

PPPEXT Working Group  
INTERNET-DRAFT  
Category: Standards Track  
<[draft-ietf-pppext-otp-00.txt](#)>  
[6](#) October 2001  
Updates: RFC [2284](#)

L. Blunk  
Merit Networks, Inc.  
J. Vollbrecht  
Interlink Networks, Inc.  
Bernard Aboba  
Microsoft

## The One Time Password (OTP) and Generic Token Card Authentication Protocols

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/lid-abstracts.txt>

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

### Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

### Abstract

EAP is an authentication protocol which supports multiple authentication mechanisms. EAP typically runs directly over the link layer without requiring IP and therefore includes its own support for in-order delivery and re-transmission. While EAP was originally developed for use with PPP, it is also now in use with IEEE 802. This document defines the One Time Password (OTP) and Generic Token Card EAP methods.

INTERNET-DRAFT

OTP and Generic Token Card

6 October 2001

## Table of Contents

<a href="#">1.</a>	Introduction .....	<a href="#">3</a>
<a href="#">1.1</a>	Specification of Requirements .....	<a href="#">3</a>
<a href="#">1.2</a>	Terminology .....	<a href="#">3</a>
<a href="#">2.</a>	Packet Format .....	<a href="#">4</a>
<a href="#">2.1</a>	EAP Request Packet .....	<a href="#">5</a>
<a href="#">2.2</a>	EAP Response Packet .....	<a href="#">6</a>
<a href="#">2.3</a>	One-Time Password .....	<a href="#">6</a>
<a href="#">2.4</a>	Generic Token Card .....	<a href="#">7</a>
<a href="#">3.</a>	References .....	<a href="#">8</a>
<a href="#">4.</a>	Security considerations .....	<a href="#">9</a>
<a href="#">4.1</a>	Packet modification attacks .....	<a href="#">10</a>
<a href="#">4.2</a>	Implementation dependence .....	<a href="#">10</a>
<a href="#">4.3</a>	Mutual authentication .....	<a href="#">10</a>
<a href="#">4.4</a>	Confidentiality .....	<a href="#">11</a>
ACKNOWLEDGMENTS .....		<a href="#">11</a>
AUTHORS' ADDRESSES .....		<a href="#">11</a>
Full Copyright Statement .....		<a href="#">12</a>

INTERNET-DRAFT

OTP and Generic Token Card

6 October 2001

## [1.](#) Introduction

EAP, defined in [\[22\]](#), is an authentication protocol which supports multiple authentication mechanisms. EAP typically runs directly over the link layer without requiring IP and therefore includes its own support for in-order delivery and re-transmission. While EAP was originally developed for use with PPP [\[1\]](#), it is also now in use with IEEE 802 [\[7\]](#). The encapsulation of EAP on IEEE 802 link layers is defined in [\[13\]](#). This document defines the One Time Password (OTP) and Generic Token Card EAP methods.

### [1.1.](#) Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [\[6\]](#).

### [1.2.](#) Terminology

This document frequently uses the following terms:

#### Authenticator

The end of the link requiring the authentication.

#### Peer

The other end of the point-to-point link (PPP), point-to-point LAN segment (IEEE 802.1X) or 802.11 wireless link, which being authenticated by the Authenticator. In IEEE 802.1X, this end is known as the Supplicant.

#### Authentication Server

An Authentication Server is an entity that provides an Authentication Service to an Authenticator. This service verifies from the credentials provided by the peer, the claim of identity made by the peer.

## Port Access Entity (PAE)

The protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the protocol functionality associated with the Authenticator, peer or both.

## Silently Discard

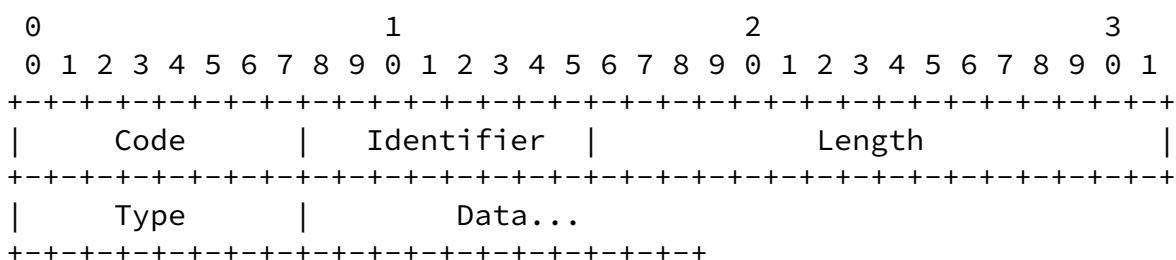
This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

## Displayable Message

This is interpreted to be a human readable string of characters, and MUST NOT affect operation of the protocol. The message encoding MUST follow the UTF-8 transformation format [5].

## 2. Packet Format

A summary of the EAP OTP and Generic Token Card Request/Response packet format is shown below. The fields are transmitted from left to right.



## Code

- 1 - Request
- 2 - Response

## Identifier

The identifier field is one octet and aids in matching responses with requests.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and Data fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and should be ignored on reception.

