

Lizenzbestimmungen

- Diese Materialien sind lizenziert für @USERINFONAME@.
- Die Materialien dürfen **ausschließlich** für die Implementation, Verbesserung oder den Betrieb von Sicherheitsmaßnahmen innerhalb der genannten Organisation genutzt werden.
- Hierfür dürfen die Materialien beliebig verändert, ergänzt oder neu gestaltet werden.
- Für alle anderen Einsatzzwecke - insbesondere für die Veröffentlichung der Materialien und deren Einsatz für Kunden des Lizenznehmers - muss im Vorfeld eine schriftliche Genehmigung der 3473 Gurus GbR eingeholt bzw. eine entsprechende Lizenz erworben werden.

Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“:** mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.

Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!

Dieser Artikel bietet einen kurzen, kompakten Überblick über die Authentifizierung auf Basis von IEEE 802.1X in Wireless LANs (Enterprise Mode).

IEEE 802.1X - Enterprise Mode (WLAN)

Der Enterprise Mode stellt eine flexible Authentifizierung für Wireless LAN nach dem Standard IEEE 802.1X zur Verfügung und ist damit quasi der große Bruder des Consumer Mode.¹⁾ In diesem Standard spielt der Accesspoint bei der Authentifizierung nur noch eine untergeordnete Rolle - er wird „Authenticator“ genannt und führt die Authentifizierung nicht mehr selbst durch, sondern ist nur noch ein Vermittler zwischen dem einbuchenden Client (dem „Supplicant“) und einem Server im internen Netz (dem „Authentication Server“).

Der Authenticator verwirft alle Pakete, die von einem noch nicht authentifizierten Client empfangen werden. Handelt es sich um die passenden Pakete in einem Anmeldevorgang? Für den Transport der Authentifizierungsinformationen zwischen Supplicant und Authenticator schreibt IEEE 802.1X das Protokoll EAPoL (Extensible Authentication Protocol over LAN) vor.²⁾ EAPoL ist ein sehr einfach aufgebautes Protokoll, das nur Punkt-zu-Punkt-Verbindungen unterhält und damit leicht abgegriffen werden kann.

Das EAPoL-Paket des Supplicants wird vom Authenticator entgegen genommen, in ein anderes Protokoll gekapselt bzw. umgewandelt und an den Authentication Server im internen Netz weitergeleitet. IEEE 802.1X schreibt hier kein Verfahren vor und empfiehlt lediglich den Einsatz des RADIUS-Protokolls und eines RADIUS-Servers. Antworten des Authentication Servers werden vom Authenticator entpackt und so dann in die Authentifizierung zwischen Supplicant und Authentication Server eingebracht. Dies kann ohne den Supplicant Zugang zum internen Netz bedeuten.

Bei WPA(2) werden im Zuge eines erfolgreichen Authentifizierungszwischen Accesspoint und Client Schlüssel ausgetauscht bzw. vom Accesspoint an den Client weitergegeben. Nur jene Daten, die mit dem korrekten Schlüssel verschlüsselt wurden, können von Supplicant und Authenticator entschlüsselt und weiterverarbeitet werden. So wird sicher gestellt, dass nur berechtigte Stationen mit der Infrastruktur kommunizieren können.

IEEE 802.1x und IEEE 802.11. Irgendwann gab es eine Abfolge der Authentifizierung und einen Teil der veränderten Protokolle. Folgende Standards geben die Authentifizierungsvorgänge (wie EAP-Methoden) an, die zwischen Supplicant und Authentication Server durchgeführt werden. Aktuell sind hier mehr als 30 vorhanden. Verfügen sie RFC definieren und zeigen die weiteren veränderten Heterogenen Implementierungen. Methodenimplimentationen werden, der neue Methoden, die benutzten, mehrteilig. Der hierdargestellte Authentifizierung (TKIP, SIM-Karte, etc.) ermöglicht die WPA-Allianz zur Zeitzeit 2009 die folgenden EAP-Methoden:

Bezeichnung	RFC	Verfahren
EAP-TLS	RFC 5216	Zwischen Supplicant und Authentication Server wird TLS-Verbindung aufgebaut. Der Supplicant wird als Zertifikat ausgetauscht.
EAP-TTLS/MS-CHAPv2	RFC 5281	Zwischen Supplicant und Authentication Server wird TLS-Verbindung aufgebaut. Über TLS-Verbindung wird weitere Authentifizierung (wie „PAP“, „CHAP“, „MS-CHAPv2“) durchgeführt. Hierfür wird das Protokoll (MS-CHAPv2) verwendet.
PEAPv0/EAP-MSCHAPv2	Draft	Ähnlich wie EAP-TTLS.

