Extensible Authentication Protocol

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#searchInput)

**Extensible Authentication Protocol** (**EAP**) is an authentication framework frequently used in network and internet connections. It is defined in RFC 3748, which made RFC 2284 obsolete, and is updated by RFC 5247. EAP is an authentication framework for providing the transport and usage of material and parameters generated by EAP methods. There are many methods defined by RFCs and a number of vendor specific methods and new proposals exist. EAP is not a wire protocol; instead it only defines the information from the interface and the formats. Each protocol that uses EAP defines a way to encapsulate by the user EAP messages within that protocol's messages.

EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism.



**Contents**

* [1Methods](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#Methods)
  + [1.1Nimble out-of-band authentication for EAP (EAP-NOOB)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#Nimble_out-of-band_authentication_for_EAP_(EAP-NOOB))
  + [1.2Lightweight Extensible Authentication Protocol (LEAP)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#Lightweight_Extensible_Authentication_Protocol_(LEAP))
  + [1.3EAP Transport Layer Security (EAP-TLS)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Transport_Layer_Security_(EAP-TLS))
  + [1.4EAP-MD5](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP-MD5)
  + [1.5EAP Protected One-Time Password (EAP-POTP)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Protected_One-Time_Password_(EAP-POTP))
  + [1.6EAP Pre-Shared Key (EAP-PSK)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Pre-Shared_Key_(EAP-PSK))
  + [1.7EAP Password (EAP-PWD)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Password_(EAP-PWD))
  + [1.8EAP Tunneled Transport Layer Security (EAP-TTLS)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Tunneled_Transport_Layer_Security_(EAP-TTLS))
  + [1.9EAP Internet Key Exchange v. 2 (EAP-IKEv2)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Internet_Key_Exchange_v._2_(EAP-IKEv2))
  + [1.10EAP Flexible Authentication via Secure Tunneling (EAP-FAST)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Flexible_Authentication_via_Secure_Tunneling_(EAP-FAST))
  + [1.11Tunnel Extensible Authentication Protocol (TEAP)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#Tunnel_Extensible_Authentication_Protocol_(TEAP))
  + [1.12EAP Subscriber Identity Module (EAP-SIM)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Subscriber_Identity_Module_(EAP-SIM))
  + [1.13EAP Authentication and Key Agreement (EAP-AKA)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Authentication_and_Key_Agreement_(EAP-AKA))
  + [1.14EAP Authentication and Key Agreement prime (EAP-AKA')](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Authentication_and_Key_Agreement_prime_(EAP-AKA'))
  + [1.15EAP Generic Token Card (EAP-GTC)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Generic_Token_Card_(EAP-GTC))
  + [1.16EAP Encrypted Key Exchange (EAP-EKE)](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP_Encrypted_Key_Exchange_(EAP-EKE))
* [2Encapsulation](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#Encapsulation)
  + [2.1IEEE 802.1X](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#IEEE_802.1X)
  + [2.2PEAP](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#PEAP)
  + [2.3RADIUS and Diameter](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#RADIUS_and_Diameter)
  + [2.4PANA](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#PANA)
  + [2.5PPP](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#PPP)
* [3See also](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#See_also)
* [4References](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#References)
* [5Further reading](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#Further_reading)
* [6External links](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#External_links)

Methods[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=1)]

EAP is an authentication framework, not a specific authentication mechanism.[[1]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-rfc3748_sec1-1) It provides some common functions and negotiation of authentication methods called EAP methods. There are currently about 40 different methods defined. Methods defined in [IETF](https://en.wikipedia.org/wiki/IETF) RFCs include EAP-MD5, EAP-POTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, and EAP-AKA'. Additionally, a number of vendor-specific methods and new proposals exist. Commonly used modern methods capable of operating in wireless networks include EAP-TLS, EAP-SIM, EAP-AKA, [LEAP](https://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol) and EAP-TTLS. Requirements for EAP methods used in wireless LAN authentication are described in [RFC 4017](https://tools.ietf.org/html/rfc4017). The list of type and packets codes used in EAP is available from the IANA EAP Registry.

The standard also describes the conditions under which the AAA key management requirements described in [RFC 4962](https://tools.ietf.org/html/rfc4962) can be satisfied.

**Nimble out-of-band authentication for EAP (EAP-NOOB)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=2)]

Nimble out-of-band authentication for EAP[[2]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-2) (EAP-NOOB) is a generic bootstrapping solution for devices which have no pre-configured authentication credentials and which are not yet registered on any server. It is especially useful for Internet-of-Things (IoT) gadgets and toys that come with no information about any owner, network or server. Authentication for this EAP method is based on a user-assisted out-of-band (OOB) channel between the server and peer. EAP-NOOB supports many types of OOB channels such as QR codes, NFC tags, audio etc. and unlike other EAP methods, the protocol security has been verified by formal modeling of the specification with [ProVerif](https://en.wikipedia.org/wiki/ProVerif) and [MCRL2](https://en.wikipedia.org/wiki/MCRL2) tools.[[3]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-3)

EAP-NOOB performs an Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) over the in-band EAP channel. The user then confirms this exchange by transferring the OOB message. Users can transfer the OOB message from the peer to the server, when for example, the device is a smart TV that can show a QR code. Alternatively, users can transfer the OOB message from the server to the peer, when for example, the device being bootstrapped is a camera that can only read a QR code.

**Lightweight Extensible Authentication Protocol (LEAP)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=3)]

*Main article:*[*Lightweight Extensible Authentication Protocol*](https://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol)

The [Lightweight Extensible Authentication Protocol](https://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol) (LEAP) method was developed by [Cisco Systems](https://en.wikipedia.org/wiki/Cisco_Systems) prior to the [IEEE](https://en.wikipedia.org/wiki/IEEE) ratification of the [802.11i](https://en.wikipedia.org/wiki/802.11i) security standard.[[4]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-4) Cisco distributed the protocol through the CCX (Cisco Certified Extensions) as part of getting 802.1X and dynamic [WEP](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) adoption into the industry in the absence of a standard. There is no native support for LEAP in any [Windows operating system](https://en.wikipedia.org/wiki/Windows_operating_system), but it is widely supported by third party client software most commonly included with WLAN (wireless LAN) devices. [LEAP](https://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol) support for Microsoft Windows 7 and Microsoft Windows Vista can be added by downloading a client add in from Cisco that provides support for both LEAP and EAP-FAST. Due to the wide adoption of LEAP in the networking industry many other WLAN vendors[[*who?*](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Words_to_watch#Unsupported_attributions)] claim support for LEAP.

LEAP uses a modified version of [MS-CHAP](https://en.wikipedia.org/wiki/MS-CHAP), an [authentication](https://en.wikipedia.org/wiki/Authentication) protocol in which user credentials are not strongly protected and easily compromised; an exploit tool called ASLEAP was released in early 2004 by Joshua Wright.[[5]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-5) Cisco recommends that customers who absolutely must use LEAP do so only with sufficiently complex passwords, though complex passwords are difficult to administer and enforce. Cisco's current recommendation is to use newer and stronger EAP protocols such as EAP-FAST, [PEAP](https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol), or EAP-TLS.

**EAP Transport Layer Security (EAP-TLS)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=4)]

EAP Transport Layer Security (EAP-TLS), defined in [RFC 5216](https://tools.ietf.org/html/rfc5216), is an IETF [open standard](https://en.wikipedia.org/wiki/Open_standard) that uses the [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) protocol, and is well-supported among wireless vendors. EAP-TLS is the original, standard wireless LAN EAP authentication protocol.

EAP-TLS is still considered one of the most secure EAP standards available, although TLS provides strong security only as long as the user understands potential warnings about false credentials, and is universally supported by all manufacturers of wireless LAN hardware and software. Until April 2005, EAP-TLS was the only EAP type vendors needed to certify for a WPA or WPA2 logo.[[6]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-6) There are client and server implementations of EAP-TLS in 3Com, Apple, [Avaya](https://en.wikipedia.org/wiki/Avaya), Brocade Communications, Cisco, Enterasys Networks, Fortinet, Foundry, Hirschmann, HP, Juniper, Microsoft, and open source operating systems. EAP-TLS is natively supported in Mac OS X 10.3 and above, [wpa\_supplicant](https://en.wikipedia.org/wiki/Wpa_supplicant), Windows 2000 SP4, Windows XP and above, Windows Mobile 2003 and above, Windows CE 4.2, and Apple's iOS mobile operating system.

Unlike most TLS implementations of [HTTPS](https://en.wikipedia.org/wiki/HTTPS), such as on the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web), the majority of implementations of EAP-TLS require client-side [X.509](https://en.wikipedia.org/wiki/X.509) certificates without giving the option to disable the requirement, even though the standard does not mandate their use.[[7]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-opensecurewireless-7)[[8]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-rfc5216s211-8) Some have identified this as having the potential to dramatically reduce adoption of EAP-TLS and prevent "open" but encrypted access points.[[7]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-opensecurewireless-7)[[8]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-rfc5216s211-8) On 22 August 2012 [hostapd](https://en.wikipedia.org/wiki/Hostapd) (and wpa\_supplicant) added support in its [Git](https://en.wikipedia.org/wiki/Git_(software)) repository for an UNAUTH-TLS vendor-specific EAP type (using the hostapd/wpa\_supplicant project [RFC 5612](https://tools.ietf.org/html/rfc5612) Private Enterprise Number),[[9]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-9) and on 25 February 2014 added support for the WFA-UNAUTH-TLS vendor-specific EAP type (using the [Wi-Fi Alliance](https://en.wikipedia.org/wiki/Wi-Fi_Alliance) Private Enterprise Number),[[10]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-10)[[11]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-11) which only do server authentication. This would allow for situations much like HTTPS, where a wireless hotspot allows free access and does not authenticate station clients but station clients wish to use encryption ([IEEE 802.11i-2004](https://en.wikipedia.org/wiki/IEEE_802.11i-2004) i.e. [WPA2](https://en.wikipedia.org/wiki/WPA2)) and potentially authenticate the wireless hotspot. There have also been proposals to use [IEEE 802.11u](https://en.wikipedia.org/wiki/IEEE_802.11u) for access points to signal that they allow EAP-TLS using only server-side authentication, using the standard EAP-TLS IETF type instead of a vendor-specific EAP type.[[12]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-12)

The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off. With a client-side certificate, a compromised password is not enough to break into EAP-TLS enabled systems because the intruder still needs to have the client-side certificate; indeed, a password is not even needed, as it is only used to encrypt the client-side certificate for storage. The highest security available is when the "private keys" of client-side certificate are housed in [smart cards](https://en.wikipedia.org/wiki/Smart_card).[[13]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-13) This is because there is no way to steal a client-side certificate's corresponding private key from a smart card without stealing the card itself. It is more likely that the physical theft of a smart card would be noticed (and the smart card immediately revoked) than a (typical) password theft would be noticed. In addition, the private key on a smart card is typically encrypted using a PIN that only the owner of the smart card knows, minimizing its utility for a thief even before the card has been reported stolen and revoked.

**EAP-MD5**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=5)]

EAP-MD5 was the only IETF Standards Track based EAP method when it was first defined in the original RFC for EAP, [RFC 2284](https://tools.ietf.org/html/rfc2284). It offers minimal security; the [MD5](https://en.wikipedia.org/wiki/MD5) [hash function](https://en.wikipedia.org/wiki/Hash_function) is vulnerable to [dictionary attacks](https://en.wikipedia.org/wiki/Dictionary_attack), and does not support key generation, which makes it unsuitable for use with dynamic WEP, or WPA/WPA2 enterprise. EAP-MD5 differs from other EAP methods in that it only provides authentication of the EAP peer to the EAP server but not mutual authentication. By not providing EAP server authentication, this EAP method is vulnerable to man-in-the-middle attacks.[[14]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-14) EAP-MD5 support was first included in [Windows 2000](https://en.wikipedia.org/wiki/Windows_2000) and deprecated in [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista).[[15]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-15)

**EAP Protected One-Time Password (EAP-POTP)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=6)]

EAP Protected One-Time Password (EAP-POTP), which is described in [RFC 4793](https://tools.ietf.org/html/rfc4793), is an EAP method developed by RSA Laboratories that uses one-time password (OTP) tokens, such as a handheld hardware device or a hardware or software module running on a personal computer, to generate authentication keys. EAP-POTP can be used to provide unilateral or mutual authentication and key material in protocols that use EAP.

The EAP-POTP method provides two-factor user authentication, meaning that a user needs both physical access to a token and knowledge of a [personal identification number](https://en.wikipedia.org/wiki/Personal_identification_number) (PIN) to perform authentication.[[16]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-16)

**EAP Pre-Shared Key (EAP-PSK)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=7)]

[[1]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-rfc3748_sec1-1)EAP Pre-shared key (EAP-PSK), defined in [RFC 4764](https://tools.ietf.org/html/rfc4764), is an EAP method for mutual authentication and session key derivation using a [pre-shared key](https://en.wikipedia.org/wiki/Pre-shared_key) (PSK). It provides a protected communication channel, when mutual authentication is successful, for both parties to communicate and is designed for authentication over insecure networks such as IEEE 802.11.

EAP-PSK is documented in an experimental RFC that provides a lightweight and extensible EAP method that does not require any public-key cryptography. The EAP method protocol exchange is done in a minimum of four messages.

**EAP Password (EAP-PWD)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=8)]

EAP Password (EAP-PWD), defined in [RFC 5931](https://tools.ietf.org/html/rfc5931), is an EAP method which uses a shared password for authentication. The password may be a low-entropy one and may be drawn from some set of possible passwords, like a dictionary, which is available to an attacker. The underlying key exchange is resistant to active attack, passive attack, and dictionary attack.

EAP-PWD is in the base of Android 4.0 (ICS), it is in FreeRADIUS [[17]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-17) and Radiator [[18]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-18) RADIUS servers, and it is in hostapd and wpa\_supplicant.[[19]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-19)

**EAP Tunneled Transport Layer Security (EAP-TTLS)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=9)]

EAP Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends [TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security). It was co-developed by [Funk Software](https://en.wikipedia.org/wiki/Funk_Software) and [Certicom](https://en.wikipedia.org/wiki/Certicom) and is widely supported across platforms. Microsoft did not incorporate native support for the EAP-TTLS protocol in [Windows XP](https://en.wikipedia.org/wiki/Windows_XP), [Vista](https://en.wikipedia.org/wiki/Windows_Vista), or [7](https://en.wikipedia.org/wiki/Windows_7). Supporting TTLS on these platforms requires third-party Encryption Control Protocol (ECP) certified software. [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) started EAP-TTLS support with [Windows 8](https://en.wikipedia.org/wiki/Windows_8),[[20]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-20), support for EAP-TTLS[[21]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-21) appeared in Windows Phone [version 8.1](https://en.wikipedia.org/wiki/Windows_Phone_8.1).[[22]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-22)

The client can, but does not have to be authenticated via a [CA](https://en.wikipedia.org/wiki/Certificate_authority)-signed [PKI](https://en.wikipedia.org/wiki/Public_key_infrastructure) certificate to the server. This greatly simplifies the setup procedure since a certificate is not needed on every client.

After the server is securely authenticated to the client via its CA certificate and optionally the client to the server, the server can then use the established secure connection ("tunnel") to authenticate the client. It can use an existing and widely deployed authentication protocol and infrastructure, incorporating legacy password mechanisms and authentication databases, while the secure tunnel provides protection from [eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping) and [man-in-the-middle attack](https://en.wikipedia.org/wiki/Man-in-the-middle_attack). Note that the user's name is never transmitted in unencrypted clear text, improving privacy.

