Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://IEEE 802.org/16**>
Title	Distributed Authentication Model for the .16j Relay network
Date Submitted	2007-04-24

Source(s)	Sheng Sun; Guo-Qiang Wang; Hang Zhang; Peiying Zhu; Wen Tong; Mo-han Fong 3500 Carling Avenue Ottawa, Ontario K2H 8E9	Voice: 1-613-763-1315 [mailto:shengs@nortel.com] [mailto:pyzhu@nortel.com]
	Jui-Tang Wang, Jen-Shun Yang, Tzu-Ming Lin, Wern-Ho Sheen, Fang-Ching Ren, Chie Ming Chou, , Ching-Tarng Hsieh, I-Kang Fu Industrial Technology Research Institute (ITRI)/ National Chiao Tung University (NCTU), Taiwan 195,Sec. 4, Chung Hsing Rd. Chutung, Hsinchu, Taiwan 310, R.O.C.	[mailto:jsyang@itri.org.tw] [mailto:rtwang@csie.nctu.edu.tw]
	Masato Okuda Fujitsu Laboratories LTD. Kamikodanaka 4-1-1, Nakahara-ku Kawasaki, Japan. 211-8588	
	Yuan-Ying Hsu Telcordia Applied Research Center Taiwan Co., Taipei, Taiwan	
	D. J. Shyy MITRE, USA	
	Yuefeng Zhou, Mike Hart Fujitsu Laboratories of Europe Ltd. Hayes Park Central Hayes Middlesex., UB4 8FE, UK	[mailto:okuda@jp.fujitsu.com]

[mailto: yyhsu@tarc-tw.research.telcordia.com]

[mailto: djshyy@mitre.org]

[mailto:Yuefeng.zhou@uk.fujitsu.com]
[mailto:Mike.hart@uk.fujitsu.com]

Re:	A response to a Call for Technical Proposal, http://wirelessman.org/relay/docs/80216j-07_007r1.pdf
Abstract	Security elements and mechanisms for .16j MMR control plane
Purpose	To incorporate the proposed text into the P802.16j Baseline Document (IEEE 802.16j-06/026r2)
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material

	contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://IEEE 802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802. 16 web site <http://IEEE 802.org/16/ipr/patents/notices>.

Distributed authentication hierarchy in MMR relay network

Sheng Sun; Guo-qiang Wang; Hang Zhang;
Peiying Zhu; Wen Tong; Mo-han Fong
Nortel
Jui-Tang Wang, Jen-Shun Yang, Tzu-Ming Lin,
Wern-Ho Sheen, Fang-Ching Ren, Chie Ming Chou,
Ching-Tarng Hsieh, I-Kang Fu

ITRI

Masato Okuda
Fujitsu Laboratories LTD.

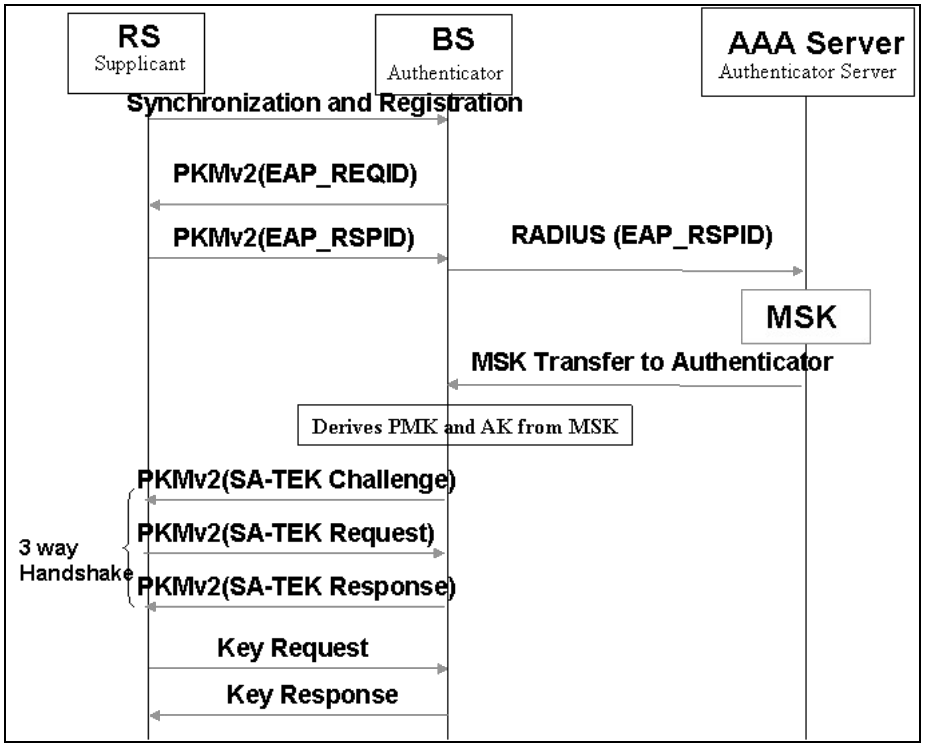
Yuan-Ying Hsu
Telcordia Applied Research Center Taiwan Co

