Question(s):  2/17
Ref.: TD 0927
Geneva, 7-16 April 2010

Source:  ITU-T Study Group 17 (Geneva, 7-16 April 2010)
Title:  Liaison reply on Recommendation ITU-T X.1034 (revised), Guideline on extensible authentication protocol based authentication and key management in a data communication network

LIAISON STATEMENT

For action to:  
For comment to:  IETF EMU Working Group
For information to:  Agreed to at Study Group 17 meeting

Contact:  Patrick Mwesigwa
          Rapporteur, Q.2/17
          Tel:  +256 4133 9004
          Email:  pmwesigwa@ucc.co.ug

Contact:  Heung Youl Youm
          Editor of X.1034 (revised)
          Tel:  +82 41 530 1328
          Email:  hyyoum@sch.ac.kr

Study Group 17 thanks the IETF EMU WG for the detailed and valuable comments on draft revised Recommendation X.1034. Question 2/17 has agreed with the comments and suggestions in your liaison statement and will address them in the further draft of ITU-T X.1034 (revised).

The detailed dispositions of comments are provided in the attachment starting with the words “SG 17 response”.

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

Attachment: 1
Dispositions of IETF comments on Recommendation ITU-T X.1034 (revised), Guideline on extensible authentication protocol based authentication and key management in a data communication network

Attention: Some or all of the material attached to this liaison statement may be subject to ITU copyright. In such a case this will be indicated in the individual document. Such a copyright does not prevent the use of the material for its intended purpose, but it prevents the reproduction of all or part of it in a publication without the authorization of ITU.
Attachment

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

Title: Response to Draft revised Recommendation ITU-T X.1034 Submission Date: 2010-04-02
URL of the IETF Web page: https://datatracker.ietf.org/public/liaison_detail.cgi?detail_id=862

From: Joseph Salowey (IETF EMU WG) <jsalowey@cisco.com>
To: ITU-T SG 17 (tsbsg17@itu.int, pmwesigwa@ucc.co.ug, hyyoum@sch.ac.kr)
Cc: paf@cisco.com
emu-chairs@tools.ietf.org
emu-ads@tools.ietf.org
emu@ietf.org
Response 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: Members of the IETF EAP Method Update working group have reviewed the revised ITU-T X.1034 document. The following is a summary of their comments:

1. Reviewers were not clear on the purpose of the document

Reviewers did not really understand the purpose of the document. There are several documents that discuss EAP method requirements and classify EAP methods such as: RFC 4017, NIST SP 800-120.

Is the group aware of these documents? What is this document providing beyond what is provided in these documents?

**SG 17 response:** The objective is to provide a guideline covering both EAP methods and key management in one piece of Recommendation for ITU-T members. However, SG17 will review SP 800-120 and RFC4017 carefully, and plan to improve current revision.

2. Out-of-Date discussion of EAP

The main part of the document does not include any reference to much of the recent EAP work such as:

RFC 5247 - Extensible Authentication Protocol (EAP) Key Management Framework
RFC 5296 - EAP Extensions for EAP Re-authentication Protocol (ERP)
RFC 5295 - Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)
RFC 5247 - Extensible Authentication Protocol (EAP) Key Management Framework

**SG 17 response:** The comment is accepted, four RFCs will be included in Bibliography section and SG17 will review them to improve the revision.
Also, in numerous places the document uses terminology specific to IEEE802. For example, the document discusses "types of PTK", and "group key handshake". Non-IEEE 802 technologies typically don't use the term "PTK", and IEEE 802.1X-REV does not include a "group key handshake".

**SG 17 response:** SG 17 will consider appropriate terminologies for the revision. The selected terminologies will be used in revision.

Moreover the "general flow of key management" described in Section 8.4 is not general at all, since this does not describe the lower layer key management used in IKEv2 or IEEE 802.16.

**SG 17 response:** The comment is accepted and SG 17 will change "general flow of key management" of the section 8.4’s title to “typical key management flow”.

3. Out-of-Date discussion of EAP-Methods

The appendices discussing EAP methods have improved, however they still contain many discrepancies with the state of the art. Appendix I claims it presents an evaluation of the most well-known EAP methods. EAP-SRP is abandoned work so it is not clear how this would qualify as well-known. EAP-MD5 cannot be used in environments that require key generation so its evaluation is not all that useful. Some additional methods are discussed in appendix III, but there are not discussed in Appendix I. It is not clear why there are two different appendices or why the focus of appendix I is mostly on Obsolete or abandoned protocols. Appendix I does not appear to provide much value. Appendix III contains many inaccuracies.

**SG 17 response:** The comment is accepted and SG 17 has developed new Table, and will cover many newly standardized EAPs in table in Appendix I. Additionally, SG17 will change “most well-known EAP methods” to “some example EAP methods”. Regarding EAP-SRP and EAP-MD5, SG17 will keep two EAPs in the revision, considering these are still used in some applications. SG17 will review Appendix III for removing inaccuracies in the future revision.

- RFC 2284 was obsolete by RFC 3748.

**SG 17 response:** This comment is accepted and RFC 2284 will be replaced with RFC 3748.

- EAP-SRP is abandoned work

**SG 17 response:** The comment is noted.

- There is a standards track PSK EAP method EAP-GPSK (RFC 5433), it would be better to include this in the analysis

**SG 17 response:** The comment is accepted.

- An improved EAP-AKA mechanism has been published in RFC 5448

**SG 17 response:** This comment is accepted.
- EAP-FAST is also a tunnel method

**SG 17 response:** This comment is accepted and will be moved into tunnel method section.

- The PEAP internet draft has been abandoned, current documentation of the PEAP protocol is available from Microsoft.

**SG 17 response:** This comment is noted and SG17 will consider this comment.

4. Out of date references

- For EAP RFC 3748 should be referenced instead of RFC 2284.

**SG 17 response:** This comment is accepted and RFC 2284 will be replaced with RFC 3748.

- RFC 2716 is been made obsolete by RFC 5216 accepted

**SG 17 response:** This comment is accepted and RFC 2716 will be replaced with RFC 5216.

- The document should reference RFC 5247 - Extensible Authentication Protocol (EAP) Key Management Framework

**SG 17 response:** This comment is accepted.

- The EAP-SRP reference is to an expired document accepted

**SG 17 response:** This comment is noted and SG17 will consider this comment.

- The PEAP reference is to an expired document

**SG 17 response:** The comment was noted and SG17 will consider this comment.

- RADIUS references should include RFC 3579

**SG 17 response:** This comment is accepted.

Attachment(s): No document has been attached