EAP-TTLS (Tunneled TLS)

EAP-TTLS (Tunneled TLS) stellt eine Variante zu EAP-TLS dar, die bei der Überprüfung des Peers anders vorgeht. Zunächst authentifiziert sich der Authenticator durch Versenden seines Zertifikats gegenüber dem Peer. Bei erfolgreicher Authentifizierung baut Letzterer einen sicheren TLS-Tunnel zum Authenticator auf und authentifiziert sich seinerseits.

Diese Authentifizierung kann sowohl mit einem Zertifikat als auch mit anderen EAP-Mechanismen (MD5-Challenge, One-Time Password) stattfinden. Wie EAP-TLS unterstützt auch EAP-TTLS das dynamische Generieren von Sitzungsschlüsseln.

Derzeit gängig ist EAP-TTLSv0 (RFC 5281). Die Variante EAP-TTLSv1 liegt bislang nur als Entwurf vor. Sie verwendet die TLS-Erweiterung TLS/IA (Inner Application), mit der Authentifizierung und Parameterübergabe zwischen Client und Server innerhalb des TLS-Steuerungskanals laufen können.

Bei EAP-TTLSv0 geschehen diese Dinge im Datenkanal. TLS/IA soll unter anderem die Sicherheit gegen Man-in-the-Middle-Angriffe auf Tunneled Authentication verbessern.

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