D. J. Shyy
MITRE

Yuefeng Zhou, Mike Hart
Fujitsu Laboratories of Europe Ltd.

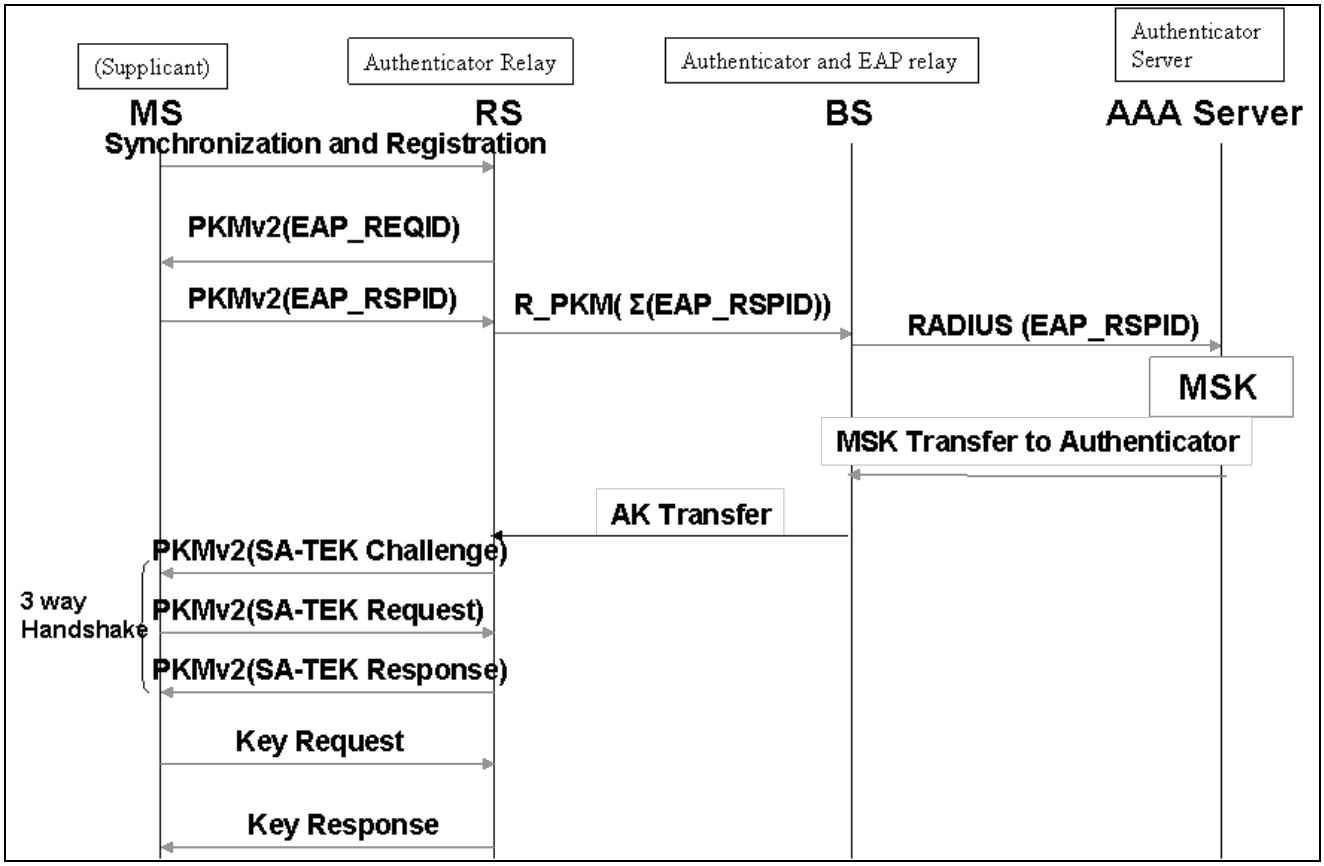
Introduction

In IEEE 802.16e PKMv2 specification, MS uses the PKM protocol to obtain authentication and traffic keying material from BS, and to support periodic re-authentication and key refresh.. Two authentication mechanisms are supported by PKM v2, namely RSA and Extensible Authentication Protocol (EAP). Either mechanism is applicable to the RS authentication within the MMR relay network as depicted in the following diagram.



During the registration process, RS could be registered as Authenticator Relay(AR) RS based on its capability and willingness to become the AR RS. (Please note: If the RS chooses to be transparent of the downstream MS/RS authentication messages, the process is discussed in contribution #201)

When a downstream RS or a MS imitates its authentication request to the AR RS, each RS/MS presents its credentials which will be an unique X.509 certificates issued by manufacturer or by external authority(if RSA PCKS#1 is chosen) or an operator specific credentials(in the case of EAP based authentication. The AR RS will intercept the downstream MS/RS's authentication request and envelop the PKM request to Aggregated PKM messages and send towards the authenticator BS. It's optional for the AR RS to aggregate the PKM Req/Rsp from multiple downstream RSs or MSs for more efficient transmission. The PKM messages transmitted between RS and the BS will be protected by the HMAC / CMAC tuple calculated from AR RS's HMAC_KEY_U or CMAC_KEY_U.



When the MSK for the downstream RS/MS is granted and sent to the authenticator BS, where the PMK and AK will be derived from MSK. Thereafter the AK will be sent over the relay link to RS, the AK will be encrypted by the secret between AR RS and BS

Aggregation of Authentication Relay Protocol