## Type

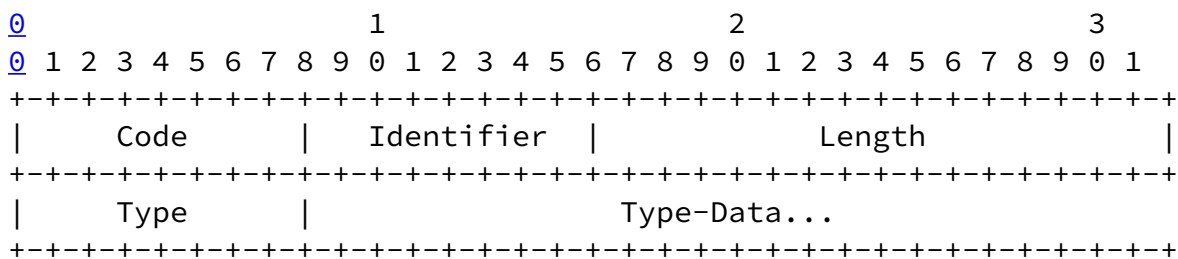
5 - OTP 6 - Generic Token Card

## Data

The format of the Data field is determined by the Code field.

### 2.1. EAP Request Packet

A summary of the EAP Request packet format is shown below. The fields are transmitted from left to right.



## Code

1

## Identifier

The Identifier field is one octet and aids in matching responses with requests. The Identifier field **MUST** be changed on each Request packet.

Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and TLS Response fields.

## Type

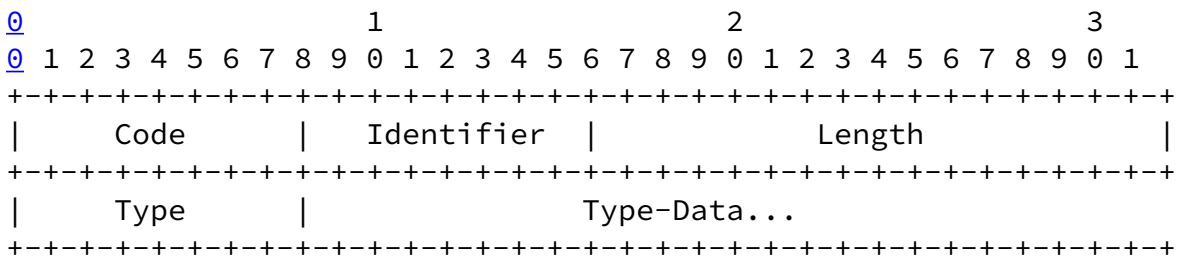
5 - OTP 6 - Generic Token Card

## Type-Data

The format of the Type-Data field is determined by the Code and Type fields.

## 2.2. EAP Response Packet

A summary of the EAP OTP And Generic Token Card Response packet format is shown below. The fields are transmitted from left to right.



## Code

## Identifier

The Identifier field is one octet and MUST match the Identifier field from the corresponding request.

## Length

The Length field is two octets and indicates the length of the EAP packet including the Code, Identifier, Length, Type, and TLS data fields.

## Type

5 - OTP 6 - Generic Token Card

## Type-Data

The format of the Type-Data field is determined by the Code and Type fields.

### [2.3.](#) One-Time Password (OTP)

#### Description

The One-Time Password system is defined in "A One-Time Password System" [\[4\]](#). The Request contains a displayable message containing an OTP challenge. A Response MUST be sent in reply to the Request. The Response MUST be of Type 5 (OTP) or Type 3 (Nak). The Nak reply indicates the peer's desired authentication mechanism Type.

## Type

5

## Type-Data

The Type-Data field contains the OTP "challenge" as a displayable message in the Request. In the Response, this field is used for the

6 words from the OTP dictionary [4]. The messages MUST not be null terminated. The length of the field is derived from the Length field of the Request/Reply packet.

#### [2.4.](#) Generic Token Card

##### Description

The Generic Token Card Type is defined for use with various Token Card implementations which require user input. The Request contains an ASCII text message and the Reply contains the Token Card information necessary for authentication. Typically, this would be information read by a user from the Token card device and entered as ASCII text.

##### Type

6

##### Type-Data

The Type-Data field in the Request contains a displayable message greater than zero octets in length. The length of the message is determined by Length field of the Request packet. The message MUST not be null terminated. A Response MUST be sent in reply to the Request with a Type field of 6 (Generic Token Card). The Response contains data from the Token Card required for authentication. The length of the data is determined by the Length field of the Response packet.

#### [3.](#) References



- [1] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, [RFC 1661](#), July 1994.
- [2] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, [RFC 1700](#), October 1994.
- [3] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", [RFC 1994](#), August 1996.
- [4] Haller, N. and C. Metz, "A One-Time Password System", [RFC 1938](#), May 1996.
- [5] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", [RFC 2044](#), October 1996.
- [6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- [7] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.
- [8] ISO/IEC 10038 Information technology - Telecommunications and information exchange between systems - Local area networks - Media Access Control (MAC) Bridges, (also ANSI/IEEE Std 802.1D- 1993), 1993.
- [9] ISO/IEC Final CD 15802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3:Media Access Control (MAC) bridges, (current draft available as IEEE P802.1D/D15).
- [10] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q/D8, January 1998.
- [11] ISO/IEC 8802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3- 1996), 1996.
- [12] IEEE Standards for Local and Metropolitan Area Networks: Demand Priority Access Method, Physical Layer and Repeater Specification For 100 Mb/s Operation, IEEE Std 802.12-1995.

