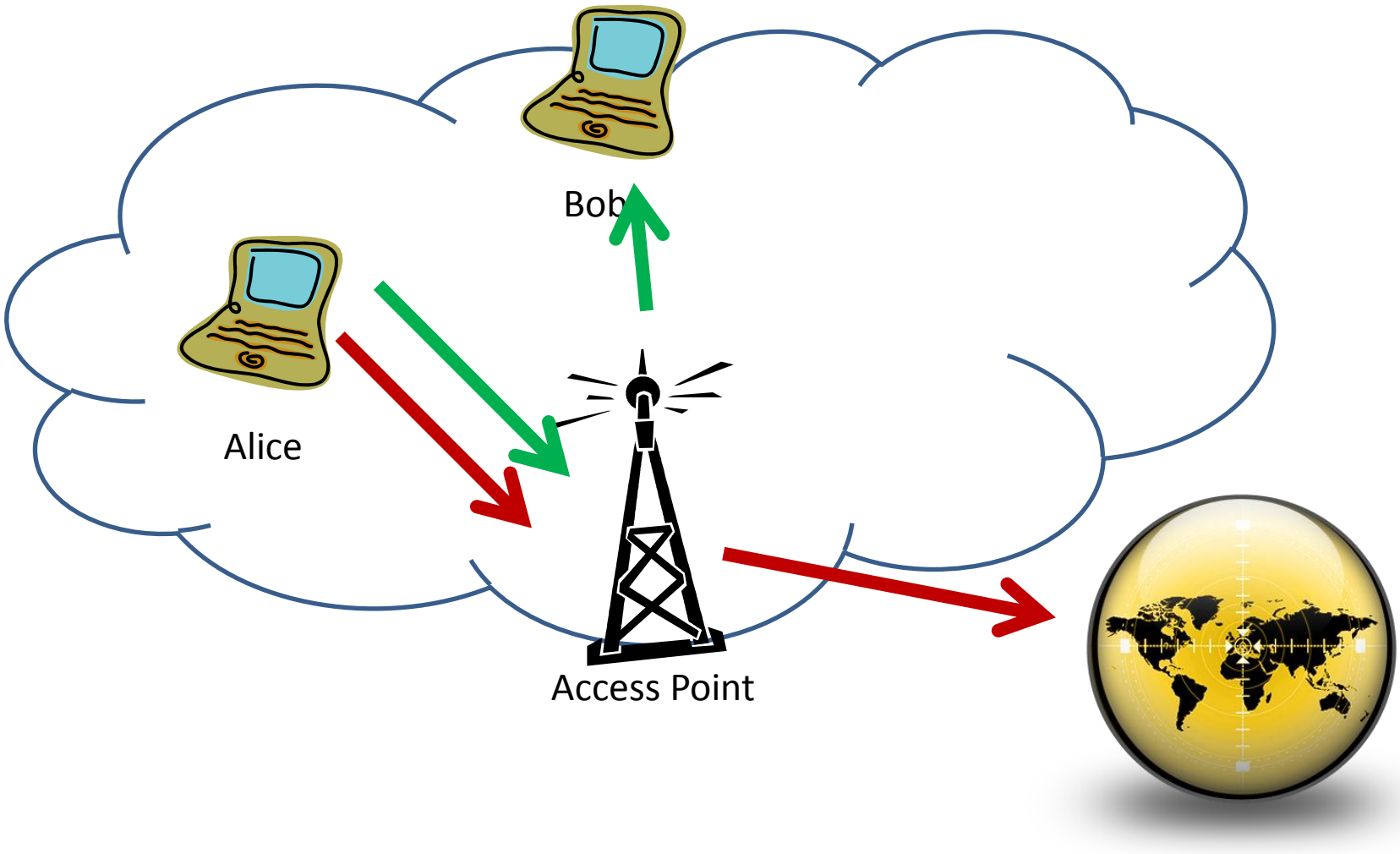
Betriebssysteme und Sicherheit – Sicherheit

