Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14075
Date:	2009-09-16
Replaces:	
Document Type:	Other Document (Defined)
Document Title:	Justification for Draft Amendment 1 to ISO/IEC 16512-2 (ITU-T X.603.1)
Document Source:	ITU-T SG 11/Q.15
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	10

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 11

TD 307 (GEN/11)

English only

Original: English

Question(s): 15/11 Mar del Plata, Argentina, 2-10 September 2009

TEMPORARY DOCUMENT

Source: Editor

Title: A.5 Justification for Draft Amendment 1 to ITU-T X.603.1|ISO/IEC 16512-2

A.5 Justification below,

Contact: Miyeon Yoon
KISA
Korea(Republic of.)

Tel: +82-2-405-5311
Fax: +82-2-405-5219
Email: myyoon@kisa.or.kr

1 Introduction

X.603.1/Draft Amd.1 “Information technology – Relayed Multicast Protocol: Specification for simplex group applications: Secure RMCP-2 Protocol” is developed in ITU-T Q.15/11 to provide security functions on X.603.1. X.603.1/Draft Amd.1 is planned for consent at SG11 meeting, September 2009. According to ITU-T Recommendation A.5 “Generic procedures for including references to documents of other organizations in ITU-T Recommendations”, this document provides A.5 justifications of referred IETF RFCs in Draft Amendment 1 to ITU-T X.603.1|ISO/IEC 16512-2.

2 Referred documents

Draft Recommendation X.603.1/Draft Amd.1 refers to:

- [IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*
- [IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*
- [IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*
- [IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*

Information of Referred IETF documents

(1) Clear descriptions of the RFCs (standards document or not, title, number, version, date, etc.).

- IETF RFC 3546, *Transport Layer Security (TLS) Extensions*, June 2003.
- IETF RFC 3830, *MIKEY: Multimedia Internet KEYing*, August 2004.
- IETF RFC 4279, *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, December 2005.
- IETF RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*, April 2006.
- IETF RFC 4535, *GSAKMP: Group Secure Association Key Management Protocol*, June 2006.

(2) Status of approval

The referred RFCs were approved by IESG (Internet Engineering Steering Group).

(3) Justification for the specific reference to the RFC

- Draft Rec. X.603.1/Draft Amd.1 refers to overall specification of IETF RFC 3546 (June 2003) for admission control for RMCP-2 session, optionally.
- Draft Rec. X.603.1/Draft Amd.1 refers to selected key management functions for derivation of encryption key part of IETF RFC 3830 (August 2004) selectively.
- Draft Rec. X.603.1/Draft Amd.1 refers to overall specification of IETF RFC 4279 (December 2005) for admission control for RMCP-2 session, optionally.
- Draft Rec. X.603.1/Draft Amd.1 refers to overall specification of IETF RFC 4346 (December 2005) for admission control for RMCP-2 session, optionally.

- Draft Rec. X.603.1/Draft Amd.1 refers to key creation and rekey-method part for derivation of encryption key part of IETF RFC 4535 (June 2006) selectively.

(4) Current information, if any, about IPR issues

IETF IPR archives at ***http://www.ietf.org/ipr.html***

(5/6) The degree of maturity and "Quality" of the RFC

The status of all the referred RFCs is "Proposed Standard".

(7) Relationship of the RFC with other existing or emerging documents

References within the referenced RFCs are listed under item (8).

(8) When a document is referenced in an ITU-T Recommendation, all explicit references within the referenced document should also be listed

IETF RFC 3546 refers to the followings:

Normative References

[1] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC:Keyed-hashing for message authentication", RFC 2104,February 1997.

[2] Fielding, R., Gettys, J., Mogul, J., Frystyk, H.,Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[3] Faltstrom, P., Hoffman, P. and A. Costello,"Internationalizing Domain Names in Applications(IDNA)", RFC 3490, March 2003.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "Internet X.509 Public Key Infrastructure:Online Certificate Status Protocol - OCSP", RFC 2560,June 1999.

