IEEE P802.1AR/D0.3-prime

Draft Standard for Local and Metropolitan Area Networks:

Secure Device Identifier

Sponsor

LAN MAN Standards Committee of the IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1

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.

This draft is an individual contribution to the Secure Device Identifier project, it has no official standing, and has not yet been reviewed or adopted by the task group.

See the introductory notes for what this draft tries to accomplish, and for project scope**, status, and** history**.**

Keywords: For keywords refer to the title page proper, following the editors' foreword.

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.

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. When a document is more than five years old and has not been reaffirmed, 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 the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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.

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. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: 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. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

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; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Editors' Foreword

<<Notes>>

<<Throughout this document, all notes such as this one, presented between angle braces, are temporary notes inserted by the Editors for a variety of purposes; these notes and the Editors' Foreword will all be removed prior to publication and are not part of the normative text.>>

<<Comments and participation in 802.1 standards development

Comments on this draft are encouraged. **PLEASE NOTE: All issues related to IEEE standards presentation style, formatting, spelling, etc. are routinely handled between the 802.1 Editor and the IEEE Staff Editors prior to publication, after balloting and the process of achieving agreement on the technical content of the standard is complete.** Readers are urged to devote their valuable time and energy only to comments that materially affect either the technical content of the document or the clarity of that technical content. Comments should not simply state what is wrong, but also what might be done to fix the problem.

Full participation in the development of this draft requires individual attendance at IEEE 802 meetings. Information on 802.1 activities, working papers, and email distribution lists etc. can be found on the 802.1 website:

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has had a policy of considering ballot comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and ambiguity in past projects. Non-members are advised that the email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum.

Comments on this document may be sent to the 802.1 email exploder, to the editor, or to the Chairs of the 802.1 Working Group and Link Security Task Group.

This draft was prepared by:

Mike Borza
Elliptic Semiconductor
362 Terry Fox Dr., Suite 220
Kanata, ON
Canada
K2K 2P5160
Email:mborza@ellipticsemi.com

John Viega
Secure Software
2010 Corporate Ridge, Suite 820
McLean, VA 22102
USA

Email: viega@securesoftware.com

Chairs of the 802.1 Working Group and Interworking Task Group.

Mick Seaman
Chair, 802.1 Interworking Task Group
160 Bella Vista Ave
Belvedere
CA 94041
USA
Email:mick_seaman@ieee.org

Tony Jeffree
Chair, 802.1 Working Group
11A Poplar Grove
Sale
Cheshire
M33 3AX
UK
+44 161 973 4278 (Tel)
+44 161 973 6534 (Fax)
Email: tony@jeffree.co.uk

PLEASE NOTE: Comments whose distribution is restricted in any way cannot be considered, and may not be acknowledged.
>>

<<The draft text and accompanying information

This document currently comprises:

- A temporary cover page, preceding the Editors' Forewords. This cover page will be removed following working group approval of this draft, i.e. prior to sponsor ballot.
- IEEE boilerplate text.
- The editors' forewords, including this text. These include an unofficial and informal appraisal of history and status, introductory notes to each draft that summarize the progress and focus of each successive draft, and requests for comments and contributions on major issues.
- A title page for the proposed standard including an Abstract and Keywords. This title page will be retained following approval.
- IEEE boilerplate text (identical to the above).
- The introduction to this standard.
- A record of participants (not included in early drafts but added prior to publication).
- The proposed revision proper.
- An Annex Z comprising the editors' discussion of issues. This annex will be deleted from the document prior to sponsor ballot.

IEEE P802.1 editors have a responsibility to attempt to craft technically coherent drafts from the resolutions of ballot comments and the other discussions that take place in the working group meetings. Preparation of drafts often exposes inconsistencies in editors instructions or exposes the need to make choices between approaches that were not fully apparent in the meeting. Choices and requests by the editors' for contributions on specific issues will be found in the editors' introductory notes to the current draft, at appropriate points in the draft, and in Annex Z. Significant discussion of more difficult topics will be found in the last of these.

The ballot comments received on each draft, and the editors' proposed and final disposition of comments, are part of the audit trail of the development of the standard and are available, along with all the revisions of the draft on the 802.1 website (for address see above).

>>

<<History and Scope

A PAR (Project Authorization Request) was drafted at the March 2005 802.1 meeting, forwarded for SEC consideration by vote of the 802.1 Working Group at its closing plenary during the July 2005 meeting of P802, and is pending approval by the IEEE-SA Standards Board, with the following Scope, Purpose, and Reason:

Scope of Proposed Project:

> 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.

Purpose of Proposed Project:

> There is presently no standard identifier for IEEE 802 devices that is cryptographically bound to that device, nor is there 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.

Reason for the Proposed Project:

> It is desirable to authenticate entities attached to a network in a secure fashion; e.g., by means of the mechanisms defined in IEEE Std 802.1X. A standardized device identity facilitates interoperable secure device authentication. User organizations have identified this as a desirable capability to simplify and standardize security management in their networks. The IETF has identified DevID or an equivalent capability as an enabling component of a solution to security issues in several of their protocols, e.g. ARP. DevID is specifically conceived to address this need.

>>

<<Introductory notes to the current draft

This preliminary draft was created to reflect the discussion that took place during the development of the PAR. Supporting material can be found in the Secure Device Identity Tutorial (www.ieee802.org/802_tutorials/july05/Secure Device Identity Tutorial.pdf) presented at the July 2005 802 meeting.

>>

<<Notes to prior drafts (excerpts of continuing relevance).
At present there are no prior drafts.
>>

<<Editors’ final checklist (items noted in development, to be applied to final text.

The IEEE approved format for the headings of Annexes (split across multiple lines) is not compatible with automatic production of the Table of Contents, and requires that the latter be manually edited after updating. Indeed the Framemaker user guide specifically cautions against constructing multi-line formats of the type used. Accordingly drafts of this standard use a slightly different format for Annex titles, though it contains the same information.

