PEAP (Serverzertifikat)

Gegenüber EAP bietet das Protokoll den Vorteil, dass unabhängig von der Authentifizierungsmethode der Austausch über TLS gesichert ist. Daher ist für diese Technik ein Serverzertifikat zwingend erforderlich. Sowohl Computer als auch der Benutzer können authentifiziert werden.

Das von Microsoft gemeinsam mit Cisco und RSA Security entwickelte PEAP existiert in mehreren Versionen, zuletzt PEAPv2. Protected EAP ähnelt EAP-TTLS sehr stark. Es baut nach der Authentifizierung des Authenticators zunächst einen sicheren Kanal via TLS auf, über den sich dann der Peer gegenüber dem Authenticator authentifiziert.

Bei dieser Methode werden der Username und das Passwort des Anwenders verifiziert.
Diese können auch die Windows Anmeldedaten sein und selbige eine Active Directory weitergeleitet werden.

Ein Root Zertifikat ist auf dem Client erforderlich, um die Gültigkeit des Radius Servers zu bestätigen.

Protokoll	PEAP	EAP-TLS	EAP-TTLS	EAP-MD5	LEAP
Standards	**Ja**	Ja	IEFT Draft	Ja	Nein (Cisco)
Sicherheitslevel	**Hoch**	Sehr Hoch	Hoch	Sehr Schwach	Schwach
Server Zertifikat erforderlich	**Ja**	Ja	Ja	Nein	Nein
Client Zertifikat erforderlich	**Nein**	Ja	Optional	Nein	Nein
Geräteauthentifizerung	**Unterstützt**	Unterstützt	Unterstützt	Nein	Nein
Implementierungs-aufwand	**Mittel**	Hoch	Mittel	Sehr gering	Gering, nur Cisco

Zufriedenheit | Unabhängigkeit | Sicherheit

K5 Netzwerksysteme GmbH · Am Giener 23 A · 55268 Nieder-Olm · Tel.: 0 61 31 / 97 155 - 0 · Fax: 0 61 31 / 97 155 - 94 · info@k5-netzwerk.de