

# Verschlüsselung und Authentifizierung

G\_76341-A

Beim HG 76341 lassen sich folgende Verschlüsselungsverfahren nutzen:

1. WEP 64bit
2. WEP 128bit
3. WPA (TKIP) mit PSK
4. WPA2 (AES) mit PSK 802.11i

Die Authentifizierung kann über 802.1x vorgenommen werden. Die Authentifizierung erfolgt über die Angabe eines Benutzers mit einem Passwort. Zur Absicherung kann ein Server-Zertifikat im HG 76341 abgelegt werden. Die Methoden TLS und TTLS benötigen ein Client-Zertifikat und einen Client-Key. Diese werden ebenfalls im HG 76341 abgelegt.

Generell ist zu sagen, dass die Anmeldeprozedur des HG 76341 beim AP länger dauert, je komplexer das Verfahren ist.

Die WEP-Verschlüsselung ohne Authentifizierung ist dabei die einfachste aber auch unsicherste Methode.

WPA/TKIP oder WPA/AES ist sicherlich schon aufwändiger aber immer noch recht schnell durchzuführen.

Aufwändige 802.1x-Methoden erfordern den Austausch vieler Datenpakete mit anschließender aufwändiger Berechnung von Schlüsselmaterial. Die Zeit für eine Anmeldung bei einem AP beträgt ca. 0,5 Sekunden kann aber auch länger dauern, wenn die Anmeldeprozedur durch Übertragungsfehler gestört wird. Diese Prozedur wird bei jedem AP-Wechsel von neuem durchgeführt.

802.1x kann bei stationären Anwendungen problemlos eingesetzt werden. Bei einer mobilen Anwendung sollte berücksichtigt werden, dass während des Roamings die Verbindung für einige Zeit (min. ca. 0,5 Sekunden) unterbrochen sein kann.

## Verschlüsselungsverfahren

Methode	WEP <sup>a</sup>	WPA(2) <sup>b</sup>	User	Passw.	Server-Zert.	Client-Zert.	Client-Key
EAP-PEAP	✓	✓	✓	✓	Optional	–	–
EAP-TTLS	✓	✓	✓	✓	Optional	✓	✓
EAP-TLS	✓	✓	✓	–	Optional	✓	✓
LEAP	✓	✓	✓	✓	–	–	–

a. Bei aktiviertem 802.1x wird kein WEP-Key angegeben.

b. Bei aktiviertem 802.1x wird kein PSK angegeben.

**GÖTTING**