



InterNational Committee for Information Technology Standards (INCITS)

Secretariat: Information Technology Industry Council (ITI)

700 K Street NW, Suite 610, Washington, DC 20001

www.INCITS.org



eb-2022-00843

Document Date: 11/1/22

To: INCITS Members

Reply To: [Rachel Porter](#)

Subject: Public Review and Comments Register for the Approval of:

INCITS 496-2012/AM 2-202x: Information Technology - Fibre Channel - Security Protocols - 2/Amendment 2 (FC-SP-2/AM 2)

Due Date: The public review is from November 18, 2022 to January 17, 2023.

Action: The InterNational Committee for Information Technology Standards ([INCITS](#)) announces that the subject-referenced document(s) is being circulated for a 60-day public review and comment period. Comments received during this period will be considered and answered. Commenters who have objections/suggestions to this document should so indicate and include their reasons.

All comments should be forwarded not later than the date noted above to the following address:

INCITS Secretariat/ITI
700 K Street NW - Suite 600
Washington DC 20001
Email: comments@standards.incits.org (preferred)

This public review also serves as a call for patents and any other pertinent issues (copyrights, trademarks). Correspondence regarding intellectual property rights may be emailed to the INCITS Secretariat at patents@itic.org.

FIBRE CHANNEL

SECURITY PROTOCOLS - 2

Amendment 2

(FC-SP-2/AM2)

REV 1.01

INCITS working draft proposed
American National Standard
for Information Technology

October 5, 2022

Secretariat: Information Technology Industry Council

NOTE:

This is a working draft American National Standard of Accredited Standards Committee INCITS. As such this is not a completed standard. The T11 Technical Committee or anyone else may modify this document as a result of comments received anytime, or during a future public review and its eventual approval as a Standard. Use of the information contained herein is at your own risk.

Permission is granted to members of INCITS, its technical committees, and their associated task groups to reproduce this document for the purposes of INCITS standardization activities without further permission, provided this notice is included. All other rights are reserved. Any duplication of this document for commercial or for-profit use is strictly prohibited.

POINTS OF CONTACT:

Steven L. Wilson (T11 Chair)
Broadcom, Inc.
1320 Ridder Park Drive
San Jose, CA 95131
Voice: 408-333-8000
E-mail: steve.wilson@broadcom.com

Craig W. Carlson (T11.3 Chair)
Marvell
12900 Whitewater Drive
Minnetonka, MN 55343
Voice: (952) 852-0511
E-mail: cwcarlson@marvell.com

Roger Hathorn
(FC-SP-2/AM2 Facilitator)
International Business Machines
9000 S. Rita Rd.
Tucson, AZ 85744
Voice: (520) 799-5950
E-mail: rhathorn@us.ibm.com

David Peterson
(FC-SP-2/AM2 Technical Editor)
Broadcom, Inc.
1320 Ridder Park Drive
San Jose, CA 95131
Voice: (408) 333-8000
E-mail: david.peterson@broadcom.com

Release Notes for version 1.01

- Letter Ballot comment resolution

Release Notes for version 1.00

- Letter Ballot version

BSR INCITS 496-2012/AM2-202x

American National Standard
for Information Technology

Fibre Channel —
Security Protocols - 2 / Amendment 2
(FC-SP-2/AM2)

Secretariat

Information Technology Industry Council

Approved (not yet approved)

American National Standards Institute, Inc.

Abstract

This amendment updates INCITS 496-2012 (FC-SP-2 and Amendment 1), to update normative references, deprecate TLS 1.0 and TLS 1.1, and add additional encryption algorithms.

American National Standard

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards. The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

CAUTION: The developers of this standard have requested that holders of patents that may be required for the implementation of the standard, disclose such patents to the publisher. However, neither the developers nor the publisher have undertaken a patent search in order to identify which, if any, patents may apply to this standard. As of the date of publication of this standard, following calls for the identification of patents that may be required for the implementation of the standard, notice of one or more claims has been received. By publication of this standard, no position is taken with respect to the validity of this claim or of any rights in connection therewith. The known patent holder(s) has (have), however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher. No further patent search is conducted by the developer or the publisher in respect to any standard it processes. No representation is made or implied that licenses are not required to avoid infringement in the use of this standard.

Published by

**American National Standards Institute
25 West 43rd Street, 4th floor New York, NY 10036**

Copyright © 202x by Information Technology Industry Council (ITI)
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of ITI, 700 K Street NW Suite 600 Washington, DC 20001.

Printed in the United States of America

Contents	Page
1 Scope	1
2 Updates	2
2.1 Subclause 2.3	2
2.2 Subclause 2.4	2
2.3 Subclause 6.3.2.3	3
2.4 Subclause B.3.2.1	4

Table	Page
Table 75 – Encryption Algorithms Transform_IDs (Transform Type 1)	3

Foreword (This foreword is not part of American National Standard
INCITS 496-2012/AM2-2022.)