According to the specifications in NWG [], the end-to-end authentication structure is depicted as that the authentication protocols between Supplicant (i.e., MS) and Auth. Relay (AR, i.e., BS) is Extended Authentication Protocol/Privacy Key Management version 2 (EAP/PKMv2) protocol, between BS and ASN-GW is the EAP/Auth.Relay protocol, and between ASN-GW and Authentication Server (AS) is EAP/AAA protocol. By inheriting from legacy end-to-end authentication structure, access RS shall be acted like an AR. In other words, access RS shall perform the transformation between EAP/PKMv2 and EAP/Auth. Relay protocols, whereas the BS need not do the transformation again.

transmitting authentication message flow for each RS or MS will consume bandwidth resource and even block the MR network due to precious radio resource for relaying. Therefore, in this contribution, we propose to aggregate authentication messages for several MSs or RSs. As shown in Fig. 7, the access RS (RS_1) acts as an aggregator, whereas the ASN-GW acts like a deaggregator and vice versa. The access RS can collect some PKMv2 messages from several different MSs or RSs within a given period T and aggregate them for forwarding to ASN-GW. Here the period T shall be less than the re-authentication interval defined for each MS or RS. The aggregations are done as following ways.

EAP/PKMv2 (MS <-> AR)	Aggregation	Aggregated EAP/Auth. Relay (AR <-> ASN-GW)

PKMv2 EAP Start	--------->	Aggregated Authentication Relay EAP Start
PKMv2 EAP Transfer	--------->	Aggregated Authentication Relay EAP Transfer
PKMv2 Authenticated EAP Start	--------->	Aggregated Authentication Relay Authenticated EAP Start
PKMv2 Authenticated EAP Transfer	--------->	Aggregated Authentication Relay Authenticated EAP Transfer

Fig 7. Authentication Message flow with Aggregated EAP/Auth. Relay

2.2 The Aggregation Message Formats

According to the messages defined in EAP/Auth.Relay protocol, we extend the TLV from single TLV to multiple TLVs and add “# of TLVs” filed to indicate the number of TLVs follows. Below messages are the formats for aggregations.