- 
- [13] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.
- [14] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-1997, 1997.
- [15] Aboba, B., Simon, D., "PPP EAP TLS Authentication Protocol", [RFC 2716](#), October 1999.
- [16] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and Palter, B., "Layer Two Tunneling Protocol L2TP", [RFC 2661](#), August 1999.
- [17] Kent, S., Atkinson, R., "IP Authentication Header", [RFC 2402](#), November 1998.
- [18] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [19] Piper, D., "The Internet IP Security Domain of Interpretation of ISAKMP", [RFC 2407](#), November 1998.
- [20] Atkinson, R., Kent, S., "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.
- [21] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.
- [22] Blunk, L., Vollbrecht, J., Aboba, B., "Extensible Authentication Protocol (EAP)", Internet draft (work in progress), [draft-ietf-pppext-rfc2284bis-00.txt](#), October 2001.

#### [4.](#) Security Considerations

Security issues are the primary topic of this RFC. Known security issues with EAP include:

- Packet modification attacks
- Implementation dependence
- Mutual authentication
- Confidentiality

INTERNET-DRAFT

OTP and Generic Token Card

6 October 2001

#### [4.1.](#) Packet modification attacks

While individual EAP methods such as [\[15\]](#) may provide for authentication and integrity protection of material sent within the data portion of an EAP message, EAP does not provide built-in support for authentication or integrity protection. This means that an attacker may modify all or portions of EAP messages, including Request and Response messages of types Identity, Notification, Nak, OTP, and Generic Token Card and Success and Failure messages. The assumption is that physical access to the link is restricted, so that such attacks are unlikely.

Where EAP is run over IP, such as within protocols supporting PPP or Ethernet tunneling [\[16\]](#), this assumption is no longer valid. In this case, the EAP exchange MUST be authenticated and integrity protected, using a mechanism such as IPsec [\[17\]](#)-[\[21\]](#).

#### [4.2.](#) Implementation dependence

The interaction of authentication protocols with link layer technologies such as PPP and IEEE 802 are highly implementation dependent.

For example, upon failure of authentication, some PPP implementations do not terminate the link, instead limiting the kind of traffic in the Network-Layer Protocols to a filtered subset, which in turn allows the user opportunity to update secrets or send mail to the network administrator indicating a problem. Similarly, while in IEEE 802.1X an authentication failure will result denied access to the controlled port, limited traffic may be permitted on the uncontrolled port.

In EAP there is no provision for retries of failed authentication. However, in PPP the LCP state machine can renegotiate the authentication protocol at any time, thus allowing a new attempt. Similarly, in IEEE 802.1X the supplicant or Authenticator can re-authenticate at any time. It is recommended that any counters used for authentication failure not be reset until after successful authentication, or subsequent termination of the failed link.

#### [4.3.](#) Mutual authentication

In EAP there is no requirement that authentication be full duplex or that the same protocol be used in both directions. It is perfectly acceptable for different protocols to be used in each direction. This will, of course, depend on the specific protocols negotiated. If a one-way authentication method is negotiated, such as OTP or Generic Token Card then the Authenticator's identity will not be verified.

For wireless media such as 802.11 [[14](#)], where physical security can no longer be assumed, mutual authentication is recommended in order to

guard against rogue access points.

#### [4.4](#). Confidentiality

Neither the OTP nor the Generic Token card methods derive session keys for use with per-packet authentication, integrity protection or confidentiality. Typically, this means that subsequent data traffic will either utilize static session keys, or will be unprotected. If the latter, then the data traffic will be vulnerable to a wide variety of attacks, including traffic insertion and session hijacking.

#### Acknowledgments

Al Rubens (Merit) also provided valuable feedback on this document, as did Glen Zorn (Cisco) and Ashwin Palekar (Microsoft).

#### Authors' Addresses

Larry J. Blunk  
Merit Network, Inc.  
[4251](#) Plymouth Rd., Suite C  
Ann Arbor, MI 48105

E-Mail: [ljb@merit.edu](mailto:ljb@merit.edu)  
Phone: 734-763-6056  
FAX: 734-647-3185

John R. Vollbrecht  
Interlink Networks, Inc.  
[775](#) Technology Drive, Suite 200  
Ann Arbor, MI 48108  
USA

Phone: +1 734 821 1205  
Fax: +1 734 821 1235  
EMail: jrv@interlinknetworks.com

Bernard Aboba  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

EMail: bernarda@microsoft.com  
Phone: +1 425 936 6605  
Fax: +1 425 936 7329

#### Full Copyright Statement

Copyright (C) The Internet Society (2001). 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-ietf-pppext-otp-00.txt](#)>, and expires April 19, 2002.