A Container Type for the Extensible Authentication Protocol (EAP)

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This memo is filed as <draft-hiller-eap-tlv-00.txt>, and expires April 28, 2003.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

The Extensible Authentication Protocol (EAP), defined in RFC 2284, provides for support of multiple authentication methods. While EAP was originally created for use with PPP, it has since been adopted for use with IEEE 802.1X "Network Port Authentication".

Since its deployment, a number of weaknesses in EAP have become apparent. These include the lack of protection for, and acknowledgement of Success and Failure messages.
This memo describes an approach that may be taken to solve these problems and others by defining a new EAP type which includes as payload standard Type-Length-Value (TLV) objects.

1. Introduction

The Extensible Authentication Protocol (EAP), described in [RFC2284], provides a standard mechanism for support of multiple authentication methods. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others.

One of the goals of EAP is to enable development of new authentication methods without requiring deployment of new code on the Network Access Server (NAS). As a result, the NAS acts as a "passthrough", and need not understand specific EAP methods.

Figure 1 describes the relationship between the EAP peer, NAS and backend authentication server. As described in the figure, the EAP conversation "passes through" the NAS on its way between the client and the backend authentication server. While the authentication conversation is between the EAP peer and backend authentication server, the NAS and backend authentication server need to have established trust for the conversation to proceed.
Using EAP-TLV, it is possible for various types of data to be passed directly between the backend authentication server and the EAP peer, and to provide functionality not included in RFC 2284 without defining a multiplicity of new EAP Types.

[Editor’s Note: In fact, I’m not sure why we couldn’t just redefine the whole of EAP in terms of this type...]

This memo is offered to the EAP WG for discussion and possible adoption as a solution to issues #10, 26 and 40.
2. Requirements language

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [RFC2119].

3. The EAP Type-Length-Value (EAP-TLV) Type

Description

EAP-TLV is a "special case" Type, more akin to the Identity and Notification Types than the authentication Types such as MD5-Challenge [RFC2284]. EAP-TLV differs from the Identity and Notification Types, however, in that a Peer MAY respond to an EAP-TLV Request with a Nak Response. This is allowed for backward compatibility with implementations that do not support the EAP-TLV Type.

Type

33

Type-Data

The Data field is variable length, and contains Type-Length-Value objects (TLVs).

3.1. TLV Format

TLVs are defined as follows:

```
+-----------------+-----------------+-----------------+-----------------+
| M | R | Type | Length |
+-----------------+-----------------+-----------------+-----------------+
| Value...        |                 |                 |
+-----------------+-----------------+-----------------+-----------------+
```

M

0 - Non-mandatory TLV
1 - Mandatory TLV

R
Reserved, set to zero (0)

Type

A 14-bit field, denoting the attribute type. Allocated AVP Types include:
0 - Reserved
1 - Reserved
2 - Reserved
3 - Acknowledged Result

Length

The length of the Value field in octets.

Value

The value of the object.

### 3.2. Result TLV

The Result TLV provides support for acknowledged Success and Failure messages within EAP. It is defined as follows:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>M</td>
<td>R</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>Status</td>
<td>Status</td>
<td>Status</td>
<td></td>
</tr>
</tbody>
</table>

M

1 - Mandatory TLV

R

Reserved, set to zero (0)

AVP Type

3 - Success/Failure

Length

2
4. Discussion

It’s not hard to come up with other uses for the EAP-TLV Type. For example, it could be used in the negotiation of language and charset for Notification messages; a MAC TLV might be defined to cryptographically protect the message (and incidentally enable mutual authentication for types that might not otherwise support it); a Response might contain an IPv6 Binding Update and the corresponding protected Success message include the address of a dynamically assigned home agent, etc.

5. Normative references


Author’s Addresses

Tom Hiller
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60566
USA

Phone: +1 630 979 7673
Email: tom.hiller@lucent.com

Ashwin Palekar
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Phone: +1 425 882 8080
EMail: ashwinp@microsoft.com
Glen Zorn  
Cisco Systems  
500 108th Avenue N.E.  
Suite 500  
Bellevue, Washington 98004  
USA  

Phone: +1 425 344 8113  
Fax: +1 425 740 0168  
EMail: gwz@cisco.com

Intellectual Property Statement
The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement
Copyright (C) The Internet Society (2002). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet
Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

Expiration Date

This memo is filed as <draft-hiller-eap-tlv-00.txt>, and expires April 28, 2003.