Fig. 8 Aggregated Authentication Relay EAP Start

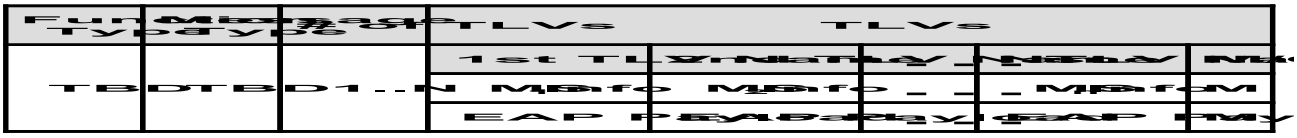


Fig. 9 Aggregated Authentication Relay EAP Transfer

Fig. 10 Aggregated Authentication Relay Authenticated EAP Start

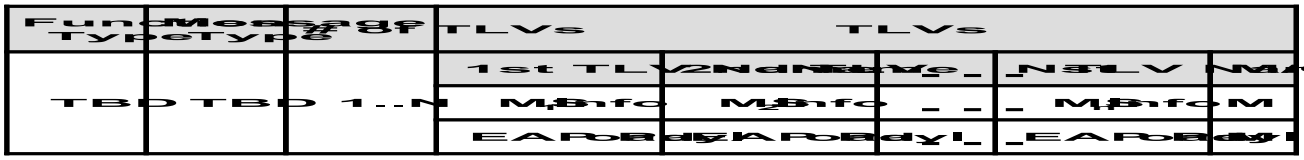


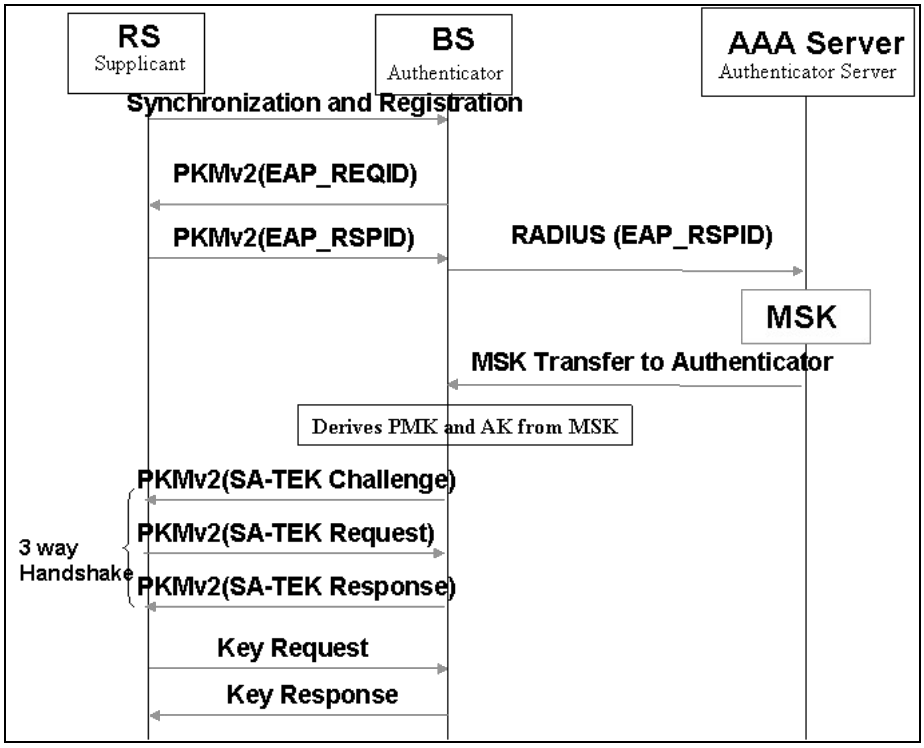
Fig. 11 Aggregated Authentication Relay Authenticated EAP Transfer