>>

IEEE P802.1AR/D0.3-prime

Draft Standard for Local and Metropolitan Area Networks:

Secure Device Identifier

Sponsor

LAN MAN Standards Committee of the IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1

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: local area networks, LANs, metropolitan area networks, MANs, security, MAC security, port based network access control, access control, authentication, authorization, MAC Service, secure association, secure device identifier.

IEEE Standards Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

Introduction to IEEE Std 802.1AR

This introduction is not part of IEEE Std 802.1AR-200X, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identifier.

A secure device identifier (DevID) is cryptographically bound to a device, and supports authentication of the device's identity. IEEE Std 802.1AR specifies globally 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.

IEEE Std 802.1AR can be used in conjunction with IEEE Std 802.1X and its amendment IEEE Std 802.1af, IEEE Std 802.1AE, 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.

This is the first edition of IEEE Std 802.1AR.

<<The "Introduction to IEEE Std xxx" clause found in the front matter for all IEEE 802.1 standards is not really an introduction to the standard per se, but really exists so that the revision history of the current standard and its relationship to prior editions, together with its relationship to (revisions of) companion standards can be easiy grasped. For a first edition this text is necessarily brief, and is mainly a repetition of the current scope together with a note that it is indeed the first edition.>>

Contents

IEEE P802.1AR

Draft Standard for Local and Metropolitan Area Networks: Secure Device Identifier

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 possesed by that user, is often used to authenticate devices such as laptop personal computers whose function is to provide a user interface and can therefore be assumed to have a human operator who can be held responsible for use of the device. However many of the devices that compose a network are designed for unattended autonomous operation. 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 be 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.

<<The initial paragraphs of the Overview (above) are intended to provide a brief ‘problem statement’ without getting embroiled in detail that can require a lengthy explanation, or whose importance can change. Clause 1.1 Introduction (below) provides a declarative statement of the architecture/major components of the solution, while clause 1.2 Scope establishes what this document actually says, breaking that down to the point that it can be checked for completeness. Given the existence of related standards from other groups (e.g. Trusted Computing Group) that can be used to provide or to complement DevID capability, an additional clause “1.3 Relationship to other standards” may prove desirable.>>

1.1 Introduction

A device with Secure Device Identifier (DevID) capability incorporates a globally unique manufacturer provided Initial Device Identifier (IDevID), stored in a way that ensures it will remain unmodified in the absence of both unrestricted access to the device and extraordinary efforts by an attacker. The device supports the creation of Locally Significant Device Identifiers (LDevIDs) by a network administrator. Each LDevID is bound to the IDevID in way that makes it impossible (to within a known and exceedingly small bound) 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.

DevIDs are designed to be used as authentication credentials with EAP and other industry standard authentication and provisioning protocols. LDevIDs can incorporate, and fully protect, additional information specified by the network administrator to support local authorization conventions. LDevIDs may be used to entirely replace IDevIDs in such a way as to assure the privacy of the user of a LDevID and the equipment in which it is installed.

<<The foregoing is most probably entirely wrong, but suffices to illustrate what sort of thing would be useful at this point in the draft.>>

1.2 Scope

For the purpose of providing reliable secure device identifiers (DevIDs) for use in authentication exchanges and provisioning protocols, this standard specifies:

a) Unique per-device identifers and their management
b) The cryptographic binding of a device to its identifiers
c) The relationship between an initially installed identity and subsequent locally significant identfiers
d) Interfaces and methods for the use of DevIDs with existing provisioning and authentication protocols.

Specifically, this standard describes and specifies the following:

e) The use and management of DevIDs in a number of application contexts (Clause 6)
f) Security objectives for DevID implementation, illustrating these by a discussion of a range of practicale implementations (Clause 6)
g) Management Information Bases (MIBs) that support the creation or deletion of LDevIDs (Clause 6)

This standard defines conformance requirements for the implementation of:

h) Devices supporting DevID capabilities (Clause 5)
i) ..

This standard uses and selects options provided by X.509 protocol specifications, but does not modify those specifications (see Clause 2 for references).

The specification and conformance requirements for .... is outside the scope of this standard (see <certain other standards>). Those standards can make use of the <some capability> specified by this standard. The <capabilities provided by this standard> can also be used, in conjuction with other administrative controls, to prevent or mitigate the effects of ARP spoofing (see <Annex C informative>).

<<The Scope clause, as illustrated by the above, comprises the following logical parts:

The introductory lines and the initial list items ((a) through (d) above) reiterate the scope of the PAR. To ensure smooth progression through the final approval stages of the draft, these should remain very little modified from the above or some other way of clearly expressing the PAR Scope text.

The following items ((e) through (g) at the time of writing) are really a step by step contents list, delineating exactly what is in scope, showing how each clause contributes to meeting the objective of the standard, and how each builds on its predecessors. The current list items are not accurate, and are merely place holders for the first draft items. In early drafts this list serves as a top down view of what is to be said, in later drafts it should accurately reflect what is done in each clause, and thus serve as a way of highlighting gaps.

The next items ((h) through (i)) state what conformance requirements are set out. This becomes important if the amount of necessary context and other supporting material is such that it is easy to miss the actual normative provisions, i.e. what implementation aspects are actually prescribed. It is less important if there is only one obvious conformance item, and should be omitted in that case.>>

The remaining text is concerned with clarifying the scope of this standard in relation to other complementary standards, some of which may appear on first sight to overlap in scope. These can be broken down into the following categories (a) other standards that can be used by this standard, and which require this standard to make choices about how they are used, while not changing them (b) standards which may make use of this standard, but whose own operation (including option restriction, selection, or definition) is wholly outside the present scope (c) generally standards or industry practices that can use this standard in a way that merits some informative (non-normative) discussion to encorage such use. Example of all of these are present in the short text above, though no current accuracy is claimed for that text.>>

2. References

The following standards contain provisions which, through reference in this text, constitute provisions of the standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of ISO and IEC maintain registers of currently valid International Standards.

