

# Nutzerauthentifizierung mit 802.1X

Torsten Kersting  
kersting@dfn.de

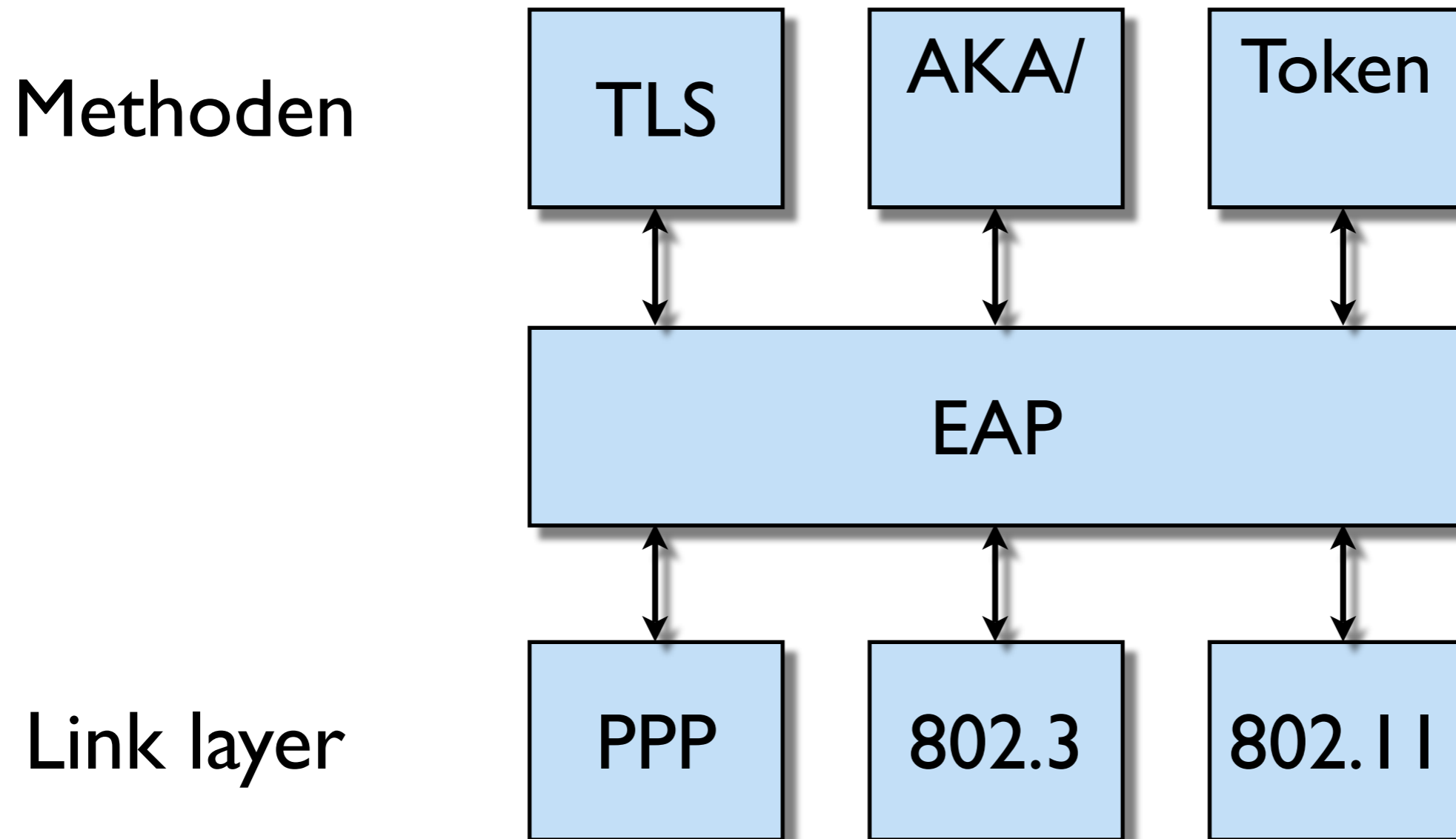
- EAP Protokoll
- EAP Methoden
- 802.1X Netzwerk Port Auth.
- 802.1X in WLAN's
- 802.11i (TKIP, CCMP, RSN)

