



DRAFT AMENDMENT ISO/IEC DIS 8802-11/Amd.7

Attributed to ISO/IEC JTC 1 by the Central Secretariat (see page iii)

Voting begins on
2005-10-07

Voting terminates on
2006-03-07

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

FAST-TRACK PROCEDURE

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

Part 11:

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

AMENDMENT 7: Specifications for Enhanced Security — WLAN Authentication and Privacy Infrastructure (WAPI)

(standards.iteh.ai)

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains — Exigences spécifiques —

Partie 11: Spécifications pour le contrôle d'accès au support et la couche physique

AMENDEMENT 7: Caractéristiques pour la sécurité améliorée — Authentification de WLAN et infrastructure privée (WAPI)

ICS 35.110

In accordance with the provisions of Council Resolution 21/1986 this DIS is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 21/1986, ce DIS est distribué en version anglaise seulement.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 8802-11:2005/DAMD 7](https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7)

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

NOTE FROM ITTF

This draft International Standard is submitted for JTC 1 national body vote under the Fast-Track Procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of ISO/IEC 8802-11 to JTC 1/SC 6.

“FAST-TRACK” PROCEDURE

1 Any P-member and any Category A liaison organization of ISO/IEC JTC 1 may propose that an existing standard from any source be submitted directly for vote as a DIS. The criteria for proposing an existing standard for the fast-track procedure are a matter for each proposer to decide.

2 The proposal shall be received by the ITTF which will take the following actions.

2.1 To settle the copyright and/or trade mark situation with the proposer, so that the proposed text can be freely copied and distributed within JTC 1 without restriction.

2.2 To assess in consultation with the JTC 1 secretariat which SC is competent for the subject covered by the proposed standard and to ascertain that there is no evident contradiction with other International Standards.

2.3 To distribute the text of the proposed standard as a DIS. In case of particularly bulky documents the ITTF may demand the necessary number of copies from the proposer.

3 The period for combined DIS voting shall be six months. In order to be accepted the DIS must be supported by 75 % of the votes cast (abstention is not counted as a vote) and by two-thirds of the P-members voting of JTC 1.

4 At the end of the voting period, the comments received, whether editorial only or technical, will be dealt with by a working group appointed by the secretariat of the relevant SC.

5 If, after the deliberations of this WG, the requirements of 3 above are met, the amended text shall be sent to the ITTF by the secretariat of the relevant SC for publication as an International Standard.

If it is impossible to agree to a text meeting the above requirements, the proposal has failed and the procedure is terminated.

In either case the WG shall prepare a full report which will be circulated by the ITTF.

6 If the proposed standard is accepted and published, its maintenance will be handled by JTC 1.

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 8802-11:2005/DAmD 7

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

Contents

2	Normative references.....	1
3	Definitions.....	2
4	Abbreviations and acronyms.....	3
5	General description.....	4
5.3	Logical service interfaces.....	4
5.3.1	SS.....	5
5.4	Overview of the services.....	5
5.4.3	Access and confidentiality control services.....	5
5.4.3.1	Authentication <u>Linkverification</u>	5
5.4.3.2	Deauthentication <u>Delinkverification</u>	7
5.4.3.3	Privacy.....	7
5.4.3.4	<u>Authentication</u>	8
5.7.5	Privacy.....	9
5.7.6	Authentication <u>Linkverification</u>	9
5.7.7	Deauthentication <u>Delinkverification</u>	11
5.8	Reference model.....	11
5.9	Establishing the security association.....	12
5.9.1	Infrastructure mode.....	12
5.9.2	IBSS mode <u>ISO/IEC 8802-11-2005/Damd-7</u>	12
6	MAC service definition.....	13
6.1	Overview of MAC services.....	13
6.1.2	Security services.....	13
7	Frame formats.....	14
7.1	MAC frame formats.....	14
7.1.3	Frame fields.....	14
7.1.3.1	Frame Control field.....	14
7.1.3.1.2	Type and Subtype fields.....	15
7.1.3.1.9	WEP <u>Protected Frame</u> field.....	15
7.2	Format of individual frame types.....	15
7.2.2	Data frames.....	15
7.2.3	Management frames.....	15
7.2.3.1	Beacon frame format.....	15
7.2.3.4	Association Request frame format.....	15
7.2.3.6	Reassociation Request frame format.....	16
7.2.3.9	Probe Response frame format.....	16
7.2.3.10	Authentication <u>Linkverification</u> frame format.....	16
7.2.3.11	Deauthentication <u>Delinkverification</u>	17

7.3	Management frame body components.....	17
7.3.1	Fixed fields.....	17
7.3.1.1	Authentication <u>Linkverification</u> Algorithm Number field.....	17
7.3.1.2	Authentication <u>Linkverification</u> Transaction Sequence Number field.....	18
7.3.1.4	Capability Information field.....	18
7.3.1.7	Reason Code field.....	19
7.3.1.9	Status Code field.....	19
7.3.2	Information element.....	20
7.3.2.25	WAPI information element.....	21
7.3.2.25.1	Authentication and Key Management Suite.....	22
7.3.2.25.2	Unicast and Multicast Cipher Suites.....	23
8	Security	23
8.1	WAI authentication and key management.....	23
8.1.1	The structure of the authentication system.....	24
8.1.1.1	Systems and Ports.....	24
8.1.1.2	Controlled and Uncontrolled access.....	25
8.1.2	WAPI security association management.....	27
8.1.2.1	WAPI security association definitions.....	27
8.1.2.2	Selection of WAPI security policy.....	30
8.1.3	Certificate.....	31
8.1.4	WAI protocol.....	37
8.1.4.1	Format of WAI protocol packet.....	37
8.1.4.2	Certificate Authentication procedure.....	42
8.1.4.3	Unicast key negotiation procedure.....	49
8.1.4.4	Multicast key / STAKKey announcement process.....	54
8.1.4.5	STAKKey establishment procedure.....	57
8.1.4.6	Pre-authentication.....	58
8.1.4.7	Cached BKSAs and WAPI key management.....	60
8.1.4.8	Rekeying.....	60
8.1.4.9	Timeout processing.....	60
8.1.4.10	Key derivation architecture.....	61
8.1.4.11	WAI protocol packet's fragmentation and defragmentation.....	63
8.1.4.12	Port control and data transmission.....	64
8.2	WPI privacy infrastructure.....	64
8.2.1	Operate mode.....	64
8.2.2	Key.....	65
8.2.3	Encapsulation and decapsulation.....	66
8.2.4	Rules for using data packet serial number PN.....	67
8.3	WAPI Authentication and key management state machine.....	68
8.3.1	WAPI ASUE Authentication and key management state machine.....	68
8.3.1.1	ASUE state machine states.....	70
8.3.1.2	ASUE state machine variables.....	71
8.3.1.3	ASUE state machine procedures.....	71