2. Proposed text changes

++++++++++++ start text proposal ++++++++++++++++++ +++++++++++++++

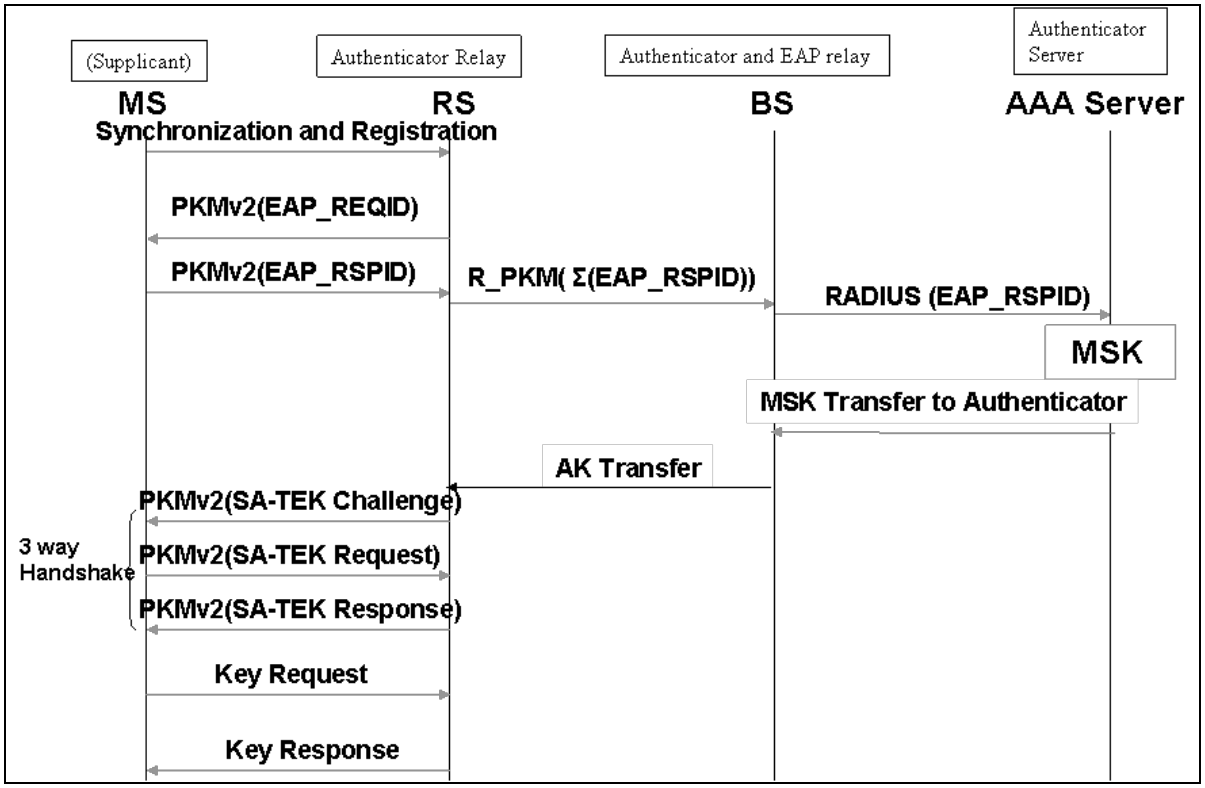
[Insert the followings after the end of section 7.1]

In IEEE 802.16e PKMv2 specification, MS uses the PKM protocol to obtain authentication and traffic keying material from BS, and to support periodic re-authentication and key refresh.. Two authentication mechanisms are supported by PKM v2, namely RSA and Extensible Authentication Protocol (EAP). Either mechanism is applicable to the RS authentication within the MMR relay network as depicted in the following diagram.



During the registration process, RS could be registered as Authenticator Relay(AR) RS based on its capability and willingness to become the AR RS.

When a downstream RS or a MS imitates its authentication request to the AR RS, each RS/MS presents its credentials which will be an unique X.509 certificates issued by manufacturer or by external authority(if RSA PCKS#1 is chosen) or an operator specific credentials(in the case of EAP based authentication. The AR RS will intercept the downstream MS/RS's authentication request and envelop the PKM request to Aggregated PKM messages and send towards the authenticator BS. It's optional for the AR RS to aggregate the PKM Req/Rsp from multiple downstream RSs or MSs for more efficient transmission. The PKM messages transmitted between RS and the BS will be protected by the HMAC / CMAC tuple calculated from AR RS's HMAC_KEY_U or CMAC_KEY_U.