- Design Fehler in statischem WEP
- Authentifizierung + Vertraulichkeit
- Wichtig im WLAN
- Aircrack-ptw Uni Darmstadt

- 802.1X: AuthN auf Link Layer
- AuthN für Nutzer
- Schutz vor Rogue Netzen
- Framework
- EAP = Framework Protokoll

- 802.1X basiert auf EAP
- Eine PPP Protokoll Nummer
- Viele AuthN Methoden
- Encapsulation
- Mit jedem Link Layer

# EAP Architektur



# EAP Paket Format

EAP:

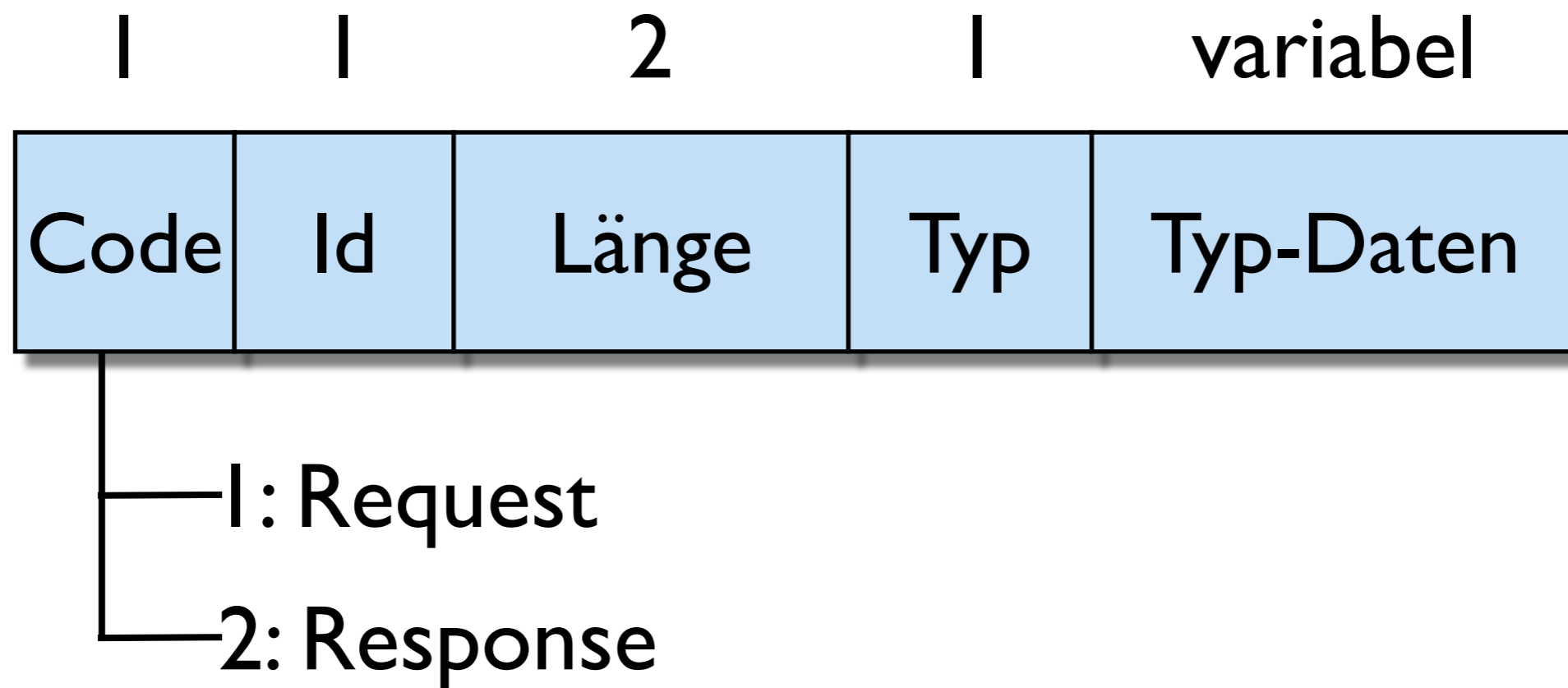


EAP über LAN:



- EAP Austausch  
zusammengesetzt aus  
Requests/Responses
- Authenticator sendet Request
- Response nur auf Anfrage
- keine unaufgeforderten  
Nachrichten