IEEE Std 802.1AE™-200X, IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.[1, 2]

IEEE Std 802.2, 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[3]

IETF RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, Mills, D. L., March 1992.[4]

IETF RFC 1321, The MD5 Message Digest Algorithm, R. Rivest, S. Dusse, April 1992.

IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, Krawczyk, H., Bellare, M., and Canetti, R., February 1997.

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), 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 2716, PPP EAP TLS Authentication Protocol, Aboba, B. and Simon, D., October 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIv2, McCloghrie, K. and Kastenholz, F., June 2000.

IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), Rigney, C., Willens, S., Rubens, A., and Simpson, W., June 2000.

IETF RFC 3232, Assigned Numbers: RFC 1700 is Replaced by an On-line Database, Reynolds, J., January 2002.

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

[1] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

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

[3] ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

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

IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, D. Harrington, R. Presuhn, B. Wijnen, December 2002.

IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), J. Case, D. Harrington, R. Presuhn, B. Wijnen, December 2002.

IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications, D. Levi, P. Meyer, B. Stewart, December 2002.

IETF RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), U. Blumenthal, B. Wijnen, December 2002.

IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), B. Wijnen, R. Presuhn, K. McCloghrie, December 2002.

IETF RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, December 2002.

IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, December 2002.

IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, December 2002.

IETF RFC 3575, IANA Considerations for RADIUS, B. Aboba, July 2003.

IETF RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), M. Chiba, G. Dommety, M. Eklund, D. Mitton and B. Aboba, July 2003.

IETF RFC 3579, RADIUS Support for Extensible Authentication Protocol (EAP), B. Aboba, P. Calhoun, September 2003.

IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, P.Congdon, September 2003.

IETF RFC 3748, Extensible Authentication Protocol (EAP), Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J., Levkowetz, H, June 2004.

ISO 6937-2: 1983, Information processing—Coded character sets for text communication—Part 2: Latin alphabetic and non-alphabetic graphic characters.[5]

ISO/IEC 7498-1: 1994, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 1: The Basic Model.

ISO/IEC 8824:1990, Information technology—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1) (Provisionally retained edition).

ISO/IEC 8825:1990, Information technology—Open Systems Interconnection—Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (Provisionally retained edition).

[5] ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

ISO/IEC TR 11802-2: 1997, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 2: Standard Group MAC addresses.

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.

<<As usual the reference list is dominated (and obscured) by SNMP references that are not directly required by provisions of this standard, but only called up as a consequence of references to a few base documents. These and other subsidiary references should probably be removed en-mass to the Bibliography. At present this reference list is only a starting point. A few references have been retained for the sole purpose of anchoring the notes on where to obtain IEEE, ISO/IEC, and IETF documents.>>

3. Definitions

Replace the contents of clause 3 with the following:

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition [B1][1], should be referenced for terms not defined in this clause.

3.1 **Authenticator:** An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

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

NOTE—For example, Extensible Authentication Protocol (EAP) and Simple Authentication and Security Layer (SASL).[2]

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

3.4 **Authentication Server:** An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides.

NOTE—The Authentication Server function can be co-located with an Authenticator, or it can be accessed remotely via a network to which the Authenticator has access.

3.5 **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.

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

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

a) The transformation from plain text to cipher text and vice versa
b) Synchronized generation of keying material
c) Digital signature computation or validation.[3]

3.8 **cryptographic mode of operation:** Also referred to as mode. An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm.[4]

3.9 **data integrity:** A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.[5]

3.10 **entity authentication:** The process of identifying and verifying the identity of an entity, using credentials issued to entities (e.g. username/password, token card, public-key-certificates, etc.).

3.11 **frame:** MAC protocol data unit (MPDU).

[1] The numbers in brackets correspond to those of the bibliography in <xref whatever>.

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

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

[4] This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 300-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

[5] This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 800-57, Recommendation for Key Management, 2005.

3.12 **IEEE 802 Local Area Network (LAN)**: IEEE 802 LANs (also referred to in the text simply as LANs) are LAN technologies that provide a MAC Service equivalent to the MAC Service defined in ISO/IEC 15802-1. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.5 (Token Ring), IEEE Std 802.11 (Wireless), and ISO 9314-2 (FDDI) LANs.

3.13 **initialization vector (IV):** A vector used in defining the starting point of an encryption process within a cryptographic algorithm.[6]

3.14 **integrity:** See data integrity.

3.15 **integrity check value (ICV):** A value that is derived by performing an algorithmic transformation on the data unit for which data integrity services are provided. The ICV is sent with the protected data unit and is recalculated and compared by the receiver to detect data modification.

3.16 **key:** See cryptographic key.

3.17 **key management:** The generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy.

3.18 **Layer Management Interface (LMI):** the interface between a protocol entity in a system and the system management, providing for the exchange of parameters with other system entities that are not attached to the service access points used and provided by the protocol entity.

3.19 **IEEE 802 Local Area Network (LAN):** IEEE 802 LANs (also referred to in the text simply as LANs) are LAN technologies that provide a MAC Service equivalent to the MAC Service defined in ISO/ IEC 15802-1. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.11 (Wireless), IEEE Std 802.17 (Resilient Packet Ring).

3.20 **MAC Security Entity (SecY):** The entity that operates the MAC Security protocol within a system.

3.21 **MAC service data unit (MSDU):** A sequence of zero or more octets that compose the data to be communicated with a single MAC Service request or indication.

3.22 **man-in-the-middle attack:** An attack on the authentication protocol run, in which the attacker positions himself between the claimant and verifier so that he can intercept and alter data traveling between them.[7]

3.23 **master key:** A secret key that is used to derive one or more cryptographic keys that are used directly to protect data transfer.

3.24 **message authentication:** If the message arrives authenticated, the cryptographic guarantee is that the message was not modified in transit and that the message originated from an entity with the proper cryptographic credentials.

