credentials match this standards credential profile for LDevID credentials 6.3.12 (LDevID Credential insert).
- f) Publish the Certification Authority (CA) Certification Practices Statement (CPS) in the PICS as specified in 6.5.1 (Creation of DevID secret).
- g) Generate an independent LDevID secret as specified in 6.5.1 (Creation of DevID secret).
- h) Generate IDevID secret internally as specified in 6.5.1 (Creation of DevID secret).
- i) Report key generation mechanism in CPS as specified in 6.5.1 (Creation of DevID secret).
- j) Document key exposure plans in their PICS as specified in 6.6.1 (Mitigating risks of key exposure).
- k) Support identity hiding as specified in 6.6.3 (Identity Hiding).

The supplier for a device for which conformance to this standard is claimed should:

- l) Have a unique issuer name in the IDevID as specified in 7.2.4 (issuer).

6. Secure Device Identifier Module

This clause describes the logical components of the DevID Module. It provides the necessary context for understanding the security requirements (and acceptable practical limitations on those requirements) for the creation, use, maintenance, and deletion of DevID credentials. An overview of DevID credentials is provided although the details of DevID fields are specified in Clause 7 (DevID Credential details).

Informative use cases are provided in Annex C as examples.

6.1 What is a device?

A device is any entity in an IEEE 802 LAN that seeks to obtain services from the network or provide services on the network. A device is defined by having a single IDevID credential.

Multiple logical or physical devices may be contained within an aggregate device. Each of these logical or physical devices will have its own unique DevID. The DevID used to identify the aggregate device may depend on the context under which the identification of the aggregate device is done. The selection of a DevID based on this context is beyond the scope of this document. Service interfaces defined in 6.3 do not refer to aggregate devices.

The DevID module is a logical security component that stores and operates on the DevID secrets and associated DevID credentials. The PICS shall describe the device the DevID module is identifying.

6.2 Components of a DevID module

The components of a DevID module are shown in Figure 6-1. Implementations may provide additional functionalities. The DevID credential and DevID secret are used by the DevID module to prove the identity of the device. It is imperative that the DevID secret is securely protected from access by any other entity. The DevID credential is publicly available to any entity that wishes to verify the identity of a device.

6.2.1 DevID credentials

The DevID module shall include the IDevID and zero or more LDevIDs. At least one LDevID credential should be supported.

The DevID module shall include the entire credential chain up to the root credential and should include the root credential. For a shallow hierarchy this requirement could be met with only the IDevID credential on the device. The root certificates should be shipped along with the device or made available by the solution manufacturer in a reasonably discoverable fashion such as on the manufacturer's Web site.

The DevID credential format shall be as described in Clause 7 (DevID Credential details).

DevIDs have to be explicitly created. IDevIDs are normally created during manufacturing or initial provisioning, and can be generated internally in the DevID module or can be created externally and subsequently transferred to secure storage within the DevID module. LDevIDs can be created at any time, in accordance with local policies, and likewise can be created internally in the DevID module, or can be created externally and transferred to the DevID module.

Following creation, DevIDs enter their active use lifetime, during which they can be used and maintained in accordance with the administrative policies of the network and device owners possessing them. IDevIDs remain in their active use state until the effective lifetime ends or the IDevID is disabled. LDevIDs can be managed by the operations detailed in 6.3 (DevID Service Interface).

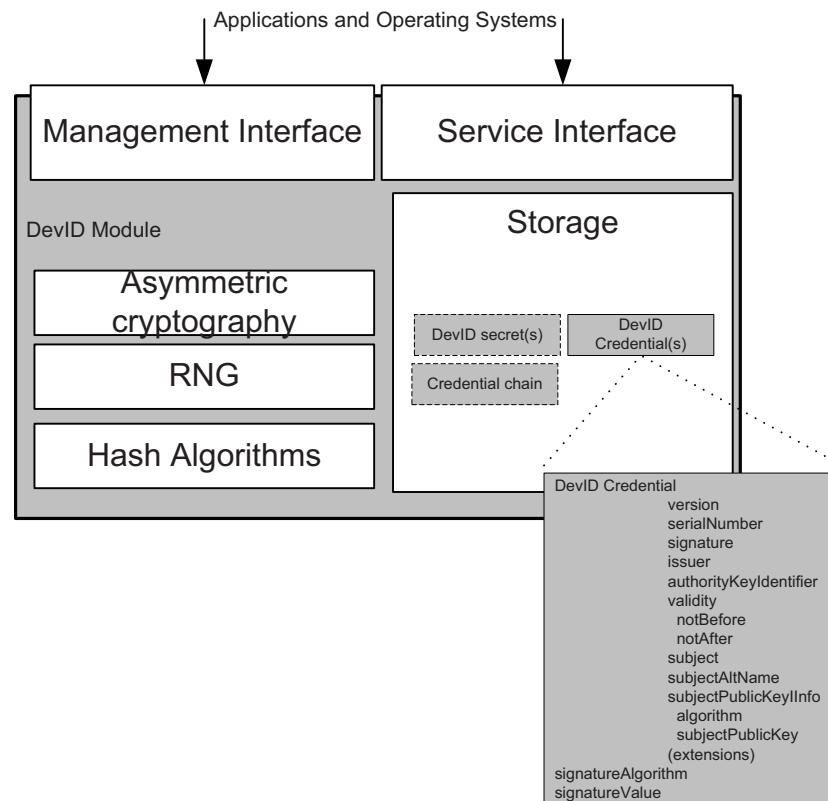


Figure 6-1— DevID components

A DevID (particularly an IDevID) continues to exist for as long as the DevID module it exists in remains operational. In order to support the standard X.509 certificate format, a certificate expiry time is specified. The GeneralizedTime value “99991231235959Z” is used for this purpose.

The CA certificates of the certificate chain shall conform to the IDevID specification as specified in 7.1 (DevID hierarchy credential fields).

6.2.2 Asymmetric cryptography

The DevID secret shall be either the secret portion of a RSA private-public key pair as defined in 7.3.1 (RSASSA-PKCS1-v1.5) or the secret portion of an P-256 elliptic curve private-public key pair as defined in 7.3.2 (ECDSA).

Since the DevID secret is used only within the DevID module in which it is installed, the underlying representation is a choice left to the implementer. Possible representations are discussed in 6.2.5 (Storage) along with estimates of the storage requirements.

Techniques for finding a suitable DevID secret are discussed in IEEE Std 1363™-2000 [B4] and NIST FIPS 186-3.

6.2.3 Hash algorithms

The DevID Module shall contain an implementation of the hash algorithm as specified in 7.3.3 (SHA-256 hash algorithm).