Two distinct versions of EAP-TTLS exist: original EAP-TTLS (a.k.a. EAP-TTLSv0) and EAP-TTLSv1. EAP-TTLSv0 is described in [RFC 5281](https://tools.ietf.org/html/rfc5281), EAP-TTLSv1 is available as an Internet draft.[[23]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-23)

**EAP Internet Key Exchange v. 2 (EAP-IKEv2)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=10)]

EAP Internet Key Exchange v. 2 (EAP-IKEv2) is an EAP method based on the [Internet Key Exchange](https://en.wikipedia.org/wiki/Internet_Key_Exchange) protocol version 2 (IKEv2). It provides mutual authentication and session key establishment between an EAP peer and an EAP server. It supports authentication techniques that are based on the following types of credentials:

**Asymmetric key pairs**

Public/private key pairs where the public key is embedded into a [digital certificate](https://en.wikipedia.org/wiki/Digital_certificate), and the corresponding [private key](https://en.wikipedia.org/wiki/Private_key) is known only to a single party.

**Passwords**

Low-[entropy](https://en.wikipedia.org/wiki/Information_entropy) bit strings that are known to both the server and the peer.

**Symmetric keys**

High-entropy bit strings that are known to both the server and the peer.

It is possible to use a different authentication [credential](https://en.wikipedia.org/wiki/Credential) (and thereby technique) in each direction. For example, the EAP server authenticates itself using public/private key pair and the EAP peer using symmetric key. In particular, the following combinations are expected to be used in practice:

EAP-IKEv2 is described in [RFC 5106](https://tools.ietf.org/html/rfc5106), and a [prototype implementation](http://eap-ikev2.sourceforge.net/) exists.

**EAP Flexible Authentication via Secure Tunneling (EAP-FAST)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=11)]

Flexible Authentication via Secure Tunneling (EAP-FAST; [RFC 4851](https://tools.ietf.org/html/rfc4851)) is a protocol proposal by [Cisco Systems](https://en.wikipedia.org/wiki/Cisco_Systems) as a replacement for [LEAP](https://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol).[[24]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-24) The protocol was designed to address the weaknesses of LEAP while preserving the "lightweight" implementation. Use of server certificates is optional in EAP-FAST. EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified.

EAP-FAST has three phases:[[25]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-25)

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase** | **Function** | **Description** | **Purpose** |
| 0 | In-band provisioning—provide the peer with a shared secret to be used in secure phase 1 conversation | Uses Authenticated Diffie-Hellman Protocol (ADHP). This phase is independent of other phases; hence, any other scheme (in-band or out-of-band) can be used in the future. | Eliminate the requirement in the client to establish a master secret every time a client requires network access |
| 1 | Tunnel establishment | Authenticates using the PAC and establishes a tunnel key | Key establishment to provide confidentiality and integrity during the authentication process in phase 2 |
| 2 | Authentication | Authenticates the peer | Multiple tunneled, secure authentication mechanisms (credentials exchanged) |

When automatic PAC provisioning is enabled, EAP-FAST has a slight vulnerability where an attacker can intercept the PAC and use that to compromise user credentials. This vulnerability is mitigated by manual PAC provisioning or by using server certificates for the PAC provisioning phase.

It is worth noting that the PAC file is issued on a per-user basis. This is a requirement in [RFC 4851](https://tools.ietf.org/html/rfc4851) sec 7.4.4 so if a new user logs on the network from a device, a new PAC file must be provisioned first. This is one reason why it is difficult not to run EAP-FAST in insecure anonymous provisioning mode. The alternative is to use device passwords instead, but then the device is validated on the network not the user.

EAP-FAST can be used without PAC files, falling back to normal TLS.

EAP-FAST is natively supported in Apple OS X 10.4.8 and newer. [Cisco](https://en.wikipedia.org/wiki/Cisco) supplies an EAP-FAST module[[26]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-26) for [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista) [[27]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-27) and later operating systems which have an extensible EAPHost architecture for new authentication methods and supplicants.[[28]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-28)

**Tunnel Extensible Authentication Protocol (TEAP)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=12)]

Tunnel Extensible Authentication Protocol (TEAP; [RFC 7170](https://tools.ietf.org/html/rfc7170)) is a tunnel-based EAP method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) protocol to establish a mutually authenticated tunnel. Within the tunnel, TLV (Type-Length-Value) objects are used to convey authentication-related data between the EAP peer and the EAP server.

In addition to peer authentication, TEAP allows peer to ask the server for certificate by sending request in [PKCS#10](https://en.wikipedia.org/wiki/Certificate_signing_request) format and the server can provision certificate to the peer in [rfc:2315 PKCS#7] format. The server can also distribute trusted root certificates to the peer in [rfc:2315 PKCS#7] format. Both operations are enclosed into the corresponding TLVs and happen in the secure way inside previously established TLS tunnel.

**EAP Subscriber Identity Module (EAP-SIM)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=13)]

EAP [Subscriber Identity Module](https://en.wikipedia.org/wiki/Subscriber_Identity_Module) (EAP-SIM) is used for authentication and session key distribution using the subscriber identity module (SIM) from the Global System for Mobile Communications ([GSM](https://en.wikipedia.org/wiki/GSM)).

GSM cellular networks use a subscriber identity module card to carry out user authentication. EAP-SIM use a SIM authentication algorithm between the client and an [Authentication, Authorization and Accounting (AAA)](https://en.wikipedia.org/wiki/AAA_protocol) server providing mutual authentication between the client and the network.

In EAP-SIM the communication between the SIM card and the Authentication Centre (AuC) replaces the need for a pre-established password between the client and the AAA server.

The A3/A8 algorithms are being run a few times, with different 128 bit challenges, so there will be more 64 bit Kc-s which will be combined/mixed to create stronger keys (Kc-s won't be used directly). The lack of mutual authentication in GSM has also been overcome.

EAP-SIM is described in [RFC 4186](https://tools.ietf.org/html/rfc4186).

**EAP Authentication and Key Agreement (EAP-AKA)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=14)]

Extensible Authentication Protocol Method for [Universal Mobile Telecommunications System](https://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System) (UMTS) Authentication and Key Agreement (EAP-AKA), is an EAP mechanism for authentication and session key distribution using the UMTS Subscriber Identity Module ([USIM](https://en.wikipedia.org/wiki/Universal_Subscriber_Identity_Module)). EAP-AKA is defined in [RFC 4187](https://tools.ietf.org/html/rfc4187).

**EAP Authentication and Key Agreement**[**prime**](https://en.wikipedia.org/wiki/Prime_(symbol)#Use_in_mathematics,_statistics,_and_science)**(EAP-AKA')**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=15)]

The EAP-AKA' variant of EAP-AKA, defined in [RFC 5448](https://tools.ietf.org/html/rfc5448), and is used for non-3GPP access to a [3GPP](https://en.wikipedia.org/wiki/3GPP) core network. For example, via [EVDO](https://en.wikipedia.org/wiki/Evolution-Data_Optimized), [WiFi](https://en.wikipedia.org/wiki/WiFi), or [WiMax](https://en.wikipedia.org/wiki/WiMax).

**EAP Generic Token Card (EAP-GTC)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=16)]

EAP Generic Token Card, or EAP-GTC, is an EAP method created by Cisco as an alternative to PEAPv0/EAP-MSCHAPv2 and defined in [RFC 2284](https://tools.ietf.org/html/rfc2284) and [RFC 3748](https://tools.ietf.org/html/rfc3748). EAP-GTC carries a text challenge from the authentication server, and a reply generated by a [security token](https://en.wikipedia.org/wiki/Security_token). The PEAP-GTC authentication mechanism allows generic authentication to a number of databases such as [Novell Directory Service](https://en.wikipedia.org/wiki/Novell_Directory_Service) (NDS) and [Lightweight Directory Access Protocol](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) (LDAP), as well as the use of a [one-time password](https://en.wikipedia.org/wiki/One-time_password).

**EAP Encrypted Key Exchange (EAP-EKE)**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=17)]

EAP with the [encrypted key exchange](https://en.wikipedia.org/wiki/Encrypted_key_exchange), or EAP-EKE, is one of the few EAP methods that provide secure mutual authentication using short passwords and no need for [public key certificates](https://en.wikipedia.org/wiki/Public_key_certificate). It is a three-round exchange, based on the [Diffie-Hellman](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange) variant of the well-known EKE protocol.

EAP-EKE is specified in [RFC 6124](https://tools.ietf.org/html/rfc6124).

Encapsulation[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=18)]

EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to [encapsulate](https://en.wikipedia.org/wiki/Encapsulation_(networking)) EAP messages within that protocol's messages.[[29]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-29)[[30]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-30)

**IEEE 802.1X**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=19)]

*Main article:*[*IEEE 802.1X*](https://en.wikipedia.org/wiki/IEEE_802.1X)

The encapsulation of EAP over [IEEE 802](https://en.wikipedia.org/wiki/IEEE_802) is defined in [IEEE 802.1X](https://en.wikipedia.org/wiki/IEEE_802.1X) and known as "EAP over LANs" or EAPOL.[[31]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-31)[[32]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-32)[[33]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-33) EAPOL was originally designed for [IEEE 802.3](https://en.wikipedia.org/wiki/IEEE_802.3) ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) wireless and [Fiber Distributed Data Interface](https://en.wikipedia.org/wiki/Fiber_Distributed_Data_Interface) (ISO 9314-2) in 802.1X-2004.[[34]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-34) The EAPOL protocol was also modified for use with [IEEE 802.1AE](https://en.wikipedia.org/wiki/IEEE_802.1AE) (MACsec) and [IEEE 802.1AR](https://en.wikipedia.org/wiki/IEEE_802.1#802.1AR) (Initial Device Identity, IDevID) in 802.1X-2010.[[35]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-35)

When EAP is invoked by an 802.1X enabled [Network Access Server](https://en.wikipedia.org/wiki/Network_Access_Server) (NAS) device such as an [IEEE 802.11i-2004](https://en.wikipedia.org/wiki/IEEE_802.11i-2004) Wireless Access Point (WAP), modern EAP methods can provide a secure authentication mechanism and negotiate a secure private key (Pair-wise Master Key, PMK) between the client and NAS which can then be used for a wireless encryption session utilizing [TKIP](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol) or [CCMP](https://en.wikipedia.org/wiki/CCMP_(cryptography)) (based on [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)) encryption.