3.25 **message digest:** The output produced by applying a hash function to a message.

3.26 **mode:** See cryptographic mode of operation.

[6] This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, 2001.

[7] This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 800-63: Electronic Authentication Guideline, 2004.

3.27 **multipoint:** Involving or potentially involving more than one participant in the role of receiver, or in the role of transmitter, in a single data transfer or set of related data transfers.

3.28 **network access port:** A point of attachment of a system to a LAN. It can be a physical port, for example, a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.

3.29 **nonce:** A non-repeating value, such as a counter, used in key management protocols to thwart replay and other types of attack.

3.30 **packet number (PN):** A monotonically increasing value used to uniquely identify a MACsec frame in the sequence of frames transmitted using an SA.

3.31 **plaintext key:** An unencrypted cryptographic key.[8]

3.32 **Port**: A service access point for the MAC Service or MAC Internal Sublayer Service.

3.33 **port access entity (PAE):** The protocol entity associated with a Port. It can support the protocol functionality associated with the Authenticator, the Supplicant, or both.

3.34 **Port Identifier:** A 16-bit number that is unique within the scope of the address of the port.

3.35 **protocol data unit (PDU):** A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.

3.36 **secret key:** A cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.[9]

3.37 **Secure Association (SA):** A security relationship that provides security guarantees for frames transmitted from one member of a CA to the others. Each SA is supported by a single secret key, or a single set of keys where the cryptographic operations used to protect one frame require more than one key.

3.38 **Secure Association Identifier (SAI):** An identifier for an SA, comprising the SCI concatenated with the Association Number (AN).

3.39 **Secure Association key (SAK):** The secret key used by an SA.

3.40 **Secure Channel (SC):** A security relationship used to provide security guarantees for frames transmitted from one member of a CA to the others. An SC is supported by a sequence of SAs thus allowing the periodic use of fresh keys without terminating the relationship.

3.41 **Secure Channel Identifier (SCI):** A globally unique identifier for a secure channel, comprising a globally unique MAC Address and a Port Identifier, unique within the system allocated that address.

3.42 **secure Connectivity Association (CA):** A security relationship, established and maintained by key agreement protocols, that comprises a fully connected subset of the service access points in stations attached to a single LAN that are to be supported by MACsec.

3.43 **spoofing:** Claiming a fraudulent identity for purposes of mounting an attack.

[8] FIPS 140-2.

[9] FIPS 140-2.

3.44 **Supplicant:** An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.

NOTE—The term *Supplicant* is used in this standard in place of the more conventional term, *peer*, used in other access control-related specifications.

3.45 **system:** A device that is attached to a LAN by one or more Ports. Examples of systems include end stations, servers, MAC Bridges, and routers.

3.46 **wiretapping:** An attack that intercepts and accesses data and other information contained in a flow in a communication system. The term is used to refer to reading information from any sort of medium used for a link or even directly from a node, such as a gateway or subnetwork switch. “Active wiretapping” attempts to alter the data or otherwise affect the flow; “passive wiretapping” only attempts to observe the flow and gain knowledge of information it contains.

<<At the time of writing this list is only a starting point, taken with little consideration from .1AE and .1X.>>

4. Acronyms and abbreviations

For the purposes of this standard, the following acronyms and abbreviations apply. *The Authoritative Dictionary of IEEE Standards Terms* <*ref*>, should be referenced for terms not defined in this clause.

AAA	authentication, authorization, and accounting
AES	Advanced Encryption Standard
AN	Association Number
CA	Secure Connectivity Association
CHAP	Challenge Handshake Authentication Protocol
CRC	Cyclic Redundancy Check
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
EAP	extensible authentication protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	EAP over LANs
ES	End Station
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
Gb/s	Gigabit per second (1 Gb/s is equivalent to 1 000 000 000 bits per second)
ICV	Integrity Check Value
IP	Internet Protocol
IV	Initialization Vector
ISS	Internal Sublayer Service
KaY	MAC Security Key Agreement Entity
LAN	IEEE 802 Local Area Network
LLC	Logical Link Control
LLDP	Link Level Discovery Protocol
LMI	Layer Management Interface
MAC	media access control
Mb/s	Megabit per second (1 Mb/s is equivalent to 1 000 000 bits per second)
MIB	Management Information Base
MPDU	MAC protocol data unit
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSDU	MAC Service Data Unit
NESSIE	New European Schemes for Signatures, Integrity, and Encryption
NIST	National Institute of Standards and Technology
PACP	Port Access Control Protocol
PAE	port access entity
PDU	protocol data unit
PN	Packet Number
RADIUS	remote authentication dial in user service
SA	Secure Association
SAI	Secure Association Identifier
SAK	Secure Association Key
SASL	Simple Authentication and Security Layer
SC	Secure Channel
SCB	Secure Channel Broadcast
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SNMP	Simple Network Management Protocol
VLAN	Virtual LAN

<<At present this list is only a starting point. As well as adding new items, the ones that are here should be checked to see whether they are actually used (in early drafts, likely to be used) and otherwise removed.>>

5. Conformance

<<This Clause (5) has not yet received any attention or modification as part of this amendment, and is included only for the editors' convenience. Any hints as to content are simply intended as a spur to action. The introductory notes to this draft may contain proposals for change in a future draft, including those required as a result of other changes in this draft.>>

A claim of conformance to this Standard is a claim that the behavior of an implementation of a Secure Device Identifier (DevID) meets the requirements of this Standard as they apply to the storage, of the MACsec protocol, management of its operation, and provision of service to the protocol clients of the SecY, as revealed through externally observable behavior of the system of which the SecY forms a part.

Conformance to this standard does not ensure that the system of which the DevID implementation forms a part is secure, or that the operation of other protocols do not provide a way for an attacker to breach that security.

5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 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 implementor 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 cliche Support the ability for, and the word ***capability*** means can be configured to.