WLAN Security

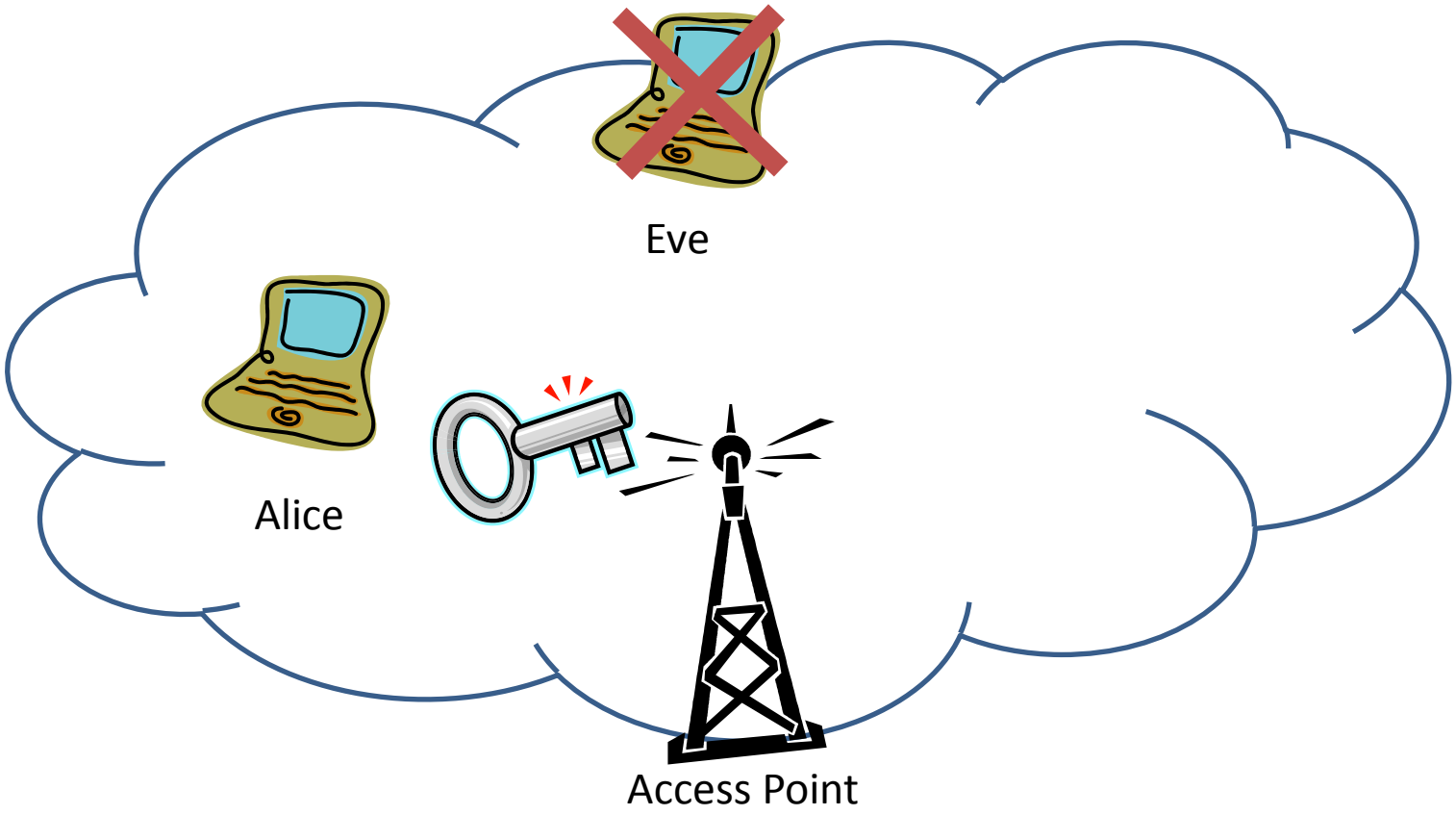
WLAN – Drahtlose Netzwerke



Sicherheitsbedenken

- Vertraulichkeit (und Integrität)
  - Sicher gegen Abhören
  - Verschlüsselung
- Zugangskontrolle
  - Sicher gegen unbefugten Zugriff
  - Authentifikation