**PEAP**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=20)]

*Main article:*[*Protected Extensible Authentication Protocol*](https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol)

The [Protected Extensible Authentication Protocol](https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol), also known as Protected EAP or simply PEAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) [tunnel](https://en.wikipedia.org/wiki/Tunneling_protocol).[[36]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-36)[[37]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-peapv2-10_abstract-37)[[38]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-38) The purpose was to correct deficiencies in EAP; EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.[[39]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-39)

PEAP was jointly developed by Cisco Systems, Microsoft, and RSA Security. PEAPv0 was the version included with [Microsoft](https://en.wikipedia.org/wiki/Microsoft) [Windows XP](https://en.wikipedia.org/wiki/Windows_XP) and was nominally defined in [draft-kamath-pppext-peapv0-00](http://tools.ietf.org/html/draft-kamath-pppext-peapv0-00). PEAPv1 and PEAPv2 were defined in different versions of *draft-josefsson-pppext-eap-tls-eap*. PEAPv1 was defined in [draft-josefsson-pppext-eap-tls-eap-00](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-00) through [draft-josefsson-pppext-eap-tls-eap-05](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-05),[[40]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-40) and PEAPv2 was defined in versions beginning with [draft-josefsson-pppext-eap-tls-eap-06](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-06).[[41]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-41)

The protocol only specifies chaining multiple EAP mechanisms and not any specific method.[[37]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-peapv2-10_abstract-37)[[42]](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_note-42) Use of the [EAP-MSCHAPv2](https://en.wikipedia.org/wiki/EAP-MSCHAPv2) and [EAP-GTC](https://en.wikipedia.org/wiki/EAP-GTC) methods are the most commonly supported.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**RADIUS and Diameter**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=21)]

*Main articles:*[*RADIUS*](https://en.wikipedia.org/wiki/RADIUS)*and*[*Diameter (protocol)*](https://en.wikipedia.org/wiki/Diameter_(protocol))

Both the [RADIUS](https://en.wikipedia.org/wiki/RADIUS) and [Diameter](https://en.wikipedia.org/wiki/Diameter_(protocol)) [AAA protocols](https://en.wikipedia.org/wiki/AAA_protocol) can encapsulate EAP messages. They are often used by [Network Access Server](https://en.wikipedia.org/wiki/Network_Access_Server) (NAS) devices to forward EAP packets between IEEE 802.1X endpoints and AAA servers to facilitate IEEE 802.1X.

**PANA**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=22)]

*Main article:*[*Protocol for Carrying Authentication for Network Access*](https://en.wikipedia.org/wiki/Protocol_for_Carrying_Authentication_for_Network_Access)

The [Protocol for Carrying Authentication for Network Access](https://en.wikipedia.org/wiki/Protocol_for_Carrying_Authentication_for_Network_Access) (PANA) is an IP-based protocol that allows a device to authenticate itself with a network to be granted access. PANA will not define any new authentication protocol, key distribution, key agreement or key derivation protocols; for these purposes, EAP will be used, and PANA will carry the EAP payload. PANA allows dynamic service provider selection, supports various authentication methods, is suitable for roaming users, and is independent from the link layer mechanisms.

**PPP**[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=23)]

*Main article:*[*Point-to-Point Protocol*](https://en.wikipedia.org/wiki/Point-to-Point_Protocol)

EAP was originally an authentication extension for the [Point-to-Point Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Protocol) (PPP). PPP has supported EAP since EAP was created as an alternative to the [Challenge-Handshake Authentication Protocol](https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol) (CHAP) and the [Password Authentication Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol) (PAP), which were eventually incorporated into EAP. The EAP extension to PPP was first defined in [RFC 2284](https://tools.ietf.org/html/rfc2284), now obsoleted by [RFC 3748](https://tools.ietf.org/html/rfc3748).

See also[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=24)]

* [Authentication protocol](https://en.wikipedia.org/wiki/Authentication_protocol)
* [Handover keying](https://en.wikipedia.org/wiki/Handover_keying)
* [ITU-T](https://en.wikipedia.org/wiki/ITU-T) [X.1035](https://en.wikipedia.org/wiki/X.1035)