# Request/Response Pakete



- Identity als initialer Request
- Unterstützung für User Input
- Statische Konfiguration
- Response/Identity
- Vor AuthN Challenge: Nutzer existent? (Manchmal)

# Typ-Code 2: Notification

- Authenticator kann Nachricht senden
- Nicht häufig mit 802.1X
- Muss beantwortet werden
- Einfache Acks Daten-Typ Feld mit Länge 0

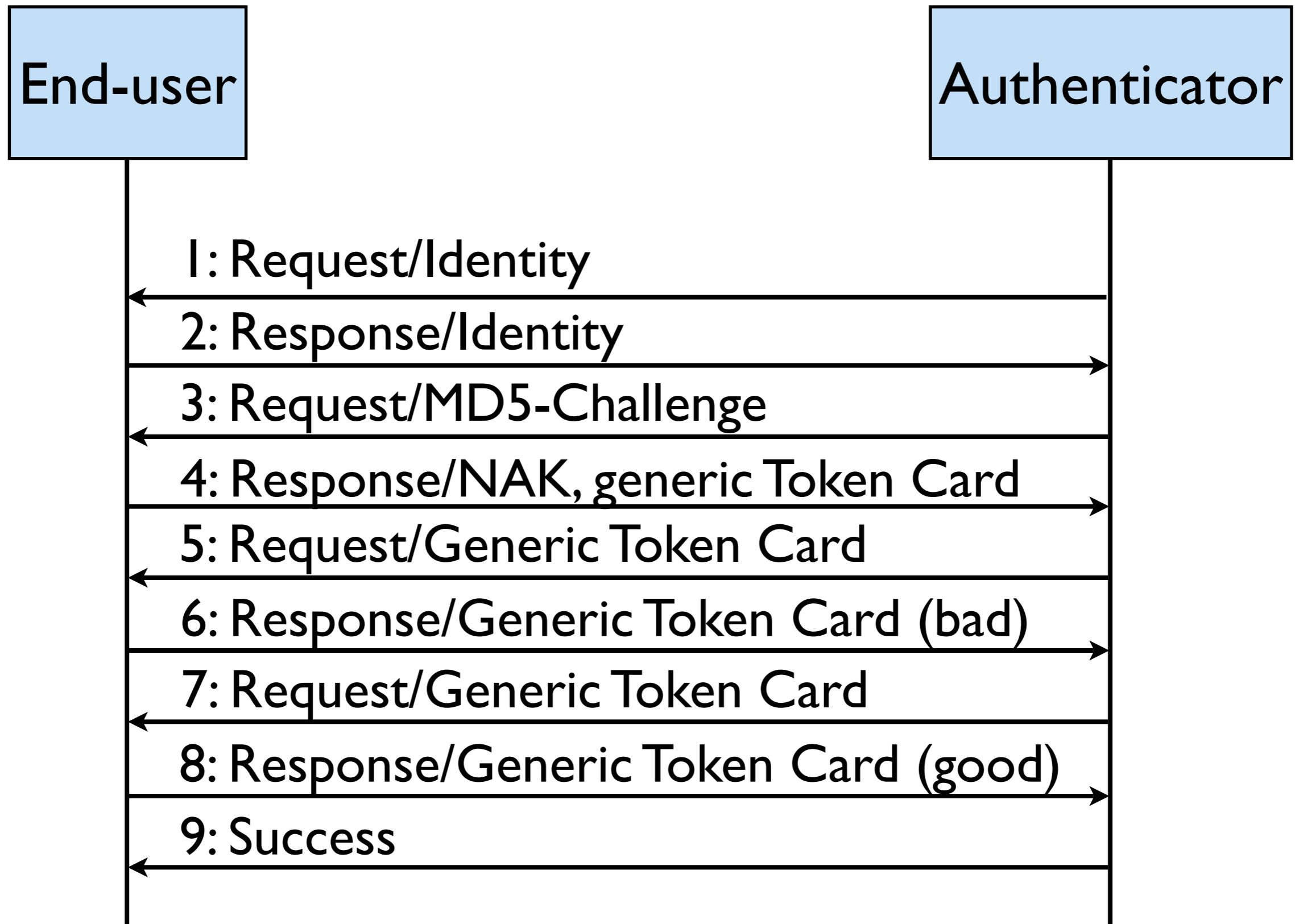
# Typ-Code 3: NAK

- Vorschlag neuer AuthN Methode
- Authenticator erstellt Challenge
- Keine Unterstützung für die AuthN Methode -> NAK
- Typ-Daten Feld 1 Byte