WEP – Die Idee



WEP

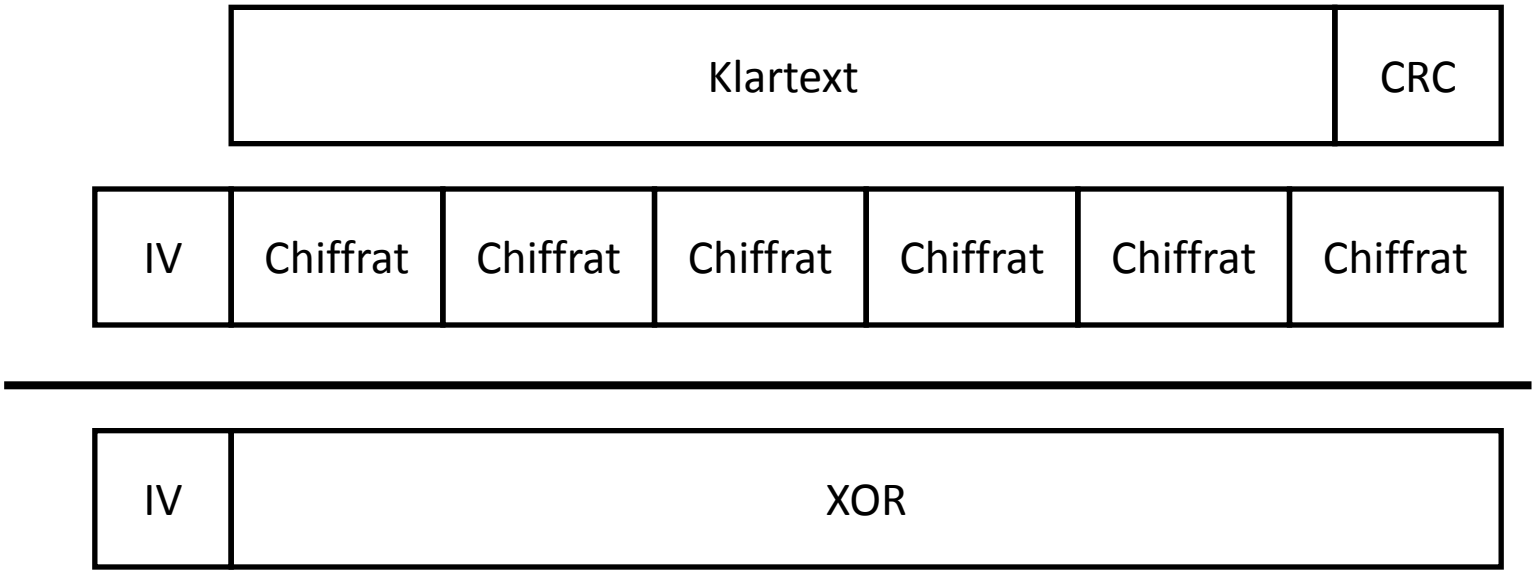
WEP = „Wired Equivalent Privacy“

- Erster Sicherheitsstandard (802.11b)
- Gemeinsamer Schlüssel aller Teilnehmer (Default)
  - Vgl. Lan Zugang
  - Nachteile:
    - Falls eine Station kompromiert wurde, müssen alle Schlüssel erneuert werden
    - Manuelle Schlüsselverteilung
    - Keine eindeutige Authentifizierung

