

EAP Working Group  
INTERNET-DRAFT  
Category: Standards Track  
<[draft-ietf-eap-otp-00.txt](#)>  
[12](#) October 2002  
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 (2002). 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, both of which provide one-way authentication, but not key generation. As a result, the OTP and Generic Token Card methods, when used by themselves, are only appropriate for use on networks where physical security can be assumed. These methods SHOULD NOT be used on wireless networks, or over the Internet, unless the EAP conversation is protected. This can be accomplished using technologies such as IPsec or TLS.

INTERNET-DRAFT

OTP and Generic Token Card

12 October 2002

## 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>	Security considerations .....	<a href="#">8</a>
<a href="#">3.1</a>	Threat model .....	<a href="#">8</a>
<a href="#">3.2</a>	Security claims .....	<a href="#">9</a>
<a href="#">3.3</a>	Packet modification attacks .....	<a href="#">9</a>
<a href="#">3.4</a>	Mutual authentication .....	<a href="#">10</a>
<a href="#">3.5</a>	Confidentiality .....	<a href="#">10</a>
<a href="#">4.</a>	Normative references .....	<a href="#">11</a>
<a href="#">5.</a>	Informative references .....	<a href="#">11</a>
	ACKNOWLEDGMENTS .....	<a href="#">12</a>
	AUTHORS' ADDRESSES .....	<a href="#">12</a>
	Intellectual property statement .....	<a href="#">13</a>
	Full Copyright Statement .....	<a href="#">13</a>

INTERNET-DRAFT

OTP and Generic Token Card

12 October 2002

## 1. Introduction

EAP, defined in [[RFC2284](#)], 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 [[RFC1661](#)], it is also now in use with IEEE 802 [[IEEE802](#)]. The encapsulation of EAP on IEEE 802 link layers is defined in [[IEEE8021X](#)]. 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 [[RFC2119](#)].

### 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

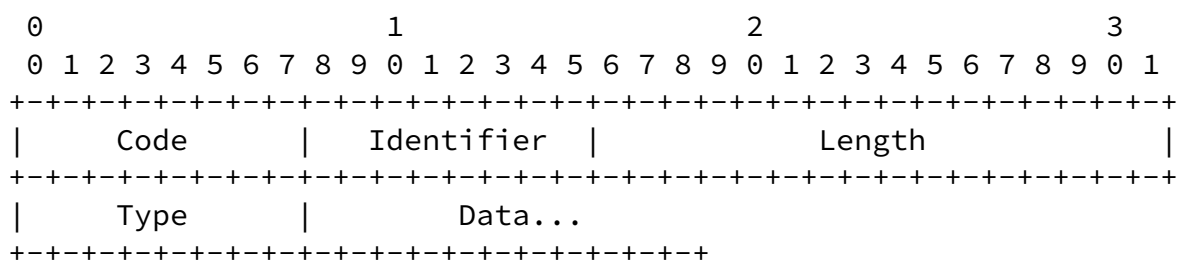
This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