# EAP AuthN Methoden

Typ Code	AuthN Protokoll	Beschreibung
4	MD5 Challenge	CHAP-ähnliche authentifizierung in EAP
6	GTC	Zur Benutzung mit Token Karten wie RSA SecurID
13	EAP-TLS	Gegenseitige Authentifizierung mit digitalen Zertifikaten
21	TTLS	Getunneltes TLS; schützt schwächere authentifizierungs Methoden durch TLS Verschlüsselung
25	PEAP	Protected EAP; schützt schwächere EAP Methoden durch TLS Verschlüsselung
18	EAP-SIM	AuthN durch Subscriber Id Module
29	MS-CHAP-V2	MS verschlüsselte Passwort Authentifikation

# Beispiel EAP Austausch

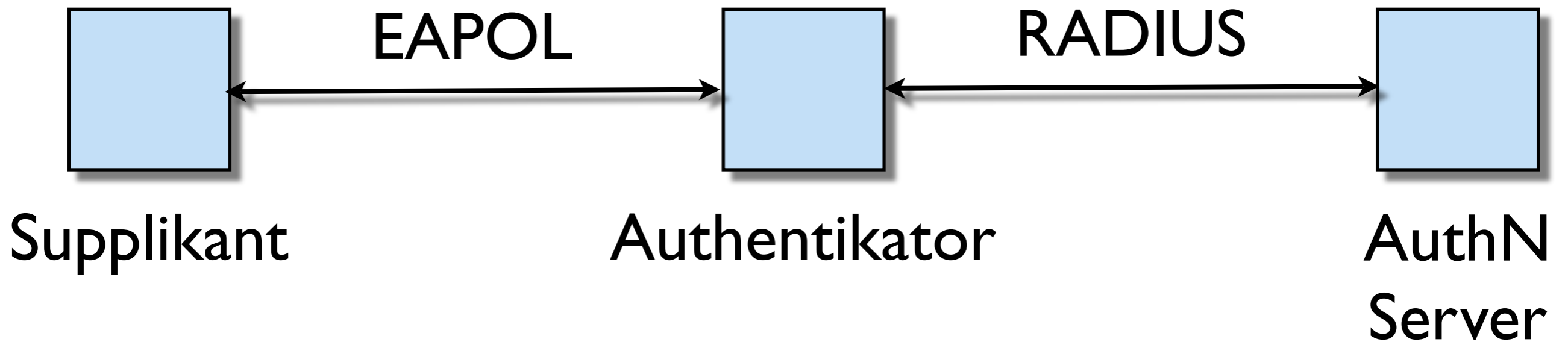


- Schutz der Nutzer Credentials
- Gegenseitige AuthN
- Schlüsselableitung

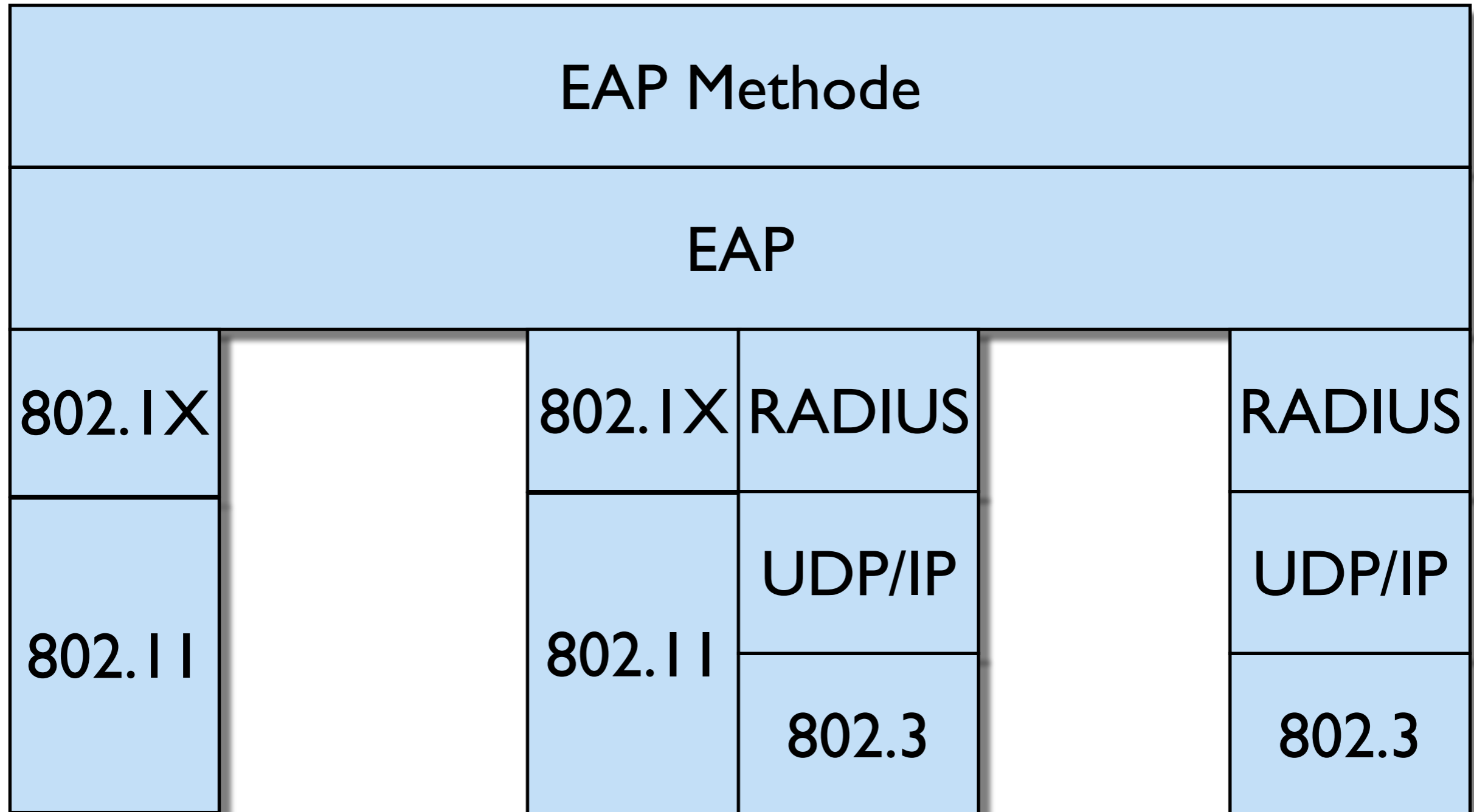
- Design gegen Abhören
- Bietet gegenseitige AuthN
- starke AuthN durch Zertifikate
- Erfüllt alle drei WLAN Anforderungen
- Nachteil: erfordert PKI

- Wiederverwendung vorhandener AuthN Systeme
- Beide zuerst TLS Tunnel
- Tunnel verschlüsselt älteres AuthN Protokoll
- TTLS mit AVPs | PEAP mit zweitem EAP Austausch

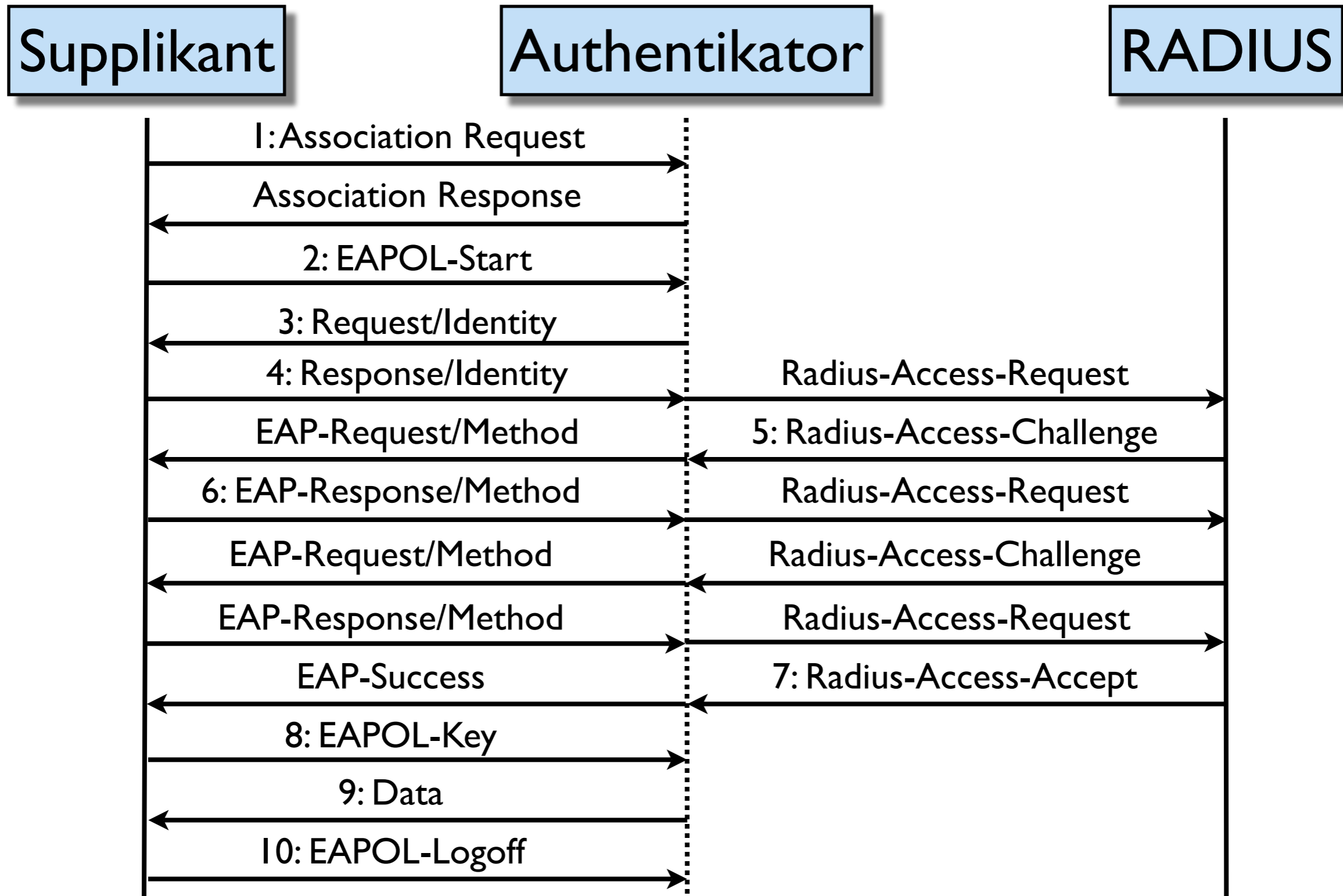
# 802.1X Aufbau



# 802.1X Architektur



# 802.1X Ablauf



- EAPOL-Key Frame
- Schlüsselaustausch nur nach erfolgreicher AuthN
- Periodische Updates möglich

- Vertraulichkeit?
- Zwei neue Link Layer  
Verschlüsselungsprotokolle
- TKIP
- CCMP

- Upgrade WEP-basierter Hardware
- RC4 Verschlüsselung
- Software und Firmware Upgrades
- Selbe Architektur und Operation wie WEP

- Basiert auf AES
- Blockchiffrierverfahren
- 802.11i empfiehlt 128-bit Schlüssel und 128-bit Blocks
- NSA empfiehlt 128-bit für „secret“ und 192 oder mehr für „top-secret“

- zwei Arten von Link Layer Verschlüsselungsprotokollen
- Paarweise Schlüssel
- Gruppenschlüssel
- PK aus authN Informationen
- GK zufällig

- Marketing Standard
- Verzögerung für 802.11i
- WPA = 3. Draft von 802.11i (2003)
- WPA2 = finaler Standard von 802.11i (2004)

# Fragen/Anmerkungen?

Torsten Kersting  
kersting@dfn.de

- Matthew S. Gast „802.11 Wireless Networks“ 2nd Edition, O`Reilly

Vielen Dank für die Aufmerksamkeit