

Workshop DFN Roaming/eduroam

30.11.2006

R. Paffrath, DFN-GS Berlin

- Logistik
- Überblick
- Hinführung zum Thema

- 802.11-Standard (WLAN, WiFi): 1997/9 verabschiedet/erweitert
 - Familie der 802-Standards (wie 802.3 Ethernet, 802.5 TokenRing, 802.16 (WiMAX) etc.)
 - spezifiziert u.a. Mediumzugriff (MAC-Layer), physikalische Schicht (2 Spreizspektrumverfahren über Radiowellen)
 - unterstützt den Ad-hoc- und den Infrastruktur-Modus
 - zahlreiche Erweiterungen: 802.11ab/g etc.
- Rasche Verbreitung bei 802.11b/g-Netzen durch u.a. lizenzfreie Frequenzen
- WEP (shared keys) für Verschlüsselung, Authentifizierung, Autorisierung: für Roaming ungeeignet, gilt bis heute als kompromittiert



802.1X-Standard

IEEE 802.1X: Port Authentifizierungsstandard

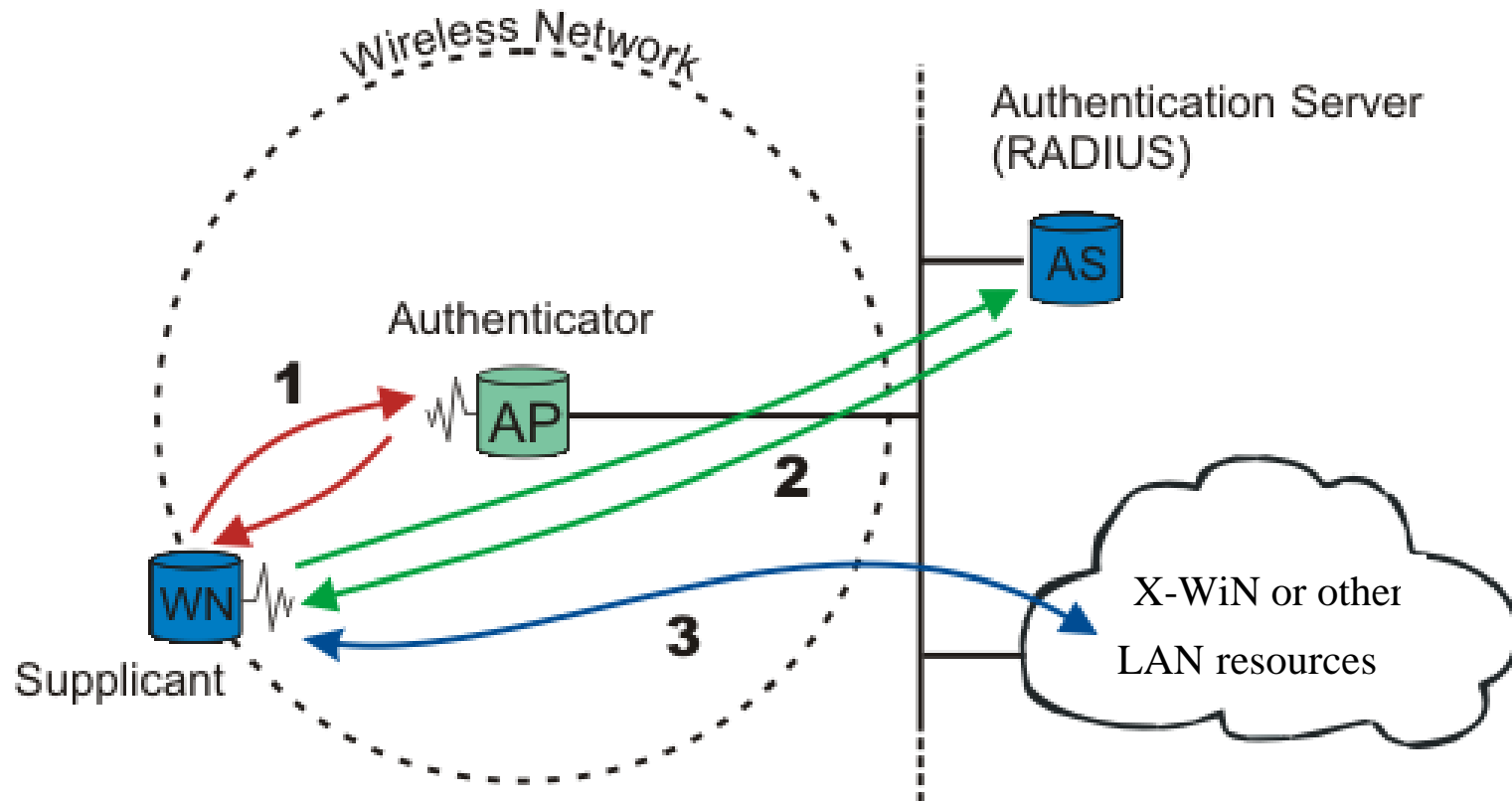
- IEEE 802.1X bedient sich u.a. der Authentifizierungsverfahren EAPoL (Extensible Authentication Protocol over LAN) und RADIUS
- IEEE 802.1X ermöglicht Austausch von EAP-Nachrichten zwischen Client, Authenticator (AP) und Authentication Server (RADIUS)
- IEEE 802.1X generiert bei erfolgreicher Authentifizierung einen dynamischen WEP Key, der in kurzen Zeitabständen erneuert werden kann