## 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 [RFC2044].

## 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

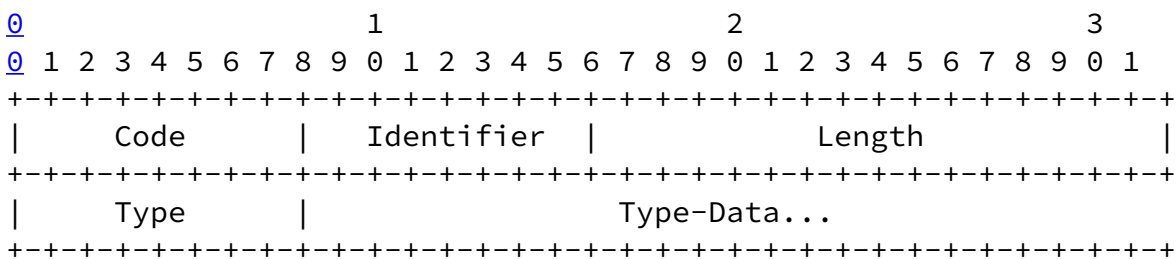
5 - OTP 6 - Generic Token Card

## 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 Type-Data fields.

## Type

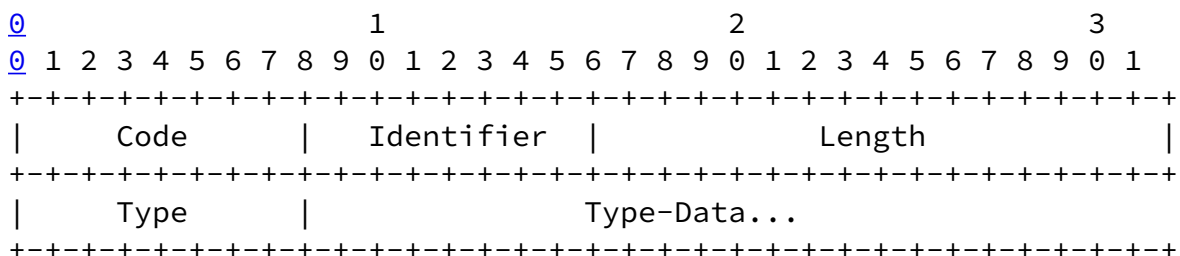
5 - OTP 6 - Generic Token Card

## Type-Data

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

## 2.2. 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 Type-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" [[RFC1938](#)]. 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(s).

## 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 [[RFC1938](#)]. 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 a displayable 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.](#) Security Considerations

EAP was designed for use with dialup PPP [[RFC1661](#)] and wired local area networks [[IEEE802](#)]. On these networks, an attacker would need to gain physical access to the telephone or switch infrastructure in order to mount an attack. While such attacks have been documented, such as in [[DECEPTION](#)], they are assumed to be rare.

However, subsequently EAP has been proposed for use on wireless networks, and over the Internet, where physical security cannot be assumed. On such networks, the security vulnerabilities are greater, as are the requirements for EAP security.

This section documents the threats that exist on physically insecure networks carrying EAP, as well as laying out the consequences of the use of the OTP and Generic Token Card methods on those networks. We then discuss mechanisms by which the threats may be mitigated.

### [3.1](#). Threat model

On physically insecure networks, it is possible for an attacker to gain access to the physical medium. This enables a range of attacks, including the following:

- [1] An adversary may try to discover user identities by snooping data packets.
- [2] An adversary may try to modify or spoof EAP packets.
- [3] An adversary may launch denial of service attacks by terminating EAP conversations.
- [4] An adversary may attempt to recover the pass-phrase by mounting an off-line dictionary attack.
- [5] An adversary may attempt to convince the Peer to connect to an untrusted network.
- [6] An adversary may attempt to disrupt the EAP negotiation in order to weaken the authentication, gain access to user passwords or remove confidentiality protection.
- [7] An adversary may attempt to mount a denial of service attack.
- [8] An attacker may attempt to take advantage of weak key derivation techniques used within EAP methods.

- [9] An attacker may attempt to take advantage of weak ciphersuites subsequently used after EAP authentication has concluded.

Where EAP is used over wireless networks, an attacker needs to be within the coverage area of the wireless medium in order to carry out these attacks. However, where EAP is used over the Internet, no such restrictions apply.

### [3.2.](#) Security claims

Of the threats described in the previous section, the OTP and Generic Token Card method only provide protection against dictionary attack (threat [4]). Since the purpose of the OTP and Generic Token Card methods is to authenticate "something the user has", neither method requires a password, and so neither method is vulnerable to dictionary attack. Identity protection is not provided, nor is authentication and integrity protection of EAP packets. The OTP and Generic Token card methods provide one-way authentication only, and therefore do not prevent the peer from connecting to an untrusted network, although another method could conceivably be run in the opposite direction. No protection is provided against "bidding down" attacks, although EAP peers and authenticators may implement policy to limit the likelihood of such an attack. No keys are derived by the OTP and Generic Token Card methods, and so it is not possible to use these methods in order to provide keying material for a subsequent ciphersuite. Neither the OTP nor the Generic Token Card method provide for protected ciphersuite negotiation.