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 <whatever> 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 Initial Device Identifier (IDevID) as specified in <Clause x>
b) Support the basic fields specified in <x.x> for each IDevID
c) Support the basic fields specified in <x.x> for each LDevID
d) Support the basic operations specified in <x.x> for each IDevID.

e) Support the basic operations specified in <x.x> for each LDevID.

A device for which conformance to this standard is claimed shall not:

f) Support creation or modification of any Device Identifier through the operation of versions of SNMP prior to v3, or through the operation of SNMP v3 on any mode other than privacy and authentication mode.

5.4 Optional capabilities

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

a) Associate additional information elements with the IDevID as specified in <x.x>.
b) Support the creation of one or more LDevID(s) as specified in <x.x>.
c) Associate additional information elements with each LDevID as specified in <x.x>.
d) Implement the capability to re-issue either or both IDevID and LDevID as specified in <x.x>.
e) Support creation or modification of LDevIDs using SNMP v3 in any mode other than privacy and authentication mode.

5.5 Recommended capabilities

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

a) Maintain the optional management records of creation and modification of DevIDs.

A device for which conformance to this standard is claimed should not:

a) Behave is such a manner as is likely to cause a breach of the peace as specified in <Clause x>.
b) <<MOVE>>issuerID: a globally unique identifier for the issuer of the credential. For manufactures a good choice will typically be the manufacturer's name including abbreviated corporate designator concatenated with the corporate entity's head office country, e.g. "Example Networks Corp CA". Another good choice will be the URL of the certificate authority server, e.g. www.example.com/devid or cert-auth.example.com
c) uniqueID: within the scope of the issuer's domain an unique identifier that will remain unique for all device credentials issued by that issuer. Examples include:
d) manufacturer's serial number
e) service provider's account name
f) device pre-programmed MAC address
g) <<MOVE>>

6. Secure device identifer use

The secure device identifier (DevID) capability allows network administrators to associate an authentication credential, for use in authentication exchanges and provisioning protocols, with devices that participate or wish to participate in their networks. Each device may have one or more such locally significant device identifiers (LDevIDs), depending on the administration of the networks in which it participates.

This clause (6) describes how IDevIDs and LDevIDs are used in a number of applications, and provides the necessary context for understanding the security requirements (and acceptable practical limitations on those requirements) for the creation and maintenance of DevIDs (see <Clause 7>).

Overview

What is a device?

For purposes of this standard a device is any entity that possesses a DevID. A device may contain and/or be a peer to other devices.

Lifecycle of a Secure DevID

About this clause

Creation of Secure DevIDs

Lifecycle of a Secure DevID: For the purposes of use the DevID never expires. In order to support standard X.509 certificate format a certificate lifetime must be used. This value should be chosen to exceed the normal device lifetime.

NOTE: this implies that the DevID credential lifetime will may extend beyond the effective 'lifetime' of the credentials (as per strict key lifetime guidelines). Alternatively we could specify that the RSA key length can be selected as appropriate for the lifetime BUT i think this is a big part of why the LDevID exists ... to protect the id of the device during actual deployment. Thus conceptually using an IDevID 10yr down the road to redeploy an almost end-of-life device (and get a new LDevID) is reasonable.

The IDevID SHOULD be used for the deployment mechanisms only. After deployment either an LDevID or other locally significant credential SHOULD be used.

Supporting infrastructure requirements

Mutual authentication of devices

Usage of IDevIDs

Usage of LDevIDs

Usage of additional information associated with DevIDs

multiple IDs at the same level of hierarchy

trees

virtualized devices

Decommissioning Secure DevIDs

Destruction of DevID objects

Revoking DevIDs

7. Device identifier storage and use

Secure device identifiers (DevIDs) are stored in such a way as to make it impractical for an attacker that does not have unrestricted access to the device, and is willing to engage in extraordinary efforts, to remove the identifer from the device and use it with another device.

This clause specifies how.

7.1 <Security Objectives>

DevIDs are used to authenticate access to networks. They do so using cryptographic data and operations. Some of this data is private. The private data in a DevID must be stored and used within a controlled boundary (the “cryptographic boundary”) and protected from plaintext access by entities outside the cryptographic boundary. To assure that their use is authentic a DevID must satisfy the following security objectives:

a) Confidentiality: DevIDs contain one or more private cryptographic key(s) and identifiers unique to that instance of DevID that must be protected from disclosure outside the cryptographic boundary. Failure to protect this data from external disclosure results in a compromised DevID that is no longer guaranteed to be bound to the device.

b) Integrity: The integrity of the public and private cryptographic keys and private identifier data is essential to ongoing use of DevIDs. Failure to protect the integrity of this data results in identifcation data that will no longer be useful for device authentication purposes.

c) Availability: A DevID is assumed to be a component of a larger device or system and available on demand. A DevID may become unavailable if its internal consistency checks fail, if it detects compromise of its protected data or if it is instructed to disable access to its protected data by an authorized management entity. Under those circumstances a DevID will become unavailable to fulfil its authentication purposes.

7.1.1 Data objects common to all DevID intances

7.1.1.1 RFC 3280 PKIX certificate

7.1.1.2 TBSCertificate ::= SEQUENCE {

7.1.1.3 version [0] EXPLICIT Version - v3,

7.1.1.4 serialNumber CertificateSerialNumber - up to 20 octets,

7.1.1.5 signature AlgorithmIdentifier - sha-1WithRSAEncryption,

7.1.1.6 issuer Name,

7.1.1.7 validity Validity,

7.1.1.8 subject Name,

7.1.1.9 subjectPublicKeyInfo SubjectPublicKeyInfo,

7.1.1.10 issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,

7.1.1.11 -- If present, version MUST be v2 or v3

7.1.1.12 subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,

7.1.1.13 -- If present, version MUST be v2 or v3

7.1.1.14 extensions [3] EXPLICIT Extensions OPTIONAL

7.1.1.15 -- If present, version MUST be v3

7.1.1.16 }

7.1.1.17

7.1.1.18

7.1.1.19 issuerID

: string[64]; human readable, should be globally unique, e.g. trademarked organization name, web address, ticker symbol, tcp/ip address