8.3.2	WAPI AE Authentication and key management state machine.....	71
8.3.2.1	AE state machine states.....	76
8.3.2.2	AE state machine variables.....	77
8.3.2.3	AE state machine procedures.....	78
10.	Layer management.....	78
10.3	MLME SAP interface.....	78
10.3.2	Scan.....	78
10.3.2.2	MLME-SCAN.confirm.....	78
10.3.4	Authenticate Linkverification.....	78
10.3.4.1	MLME-AUTHENTICATE LinkVerify .request.....	78
10.3.4.2	MLME-AUTHENTICATE LinkVerify.confirm.....	80
10.3.4.3	MLME-AUTHENTICATE LINKVERIFY .indication.....	81
10.3.5	Deauthenticate DELINKVERIFY.....	82
10.3.5.1	MLME-DEAUTHENTICATE DELINKVERIFY. request.....	82
10.3.5.2	MLME-DEAUTHENTICATE DELINKVERIFY.confirm.....	83
10.3.5.3	MLME-DEAUTHENTICATE DELINKVERIFY. indication.....	84
10.3.6	Associate.....	85
10.3.6.1	MLME-ASSOCIATE.request.....	85
10.3.6.3	MLME-ASSOCIATE.indication.....	86
10.3.7	Reassociate.....	86
10.3.7.1	MLME-REASSOCIATE.request.....	86
10.3.7.3	MLME-REASSOCIATE.indication.....	87
10.3.17	MLME-SETWPIKEYS.....	87
10.3.17.1	MLME-SETWPIKEYS.request.....	87
10.3.17.2	MLME-SETWPIKEYS.confirm.....	89
10.3.18	MLME-DELETEWPIKEYS.....	89
10.3.18.1	MLME-DELETEWPIKEYS.request.....	89
10.3.18.2	MLME-DELETEWPIKEYS.confirm.....	90
10.3.19	MLME-STAKEYESTABLISHED.....	91
10.3.19.1	MLME-STAKEYESTABLISHED.indication.....	91
10.3.20	SetProtection.....	91
10.3.20.1	MLME-SETPROTECTION.request.....	91
10.3.20.2	MLME-SETPROTECTION.confirm.....	93
10.3.21	MLME-PROTECTEDFRAMEDROPPED.....	93
10.3.21.1	MLME- PROTECTEDFRAMEDROPPED.indication.....	93
11	MLME	94
11.3	Association and reassociation.....	94
11.3.1	Linkverification—originating STA.....	94
11.3.2	Linkverification—destination STA.....	94
11.3.3	Delinkverification—originating STA.....	95
11.3.4	Delinkverification—destination STA.....	95
11.4	Association, reassociation, and disassociation.....	95

11.4.1	STA association procedures.....	95
11.4.2	AP association procedures.....	96
11.4.3	STA reassociation procedures.....	97
11.4.4	AP reassociation procedures.....	97
11.4.5	STA disassociation procedures.....	98
11.4.6	AP disassociation procedures.....	98
Annex A	(normative) Protocol Implementation Conformance Statements (PICS)	99
A.4	PICS proforma—ISO/IEC 8802.11,2005 Edition.....	99
A.4.4	MAC protocol.....	99
Annex C	(normative) Formal description of MAC operation.....	102
Annex D	(normative) ASN.1 encoding of the MAC and PHY MIB.....	163
Annex H	(informative) Reference implementations of the frame authentication algorithm and the key derivation algorithm and the test vectors.....	191
H.1	Frame authentication algorithm.....	191
H.1.1	Reference implementation.....	191
H.1.2	Test vectors.....	193
H.2	Key derivation algorithm.....	194
H.2.1	Reference implementation.....	194
H.2.2	Test vectors.....	195
Annex I	(Informative) The example of WAI parameters and WPI block cryptographic algorithm	199
I.1	Principle.....	199
I.2	Algorithm used in China.....	199
I.3	ECC parameters used in China.....	199

List of figures

Figure 11—Portion of the ISO/IEC basic reference model covered in this amendment.....	11
Figure 11a—The establishment of security association under the basic mode.....	12
Figure 13—Frame Control field.....	14
Figure 24— Authentication <u>Linkverification</u> Algorithm Number fixed field.....	18
Figure 25— Authentication <u>Linkverification</u> Transaction Sequence Number fixed field.....	18
Figure 42a—WAPI Information Element format.....	21
Figure 42b—Pre-authentication.....	22
Figure 42c—Suite selector format.....	22
Figure 42d—Suite selector format.....	23
Figure 43a—Uncontrolled and controlled ports.....	25
Figure 43b—Authentication state on controlled port.....	26
Figure 43c—Usage of the controlled and uncontrolled port.....	27
Figure 43d—ASUE, AE and ASE roles.....	27
Figure 43e—Format of certificate.....	32
Figure 43f—Definition of certificate content.....	33
Figure 43g—Extension Attribute format.....	35
Figure 43h—Issue format of the certificate.....	35
Figure 43i—Digest field.....	36
Figure 43j—Attribute field.....	36
Figure 43k—Format of WAPI protocol packet in WAI authentication system.....	37
Figure 43l—FLAG.....	38
Figure 43m—Certificate.....	39
Figure 43n—Identity.....	39
Figure 43o—ADDID.....	40
Figure 43p—Attribute format.....	40
Figure 43q—Signature attribute.....	40
Figure 43r—Certificate Verification Result.....	41
Figure 43s—Identity List.....	42
Figure 43t—Certificate Authentication procedure.....	42
Figure 43u—The format of the Data field of Authentication Activation packet.....	42
Figure 43v—The format of the Data field of access authentication request packet.....	44
Figure 43w—The format of the Data field of Certificate Authentication Request packet.....	45
Figure 43x—The format of the Data field of Certificate Authentication Response packet.....	46
Figure 43y—The format of the Data field of Access Authentication Response packet.....	48
Figure 43z—Unicast key negotiation procedure.....	50
Figure 43aa—The format of the Data field of Unicast Key Negotiation Request packet.....	50
Figure 43ab—The format of the Data field of Unicast Key Negotiation Responding packet	51
Figure 43ac—The format of the Data field Unicast Key Negotiation Confirmation packet.....	53
Figure 43ad—Multicast key / inter-station key announcing procedure.....	54
Figure 43ae—The format of the Data field of Multicast key / STAKey announcement packet.....	54

Figure 43af—The format of the Data field of the multicast key/STakey response packet.....	56
Figure 43ag—The flow chart of the STakey establishment.....	57
Figure 43ah—The format of the Data field in the STakey establishment request packet.....	58
Figure 43ai—The format of the Data field in the pre-authentication start packet.....	59
Figure 43aj—BK key derivation architecture.....	61
Figure 43ak—Unicast key derivation architecture.....	62
Figure 43al—Multicast / STakey derivation architecture.....	62
Figure 43am—Preshared key derivation architecture.....	63
Figure 43an—Operate modes.....	65
Figure 43ao—WPI's MPDU encapsulation structure.....	66
Figure 43ap—Integrity check data.....	67
Figure 43aq—ASUE state machine, Part 1.....	69
Figure 43ar—ASUE state machine, Part 2.....	70
Figure 43as—AE state machine, Part 1.....	73
Figure 43at—AE state machine, Part 2.....	74
Figure 43au—AE state machine, Part 3.....	74
Figure 43av—AE state machine, Part 4.....	75
Figure 43aw—AE state machine, Part 5.....	75

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 8802-11:2005/DAmD 7](https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7)

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

List of tables

Table 1—Valid type and subtype combinations.....	15
Table 5—Beacon frame body.....	15
Table 7—Association Request frame body.....	16
Table 9—Reassociation Request frame body.....	16
Table 12—Proble Response frame body.....	16
Table 13— Authentication <u>Linkverification</u> frame body.....	17
Table 15— Deauthentication <u>Delinkverification</u> frame body.....	17
Table 18—Reason codes.....	19
Table 19—Status codes.....	20
Table 20—Element IDs.....	21
Table 20f—Authentication and Key Management Suites.....	22

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEC 8802-11:2005/DAmD 7

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 8802-11:2005/DAmD 7

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

“The editing instructions are shown in ***bold italic***. Four editing instructions are used: ***change***, ***delete***, ***insert***, and ***replace***. ***Change*** is used to make small corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed either by using ~~strike through~~ (to remove old material) or underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instructions. Replace is used to make large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions.”

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 8802-11:2005/DAmD 7](https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7)

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 8802-11:2005/DAmD 7

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>

2. Normative references

Insert the following references at the appropriate locations in Clause 2:

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

FIPS 180-2, Secure Hash Standard (SHS), August 2002.

IETF RFC2104, HMAC: Keyed-Hashing for Message Authentication

ITU-T Recommendation X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

ISO/IEC 15946 Information technology - Security techniques - Cryptographic techniques based on elliptic curves

ISO/IEC 10116: 1997 (2nd edition) Information technology - Security techniques - Modes of operation for an n-bit block cipher algorithm.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 8802-11:2005/DAmD 7](https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7)

<https://standards.iteh.ai/catalog/standards/sist/b2ae3e23-7481-4971-92ad-200922fe6df0/iso-iec-8802-11-2005-damd-7>