INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

COM 17 – LS 300 – E

English only

Original: English

Question(s):	5/17	Geneva, 15-19 September 2008

Ref. : TD 4133Rev1

Source:	ITU-T SG 17 (Geneva, 15-19 September 2008)
Title:	Response to the IETF on a LS regarding the Recommendation ITU-T X.1034, Guidelines on extensible authentication protocol based authentication and key management in a data communication network

LIAISON STATEMENT

To:	IETF EMU Working Group
Approval:	Agreed to at SG 17 meeting
For:	Information
Deadline:	N/A

Contact:	Herbert Bertine Chairman, SG 17	Tel.: + 1 732 946 8781 Email: hbertine@optonline.net
	Zachary Zeltsan Rapporteur, Q.5/17	Tel: +1 908 582 2359 Email: zeltsan@alcatel-lucent.com

Study Group 17 thanks the IETF EMU WG for the detailed and valuable comments. SG 17 has agreed with the comments and suggestions provided in your liaison statement and decided to address them in an Amendment to the ITU-T Recommendation X.1034, which will be developed in 2009.

SG 17 is looking forward to cooperation with the IETF EMU WG on the EAP-related matters.

The detailed dispositions of the comments are provided in an attachment to this liaison statement. In the attachment the original comments are followed by the dispositions, which start with the words "**SG 17 response:**"

Attachment

Dispositions of the comments provided in the liaison statement from the IETF on the ITU-T Recommendation X.1034, *Guideline on extensible authentication protocol based authentication and key management in a data communication network*

Title: Response to Liaison Statement on ITU-T Recommendation X.1034 Submission Date: 2008-09-11 URL of the IETF Web page: https://datatracker.ietf.org/public/liaison_detail.cgi?detail_id=470

From: Joseph Salowey(IETF EMU WG) <jsalowey@cisco.com>

To: ITU-T SG 17(tsbsg17@itu.int ,zeltsan@alcatel-lucent.com)

Cc: emu-chairs@tools.ietf.org

emu@ietf.org

emu-ads@ietf.org

sob@harvard.edu

Reponse Contact: emu@ietf.org

emu-chairs@tools.ietf.org

emu-ads@tools.ietf.org

Technical Contact: emu-chairs@tools.ietf.org

Purpose: In response

Body: The EAP Method update (EMU) working group in the IETF has reviewed the document "ITU-T Recommendation X.1034" that is the subject of a liaison statement submitted on 2008-08-06. Does the ITU-T have further plans in this area, such as more EAP method analysis or definition? If so, perhaps more coordination between the IETF and the ITU-T in this area is needed.

SG 17 response: SG 17 plans to publish an amendment to X.1034, which will provide additional analysis of the EAP methods. If necessary, the amendment will also provide new definitions.

The members of EMU WG provided the following comments, which we hope are useful in finalizing the contents of X.1034.

A. Comments on section 3.2

1. It is not clear if the definition of PFS aligns with the definition in other documents such as from the "Handbook of applied cryptography" (http://www.cacr.math.uwaterloo.ca/hac/about/chap12.pdf).

SG 17 response: The comment is accepted. SG 17 plans to provide the requested clarifications using the source provided by the IETF.

2. The server compromised-based attack appears not to be an attack, but rather a way to mitigate the server compromised attack. These definitions are not clear.

SG 17 response: The comment is accepted and will be addressed in the amendment.

B. Comments on section 6.1

1. In figure 1 - Replace TDP with TCP, SCP with SCTP and "UDP or IP" with "UDP over IP"

2. Throughout the document replace DIAMETER with Diameter.

3. The following sentence is misleading: "the authenticator exchanges random numbers with the supplicant to obtain a fresh cryptographic key; thus resulting in perfect forward secrecy." Fresh keys are not sufficient to fulfill the criteria for PFS.

SG 17 response: The comments B.1, B.2 and B.3 are accepted and will be addressed in the amendment.

C. Comments on section 7.2 and 7.5

1. The "Prevention of domino effect or Denning Sacco attack" is a property of the system and not specific to the EAP method.

SG 17 response: SG 17 agrees with this statement. The comment will be addressed.

2. Authorization is not communicated in EAP. It is communicated from the Authentication server to the authenticator based on the identity authenticated by EAP.

SG 17 response: This comment is accepted and will be addressed.

3. The requirement for "Protection against server compromised dictionary attack" is not clear. If encrypted storage is all that is necessary then why is this a property of a protocol and not just a specific implementation detail?

SG 17 response: SG 17 agrees with this statement. The comment will be addressed.

4. Section 7.5 states that the appendix can be used to select from many existing EAP methods, however section I only analyzes a small subset of EAP methods.

SG 17 response: SG 17 plans to cover more EAP methods in the planned amendment.

D. Comments on table I-1:

General: EAP-MD5 and EAP-SRP are not widely deployed. This section claims to analyze "well-known" EAP methods, however it only analyzes two of the many methods that are deployed. There are EAP methods that provide additional properties but they are not listed in the table. There are more detailed investigations available, such as http://www-public.tu-bs.de:8080/~y0013790/thesis-otto-eapmethods.pdf.

SG 17 response: SG 17 plans to cover more EAP methods in the planned amendment taking into consideration the source provided by the IETF. The material on the EAP-SRP method will be removed.

1. EAP-SRP

i. EAP-SRP is not defined in RFC 2945. There is no current documentation for an EAP-SRP (There was a draft that expired many years ago). It is not clear what this evaluation was done against.

SG 17 response: The material on EAP-SRP will be removed.

2. EAP-MD5

i. EAP-MD5 does not provide mutual authentication or resistance to dictionary attacks

ii. EAP-MD5 does not provide protection from dictionary attacks. EAP-MD5 can be used with passwords.

iii. In general EAP-MD5 is not very useful since it does not generate session keys. It would be more appropriate to include EAP-GPSK.

SG 17 response: The comments on EAP-MD 5 are accepted and will be addressed in the amendment.

4. EAP-TLS

i. EAP-TLS Can provide user identity privacy (RFC 5216, section 2.1.4)

ii. EAP-TLS provides fragmentation support

iii. EAP-TLS does not use passwords and hence it is more appropriate to say that password-based issues are not applicable.

iv. RFC 5216 provides unique naming for keys and sessions for EAP-TLS

SG 17 response: The comments regarding the EAP-TLS method are accepted and will be addressed in the amendment.

5. EAP-AKA

i. EAP-AKA provides support for user privacy

ii. EAP-AKA does not use passwords and hence it is more appropriate to say that this issue is not applicable.

iii. RFC 5247 provides unique naming for keys and sessions in EAP-AKA

SG 17 response: The comments regarding the EAP-AKA method are accepted and will be addressed in the amendment.

E. Comments on Bibliography

1. RFC-2716 is obsolete, EAP-TLS is defined in RFC 5216 2. draft-ietf-eapkeying-21.txt has been published as RFC 5247

SG 17 response: The references to these specifications will be updated.