- EAPoL-Start: Client initiiert eine Authentifizierung
- EAP-Packet: Enthält gekapselte EAP-Packet-Nachrichten (EAP-Request, -Response, -Success, -Failure, ...)
- EAPoL-Logoff: Client teilt dem AP mit, dass er die Authentifizierung beenden möchte
- EAPoL-Key: Dient zum Austausch von Schlüsselinformationen zwischen Client und AP
- EAPoL-Encapsulated-ASF-Alert: Fehlermeldung

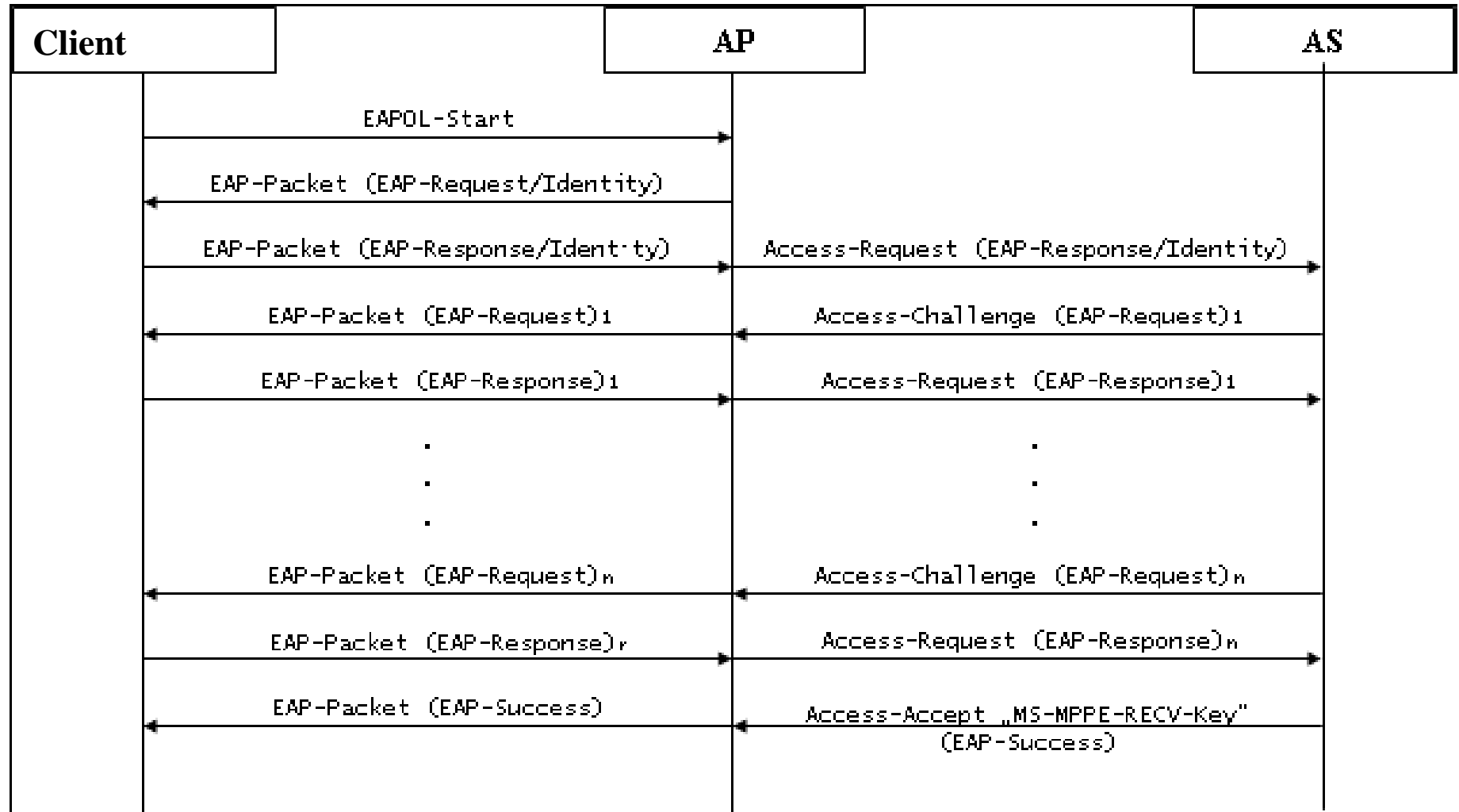
- EAP-TLS
 - erfordert eine PKI: Client und Server authentifizieren sich gegenseitig
 - Identität ist sichtbar
- EAP-TTLS/PEAP
 - Zwei-Phasen-Protokoll
 - Tunnel Verfahren: Äußere und innere Identität erforderlich, weiteres Auth-Protokoll (PEAP erfordert EAP-Method)
 - Server authentifiziert sich
 - Identität lässt sich verstecken

- Access Request: Benutzerinformationen, transportiert EAP-Response Nachrichten
- Access Challenge: AS benötigt Antwort auf ein Challenge vom Benutzer, transportiert EAP-Request-Nachrichten
- Access-Accept: gestattet Benutzer Netzzugriff, zusätzlich wird ein Sitzungsschlüssel übertragen (MS-MPPE-RECV-Key), transportiert EAP-Success-Nachrichten
- Access-Reject: Zugriff verweigert, transportiert EAP-Failure-Nachrichten