When the MSK for the downstream RS/MS is granted and sent to the authenticator BS, where the PMK and AK will be derived from MSK. Thereafter the AK will be sent over the relay link to RS, the AK will be encrypted by the secret between AR RS and BS

Aggregation of Authentication Relay Protocol

According to the specifications in NWG [], the end-to-end authentication structure is depicted as that the authentication protocols between Supplicant (i.e., MS) and Auth. Relay (AR, i.e., BS) is Extended Authentication Protocol/Privacy Key Management version 2 (EAP/PKMv2) protocol, between BS and ASN-GW is the EAP/Auth.Relay protocol, and between ASN-GW and Authentication Server (AS) is EAP/AAA protocol. By inheriting from legacy end-to-end authentication structure, access RS shall be acted like an AR. In other words, access RS shall perform the transformation between EAP/PKMv2 and EAP/Auth. Relay protocols, whereas the BS need not do the transformation again.

transmitting authentication message flow for each RS or MS will consume bandwidth resource and even block the MR network due to precious radio resource for relaying. Therefore, in this contribution, we propose to aggregate authentication messages for several MSs or RSs. As shown in Fig. 7, the access RS (RS_1) acts as an aggregator, whereas the ASN-GW acts like a deaggregator and vice versa. The access RS can collect some PKMv2 messages from several different MSs or RSs within a given period T and aggregate them for forwarding to ASN-GW. Here the period T shall be less than the re-authentication interval defined for each MS or RS. The aggregations are done as following ways.

EAP/PKMv2 (MS <-> AR)	Aggregation	Aggregated EAP/Auth. Relay (AR <-> ASN-GW)
PKMv2 EAP Start	--------->	Aggregated Authentication Relay EAP Start

PKMv2 EAP Transfer	--------->	Aggregated Authentication Relay EAP Transfer
PKMv2 Authenticated EAP Start	--------->	Aggregated Authentication Relay Authenticated EAP Start
PKMv2 Authenticated EAP Transfer	--------->	Aggregated Authentication Relay Authenticated EAP Transfer

Fig 7. Authentication Message flow with Aggregated EAP/Auth. Relay

2.2 The Aggregation Message Formats

According to the messages defined in EAP/Auth.Relay protocol, we extend the TLV from single TLV to multiple TLVs and add “# of TLVs” filed to indicate the number of TLVs follows. Below messages are the formats for aggregations.

Fig. 8 Aggregated Authentication Relay EAP Start

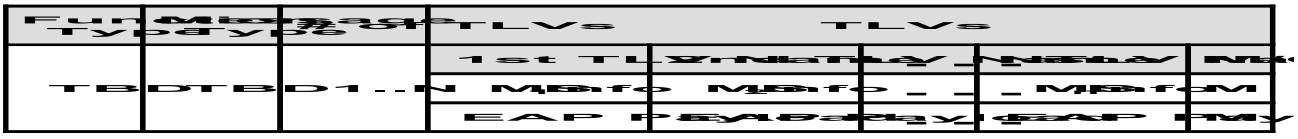


Fig. 9 Aggregated Authentication Relay EAP Transfer

Fig. 10 Aggregated Authentication Relay Authenticated EAP Start

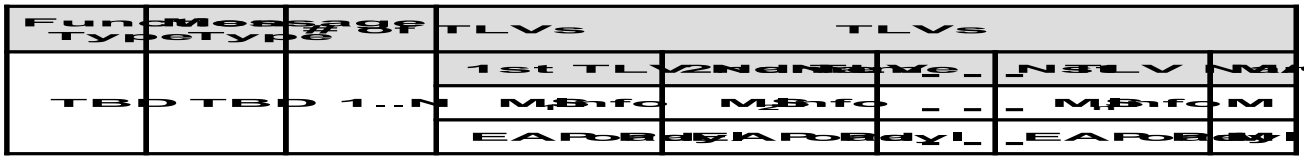


Fig. 11 Aggregated Authentication Relay Authenticated EAP Transfer

++++++++++++++++++++ *End of text proposal* ++++++++++++++++++++