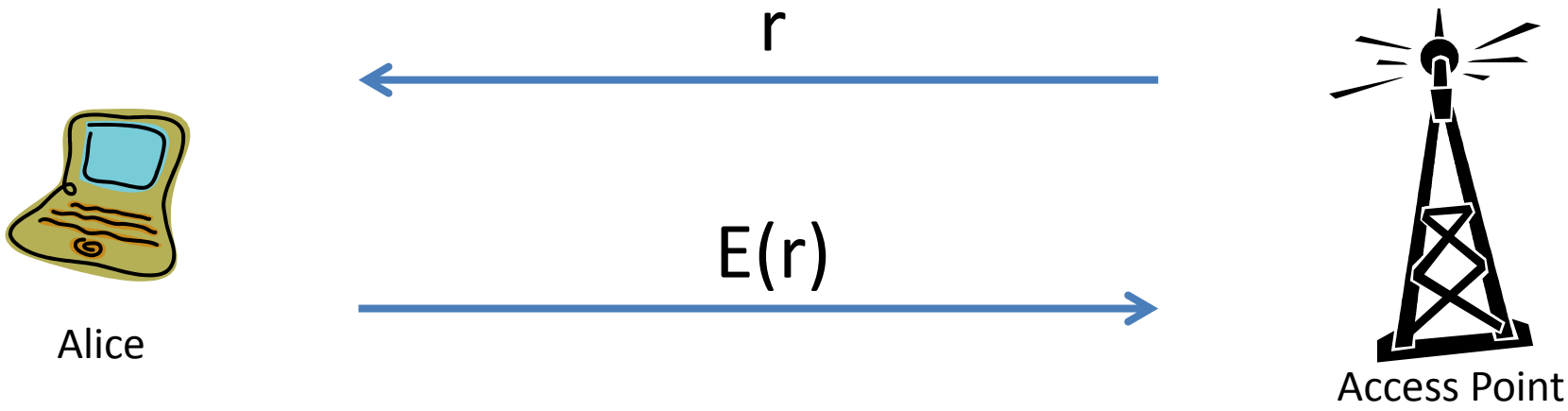
WEP – Encryption I

- Wähle IV
  - 24 Bit
- Verschlüssele IV mit fixem Schlüssel bis Paketlänge erreicht
  - RC4 (40 – default - oder 104 Bit)
- Berechne CRC32 Checksumme
- XOR Schlüssel mit Datenpaket und CRC

WEP – Encryption II



WEP - Authentication



WEP – Angriffe I

- Schlüssel ist nicht notwendig, es reicht IV (24 Bit)
  - XOR zweier Pakete mit gleichem IV kann entschlüsselt werden
  - Alle IV verbraucht nach

    2^24*1500*8 / 11*10^6 ≈ 5 Stunden
  - Birthday Attacke: 11 Minuten !
  - Viele Hersteller beginnen IV bei 0 und zählen hoch
  - Richtige CRC → Richtig entschlüsselt

WEP – Angriffe II

- Authentifikation
  - XOR zwischen challenge und response

    $r \oplus E(r) = \text{Key Stream}$
  - Impersonifikation
    - Empfange challenge r
    - Sende $r \oplus r' \oplus E(r) = E(r')$

WEP – Angriffe III

- Replay Attacken
  - IVs dürfen wieder verwendet werden
- Paketmodifikationen
  - Bitflips durch XOR
  - CRC32 ist linear

    $CRC32(x + y) = CRC32(x) + CRC32(y)$
  - Vertraulichkeit impliziert nicht Integrität

WEP – Angriffe IV

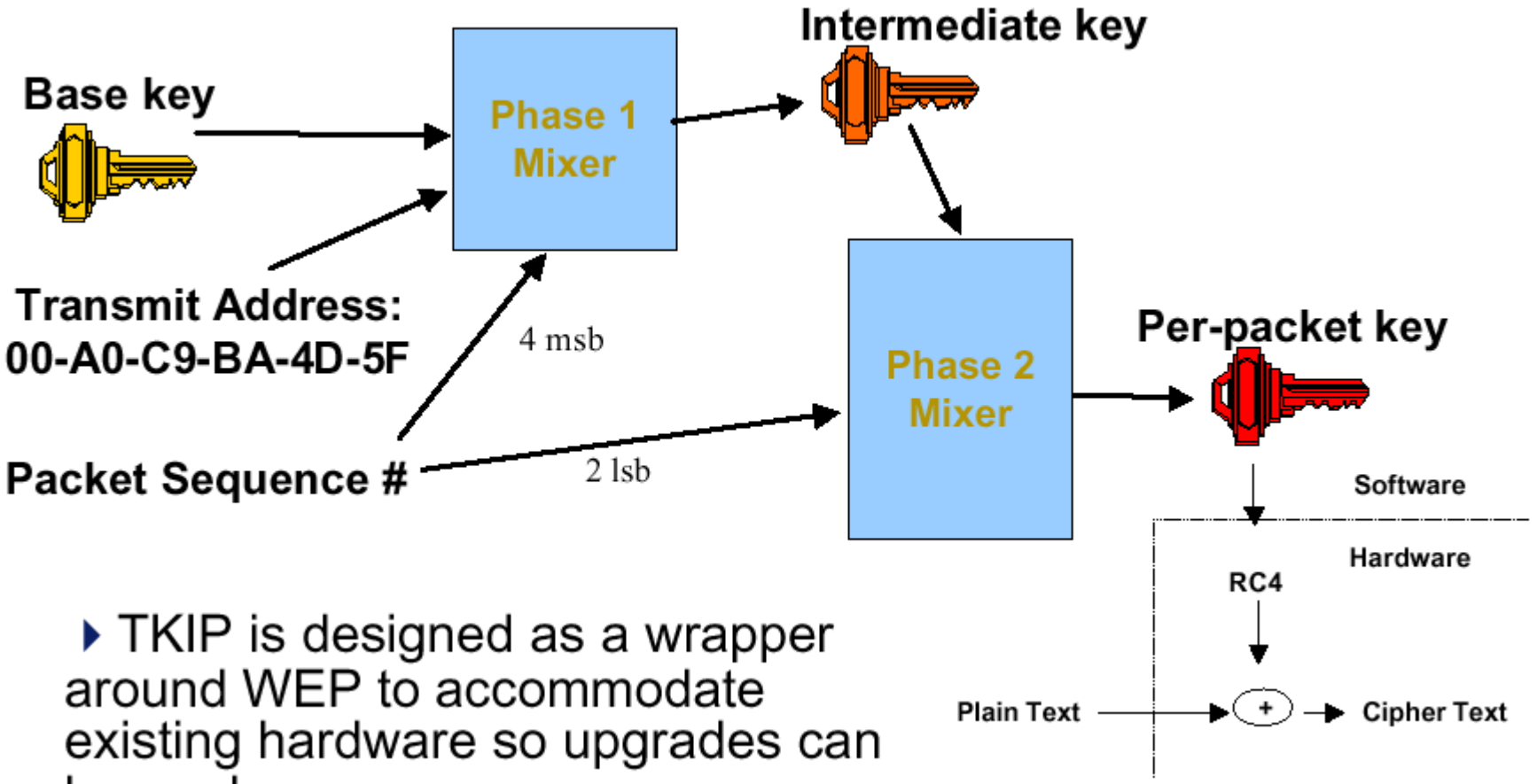
- Authentifikation
  - Keine Access Point Authentifikation
    - Angreifer kann Verkehr umleiten
  - Keine Benutzerauthentifikation
- RC4 Implementierungsfehler
  - Die ersten 256 Bytes des Key Stromes müssen verworfen werden
  - WEP tut das nicht
  - Schlüssel deutlich leichter zu brechen