B.z..chn.n.	RFC	V.rf.hr.n
PEAPv1/EAP-GTC	-	Pr...r...r.. Pr...k... v.. CISCO. Üb.r TLS-V.rb..... ..r. A..h.....z.r... .b.r G...r.c T.k.. C.r. (H.r.w.r.)
EAP-SIM	RFC 4186	A..h.....z.r... .r..... .b.r SIM-K.r...
EAP-AKA	RFC 4187	A..h.....z.r... .r..... .b.r ... UMTS SIM-K.r.. (UMTS A..h....c..... ... K.y A.r.....)
EAP-FAST	RFC 4851	Pr...k... v.. CISCO („F..x.b.. A..h....c..... v.. S.c.r. T.....“), h.....ch. D...r.b..... v.. Sch.....

E..r Üb.rb..ck .b.r ... h..... EAP-M..h....ch .rr.ch.....ch..r.ch.... S.... v.. W.k.....h....

<....r....> D.r E...r.r... M...rZ. w.r..., w... ... G.r...V..... ...h.....Z..r. ... v.rw..... w.r...
.....:

1. E.r.... .r M.... .r G.r... ..ch. ..hrch, ... Üb.rb..ck z. b.h.....
2. E. h.r.r.ch. K..... ... G.h.. v.. .b.... G.r.....
3. D.. ..b.... G.r... b..... ..ch .b.rr.. Z...r... h..w..ch. v.r.r.....w.r..... H..... S.. w.r... z.B.
v.r...h.. ...r ... N..z.r .r G.r... ..h.r.. z.T. ..ch. z.r V.rw..... bzw. z.. U...r.h....
4. ...

</....>

Schw.ch..... E...r.r... M...

D.r E...r.r... M... b..... ... M....chk...r ...z.. R..h. v.. A..h.....z.r..... ... j.w....z.w.h.... L....r
b..... ..chrb..... V.r..hr..z. R..h. v..ch.r.. A..h.....z.r.....

<....> D.. A..w.h. ..r EAP-M..h....r..... v.r..... w.r.... D.. A..h.....z.r..... b.....
h.h. S.ch.rh....:

- EAP-TLS
- EAP-TTLS-PAP/CHAP/MS-CHAP/MS-CHAPv2
- EAP/PEAPv0-TLS/MS-CHAPv2

</....>

[b....r....r....h....c.....-..rv.r](#) N.ch .r A..w.h. ..r EAP-M..h.... b.....r.. A.....rkr.. K.....r.....
w.r.... A... b..... K..... (.. ..b.... G.r..., ..r Acc..... ..r A..h.....z.r.....rv.r)r..... k.....r.r.
w.r..., .. S.ch.rh... ..r IT-l..r...r.k..r ..ch. z.hr.... B.....r. w.ch...b.,b.... G.r... v.r.ch.,
..chch...ß.ch b.. ..r r.ch..... l..r...r.k..r ..z..... D...rr C..... ..r L... .., ... A..h.....z.r.....rv.r
...b..z. ...h.....z.r., b.v.r .r .h. kr...ch. l...r..... .b.r.b.. A..... b...h. ... G...hr, A.r....r
v.r...r.. w.r..

<....r....>

- D.r A..h.....z.r.....rv.r SSL-Z.r...k.. ..
- D.. C..... SSL-Z.r...k.. .r....:
 - D.r S.rv.r.... .. Z.r...k..r... w.r....
 - D.r A.....r ... Z.r...k...r... w.r....
 - D.. CA v.. C..... ... v.r.r.....w.r...h.. w.r....

</....>

[search?q=..c....%3A.....r%26.....r&btnl=lucky](#)

Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“**: mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.

Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!

¹⁾

IEEE 802.1X definiert den generellen Aufbau einer Authentifizierung und Autorisierung von Clients in IEEE 802-Netzen, definiert das Protokoll EAPoL (Extensible Authentication Protocol over LAN) und empfiehlt den Einsatz von RADIUS. Deshalb wird der Enterprise Mode auch häufig WPA(2)-EAPoL, WPA(2)-EAP, WPA(2)-RADIUS oder WPA(2)-802.1X genannt.

²⁾

EAPoL war ursprünglich nur für Ethernet-LAN gedacht, wurde aber mit seiner Revision des Standards 2004 auf einen ganz anderen LAN-Technologie (unter anderem auf WLAN) ausgeweitet.