References[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=25)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-rfc3748_sec1_1-0) [***b***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-rfc3748_sec1_1-1) [RFC 3748](https://tools.ietf.org/html/rfc3748), § 1
  2. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-2) *Aura, Tuomas; Sethi, Mohit (2020-07-21).*[*"Nimble out-of-band authentication for EAP (EAP-NOOB) Draft"*](https://tools.ietf.org/html/draft-ietf-emu-eap-noob)*. IETF Trust.*
  3. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-3) [EAP-NOOB Model on GitHub](https://github.com/tuomaura/eap-noob/tree/master/protocolmodel)
  4. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-4) *George Ou (January 11, 2007).*[*"Ultimate wireless security guide: An introduction to LEAP authentication"*](https://www.techrepublic.com/article/ultimate-wireless-security-guide-an-introduction-to-leap-authentication/)*.*[*TechRepublic*](https://en.wikipedia.org/wiki/TechRepublic)*. Retrieved 2008-02-17.*
  5. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-5) *Dan Jones (October 1, 2003).*[*"Look Before You LEAP"*](https://web.archive.org/web/20080209200945/http:/www.unstrung.com/document.asp?doc_id=41185)*. Unstrung. Archived from*[*the original*](http://www.unstrung.com/document.asp?doc_id=41185)*on February 9, 2008. Retrieved 2008-02-17.*
  6. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-6) [*"Understanding the updated WPA and WPA2 standards"*](http://blogs.techrepublic.com.com/Ou/?p=67)*. techrepublic.com. Retrieved 2008-02-17.*
  7. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-opensecurewireless_7-0) [***b***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-opensecurewireless_7-1) *Byrd, Christopher (5 May 2010).*[*"Open Secure Wireless"*](https://web.archive.org/web/20131212085700/http:/riosec.com/files/Open-Secure-Wireless.pdf)*(PDF). Archived from*[*the original*](http://riosec.com/files/Open-Secure-Wireless.pdf)*(PDF) on 12 December 2013. Retrieved 2013-08-14.*
  8. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-rfc5216s211_8-0) [***b***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-rfc5216s211_8-1) [*RFC 5216*](https://tools.ietf.org/html/rfc5216)*: The EAP-TLS Authentication Protocol,*[*Internet Engineering Task Force*](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force)*, March 2008, The certificate\_request message is included when the server desires the peer to authenticate itself via public key. While the EAP server SHOULD require peer authentication, this is not mandatory, since there are circumstances in which peer authentication will not be needed (e.g., emergency services, as described in [UNAUTH]), or where the peer will authenticate via some other means.*
  9. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-9) [*"Add UNAUTH-TLS vendor specific EAP type"*](https://archive.today/20130213070147/http:/hostap.epitest.fi/gitweb/gitweb.cgi?p=hostap.git;a=commit;h=065d2895b4693e8c923580dbfa31123297c8bb7d)*.*[*hostapd*](https://en.wikipedia.org/wiki/Hostapd)*. Archived from*[*the original*](http://hostap.epitest.fi/gitweb/gitweb.cgi?p=hostap.git;a=commit;h=065d2895b4693e8c923580dbfa31123297c8bb7d)*on 2013-02-13. Retrieved 2013-08-14.*
  10. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-10) [*"HS 2.0R2: Add WFA server-only EAP-TLS peer method"*](https://archive.today/20140930045346/http:/hostap.epitest.fi/gitweb/gitweb.cgi?p=hostap.git;a=commitdiff;h=8e5fdfabf69a7692d1a0d04f00fa103e9ff72010)*.*[*hostapd*](https://en.wikipedia.org/wiki/Hostapd)*. Archived from*[*the original*](http://hostap.epitest.fi/gitweb/gitweb.cgi?p=hostap.git;a=commitdiff;h=8e5fdfabf69a7692d1a0d04f00fa103e9ff72010)*on 2014-09-30. Retrieved 2014-05-06.*
  11. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-11) [*"HS 2.0R2: Add WFA server-only EAP-TLS server method"*](https://archive.today/20140930045348/http:/hostap.epitest.fi/gitweb/gitweb.cgi?p=hostap.git;a=commitdiff;h=b61e70c4f37837baf17956817f8d80a586f75770)*.*[*hostapd*](https://en.wikipedia.org/wiki/Hostapd)*. Archived from*[*the original*](http://hostap.epitest.fi/gitweb/gitweb.cgi?p=hostap.git;a=commitdiff;h=b61e70c4f37837baf17956817f8d80a586f75770)*on 2014-09-30. Retrieved 2014-05-06.*
  12. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-12) *Byrd, Christopher (1 November 2011).*[*"Open Secure Wireless 2.0"*](https://web.archive.org/web/20131126183610/http:/riosec.com/open-secure-wireless-2.0)*. Archived from*[*the original*](http://riosec.com/open-secure-wireless-2.0)*on 26 November 2013. Retrieved 2013-08-14.*
  13. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-13) *Rand Morimoto; Kenton Gardinier; Michael Noel; Joe Coca (2003).*[*Microsoft Exchange Server 2003 Unleashed*](https://books.google.com/books?id=5x7iLC7fKIAC&pg=PA244)*. Sams. p. 244.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-672-32581-6*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-672-32581-6)*.*
  14. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-14) [*"Alternative Encryption Schemes: Targeting the weaknesses in static WEP"*](https://arstechnica.com/articles/paedia/security.ars/4)*. Ars Technica. Retrieved 2008-02-17.*
  15. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-15) [*"922574"*](http://support.microsoft.com/kb/922574)*, Knowledge Base, Microsoft*
  16. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-16) [*"EAP-POTP Authentication Protocol"*](http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-027.html)*. Juniper.net. Retrieved 2014-04-17.*
  17. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-17) [FreeRADIUS EAP module rlm\_eap\_pwd](http://code.metager.de/source/xref/freeradius/server/src/modules/rlm_eap/types/)
  18. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-18) [Added support for EAP-PWD per RFC 5931](http://www.open.com.au/pipermail/radiator-announce/2012-June/000018.html)
  19. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-19) [Secure-authentication with only a password](http://community.arubanetworks.com/t5/Technology-Blog/Secure-authentication-with-only-a-password/ba-p/36524)
  20. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-20) [Extensible Authentication Protocol (EAP) Settings for Network Access](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh945104(v=ws.11))
  21. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-21) [*"802.1x / EAP TTLS support? – Windows Phone Central Forums"*](http://forums.wpcentral.com/windows-phone-8/200619-802-1x-eap-ttls-support.html)*. Forums.wpcentral.com. Retrieved 2014-04-17.*
  22. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-22) [*"Enterprise Wi-Fi authentication (EAP)"*](https://technet.microsoft.com/library/dn643706.aspx)*. Microsoft.com. Retrieved 2014-04-23.*
  23. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-23) [TTLSv1 Internet draft](https://tools.ietf.org/html/draft-funk-eap-ttls-v1-01)
  24. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-24) [*"Ultimate wireless security guide: A primer on Cisco EAP-FAST authentication"*](https://web.archive.org/web/20080324094115/http:/articles.techrepublic.com.com/5100-1035-6148557.html)*. techrepublic.com. Archived from*[*the original*](http://articles.techrepublic.com.com/5100-1035-6148557.html)*on 2008-03-24. Retrieved 2008-02-17.*
  25. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-25) [*"EAP-FAST > EAP Authentication Protocols for WLANs"*](http://www.ciscopress.com/articles/article.asp?p=369223&seqNum=5)*. Ciscopress.com. Retrieved 2014-04-17.*
  26. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-26) [[1]](http://www.cisco.com/en/US/docs/wireless/wlan_adapter/eap_types/fast/admin/guide/FAST_admin.html) [Archived](https://web.archive.org/web/20090210002337/http:/www.cisco.com/en/US/docs/wireless/wlan_adapter/eap_types/fast/admin/guide/FAST_admin.html) February 10, 2009, at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine)
  27. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-27) [How do I install CISCO EAP-FAST on my computer?](http://blogs.msdn.com/eapteam/archive/2008/10/17/how-do-i-install-cisco-eap-fast-on-my-computer.aspx)
  28. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-28) [EAPHost in Windows](http://www.microsoft.com/technet/technetmag/issues/2007/05/CableGuy/default.aspx)
  29. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-29) *"HTTPS, Secure HTTPS". Springer Reference. SpringerReference. Springer-Verlag. 2011.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1007/springerreference\_292*](https://doi.org/10.1007%2Fspringerreference_292)*.*
  30. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-30) *Plumb, Michelle, CAPPS : HTTPS Networking,*[*OCLC*](https://en.wikipedia.org/wiki/OCLC_(identifier))[*944514826*](https://www.worldcat.org/oclc/944514826)
  31. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-31) [RFC 3748](https://tools.ietf.org/html/rfc3748), § 3.3
  32. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-32) [RFC 3748](https://tools.ietf.org/html/rfc3748), § 7.12
  33. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-33) IEEE 802.1X-2001, § 7
  34. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-34) IEEE 802.1X-2004, § 3.2.2
  35. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-35) IEEE 802.1X-2010, § 5
  36. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-36) Microsoft's PEAP version 0, [draft-kamath-pppext-peapv0-00](http://tools.ietf.org/html/draft-kamath-pppext-peapv0-00), §1.1
  37. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-peapv2-10_abstract_37-0) [***b***](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-peapv2-10_abstract_37-1) Protected EAP Protocol (PEAP) Version 2, [draft-josefsson-pppext-eap-tls-eap-10](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10), abstract
  38. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-38) Protected EAP Protocol (PEAP) Version 2, [draft-josefsson-pppext-eap-tls-eap-10](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10), §1
  39. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-39) Protected EAP Protocol (PEAP) Version 2, [draft-josefsson-pppext-eap-tls-eap-07](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-07), §1
  40. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-40) Protected EAP Protocol (PEAP), [draft-josefsson-pppext-eap-tls-eap-05](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-05), §2.3
  41. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-41) Protected EAP Protocol (PEAP), [draft-josefsson-pppext-eap-tls-eap-06](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-06), §2.3
  42. [**^**](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#cite_ref-42) Protected EAP Protocol (PEAP) Version 2, [draft-josefsson-pppext-eap-tls-eap-10](http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10), §2