802.1X Authentifizierung



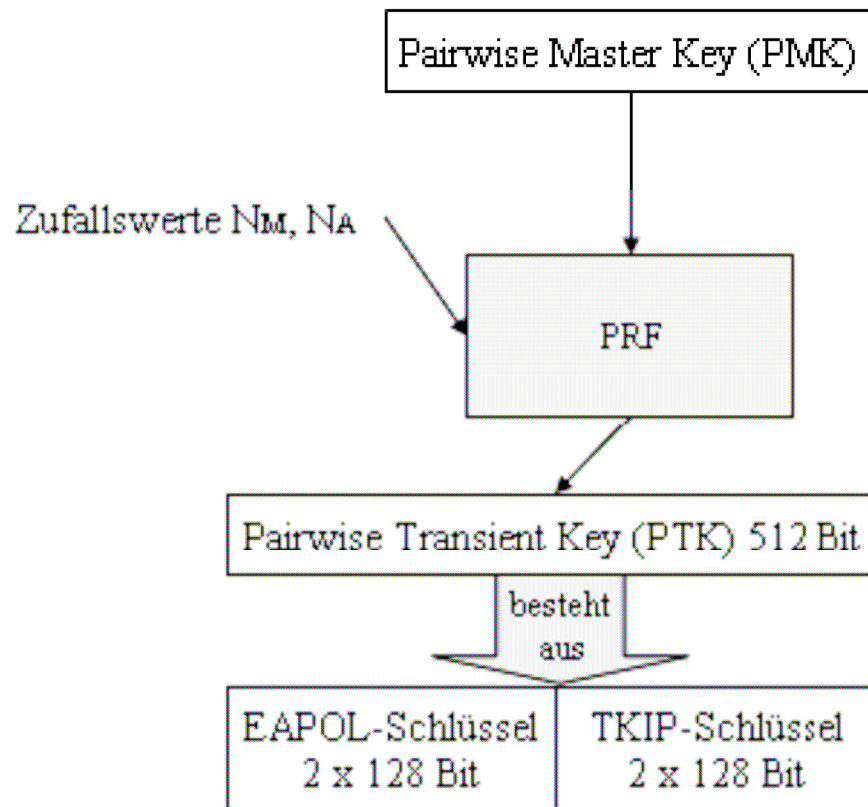
802.1X: Ablauf der Authentifizierung



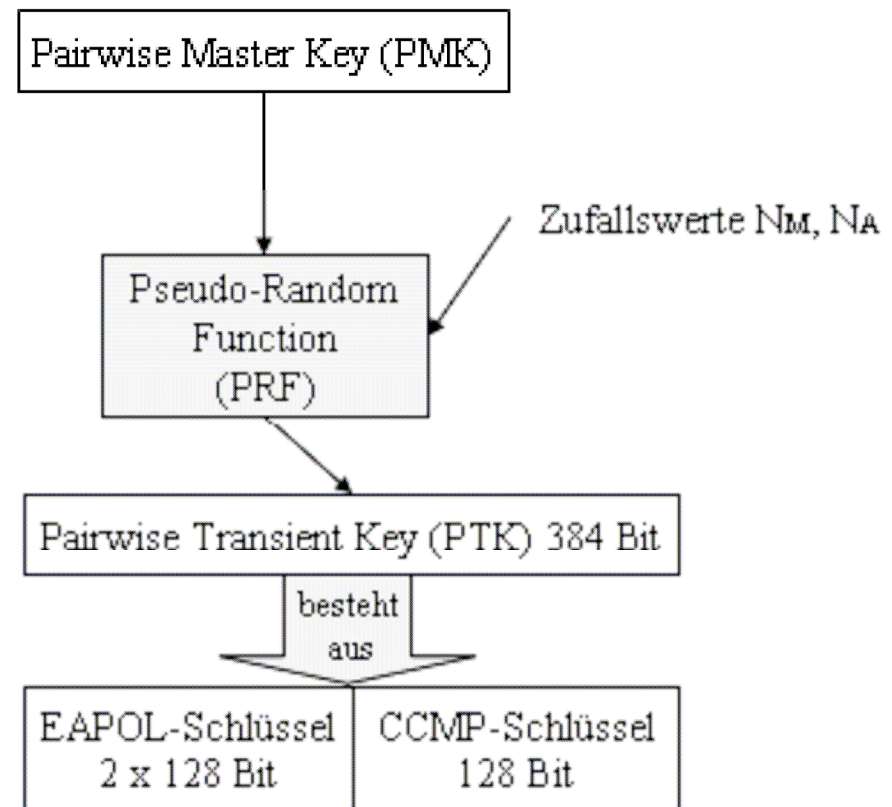
- 802.1X besitzt kein Schlüsselmanagement
- 802.11i legt eine neue Sicherheits-Infrastruktur fest (RSN): definiert TKIP, CCMP, enthält Schlüsselmanagement
- TKIP (Temporal Key Integrity Protokoll) ist kompatibel zu Geräten, die nur WEP können
- CCMP (Counter-Mode/CBC-MAC Protokoll) dient der Einhaltung der RSN: Authentizität, Vertraulichkeit, Integrität und Schutz vor Replay-Angriffen

802.11i Schlüsselmanagement (1)

Pairwise Transient Key für TKIP



Pairwise Transient Key für CCMP



4-way-handshake-Verfahren