[6] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure - Operation Protocols: FTP and HTTP",RFC 2585, May 1999.

[7] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[8] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[9] Berners-Lee, T., Fielding, R. and L. Masinter,"Uniform Resource Identifiers (URI): Generic Syntax",RFC 2396, August 1998. [10] Myers, J., "SMTP Service Extension for Authentication", Work in Progress.

[10] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[11] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, "Information Systems - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks."

[12] ITU-T Recommendation X.509(2000) Corrigendum 1(2001) | ISO/IEC 9594-8:2001/Cor.1:2002, Technical Corrigendum 1 to ISO/IEC 9594:8:2001.

Informative References

[1] Medvinsky, A. and M. Hur, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)", RFC 2712,October 1999.

[2] J. Mikkelsen, R. Eberhard, and J. Kistler, "General ClientHello extension mechanism and virtual hosting," ietf-tls mailing list posting, August 14, 2000.

[3] Chown, P., "Advanced Encryption Standard (AES)Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

IETF RFC 3830 refers to the followings:

Normative References

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

[2] Aboba, B. and M. Beadles, "The Network Access Identifier",RFC 2486, January 1999.

[3] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[4] PKCS #1 v2.1 - RSA Cryptography Standard, RSA Laboratories,June 14, 2002, www.rsalabs.com

[5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[6] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434,October 1998.

[7] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.

[8] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K.Norrman, "The Secure Real Time Transport Protocol", RFC 3711, March 2004.

[9] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396,August 1998.

[10] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[11] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, September 2002.

Informative References

[1] Canetti, R. and H. Krawczyk, "Analysis of Key-Exchange Protocols and their use for Building Secure Channels",Eurocrypt 2001, LNCS 2054, pp. 453-474, 2001.

[2] Bellare, M., Desai, A., Jokipii, E., and P. Rogaway, "A Concrete Analysis of Symmetric Encryption: Analysis of the DES Modes of Operation", in Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997,pp. 394-403.

[3] Hastad, J. and M. Naslund: "Practical Construction and Analysis of Pseduo-randomness Primitives", Proceedings of Asiacrypt 2001, LNCS. vol 2248, pp. 442-459, 2001.

[4] Johnson, D.B., "Theoretical Security Concerns with TLS use of MD5", Contribution to ANSI X9F1 WG, 2001.

[5] "Security Requirements for Cryptographic Modules", Federal Information Processing Standard Publications (FIPS PUBS)140-2, December 2002.

[6] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm,"Group Key Management Architecture", Work in Progress.

[7] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[8] Harney, H., Colegrove, A., Harder, E., Meth, U., and R.Fleischer, "Group Secure Association Key Management Protocol", Work in Progress.

[9] Menezes, A., van Oorschot, P., and S. Vanstone, "Handbook of Applied Cryptography", CRC press, 1996.

[10] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[11] ISO/IEC 9798-3: 1997, Information technology – Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques.

[12] ISO/IEC 11770-3: 1997, Information technology – Security techniques - Key management - Part 3: Mechanisms using digital signature techniques.

[13] ISO/IEC 18014 Information technology - Security techniques - Time-stamping services, Part 1-3.

[14] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K.Norrman, "Key Management Extensions for SDP and RTSP", Work in Progress.

[15] Burrows, Abadi, and Needham, "A logic of authentication", ACM Transactions on Computer Systems 8 No.1 (Feb. 1990),18-36.

[16] Lenstra, A. K. and E. R. Verheul, "Suggesting Key Sizes for Cryptosystems", http://www.cryptosavvy.com/suggestions.htm

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

[18] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C.Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[19] Eastlake, 3rd, D., Crocker, S., and J. Schiller,"Randomness Requirements for Security", RFC 1750, December 1994.

[20] Schulzrinne, H., Rao, A., and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, April 1998.

[21] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[22] NIST, "Description of SHA-256, SHA-384, and SHA-512", http://csrc.nist.gov/encryption/shs/sha256-384-512.pdf

[23] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,A., Peterson, J., Sparks, R., Handley, M., and E. Schooler,"SIP: Session Initiation Protocol", RFC 3261, June 2002.

[24] Dierks, T. and C. Allen, "The TLS Protocol - Version 1.0", RFC 2246, January 1999.

IETF RFC 4279 refers to the followings:

Normative References

[AES] Chown, P., "Advanced Encryption Standard (AES)Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RANDOMNESS] Eastlake, D., 3rd, Schiller, J., and S. Crocker,"Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0",RFC 2246, January 1999.

[UTF8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RELATIONAL] Segmuller, W., "Sieve Extension: Relational Tests", RFC 3431, December 2002.

[SIEVE] Showalter, T., "Sieve: A Mail Filtering Language", RFC 3028, January 2001.

Informative References

[ACAP] Newman, C. and J. Myers, "ACAP – Application Configuration Access Protocol", RFC 2244, November 1997.

IETF RFC 4346 refers to the followings:

Normative References

[AES] National Institute of Standards and Technology,"Specification for the Advanced Encryption Standard (AES)" FIPS 197. November 26, 2001.

[3DES] W. Tuchman, "Hellman Presents No Shortcut Solutions To DES," IEEE Spectrum, v. 16, n. 7, July 1979, pp. 40-41.

[DES] ANSI X3.106, "American National Standard for Information Systems-Data Link Encryption," American National Standards Institute, 1983.

[DSS] NIST FIPS PUB 186-2, "Digital Signature Standard," National Institute of Standards and Technology, U.S.Department of Commerce, 2000.

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

[IDEA] X. Lai, "On the Design and Security of Block Ciphers," ETH Series in Information Processing, v. 1, Konstanz:Hartung-Gorre Verlag, 1992.

[MD5] Rivest, R., "The MD5 Message-Digest Algorithm ", RFC 1321, April 1992.

[PKCS1A] B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1:RSA Cryptography Specifications Version 1.5", RFC 2313,March 1998.

[PKCS1B] J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards(PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[PKIX] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280,April 2002.

[RC2] Rivest, R., "A Description of the RC2(r) Encryption Algorithm", RFC 2268, March 1998.

[SCH] B. Schneier. "Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2ed", Published by John Wiley & Sons, Inc. 1996.

[SHA] NIST FIPS PUB 180-2, "Secure Hash Standard," National Institute of Standards and Technology, U.S. Department of Commerce., August 2001.

[REQ] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434,October 1998.

[TLSAES] Chown, P., "Advanced Encryption Standard (AES)Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[TLSEXT] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J.,and T. Wright, "Transport Layer Security (TLS)Extensions", RFC 3546, June 2003.

[TLSKRB] Medvinsky, A. and M. Hur, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)", RFC 2712,October 1999.

Informative References

[AH-ESP] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

Eastlake 3rd, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.

[BLEI] Bleichenbacher D., "Chosen Ciphertext Attacks against Protocols Based on RSA Encryption Standard PKCS #1" in Advances in Cryptology -- CRYPTO'98, LNCS vol. 1462,pages: 1-12, 1998.

[CBCATT] Moeller, B., "Security of CBC Ciphersuites in SSL/TLS: Problems and Countermeasures", http://www.openssl.org/~bodo/tls-cbc.txt.

[CBCTIME] Canvel, B., "Password Interception in a SSL/TLS Channel", http://lasecwww.epfl.ch/memo_ssl.shtml, 2003.

[ENCAUTH] Krawczyk, H., "The Order of Encryption and Authentication for Protecting Communications (Or: How Secure is SSL?)", Crypto 2001.

[KPR03] Klima, V., Pokorny, O., Rosa, T., "Attacking RSA-based Sessions in SSL/TLS", http://eprint.iacr.org/2003/052/, March 2003.