7.1.1.20 uniqueID

: string[32]; an identifier globally unique to the issuer, e.g. serial number, factory programmed MAC address

7.1.2 devicePubKey

: RSA-2048; per X.509 key block - needs format definition // rationale from FIPS 201

7.1.2.1 reusable - move to mgmt intf as read-only or delete

: uint1;

7.1.2.2 reused - move to mgmt intf as read-only or delete

: unit1;

7.1.2.3 version

: uint3; // standard version = 0

7.1.2.4 reserved

: uint3; (uint5 if reused/reusable move out of DevID)

7.1.2.5 signature

: RSASSA-PSS; // from PKCS#1 ver. 2.1

7.1.3 Data objects specific to IDevID instances

issuer-specific extension data: string[] - size limitation based on max size less than minimax client data frame size, no fragmentation, e.g. ~1500 octets - sum of other fields - some allowance for protocol overhead

7.1.4 Data objects specific to LDevID instances

not-before-date, expiry-date - revisit when decision is made about certificate format

- required field (must be present, but not necessarily a real date, e.g.)

- but not necessary to check (against wall time) during authentication

issuer-specific extension data: string[] - size limitation based on max size less than minimax client data frame size, no fragmentation, e.g. ~1500 octets - sum of other fields - some allowance for protocol overhead

- deal with privacy

7.2 Device identifier service interface

7.2.1 initialization

need to deal with virtualized and multiple devices reusing the same crypto operators & other hardware in a DevID module

- **at boot time or reset**

- physical device: initialize yourself - returns status after internal intialization, phase 1 of a 2 phase process

OK

FAIL - causes internal registers to be cleared

IN PROGRESS - initialization in progress and DevID module not ready

- go operational (phys device)- following successful initialization, finish start-up including any external initial values required to act as DevID, e.g. entropy insertion (seeding), loading an encrypted DevID blob,

    - supplied entropy must be mixed into the RNG according to a specified algorithm (operation) if it is supplied

    - modules that require arguments must not go operational until they've received the arguments they need

- it's illegal to call this service more than once per initialization - specify what action is taken

    - expected response is to do nothing, i.e. do not re-seed, nor acccept key blobs or other initializer

return values : pass/fail/in progress/attempt to repeat operation

Post boot - pertain to LDevIDs, ephemeral (anonymous) DevIDs, virtual DevIDs

- can be installed at any time

- install new LDevID -

    - binds LDevID to the IDevID - simply means LDevID is installed in the DevID module (explicit binding of LDevID to IDevID is external to DevID spec, eg. in a Database)

    - insertion of externally generated keys is an optional requirement

    - similarly internal generation of keys is an optional requirement (but one of the two must be supported if LDevIDs are supported)

7.2.2 operation

- generate LDevIDs, IDevIDs - optional capability

    - generate a key pair

    - associate issuer||uniqeID data to the key pair

    - return a keyhandle or ERROR (error-code)

- insert xDevIDs - optional capability (but one of "generate" or "insert" is required)

    - cleartext insertion of key pair

    - per "generate", create an association between key pair and ID data

    - return a keyhandle or ERROR(error-code)

- create an xDevID certificate signing request (or just sign it)

- sign a piece of data:

    - to be used in authentication protocols

- takes as input keyhandle and the data to be signed

- object to be signed is arbitrary length,

- note to implementor: must be aligned and padded by by the DevID

shut-down

No specific requirents.

[RNG states may be saved during shutdown but that’s not appropriate to this discussion. Deal with this elsewhere by reference to best practices for these devices.]

[LDevIDs that require persistent storage should be stored at time of creation. Make sure this is dealt with in appropriate part of document.]

7.2.3 management

To be provided via a service interface (e.g. LMI with MIB and API)

DevID MIB components may be accessible with read or read/write attributes.

Access controls: user vs. administrator - must provide access controls to separate functions accessible to users vs. administrators, need to discuss authentication of clients to a role

DevID object members -

7.3 Cryptographic Primitives

RSA-2048

SHA-256

RNG

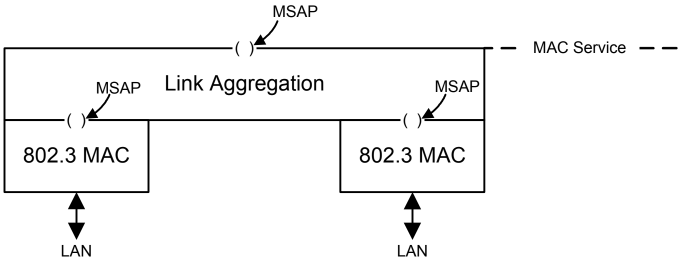

Figure 7-1—A diagram

8. Management protocol

8.1 Introduction

This clause defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects for creating and managing secure device identifiers, based on the specifications contained in <Clause X>. This clause includes a MIB module that is compliant to SMIv2.

8.2 The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of [IETF RFC 3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in [IETF RFC 2578], [IETF RFC 2578],[IETF RFC 2579], [IETF RFC 2579] and [IETF RFC 2580].

8.3 Relationship to other MIBs

8.3.1 System MIB

It is assumed that a system implementing this MIB will also implement the “system” group defined in [IETF RFC 3418] (or at least that subset of the system group defined in[IETF RFC 1213]).

8.3.2 Relationship to the Interfaces MIB

It is assumed that a system implementing this MIB module will implement the “interfaces” group defined in [IETF RFC 2863], the Interfaces Group MIB. This MIB includes the clarifications mandated by [IETF RFC 2863] for any MIB that is medium-specific or an adjunct of the Interfaces Group MIB.