Further reading[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=26)]

* "AAA and Network Security for Mobile Access. RADIUS, DIAMETER, EAP, PKI and IP mobility". M Nakhjiri. John Wiley and Sons, Ltd.

External links[[edit](https://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&action=edit&section=27)]

* [RFC 3748](https://tools.ietf.org/html/rfc3748): Extensible Authentication Protocol (EAP) (June 2004)
* [RFC 5247](https://tools.ietf.org/html/rfc5247): Extensible Authentication Protocol (EAP) Key Management Framework (August 2008)
* [Configure RADIUS for secure 802.1x wireless LAN](https://www.techrepublic.com/article/ultimate-wireless-security-guide-microsoft-ias-radius-for-wireless-authentication/6148579)
* [How to self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication](https://www.techrepublic.com/article/ultimate-wireless-security-guide-self-signed-certificates-for-your-radius-server/6148560)
* [Extensible Authentication Protocol](https://technet.microsoft.com/en-us/network/bb643147.aspx) on Microsoft TechNet
* [EAPHost in Windows Vista and Windows Server 2008](http://www.microsoft.com/technet/technetmag/issues/2007/05/CableGuy/default.aspx)
* [WIRE1x](http://wire.cs.nctu.edu.tw/wire1x/)
* ["IETF EAP Method Update (emu) Working Group"](https://web.archive.org/web/20071023234216/http:/www.ietf.org/html.charters/emu-charter.html)
* [[2]](http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-027.html)