[PKCS6] RSA Laboratories, "PKCS #6: RSA Extended Certificate Syntax Standard," version 1.5, November 1993.

[PKCS7] RSA Laboratories, "PKCS #7: RSA Cryptographic Message Syntax Standard," version 1.5, November 1993.

[RANDOM] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086,June 2005.

[RSA] R. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.

[SEQNUM] Bellovin, S., "Defending Against Sequence Number Attacks",RFC 1948, May 1996.

[SSL2] Hickman, Kipp, "The SSL Protocol", Netscape Communications Corp., Feb 9, 1995.

[SSL3] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.

[SUBGROUP] Zuccherato, R., "Methods for Avoiding the "Small-Subgroup" Attacks on the Diffie-Hellman Key Agreement Method for S/MIME", RFC 2785, March 2000.

[TCP] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", RFC 4103, June 2005.

[TIMING] Boneh, D., Brumley, D., "Remote timing attacks are practical", USENIX Security Symposium 2003.

[TLS1.0] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0",RFC 2246, January 1999.

[X501] ITU-T Recommendation X.501: Information Technology – Open Systems Interconnection - The Directory: Models, 1993.

[X509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - "The Directory - Authentication Framework". 1988.

[XDR] Srinivasan, R., "XDR: External Data Representation Standard", RFC 1832, August 1995.

IETF RFC 4535 refers to the followings:

Normative References

[DH77] Diffie, W., and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, June 1977.

[FIPS186-2] NIST, "Digital Signature Standard", FIPS PUB 186-2, National Institute of Standards and Technology, U.S.Department of Commerce, January 2000.

[FIPS196] "Entity Authentication Using Public Key Cryptography," Federal Information Processing Standards Publication 196, NIST, February 1997.

[IKEv2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2412] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[RFC2627] Wallner, D., Harder, E., and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, June 1999.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names",RFC 4514, June 2006.

[RFC4534] Colegrove, A. and H. Harney, "Group Security Policy Tokenv1", RFC 4534, June 2006.

Informative References

[BMS] Balenson, D., McGrew, D., and A. Sherman, "Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization", Work in Progress, February 1999.

[HCM] H. Harney, A. Colegrove, P. McDaniel, "Principles of Policy in Secure Groups", Proceedings of Network and Distributed Systems Security 2001 Internet Society, San Diego, CA, February 2001.

[HHMCD01] Hardjono, T., Harney, H., McDaniel, P., Colegrove, A.,and P. Dinsmore, "Group Security Policy Token:Definition and Payloads", Work in Progress, August 2003.

[RFC2093] Harney, H. and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification", RFC 2093, July 1997.

[RFC2094] Harney, H. and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094, July 1997.

[RFC2408] Maughan D., Schertler M., Schneider M., and Turner J.,"Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, Proposed Standard, November 1998

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC2522] Karn, P. and W. Simpson, "Photuris: Session-Key Management Protocol", RFC 2522, March 1999.

[RFC4523] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates", RFC 4523, June 2006.

[RFC2974] Handley, M., Perkins, C., and E. Whelan, "Session Announcement Protocol", RFC 2974, October 2000.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E.Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[RFC4086] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

(9) Qualification of referenced organization

IETF is a qualified organization for including references in ITU-T Recommendations under Recommendation A.5 Procedures.

(10) A Full Copy of Existing Document

The referred IETF RFCs are available on the following website:

- IETF RFC 3546 “Transport Layer Security (TLS) Extensions”: available at “http://www.rfc-editor.org/rfc/rfc3546.txt”
- IETF RFC 3830 “MIKEY: Multimedia Internet KEYing”: available at “http://www.rfc-editor.org/rfc/rfc3830.txt”
- IETF RFC 4279 “Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)”: available at “http://www.rfc-editor.org/rfc/rfc4279.txt”

- IETF RFC 4346 “The Transport Layer Security (TLS) Protocol Version 1.1”: available at “http://www.rfc-editor.org/rfc/rfc4346.txt”

_____