Dann kam WPA ...

- Verschlüsselung: TKIP
  - Selber RC4 symmetrischer Algorithmus, aber 128 Bit Schlüssel
  - Ersetze CRC durch MAC (genannt MIC)
  - Paketnummerierung
  - Pro paket wird der Schlüssel vermischt
  - Schlüsselerneuerung

$\Rightarrow$ Jedes Paket verwendet anderen Schlüssel

WPA – Schlüsselvermischung



- TKIP is designed as a wrapper around WEP to accommodate existing hardware so upgrades can be made

Quelle: Brian Miller

WPA – Schlüsselerneuerung

- Temporärer (Basis) Schlüssel
  - 128 Bit für RC4, 64 bit for MAC
- Erneuerungsschlüssel
  - Wird zur Verschlüsselung der Schlüsselerneuerung verwendet
- Master Schlüssel
  - Wird verwendet um Erneuerungsschlüssel zu verteilen
  - An Authentifizierung gebunden

WPA – Authentifizerung

- RADIUS Server an Access Point angebunden
- IEEE 802.1X / EAP Protokoll
- Verschiedene Protokolle und Methoden
  - Client Zertifikate (EAP-TLS)
  - Benutzername / Passwort (LEAP)
  - Passwörter (EAP-PSK) – personal mode
  - etc.

WEP vs. WPA

- Gemeinsamer Schlüssel
- RC4 mit 40 Bit
- CRC32
- Gleicher Schlüssel Enc/Auth
- Nur Station Authentifikation
- Replay Angriffe
- Schlüsselverbrauch

- Benutzerabhängige Schlüssel möglich
- RC4 mit 128 Bit (HW-kompatibilität)
- MAC
- Unterschiedliche Schlüssel Enc/Auth
- Gegenseitige Authentifikation
- Paketnummerierung
- Re-keying

WPA2

- AES statt RC4
- Hardwareupgrade benötigt

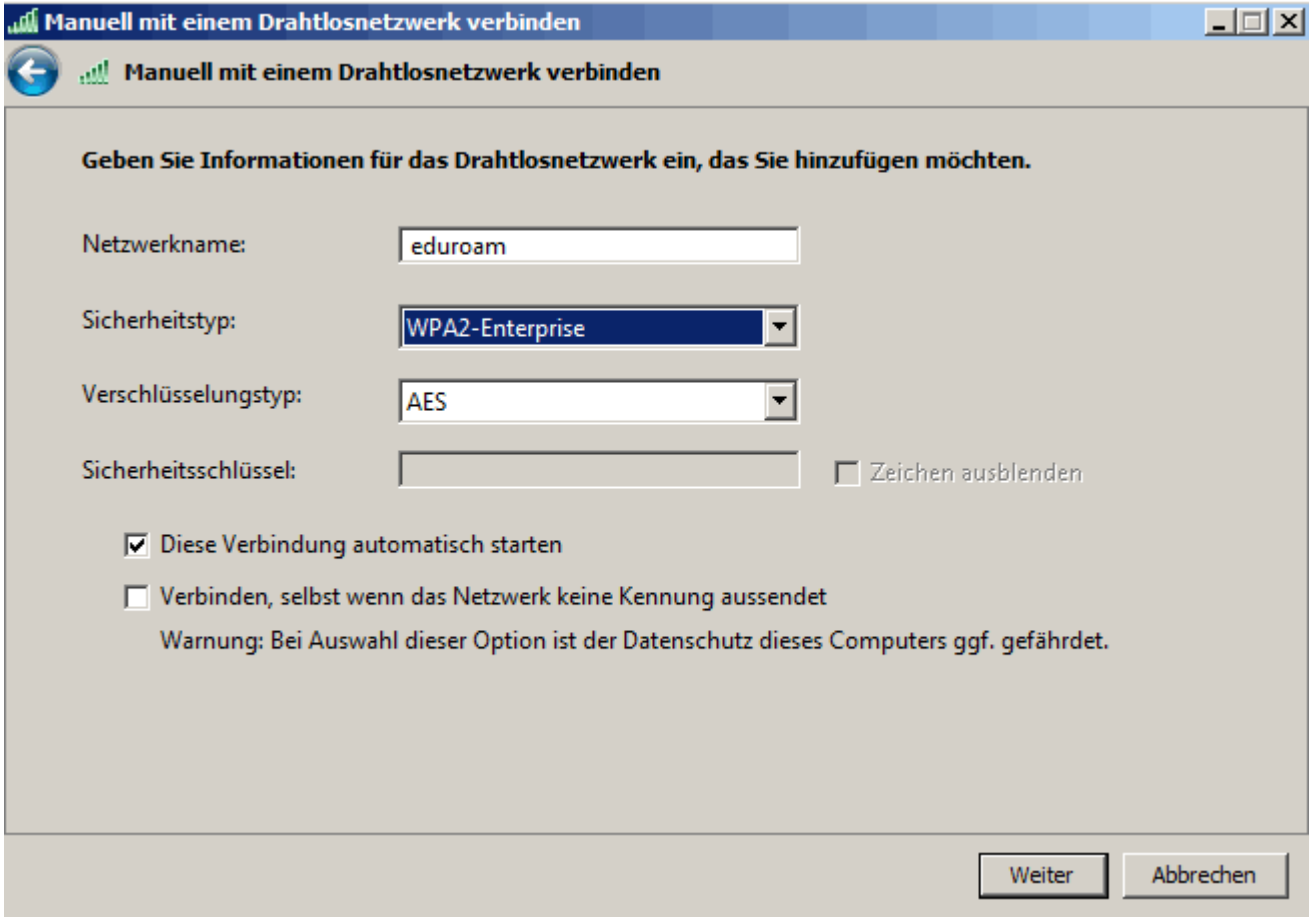
Schlussfolgerungen

- Die falsche Verwendung von Kryptographie kann fatal sein
  - Sichere Komponenten (RC4, Challenge-Response, etc.) können zu unsicherem System zusammengesetzt werden
  - Experten können hilfreich sein
- Ein gebrochenes System zu ersetzen, kann sehr schwierig sein

Anwendung

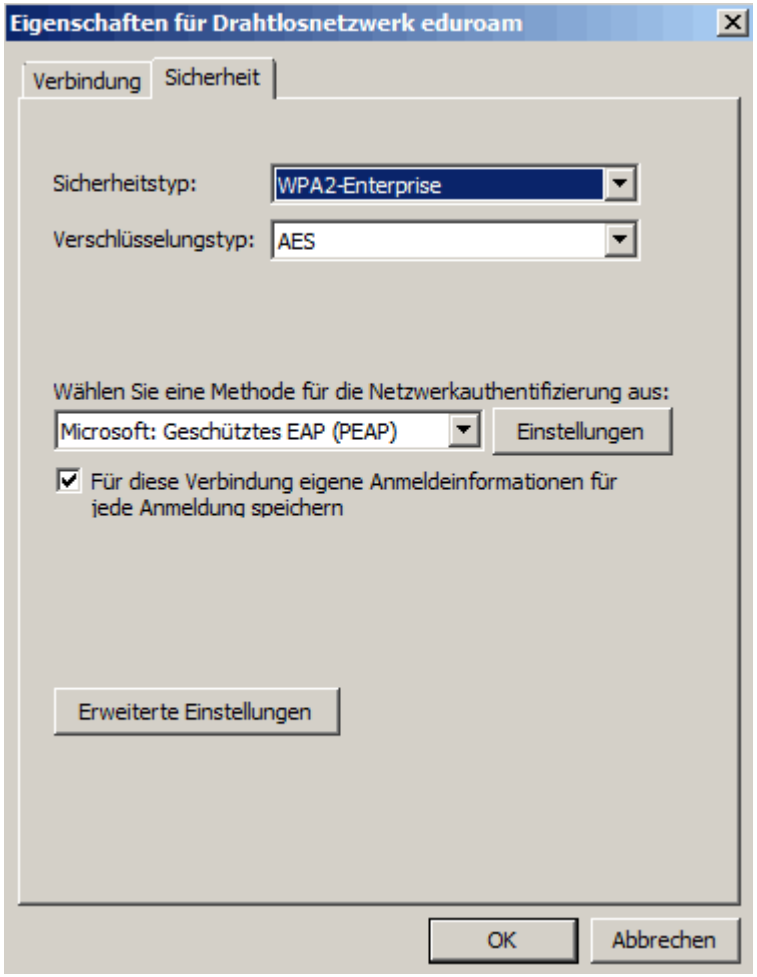
- Eduroam
  - Weltweite Verfügbarkeit
  - Abgesichert mit WPA2
  - Authentifikation
    - RADIUS für tu-dresden.de
    - ZIH-Zugang