8.4 Security considerations

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/ vulnerability:

<<to be explicitly detailed>>

<<additional vulnerabilities to be explicitly described>>

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module. Use of versons of SNMP prior to v3, or the use of SNMP v3 without invocation of its cryptographic mechanisms (for authentication and privacy) is not consistent with the security goals of this standard..

8.5 Definitions for Secure Device Identifier MIB

In the MIB definition below, should any discrepancy between the DESCRIPTION text and the corresponding definition in <Clause X> occur, the definition in <Clause X> shall take precedence.

```
-- *****************************************************************
-- IEEE8021-DEVID-MIB
--
-- Definitions of managed objects supporting IEEE 802.1AR
-- Secure Device Identifier (DevID).
--
-- May 2005
--
-- *****************************************************************

IEEE8021-DEVID-MIB DEFINITIONS ::= BEGIN

-- -----------------------------------------------------------------
-- IEEEE802.1AR MIB
-- -----------------------------------------------------------------

<<to be supplied>>
```

Annex A

<<This Annex has not yet received any attention, and is included only for the editors' convenience.>>

(normative)

PICS Proforma[1]

A.1 Introduction

The supplier of a protocol implementation that is claimed to conform to this standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS s a statement of the capabilities and options of the protocol that have been implemented. The PICS can have a number of uses, including use

a) By the protocol implementor, as a checklist to reduce the risk of failure to conform to the standard through oversight.
b) By the supplier and acquirer—or potential acquirer—of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma.
c) By the user—or potential user—of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that although interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs).
d) By a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.2 Abbreviations and special symbols

A.2.1 Status symbols

M	Mandatory
O	Optional
O.n	Optional, but support of at least one of the group of options labeled by the same numeral *n* is required
X	Prohibited
pred:	Conditional-item symbol, including predicate identification (see A.3.4)
¬	Logical negation, applied to a conditional item's predicate

A.2.2 General abbreviations

N/A	Not applicable
PICS	Protocol Implementation Conformance Statement

[1] *Copyright release for PICS proformas:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

A.3 Instructions for completing the PICS proforma

A.3.1 General structure of the PICS proforma

The first part of the PICS proforma, implementation identification and protocol summary, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PICS proforma is a fixed-format questionnaire, divided into several subclauses, each containing a number of individual items. Answers to the questionnaire items are to be provided in the right-most column, either by simply marking an answer to indicate a restricted choice (usually Yes or No), or by entering a value or a set or range of values. (Note that there are some items in which two or more choices from a set of possible answers can apply; all relevant choices are to be marked.)

Each item is identified by an item reference in the first column. The second column contains the question to be answered; the third column records the status of the item—whether support is mandatory, optional, or conditional; see also A.3.4. The fourth column contains the reference or references to the material that specifies the item in the main body of this standard, and the fifth column provides the space for the answers.

A supplier may also provide (or be required to provide) further information, categorized as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labeled *Ai* or *Xi,* respectively, for cross-referencing purposes, where *i* is any unambiguous identification for the item (e.g., simply a numeral). There are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformation Statement for the implementation in question.

NOTE—Where an implementation is capable of being configured in more than one way, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case that makes for easier and clearer presentation of the information.

A.3.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations, or information about aspects of the implementation that are outside the scope of this standard but that have a bearing on the answers to some items.

References to items of Additional Information may be entered next to any answer in the questionnaire and may be included in items of Exception Information.

A.3.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No preprinted answer will be found in the Support column for this; instead, the supplier shall write the missing answer into the Support column, together with an *Xi* reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item.

An implementation for which an Exception item is required in this way does not conform to this standard.

NOTE—A possible reason for the situation described above is that a defect in this standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.3.4 Conditional status

A.3.4.1 Conditional items

The PICS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply—mandatory or optional—are dependent upon whether or not certain other items are supported.

Where a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the "Not Applicable" answer is selected. Otherwise, individual conditional items are indicated by a conditional symbol in the Status column.

A conditional symbol is of the form "**pred:** S," where **pred** is a predicate as described in A.3.4.2, and S is a status symbol, M or 0.

If the value of the predicate is true (see A.3.4.2), the conditional item is applicable, and its status is indicated by the status symbol following the predicate: the answer column is to be marked in the usual way. If the value of the predicate is false, the "Not Applicable" (N/A) answer is to be marked.

A.3.4.2 Predicates

A predicate is one of the following:

a) An item-reference for an item in the PICS proforma: The value of the predicate is true if the item is marked as supported, and is false otherwise.
b) A predicate-name, for a predicate defined as a boolean expression constructed by combining item-references using the boolean operator OR: The value of the predicate is true if one or more of the items is marked as supported.
c) A predicate-name, for a predicate defined as a boolean expression constructed by combining item-references using the boolean operator AND: The value of the predicate is true if all of the items are marked as supported.
d) The logical negation symbol "¬" prefixed to an item-reference or predicate-name: The value of the predicate is true if the value of the predicate formed by omitting the "¬" symbol is false, and vice versa.

Each item whose reference is used in a predicate or predicate definition, or in a preliminary question for grouped conditional items, is indicated by an asterisk in the Item column.

A.4 PICS proforma for IEEE 802.1AR

A.4.1 Implementation identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification—e.g., name(s) and version(s) of machines and/or operating system names	

NOTES

1—Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.
2—The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).