As a result, the OTP and Generic Token Card methods, when used by themselves, are only appropriate for use on networks where physical security can be assumed. These methods SHOULD NOT be used on wireless networks, or over the Internet, unless the EAP conversation is protected. This can be accomplished using technologies such as IPsec [[RFC2401](#)] or TLS [[RFC2246](#)].

The following security issues are discussed in more depth in the sections that follow:

- Identity protection
- Packet modification attacks
- Mutual authentication
- Confidentiality

### [3.3.](#) Identity protection

Both the OTP and Generic Token Card methods assume that an Identity exchange has taken place prior to invoking the method, so that

INTERNET-DRAFT

OTP and Generic Token Card

12 October 2002

parameters unique to the user's claimed identity can be retrieved by the authenticator and used in the authentication. Since EAP Identity Request and Response methods are sent in the clear, an attacker may obtain the user identity.

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

Neither the Generic Token Card nor the OTP method provide for authentication and integrity protection of material sent within the data portion of an EAP message. EAP also 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 as well as Success and Failure messages. Therefore the Generic Token card and OTP methods assume that physical access to the link is restricted, so that such attacks are unlikely.

However, where EAP is run over wireless networks or over IP, such as within protocols supporting PPP or Ethernet tunneling [[RFC2661](#)], physical security can no longer be assumed. In this case, the Generic Token card and OTP methods SHOULD be authenticated and integrity protected by alternate means. This can be achieved, for example, by encapsulating the EAP exchange within protocols such as IPsec [[RFC2401](#)] or TLS [[RFC2246](#)].

#### [3.5.](#) 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.

The OTP and Generic Token Card methods only provide for one-way authentication; that is, they authenticate the EAP peer to the authenticator. Therefore the authenticator's identity remains unverified.

Where physical security can be assumed, such one-way authentication may be acceptable; however, for wireless media such as 802.11 [[IEEE80211](#)] or

for EAP use over IP, where physical security can no longer be assumed, mutual authentication is necessary to guard against rogue authenticators. As a result, in these situations, the OTP and Generic Token Card methods cannot by themselves provide adequate security.

### [3.6.](#) 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. Where EAP is run over wireless networks, such as 802.11 [[IEEE80211](#)], there may be an expectation that keys for link layer ciphersuites will be provided by the EAP method. This implies that the OTP and Generic Token Card methods will not be acceptable for use in such situations, since if they are used, then data traffic will be vulnerable to a wide variety of attacks, including traffic insertion, snooping and session hijacking.

## [4.](#) Normative References

- [RFC1661]      Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, [RFC 1661](#), July 1994.
- [RFC1938]      Haller, N. and C. Metz, "A One-Time Password System", [RFC 1938](#), May 1996.
- [RFC2044]      Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", [RFC 2044](#), October 1996.
- [RFC2119]      Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- [RFC2284]      Blunk, L., Vollbrecht, J., "Extensible Authentication Protocol (EAP)", [RFC 2284](#), March 1998.

## [5.](#) Informative References

- [RFC2246]      Dierks, T., Allen, C., "The TLS Protocol", [RFC 2246](#), January 1999.
- [RFC2401]      Atkinson, R., Kent, S., "Security Architecture for the

Internet Protocol", [RFC 2401](#), November 1998.

- [RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and Palter, B., "Layer Two Tunneling Protocol L2TP", [RFC 2661](#), August 1999.
- [DECEPTION] Slatalla, M., and Quittner, J., "Masters of Deception," HarperCollins, New York, 1995.
- [IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.
- [IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

- [IEEE80211] 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. 802.11-1999, 1999.

## 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](mailto:jrv@interlinknetworks.com)

Bernard Aboba  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

EMail: [bernarda@microsoft.com](mailto:bernarda@microsoft.com)  
Phone: +1 425 706 6605  
Fax: +1 425 936 7329

#### 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 implementers 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-ietf-eap-otp-00.txt](#)>, and expires April 19, 2003.