Einrichtung – Windows I



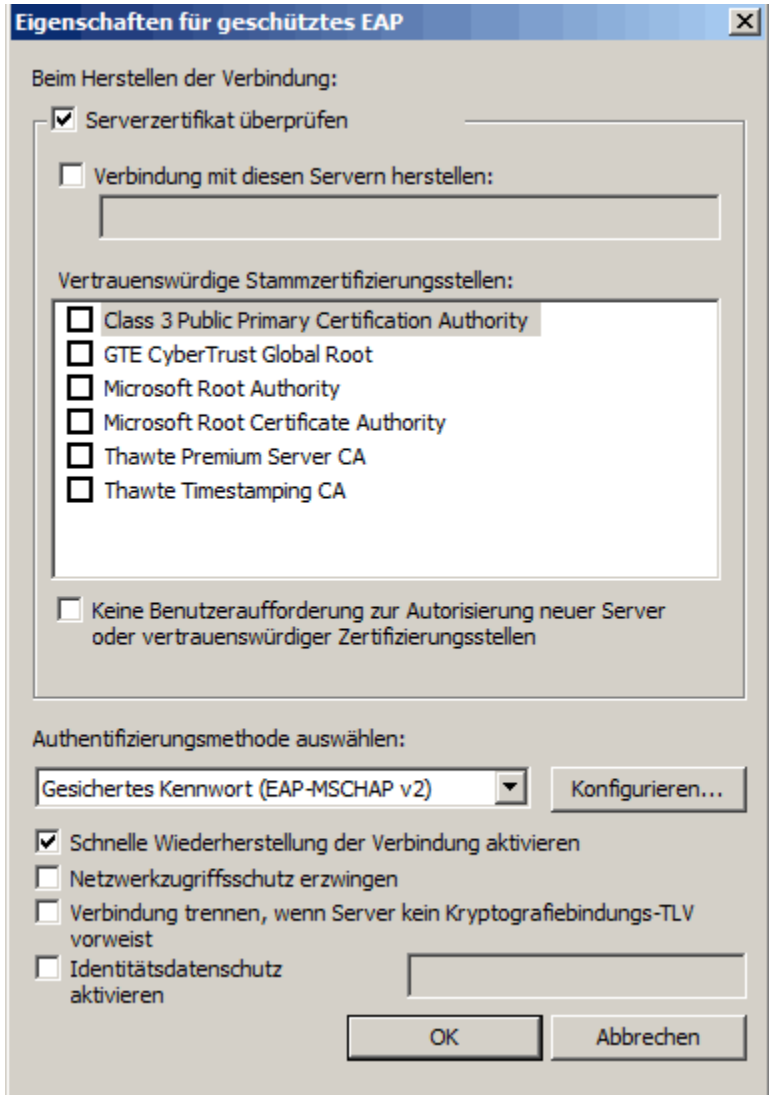
Quelle: ZIH

Einrichtung – Windows II



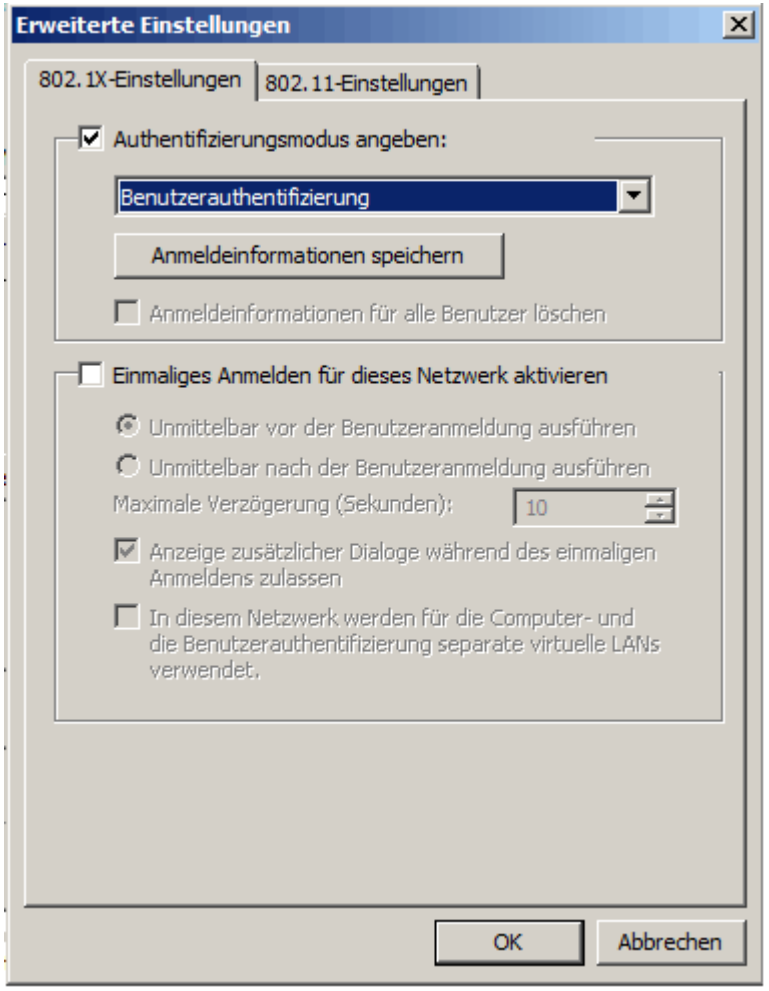
Quelle: ZIH

Einrichtung – Windows III



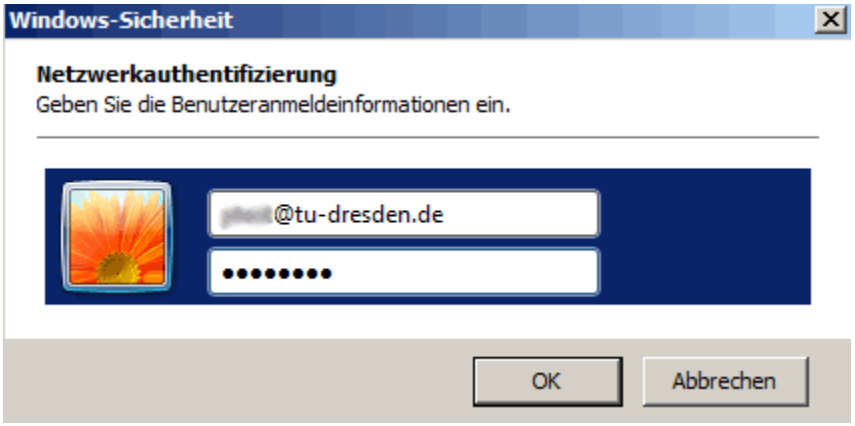
Quelle: ZIH

Einrichtung – Windows IV



Quelle: ZIH

Einrichtung – Windows V



Quelle: ZIH