A.4.2 Protocol summary, IEEE Std 802.1AR-200X

Identification of protocol specification	IEEE Std 802.1AR-2007, IEEE Standards for Local and Metropolitan Area Networks: Secure Device Identifier
Identification of amendments and corrigenda to the PICS proforma that have been completed as part of the PICS	Amd. : Corr. : Amd. : Corr. :
Have any Exception items been required? (See A.3.3: The answer Yes means that the implementation does not conform to IEEE Std 802.1X-2004.)	No [ ] Yes [ ]

Date of Statement	

A.5 Major capabilities and options

Item	Feature	Status	References	Support
	Does the implementation:			
IDEV	Contain an Initial Device Identifier (IDevID) that meets the requirements of <Clause 8>	M	<5.3(x)>, <x.x, y.y>, A.6	Yes[ ]
LDEV	Provide for the creation and management of Locally significant Device Identifiers (LDevID)	M	<5.3(x)>, <x.x, y.y>, A.7	Yes[ ]
EFMT	Support the secure association of additional items of information with each LDevID	O	<5.3(x)>, <x.x, y.y>, <A.X>	Yes[ ] No [ ]
STOR	Meet the minimum requirements for secure storage of DevIDs specified in <Clause 7>.	M	<5.3(x)>, <x.x, y.y>, <A.X>	Yes[ ]
ESTOR	Satisfy some or all of additional criteria for secure storage of DevIDs specified in <Clause 7>.	O	<5.3(x)>, <x.x, y.y>, <A.X>	Yes[ ] No [ ]
MIB	Support creation and management of LDevIDs using the MIB specified in <Clause 9>.	O	<5.3(x)>, <x.x, y.y>, <A.X>	Yes[ ] No [ ]
SNMP	Support access to the MIB specified in <Clause 9> using SNMP v3 or higher?	O	<x.x>, <A.X>	Yes[ ] No [ ]
SNMX	Support access to DevID parameters using any version of SNMP prior to v3?	X	<5.3(x)>	No [ ]

A.6 IDevID

Item	Feature	Status	References	Support
IDEV-1		M	<x.x>	Yes[ ]
IDEV-2		M	<x.x>	Yes[ ]
IDEV-3	Is it possible to remove the IDevID.	X	<x.x>	No [ ]

A.7 LDevID creation and management

Item	Feature	Status	References	Support
LDEV-1		M	<x.x>	Yes[ ]
LDEV-2		M	<x.x>	Yes[ ]
LDEV-3		O	<x.x>	Yes[ ] No [ ]

PREDICATES:

<placeholder for the editor’s convenience, no predicates defined at present>

Annex B

(informative)

Bibliography

[B1] IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition.

[B2] IETF RFC 787, RFC 787 - Connectionless data transmission survey/tutorial, A. Lyman. Chapin, July 1981

[B3] IETF RFC 2279, UTF-8, a Transformation format of ISO 10646, Yergeau, F., January 1998.

[B4] IETF RFC 2406, IP Encapsulating Security Payload (ESP), Kent, S., Atkinson, R., November 1998.

[B5] IETF RFC 2737, Entity MIB (Version 2), McCloghrie, K., Bierman, A., December 1999.

[B6] IETF RFC 3232, Assigned Numbers: RFC 1700 is Replaced by an On-line Database, Reynolds, J., January 2002.

[B7] IETF RFC 3410, Introduction and Applicability Statements for Internet-Standard Management Framework, Case, J., Mundy, R.,Partain, D., and Stewart, B., December 2002

[B8] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Manage-ment Frameworks, Harrington, D., Presuhn, R., and Wijnen, B., December 2002.

[B9] ISO 6937-2: 1983, Information processing—Coded character sets for text communication—Part 2: Latin alphabetic and non-alphabetic graphic characters.[1]

[B10] ISO/IEC TR 11802-2: 1997, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 2: Standard Group MAC addresses.

[B11] Fowler, M., "UML Distilled: A Brief Guide to the Standard Object Modeling Language, Third Edition", Pearson Education Inc., Boston, 2004, ISBN 0-321-19368-7.

[B12] McGrew, D. A., Viega, J., "The Security and Performance of the Galois/Counter Mode (GCM) of Operation (Full Version), http://eprint.iacr.org/2004/193.pdf.

<<The above list probably has some overlap with the References, and it is likely that may items in the References are not strictly required by this standard, and should be moved here.>>

[1] ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

Annex C

<<This Annex has not yet received any attention or modification as part of this amendment, and is included only for the reviewers' convenience.>>

(informative)

Example Authentication Protocol

Use of the Trusted Computing Group TPM blob to support DevID

Intro and background.

C.1 Basics

Stuff.

Annex D

<<The definitive source of this annex was not avaliable to the editor at the time of preparation of this draft, and has therefore been omitted. It is not anticipated that there will be any changes to this annex as a consequence of the .1af amendment, with the possible exception of introductory material that places some of the attributes within the scope of one of the .1X application scenarios.>>

(informative)

IEEE 802.1X RADIUS Usage Guidelines[1]

[1] The material in this annex was derived from IETF RFC 3580, developed in collaboration between participants in the Internet Engineering Task Force (IETF) and the IEEE 802.1 Working Group.

Annex Z

(informative)

Commentary

<<Editor's Note: This is a temporary Annex, a place to record technical issues and their disposition. This annex will be removed prior to Sponsor Ballot, and preserved on the 802.1 web site for future reference[1].>>

<<The order of discussion of issues is intended to help the reader understand first what is the draft, secondly what may be added, and thirdly what has been considered but will not be included. In pursuit of this goal, issues where the proposed disposition is "no change" will be moved to the end. The description of issues is updated to reflect our current understanding[2] of the problem and its solution: where it has been considered useful to retain the original comment, in whole or part, either to ensure that its author does not feel that it has not been sufficiently argued or the editor suspects there may be further aspects to the issue, that has been done as a footnote.>>

Q: Will/Should it be possible to a) load the IDevID from an external location at each system initialization? b) export/import a IDevID.

7.1 - possible fourth clause

a) Privacy: A DevID may provide the capability to implement per device identities that protect the privacy of the device. while maintaining the integrity of the binding of the identity to that device.

[1] The footnotes in this annex provide further background to its development. Most of the highly subjective material, who said what and were they were right etc. together with temporary notes on blind alleys will be put into the footnotes so that they can be easily stripped out when the final annex is preserved.

[2] This annex is not intended therefore to be a complete historical record of the development of the draft. The formal record is largely captured in the Disposition of Comments on each ballot.