This amendment updates INCITS 496-2012 (FC-SP-2 and Amendment 1), to update normative references, deprecate TLS 1.0 and TLS 1.1, and add additional encryption algorithms.

This amendment was developed by the INCITS Fibre Channel Technical Committee during 2022. The amendment approval process started in 2022.

Requests for interpretation, suggestions for improvements or addenda, or defect reports are welcome. They should be sent to the INCITS Secretariat, Information Technology Industry Council, 700 K Street NW | Suite 600 | Washington, DC 20001.

This amendment was processed and approved for submittal to ANSI by the International Committee for Information Technology Standards (INCITS). Committee approval of the standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, INCITS had the following members:

Introduction

This standard is one of the Fibre Channel family of standards. This standard describes the protocols used to implement security in a Fibre Channel Fabric. This standard includes the definition of protocols to authenticate Fibre Channel entities, protocols to set up session keys, protocols to negotiate the parameters required to ensure frame-by-frame integrity and confidentiality, and protocols to establish and distribute policies across a Fibre Channel Fabric.

American National Standard
for Information Technology —

Fibre Channel — Security Protocols - 2 / Amendment 2 (FC-SP-2/AM2)

1 Scope

This amendment updates INCITS 496-2012, FC-SP-2 and Amendment 1, to:

- a) update normative references;
- b) deprecate TLS 1.0 and TLS 1.1; and
- c) add additional encryption algorithms.

2 Updates

2.1 Subclause 2.3

Add:

INCITS 562-202x, Fibre Channel - Framing and Signaling - 6 (FC-FS-6)

2.2 Subclause 2.4

Update the subclause with the following changes:

~~RFC 2246, The TLS Protocol Version 1.0, January 1999~~

~~RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, April 2006~~

RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016

RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018

RFC 8996, Deprecating TLS 1.0 and TLS 1.1, March 2021

The following documents are available from
<http://grouper.ieee.org/groups/1363/passwdPK/contributions.html#Wu:srp.stanford.edu/doc.html>

The following documents are available from <http://www.rsasecurity.com/>:

~~PKCS #1: RSA Cryptography Specifications Version 2, September 1998,
<http://www.rsasecurity.com/rsalabs/>~~

2.3 Subclause 6.3.2.3

Replace table 75 with the following:

Table 75 – Encryption Algorithms Transform_IDs (Transform Type 1)

Transform_ID ^a	Encryption Algorithm	Reference
3	ENCR_3DES	RFC 2451
11	ENCR_NULL	RFC 2410
12	ENCR_AES_CBC	RFC 3602
13	ENCR_AES_CTR	RFC 3686
20 ^b	ENCR_AES_GCM ^c (with a 16 bytes ICV)	RFC 4106 ^d
21 ^e	ENCR_NULL_AUTH_AES_GMAC ^c	RFC 4543 ^d
1 024 .. 2 047	FC specific	
1046	ENCR_AES_GCM ^c with end-to-end encryption protection	RFC 4106 ^d FC-FS-6
1047	ENCR_AES_AUTH_AES_GMAC ^c with end-to-end encryption protection	RFC 4543 ^d FC-FS-6
2 048 .. 65 535	Vendor Specific	
all others	Reserved to IANA	

^a These values are a subset of those specified by IANA in the "IKEv2 Parameters" registry (see <http://www.iana.org/assignments/ikev2-parameters>).

^b ENCR_AES_GCM with a 8 or 12 bytes ICV shall not be used.

^c ENCR_AES_GCM and ENCR_NULL_AUTH_AES_GMAC may be used with a 128 bit key, a 192 bit key or a 256 bit key. If ENCR_AES_GCM or ENCR_NULL_AUTH_AES_GMAC is implemented, support for the 128 bit key is mandatory, support for the 192 bit and 256 bit key is optional. The key size is specified by using the Key Length Transform Attribute (see 6.3.2.5).

^d This standard requires a variation in the content of the Additional Authentication Data (AAD) field from that specified in the RFC. The AAD field specified by the RFC shall be prefixed by the modified Fibre Channel Frame_Header (see FC-FS-3) to construct the AAD field required by this standard.

^e ENCR_NULL_AUTH_AES_GMAC is used only for authentication, but is documented as an encryption algorithm so that it can use an initialization value.

2.4 Subclause B.3.2.1

Replace

KMIP servers conformant to this Authentication Suite shall support TLSv1.0 (see RFC 2246) to establish and maintain channel confidentiality and integrity, and may support TLS v1.1 (see RFC 4346) and TLSv1.2 (see RFC 5246)

with

As specified in RFC 8996, the use of TLSv1.0 and TLSv1.1 is deprecated.

KMIP servers conformant to this Authentication Suite shall support TLSv1.2 (see RFC 5246) to establish and maintain channel confidentiality and integrity, and may support TLS v1.3 (see RFC 8446).