


|                    |  |                |  |  |
|--------------------|--|----------------|--|--|
| <b>Lernfeld 3</b>  | <b>WLAN - Sicherheit und Authentifizierung</b> |                |  |  |
| Name: Maixm Göring | Datum: 11.03.2025                              | Klasse: FI-A46 | Blatt Nr.: 2/4   |  |

### Thema: „WLAN-Sicherheit und Authentifizierung“

#### Fragen/Aufgaben?

- Beschreiben Sie in Stichworten die Verfahren WPA2 und WPA3?
- Erklären Sie den Unterschied zwischen WPA2 Personal Mode und WPA2 Enterprise Mode? Welche Sicherheitslücke hat der WPA2 Personal Mode?
- Welche Bedeutung hat die Funktion WPS?
- Welche 4 WLAN-Authentifizierungs-Verfahren gibt es?  
Beschreiben Sie stichwortartig die Verfahren.

#### Internet Adressen:


[www.elektronik-kompendium.de/sites/net/1403011.htm](http://www.elektronik-kompendium.de/sites/net/1403011.htm)

[www.elektronik-kompendium.de/sites/net/1101181.htm](http://www.elektronik-kompendium.de/sites/net/1101181.htm)

#### Meine Ergebnisse:

1. Beschreiben Sie in Stichworten die Verfahren WPA2 und WPA3:
  - WPA2:
    - Standard zur Authentifizierung und Verschlüsselung von WLANs, eingeführt 2004.
    - Basierend auf dem IEEE 802.11i-Standard.
    - Verwendet das AES-basierte Verschlüsselungsverfahren CCMP.
    - Gilt als sicherer als WEP und WPA.
  - WPA3:
    - Nachfolger von WPA2, eingeführt 2018.
    - Bietet robustere Authentifizierung und stärkere Kryptografie.
    - Verwendet das SAE-Protokoll für sicheren Schlüsselaustausch.
    - Bietet individuelle Verschlüsselung für jedes Gerät.
2. Erklären Sie den Unterschied zwischen WPA2 Personal Mode und WPA2 Enterprise Mode. Welche Sicherheitslücke hat der WPA2 Personal Mode?
  - WPA2 Personal Mode (PSK):
    - Verwendet ein gemeinsames Passwort für alle Nutzer.
    - Einfach einzurichten, geeignet für kleine Netzwerke.



|     |                                |  |  |
|-----|--------------------------------|--|--|
| ITS | AD / DC<br>FS6X_02_AB_01_AD_AC | OSZ  IMT |  |
|     | Blatt Nr.: 2/6                 | Lfd. Nr.: 01   |  |

- WPA2 Enterprise Mode:
  - Verwendet individuelle Zugangsdaten (Benutzername und Passwort) für jeden Nutzer.
  - Nutzt IEEE 802.1x für die Authentifizierung.
  - Geeignet für größere Netzwerke mit Bedarf an zentraler Benutzerverwaltung.
- Sicherheitslücke im WPA2 Personal Mode:
  - Anfällig für Brute-Force-Angriffe, insbesondere bei schwachen Passwörtern.
  - Ein gemeinsames Passwort erhöht das Risiko bei dessen Kompromittierung.


### 3. Welche Bedeutung hat die Funktion WPS?

- WPS (Wi-Fi Protected Setup):
  - Erleichtert die Verbindung von Geräten mit einem WLAN-Netzwerk.
  - Bietet Methoden wie PIN-Eingabe oder Knopfdruck zur Authentifizierung.
  - Vereinfacht die Einrichtung, kann jedoch Sicherheitsrisiken bergen.

### 4. Welche 4 WLAN-Authentifizierungs-Verfahren gibt es? Beschreiben Sie stichwortartig die Verfahren.

- Open System:
  - Keine Authentifizierung erforderlich.
  - Zugang durch Kenntnis der SSID.
  - In der Regel unverschlüsselte Verbindung.
- Personal Mode (PSK/SAE):
  - Authentifizierung mittels eines gemeinsamen Passworts.
  - Einfach einzurichten, geeignet für kleine Netzwerke.
- Enterprise Mode (IEEE 802.1x):
  - Individuelle Zugangsdaten für jeden Nutzer.
  - Zentrale Verwaltung und Authentifizierung.
  - Geeignet für größere Netzwerke.
- WPS (Wi-Fi Protected Setup):
  - Vereinfachte Authentifizierung per PIN oder Knopfdruck.
  - Erleichtert die Verbindung von Geräten.
  - Kann Sicherheitsrisiken bergen.



|                    |  |                |  |  |
|--------------------|--|----------------|--|--|
| <b>Lernfeld 3</b>  | <b>WLAN - Sicherheit und Authentifizierung</b> |                | <b>OSZ</b>  <b>IMT</b> |  |
| Name: Maixm Göring | Datum: 11.03.2025                              | Klasse: FI-A46 | Blatt Nr.: 2/4   |  |

**Eventuelle zusätzlich herausgesuchte Materialien:**

Name der Daten:

Inhalt:

