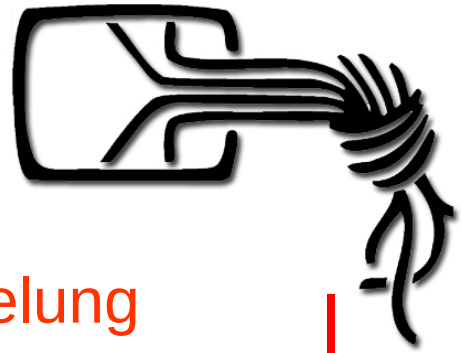
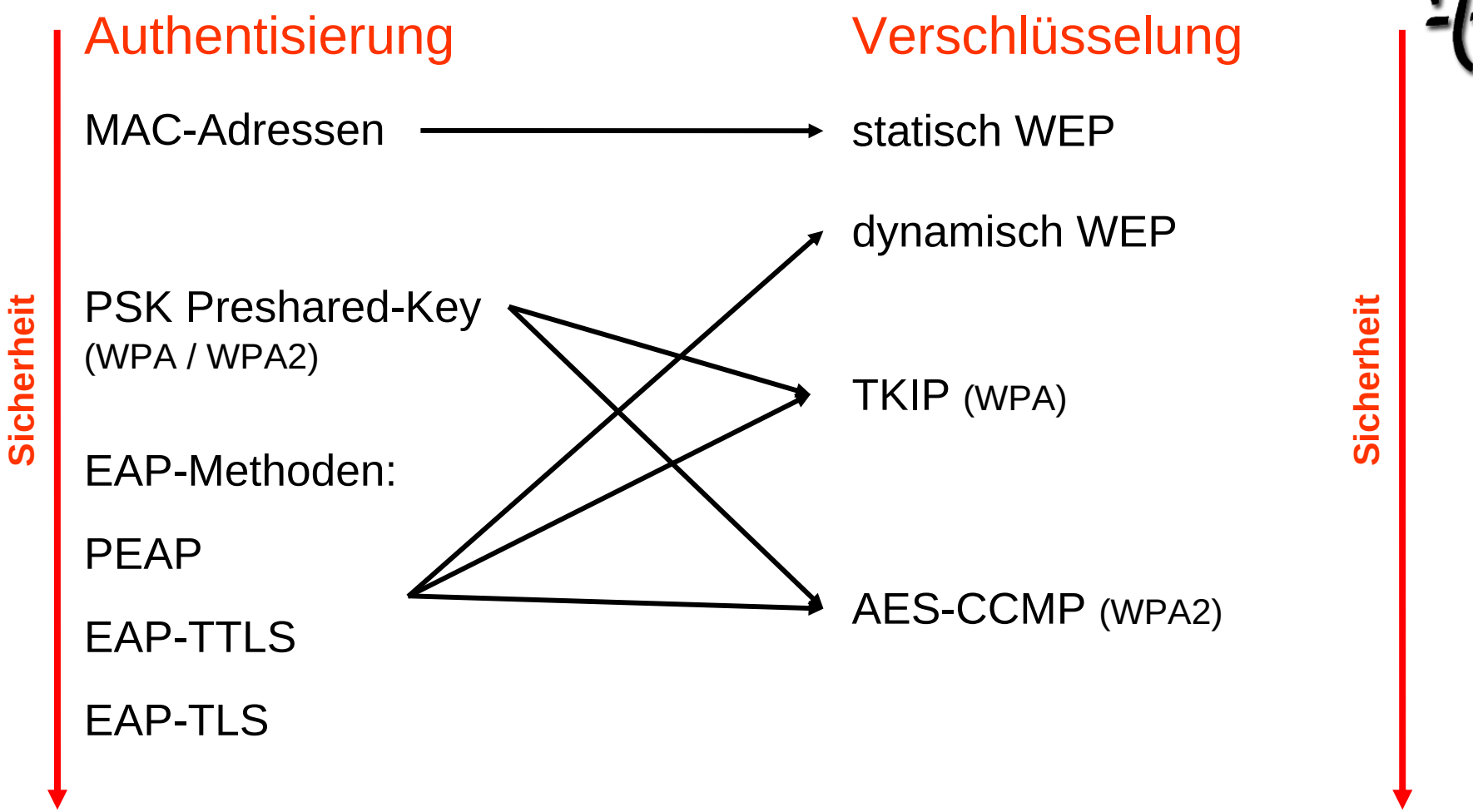
Übersicht

- Pre 802.11i Security (WEP, MAC) etc.
- Verwendung und Implementierung von 802.1x
- Ablauf einer Verbindung unter 802.1x
- Was ist TKIP (WPA)?
- Was ist AES-CCMP (WPA2)?

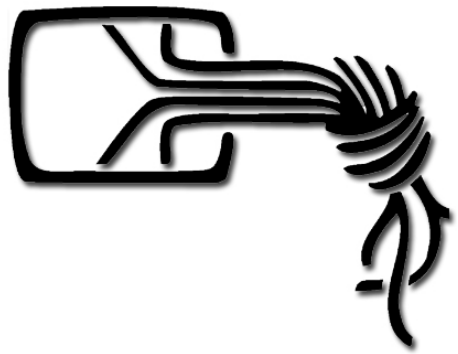
Danksagung an Fred Haisch von der Firma Proxim für die meisten Grafiken zum Thema WPA/WPA2 und Eicke Schomann von Juniper für die Radius Geschichten.

Authentisierung & Verschlüsselung vom Standpunkt der Sicherheit





Sicherheit nach IEEE 802.11



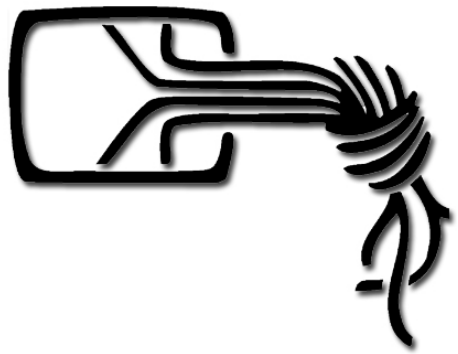
- Standard sind:
  - Authentisierung anhand der MAC-Adressen
  - Verschlüsselung nach WEP
- Properitäre Erweiterungen dazu sind:
  - Closed Wired Network
  - WEPPlus

MAC-Adressen Authentifikation

- Die vom Hersteller in die Wirelesskarte „eingebrannte“ Adresse wird vom Netzwerk bei der Anmeldung überprüft.
  - Lokale Zuganglisten im AP (für SOHO User)
  - AP fragt zentralen (RADIUS) Server (für Firmenkunden)

- Nachteil: Hält leider niemanden vom Einbruch ab!
  - Ein Hacker kann mit einem Wireless Sniffing Programm ihren Netzwerk datenaustauch überwachen und danach eine der MAC-Adressen benutzen die Sie authorisiert haben.
  - Um die MAC Adresse zu ändern braucht man:
    - Windows: http://www.klcconsulting.net/smac (15 USD)
    - Linux: ifconfig eth0 hw ether 00:02:2d:ff:00:ff (0 USD)

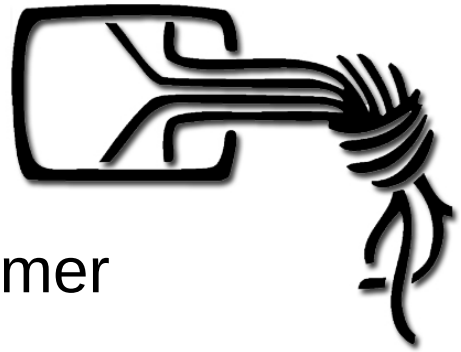
MAC Adressen „in der Luft“



```
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x4108 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x41
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 2585
    BSS Id: 00:02:2d:1b:3e:58 (Agere_1b:3e:58)
    Source address: 00:02:2d:40:64:86 (Agere_40:64:86)
    Destination address: 00:06:25:ff:95:8e (LinksysG_ff:95:8e)
    Fragment number: 0
    Sequence number: 67
    WEP parameters
        Initialization Vector: 0x0b0931
        Key: 0
        WEP ICV: 0x975415b1 (not verified)
Data (72 bytes)

0000  08 41 02 01 00 02 2d 1b 3e 58 00 02 2d 40 64 86   .A....-.>X..-@d.
0010  00 06 25 ff 95 8e 30 04 0b 09 31 00 a3 a4 fd 36   ..%...0...1....6
0020  67 fb bd aa 88 cf bf de 92 ec d7 3a 3f 74 26 83   g..........:?t&.
0030  bc cf 65 40 2d e7 41 f1 77 b6 7d a7 0f 7e 01 1e   ..e@-.A.w.}..~..
0040  d9 ef f6 92 11 28 f4 57 d6 ee 8f 99 5e bf a2 ab   .....(.W....^...
0050  e4 e1 86 84 41 5f 69 0b 0f 9f 4e e4 81 b4 2a 3e   ....A_i...N...*>
0060  26 36 ac 02 97 54 15 b1                           &6...T..
```

Verschlüsselung nach WEP



- Gruppenschlüssel mit 40 oder 104 Bit geheimer Verschlüsselungsanteil
- Öffentlich übertragener 24 Bit Initialisierungsvektor der dafür sorgt, dass Pakete gleichen Inhalts unterschiedlich verschlüsselt werden (daher Gesamt-anteil von 64/128 Bit an der Verschlüsselung)
- Jeder Teilnehmer hat den gleichen Schlüssel und kann daher auch die Pakete von anderen Teilnehmern entschlüsseln
- Schlüssel muß „geheim“ ausgetauscht werden

WEP interna

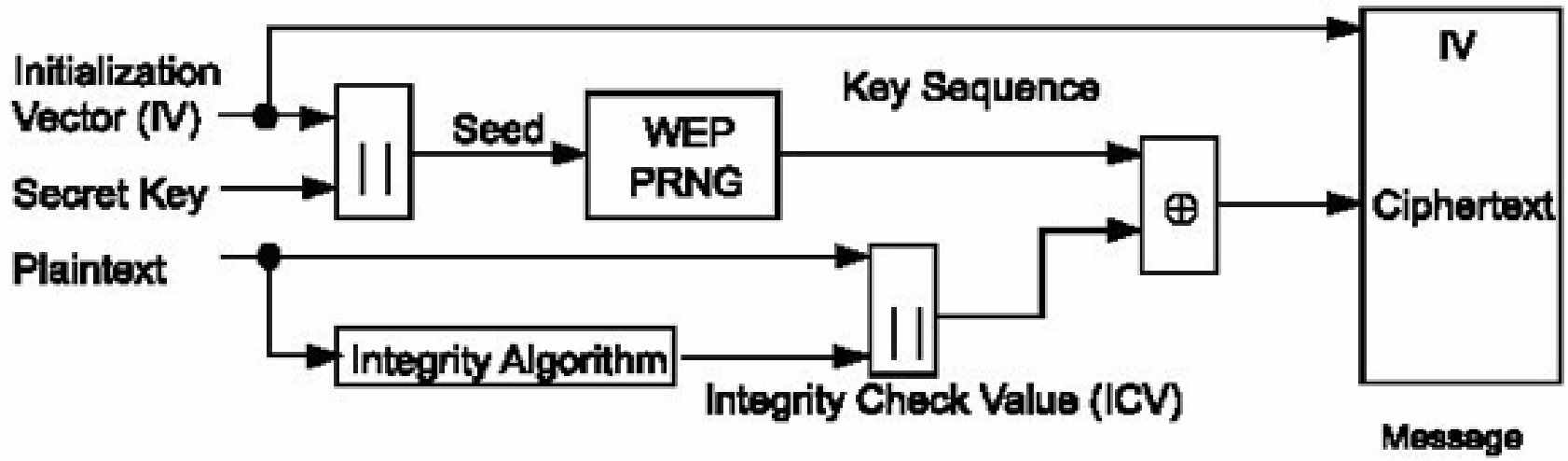
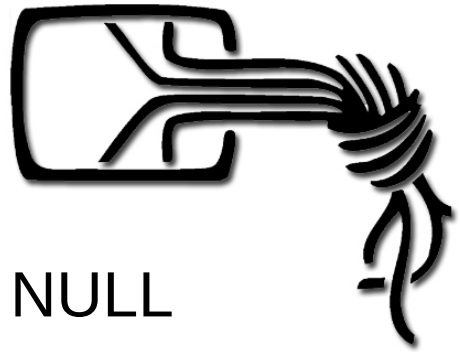


Figure 44—WEP encipherment block diagram

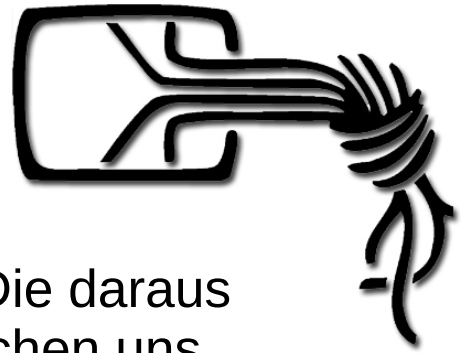
- Gruppenschlüssel und Initialisierungsvektor bilden gemeinsam Startwert für einen Zufallszahlen Generator.
- IV (24Bit Zahl) wird „normalerweise“ nach jedem Packet um 1 erhöht.
- Zufallszahlengenerator basiert auf RC4 Algorithmus um eine Kette vom mathematischen Zufall zu erzeugen.
- Der Klartext wird mit dem erzeugten Zufall mittels einem Exklusiv oder verknüpft um den Schlüsseltext zu erzeugen
- Der verwendete IV wird unverschlüsselt mit dem Schlüsseltext mitgesendet.

Geschlossenes Netz



- Im Beacon des AP wird Netzname/SSID auf NULL gesetzt.
- Hacker sieht den Netznamen nicht und kann sich nicht anmelden.
- Es kommen nur Clients rein die bei der Anmeldung den richtigen Netznamen melden.
- Properitäre Methode die aber inzwischen von den meisten Herstellern übernommen wurde.
- Macht manchmal Ärger mit Windows-XP Zeroconfiguration-Tool.
- Hacker muß nur warten bis ein Client sich am Netz anmeldet um den übertragenen Netznamen abzufangen.

Kritik und Fehler in IEEE 802.11



- Fehlende Hinzuziehung von Kryptographieexperten. Die daraus resultierenden offensichtlichen Designschwächen machen uns heute das Leben schwer.
  - Fehlende mit Einbeziehung der 802.11 Managementebene in das Sicherheitsprotokoll (Deauth-Attacken u.s.w.)
  - Authentisierung nur nach MAC-Adressen war schon 1999 bekannt schwach.
  - Um eventuell ein paar Bytes am ende des Paketes zu sparen wurde aus dem (gar nicht so schlechten) Block Verschlüsselungsalgorithmus RC4 ein Zufallszahlengenerator gebaut der leider inzwischen Probleme bereitet.
  - Keine klare Vorschrift wie mit dem IV umzugehen ist z.B.
    - Was ist sein Startwert?
    - Er **muß** leider nicht nach jedem Packet um eins erhöht werden. (ermöglicht Replay-Attacken).
  - Die Paketprüfsumme (CRC) kann unabhängig vom verschlüsselten Packet errechnet werden (nicht keyed wie HMAC bei IPSec).

Probleme mit WEP Teil1

- August 2001 die Kryptografen Fluhrer, Mantin, Shamir veröffentliche Papier das eine theoretische Schwäche aufzeigt. Der WEP Zufallszahlengenerator ist am Anfang nicht zufällig genug und „bestimmte“ IV‘s lassen leider Rückschlüsse auf den Gruppenschlüssel zu.
  - Zwei Wochen später: Erste Implementation der Attacke durch das Linux-Tool „Airsnort“. Eine erfolgreiche Attacke benötigt:
  - Ermittelte Pakete (**die Länge ist dabei egal**) in denen IV‘s einer bestimmten Sorte vorkommen. Da der IV normalerweise immer um einen pro Packet erhöht wird und nicht alle IV‘s zum erfolg führen wird für eine erfolgreiche Attacke die Anzahl von 4.000.000 Paketen benötigt.
  - Kann durch Wordbuch-Attacke beschleunigt werden wenn WEP Schlüssel nicht zufällig genug gewählt wurde.
- Einige Hersteller entwickeln Methoden á la WEP-Plus um die Kompromitierenden IV‘s zu vermeiden und WEP wieder „sicher“ zu machen.

Probleme mit WEP Teil2

- September 2004: Ein Hacker namens KoreK publiziert neue statistische Ansätze um WEP-Schlüssel zu brechen. Sofort werden neue Tools entwickelt von denen „aircrack“ das bekannteste ist. Ab jetzt gilt:

  - Ein 64Bit Schlüssel benötigt ~150.000 Pakete
  - Ein 128Bit Schlüssel benötigt ~500.000 – 1.000.000 Pakete
  - Auch Verfahren wie WEP-Plus sind nicht mehr sicher.

  Beispiel: Bei **nur** 11mbit/s Übertragungsrate werden bei einem simplen FTP-Download ca. 106MB übertragen (das ist einmal SP2 für Win-XP) was nur 5Minuten dauert! Danach könnte schon ein 64Bit Schlüssel gebrochen werden.

Passive Attacke auf WEP

- Feststellen wo es sich lohnt einzubrechen. Netstumbler / Kismet um zu sehen wo AP‘s / Netze sind. Eventuelle Verbindung mit GPS-Empfänger zur Katalogisierung.
- Mit einem Sniffer (ethereal) feststellen was für Informationen das Netz von sich aus preisgibt (z.B. MAC-Adressen von Clients die das Netz benutzen dürfen).
- Sammeln einer großen Menge an Paketen. (airodump) Braucht eventuell Zeit (je nach Netzauslastung). Kann nicht festgestellt werden da der Hacker nur lauscht.
- Auswerten mit „aircrack“
- Anwenden der gesammelten Informationen.

Aktive Attacke auf WEP Teil1

- Ziel: Schneller an die benötigte Anzahl von Paketen zu kommen wenn die Netzlast zu gering ist. Basiert meist auf Replay-Attacken. Beispiel:
  - Ein Client bucht sich in ein Netz ein (wenn er schon drin ist kann der Hacker auch eine gespoofte Deauthentisierung zum Client schicken. Dieser denkt der AP hätte ihn von Netz getrennt und loggt sich neu ein.)
  - Der Hacker zeichnet das auf und sucht nach Paketen. Am besten der ARP-Anfrage des Clients nach dem Gateway (sonst sind auch DHCP, Ping und Netbios anfragen gut geeignet).
  - Das aufgezeichnete Packet wird vom Hacker wieder und wieder abgespielt. (Es ist zwar immer der gleiche IV aber das ist leider Standartkonform!)
  - Die (eventuelle) Antwort aus dem Netz wird aber mit dem IV des AP‘s gesendet und dieser erhöht brav den IV mit jedem gesendeten Paket.

Folge: Zwar nur „halbe Kraft“ aber unabhängig von der normalen Netzlast denn die „erzeugt“ der Hacker selber.

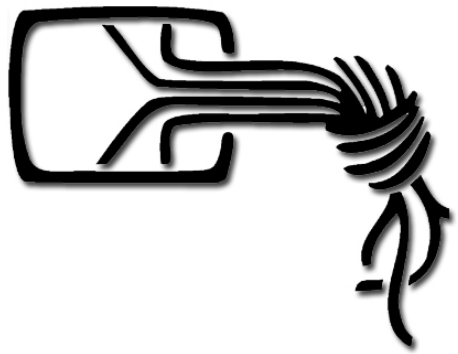
Aktive Attacke auf WEP Teil2

- Die Forscher Bittau, Handley und Lackey haben ein Papier http://www.cs.ucl.ac.uk/staff/M.Handley/papers/fragmentation.pdf veröffentlicht das eine Attacke aufzeigt die nicht auf kryptografischer Weise basiert.
- Es nutzt den Umstand das man Fragmente eines Gesammtpackets schicken kann die aber alle denselben WEP Schlüssel verwenden. Da der Anfang der Packete meist immer gleich aussieht kann man mit etwas geschick einen validen XOR Stream ermitteln den man nutzen kann um das WLAN zu nutzen und valide Packte einzuschleusen. z.B. für ARP-Replay
- Benötigt die zuhilfename eines PC im Internet der als “Reflektor” dient. (Angriffsdaten müssen extern gesammelt werden)
- Der Proof of Concept „wesside“ braucht ca 2 Sekunden dafür. http://www.toorcon.org/2005/slides/abittau/ abittau-fragattackinpractice.tgz

Aktive Attacke auf WEP Teil3

- April 2007 Die Forscher Erik Tews, Andrei Pychkine und Ralf-Philipp Weinmann veröffendlichen ein Papier das eine weiterentwicklung (und Anwendung) einer von Andreas Klein entwickelten Theorie darstellt.
- Das Tool aircrack-ptw implementiert diese Attacke.
- Aus einem Datenstrom werden Felder die warscheinlich immer denselben Wert haben (z.B. bestimmte Felder im TCP-Header) genommen und „summiert“. Dadurch entstehen statistische Warscheinlichkeiten die den Key erraten lassen.
- Erneute drastische Senkung der benötigten Packete:
  - 40.000 für eine 50% Erfolgswarscheinlichkeit
  - 85.000 für eine 90% Erfolgswarscheinlichkeit
- Version 1 von aircrack-ptw implementiert dieses mittels ARP-Replay -> kann schon nach einer Minute zum Erfolg führen!

Extensible Authentication Protocol (EAP)

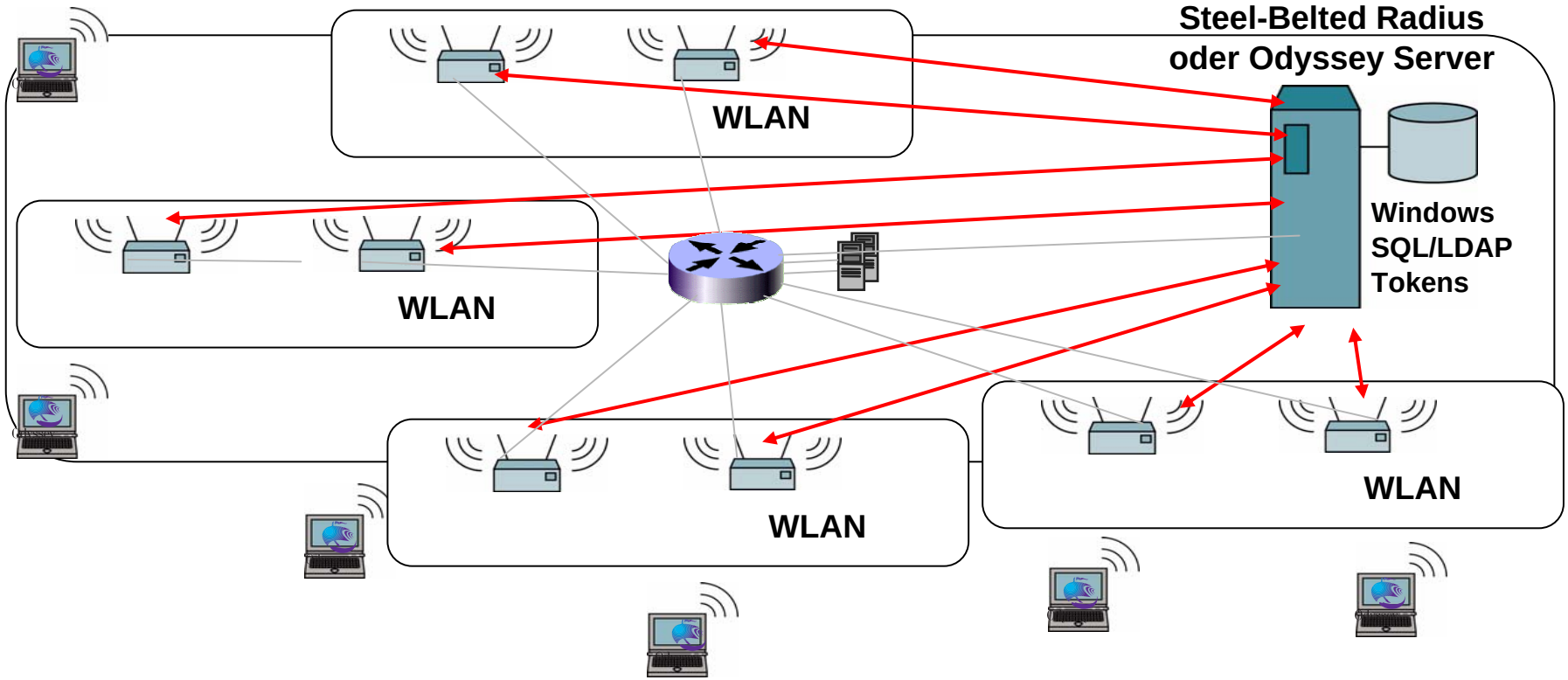


- EAP – Rahmen für unterstützte Authentisierungsmethoden
- Entwickelt um die Verhandlung der Authentisierung und dem Informationsaustausch zwischen dem Client und dem Authenticator durchzuführen
  - Ermöglicht dem RADIUS Server die Sicherheit durch Auswahl der Authentisierungsmethoden zu gewährleisten
- Die Verhandlung geschieht zwischen dem AAA Server und dem Client
  - Der RADIUS Server muss Entscheidungen treffen, und nicht auf sie reagieren
  - Access Point agiert als Übermittler zwischen dem Client und dem Authenticator

Wie arbeitet 802.1x?

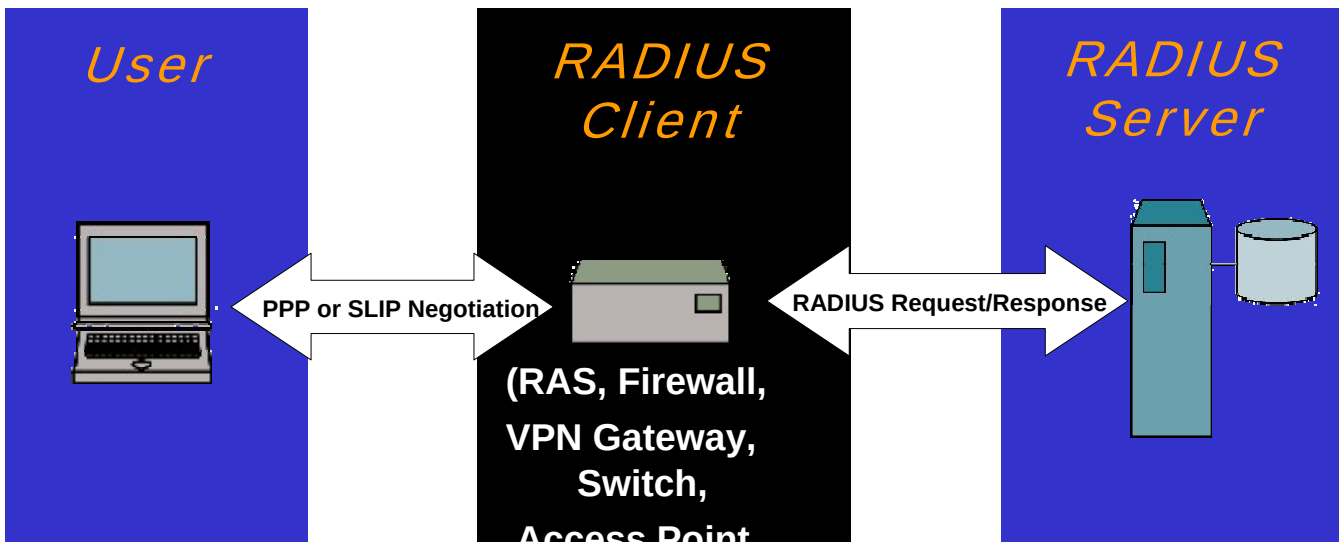
- 802.1x (Port basierende Netzwerkszugangskontrolle)
  - Bietet ein Gerüst für unterschiedliche Authentisierungmethoden (EAP-XXX)
  - Bietet ein System zur Verteilung von Schlüsseln die zur Datenverschlüsselung benutzt werden (wenn WLAN genutzt wird)
  - Kann für LAN und WLAN benutzt werden
- 802.1x definiert 3 Komponenten:
  - Supplicant
    - Ein Endnutzer der Zugang zum Netzwerk wünscht (STA, WLAN Client, PC mit Netzwerkanschluss)
  - Authenticator
    - Kontrolleinheit die den Zugriff auf das LAN verwaltet (Access Point, Layer-2 Switch)
    - Etabliert eine Datenverschlüsselung zwischen Client und ihm, wenn angefordert
  - Authentication Server (RADIUS Server)
    - Authentisiert den Endnutzer
    - Verhandelt Schlüsselmaterial mit dem Supplicant
    - Leitet das Schlüsselmaterial an den Authenticator weiter damit dieser es nutzen kann
- Port Authentication Entities (PAEs)
  - Definiert im 802.1x Standard auf Seiten des Supplicanten und Authenticator mit folgenden zwei Zuständen
    - Authorisiert (Enabled): Jemand hat vollen Zugriff auf das Netzwerk
    - Unauthorized (Disabled): Nur 802.1x die zur Anmeldung dienen werden durchgelassen

Das Netzsetup



Was ist RADIUS?

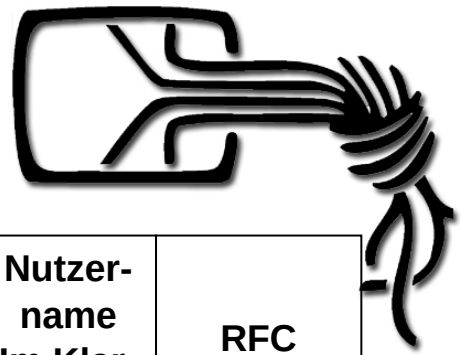
- **Steht für Remote Authentication Dial In User Service**
- **Client/Server Protokoll das Remote Access Servers in die Lage versetzt mit einem zentralen Server zu kommunizieren, und Benutzer die auf das Netzwerk zugreifen möchten Authentifizieren und Autorisieren kann**
- **Standardisierte Methode Informationen zwischen RADIUS Client und Server auszutauschen**



RADIUS AAA Services

- **Authentifizierung**
  - **‘Wer bist Du und hast du die Erlaubnis das zu tun was du anforderst?’**
  - **Passen Benutzername/Passwort zum Profil?**
- **Autorisation**
  - **‘Stehen genügend Informationen für die Verbindung zur Verfügung?’**
  - **‘Was darf der User online tun?’**
  - **User/Session-spezifische Konfiguration**
  - **Beispiele:**
    - Welche IP-Adresse wird zugewiesen?
    - Wie lang darf die Verbindung zum Internet bestehen?
- **Accounting**
  - **Protokolliert die Benutzung während der Verbindung**
  - **Sortiert, filtert, organisiert Attribute**
  - **Versendet Attribute überall hin (Logfiles, Proxy, SQL)**

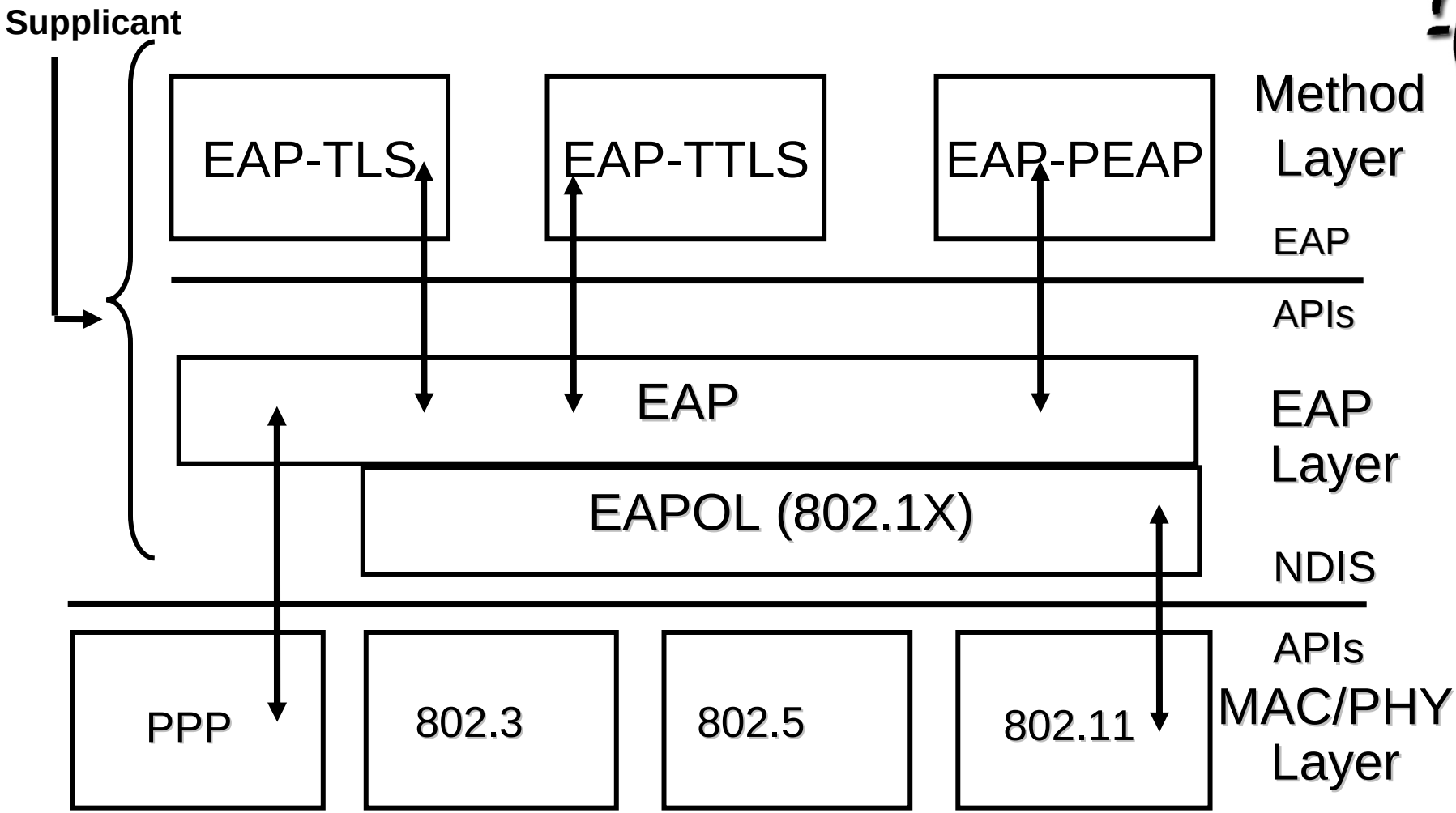
Übersicht über die gebräuchlichsten EAP-Methoden



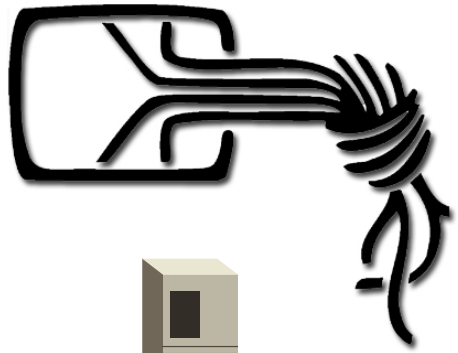
EAP Typ	Offen/ Properitär	Beider-seitige Auth	Authentisierungszertifikate		Schlüssel-gene-rierung	Nutzer-name Im Klar-Text	RFC
			Supplicant	Authenticator			
MD5	Offen	Nein	Username/Pwd	Keines	Nein	Ja	1321
TLS*	Offen	Ja	Zertifikat	Zertifikat	Ja	Ja	2716
TTLS*	Offen	Ja	Username/Pwd	Zertifikat	Ja	Nein	IETF Draft
PEAP*	Offen	Ja	Username/Pwd	Zertifikat	Ja	Nein	IETF Draft
SIM*	Offen/GSM	Ja	SIM		Ja		IETF Draft
AKA	Offen/UMTS	Ja	USIM		Ja		IETF Draft
SKE	Offen/CDMA	Ja			Ja		IETF Draft
LEAP	Properitär	Ja	Username/Pwd		Ja	Ja	

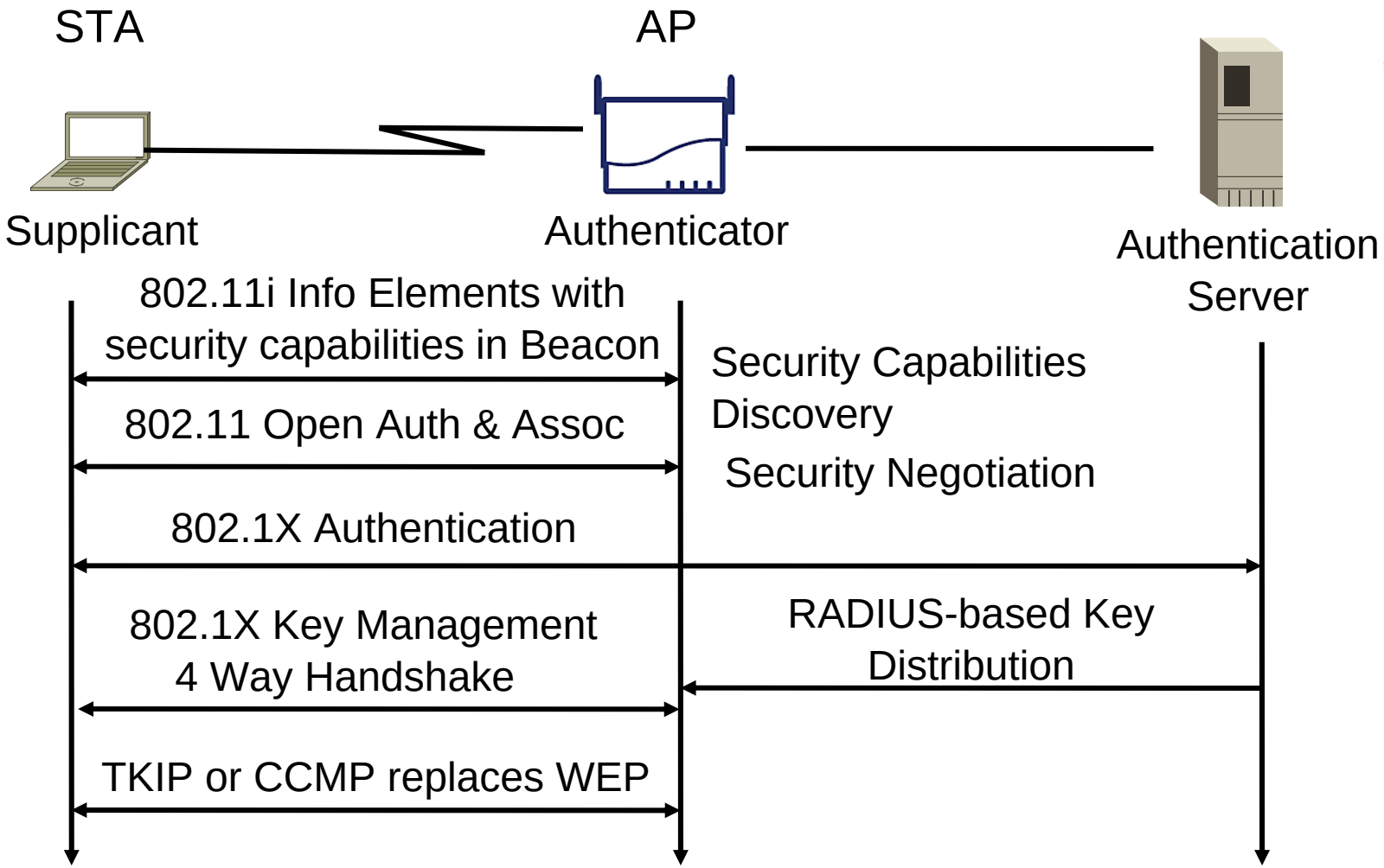
* Benutzt die Wi-Fi für die WPA/WPA2 Zertifizierungstests

Die Beziehungen zwischen EAP Methoden, EAP, 802.1X, und 802.11 und dem Netzwerk

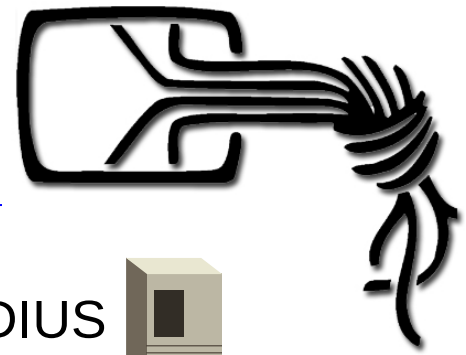


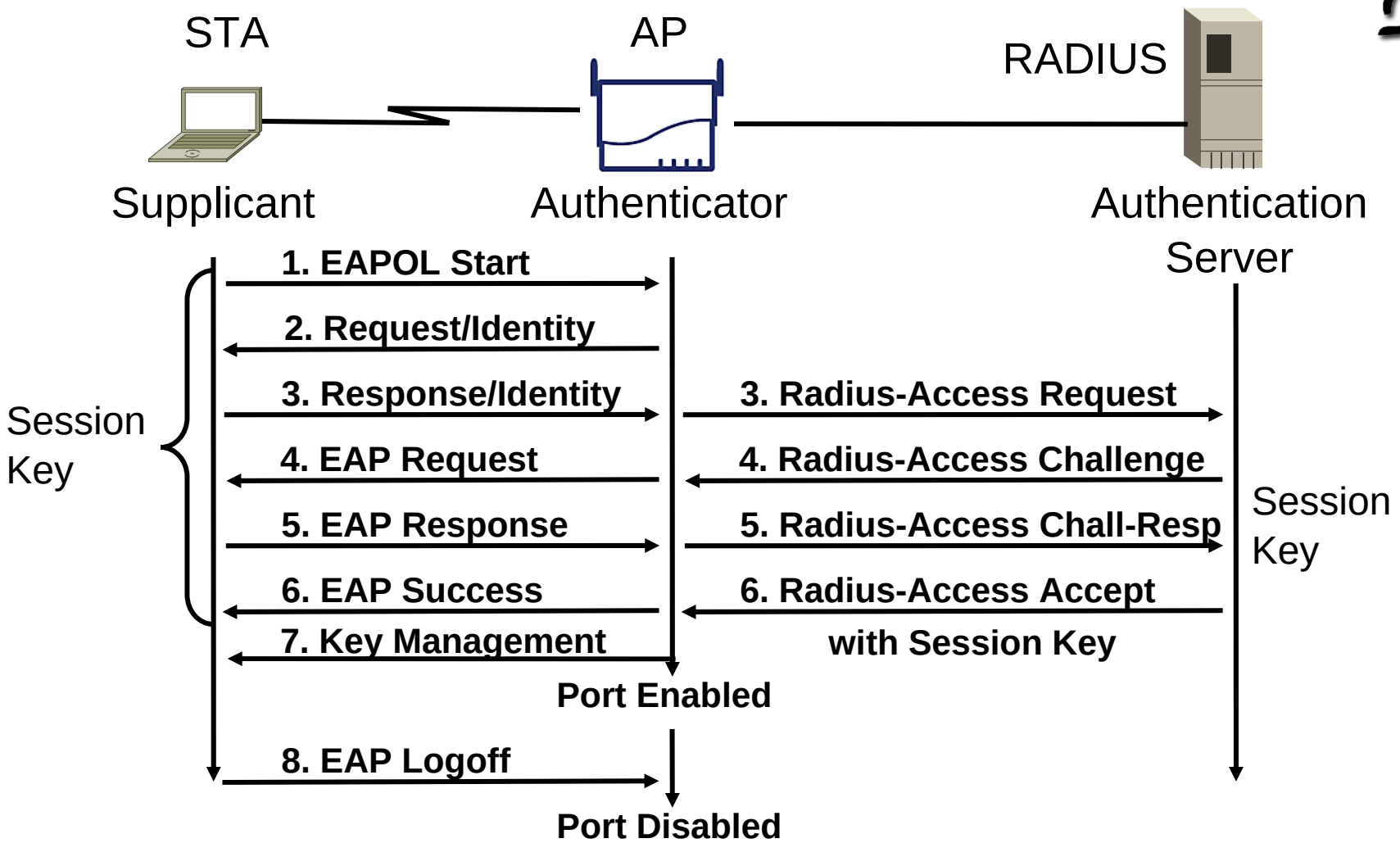
Grober Ablauf einer 801.1x Authentisierung



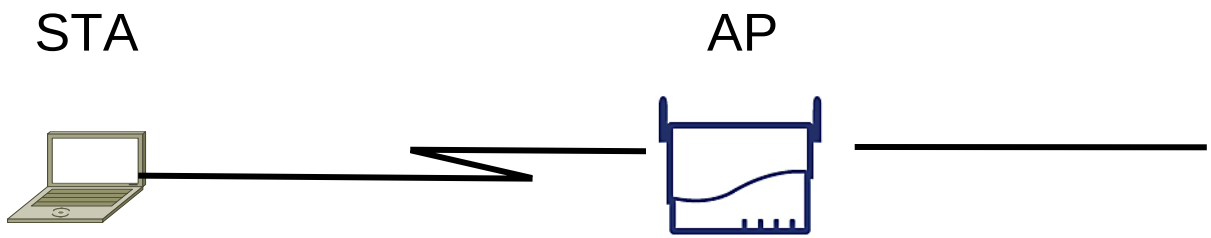


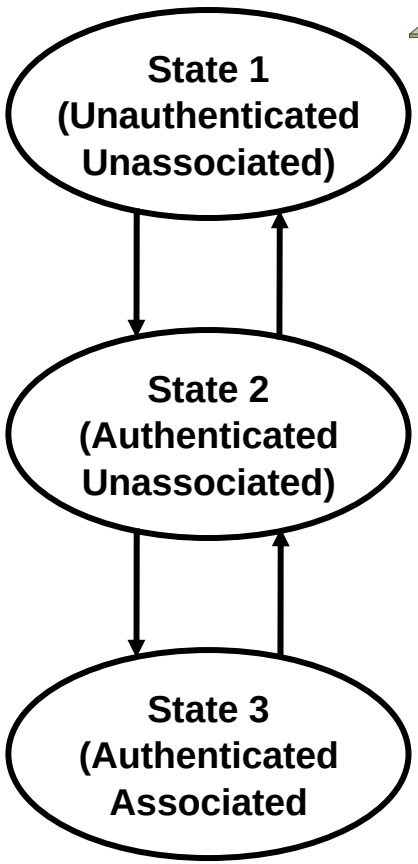
Komplette 802.1x Authentisierung

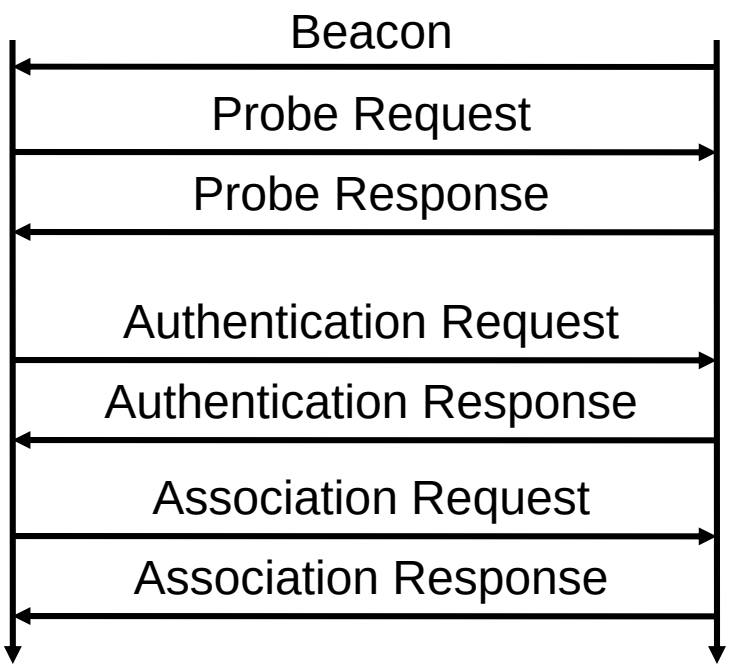




Traditionelle Anmeldung eines Clients an einen Access Point





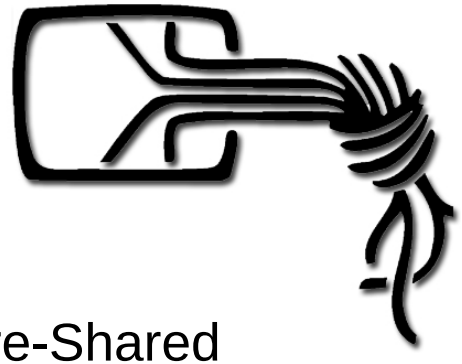


- Authentication
  - Open
  - Shared Key
- Confidentiality & Data Integrity
  - None
  - WEP* (Optional)

Ziele des IEEE 802.11i Standards

- Beseitigen aller Probleme des alten Sicherheitsstandards
- Bietet eine state-of-the-art Sicherheitslösung für WLAN
- Skalierbare Lösung
  - Zentralisierte Authentisierung
  - Automatische Schlüsselverteilung
- BEIDSEITIGE Authentisierung
- Integrierung von neuen Authentisierungsalgorithmen
- Integrierung von neuen Verschlüsselungs- und Prüfsummenalgorithmen
- Benutzung von anerkannten Sicherheitsmethoden wann immer es möglich ist. (Beratung durch anerkannte Kryptologen)
- Unterstützung von Firmen und Heimnetzen

Vorgehensweise der Änderungen

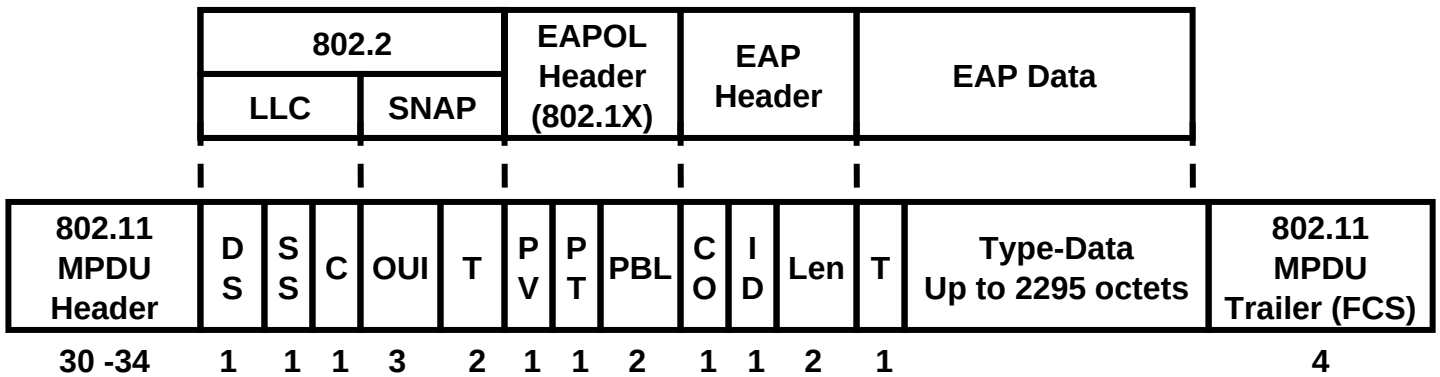


- Erster Schritt – Bessere Authentisierung
  - Benutzung von 802.1x (erstellt by 802.1aa) oder Pre-Shared Key
  - Erfordert beidseitige Authentisierung
  - Unterstützung von vielen EAP Authentisierungsmethoden (EAP-XXX)
- Zweiter Schritt – Sicherstellung der Schlüsselverteilung
- Dritter Schritt – Erstellung von sicheren Verschlüsselungsmethoden
  - Ablösung von WEP durch TKIP als “Workaround”
  - Neue state-of-the-art Methode basierend auf AES (CCMP)
- Vierter Schritt – Dinge die das Leben leichter machen
  - Schnelles Roaming zwischen APs (Schlüsselverteilung schon vor dem Roaming)
  - Sicherheit auch für Peer-to-Peer Netzwerke

Die Konzepte von 802.11i

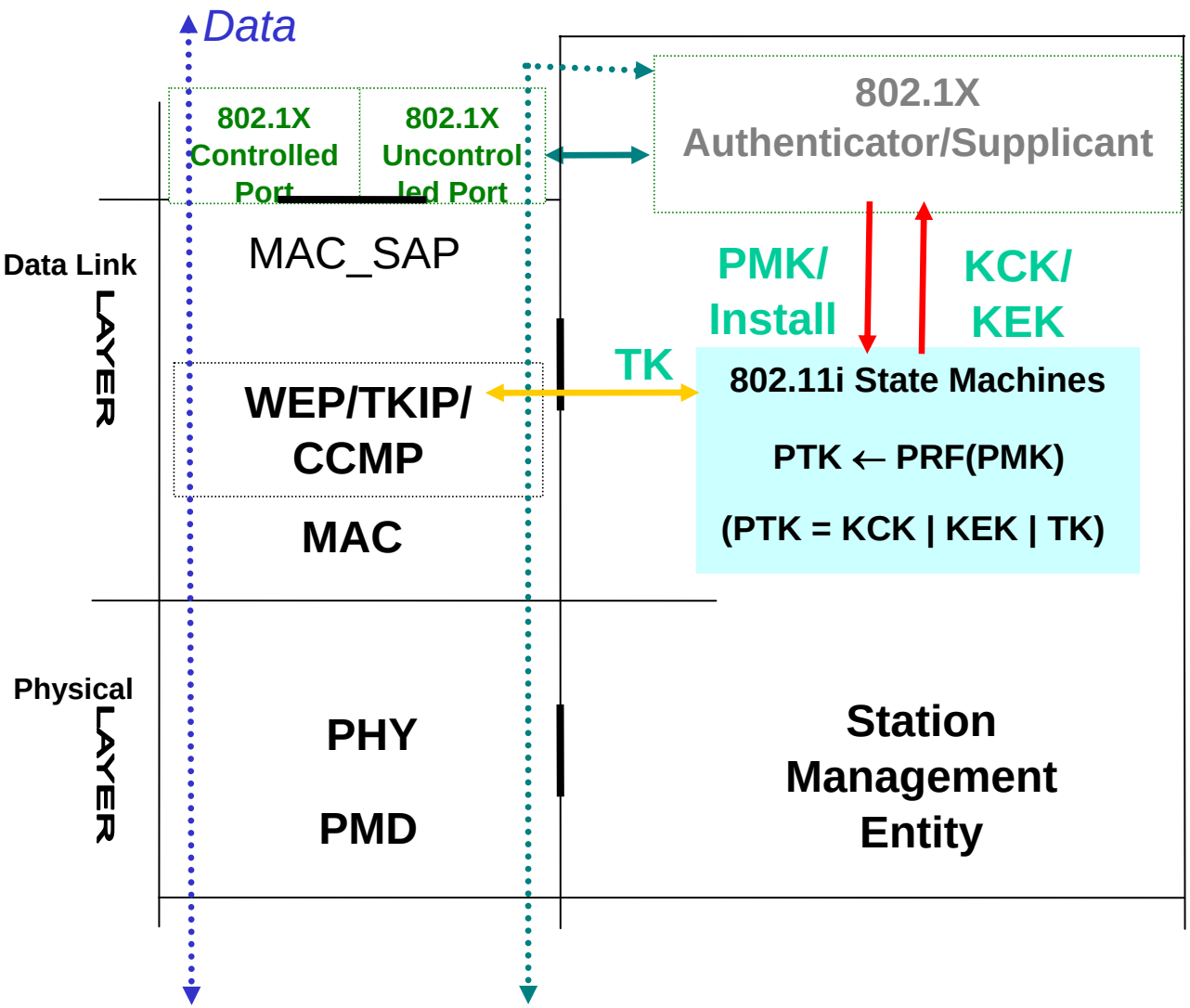
- AES-CCMP – Ein neues Verschlüsselungsprotokoll basierend auf AES-128 im CCM Modus
- TKIP – Stärkeres, neues Verschlüsselungsprotokoll basiernd auf WEP aber so konzipiert, das es per Softwareupdate in basierenden Netzwerken integriert werden kann.
- WEP – Das ursprüngliche 802.11 Verschlüsselungsprotokoll
- RSNA State Machine – Übt die Kontrolle über 802.11i aus
- PRF – Pseudo-Random Function, für Generierung von Sitzungsschlüsseln
- KCK – Key Confirmation Key = Sitzungsschlüssel der für die Authentisierung von EAP-packeten benutzt wird
- PMK – Pairwise Master Key = Einmaliger, generierter Sitzungsschlüssel der aus der Authentisierung abgeleitet ist.
- KEK – Key Encryption Key = Sitzungsschlüssel für die Verschlüsselung von neuen Schlüsseln
- TK – Temporal Key = Aktuell benutzter Verschlüsselungsschlüssel
- 4-Way Handshake – Teil des 802.11i Schlüsselverteilungsprotokoll
- RSN IE -- Datenstruktur für das publizieren und aushandeln von Sicherheitseigenschaften

Format einer EAP-Meldung innerhalb des EAPOL-Frames

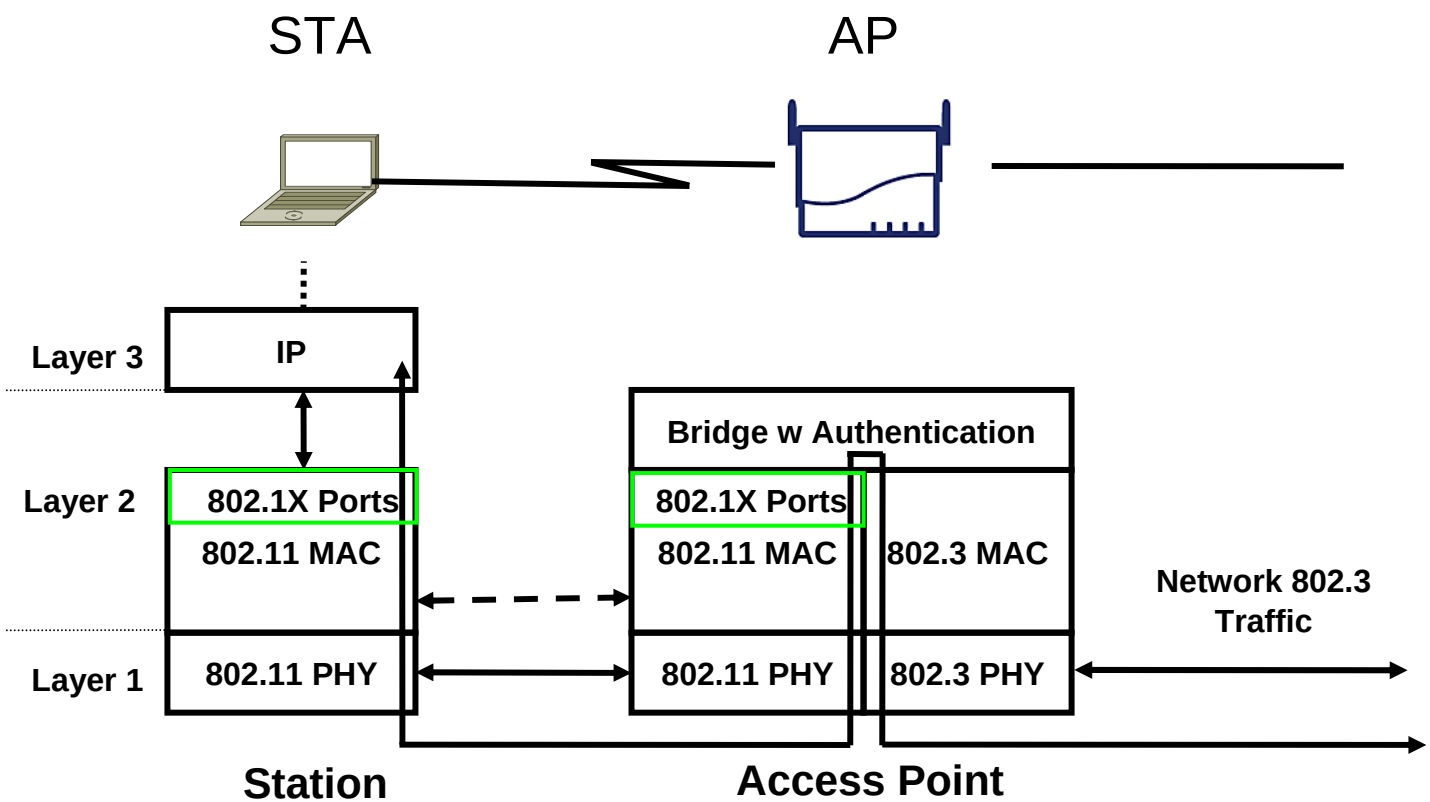


- DS & SS = 0xAA => ein IEEE 802.2 Sub-Network Access Protocol (SNAP) Kopf folgt dem LLC-kopf.
- C = 0x03 => Info Packet ohne Sequenznummer
- SNAP OUI = 0x000000 => Ein standart Ethernet Typ wird benutzt.
- SNAP Type = 0x888E => Als nächstes folgt ein 802.1X Packetkopf
- PV = 802.1X Protokoll versionsnummer, zur Zeit 0001
- PT = 802.1X Packet Typ, 00 => EAP Packet, 01 => Start, 03 => Schlüssel
- PBL = Packet Body Length

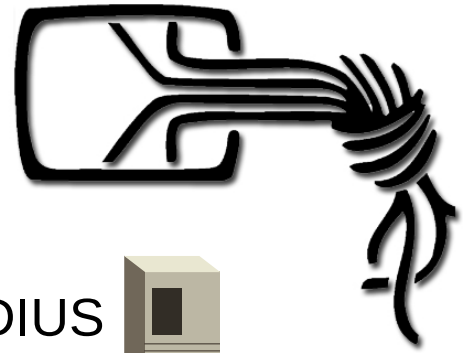
Die Architektur von 802.11i

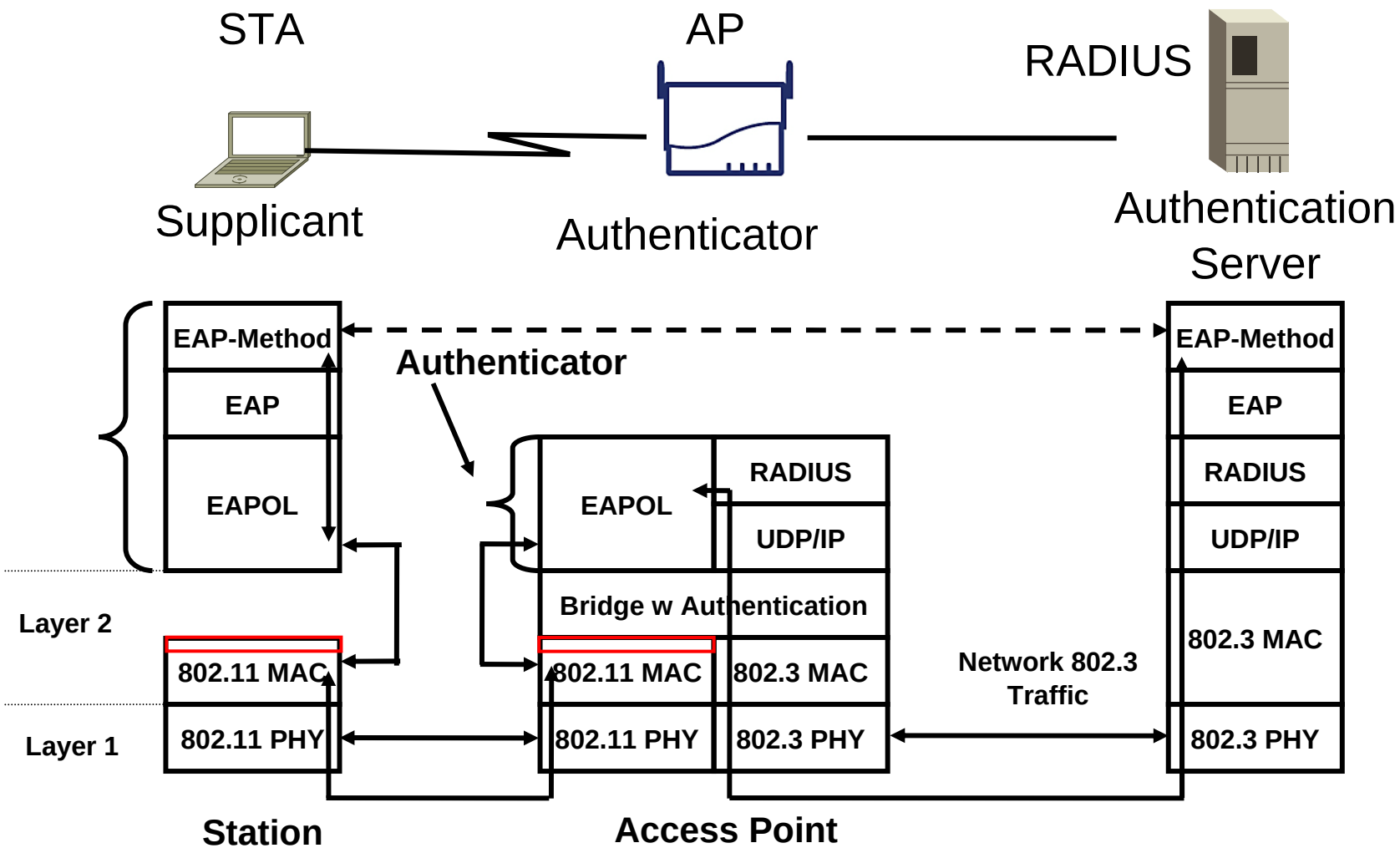


Durchlauf von Meldungen durch den 802.11/802.1x Protokollstapel

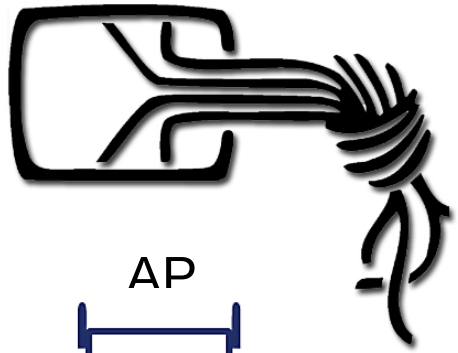


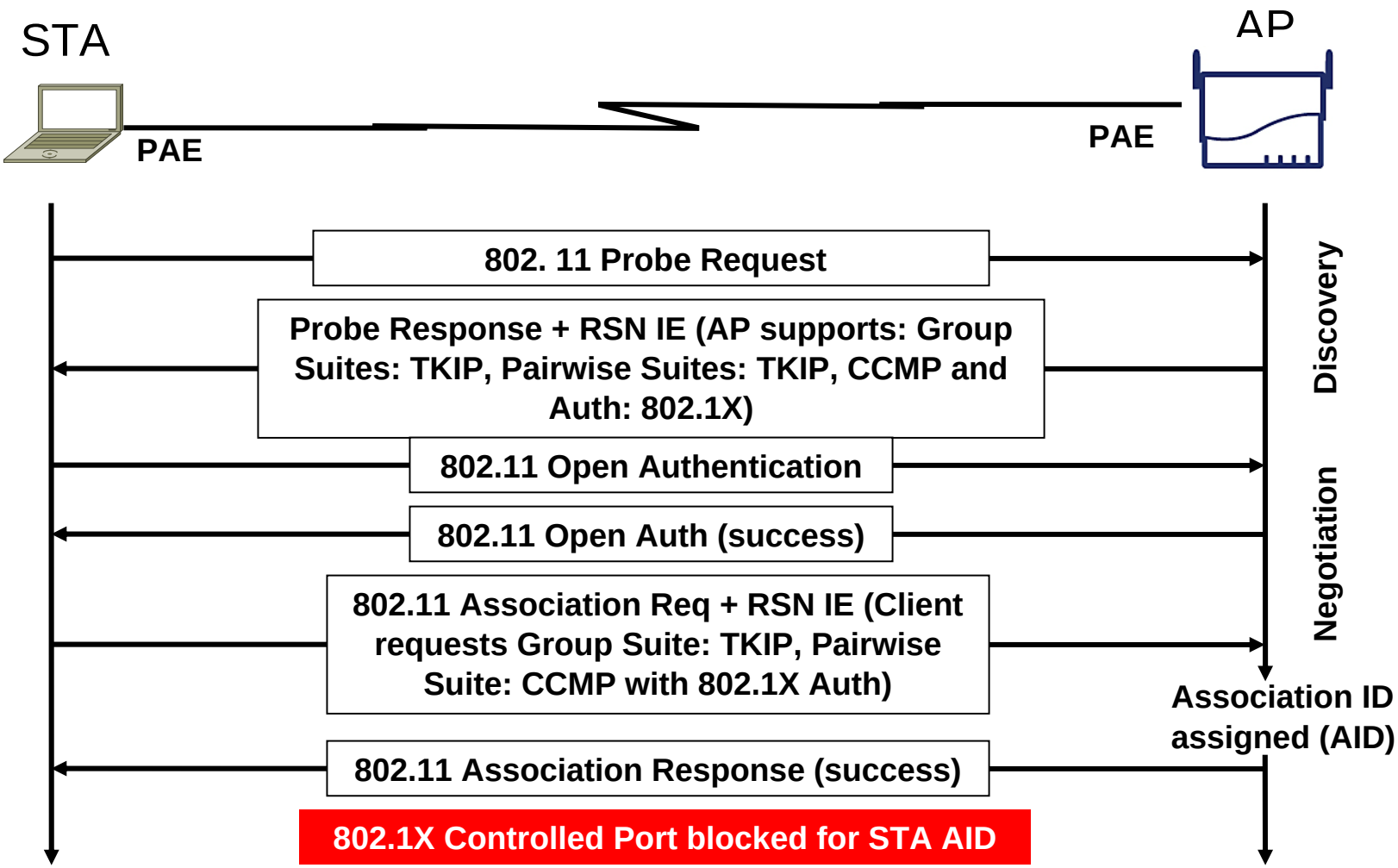
Aufbau des 802.1x Protokollstapels



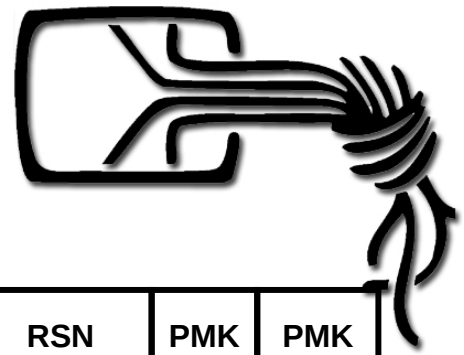


Phase 1 – Finden des richtigen Access Points und verbinden mit ihm.





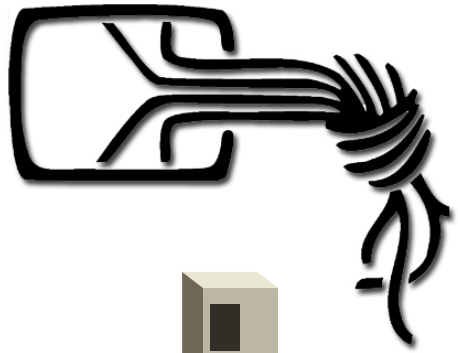
Was steht in den RSN-informations Packeten

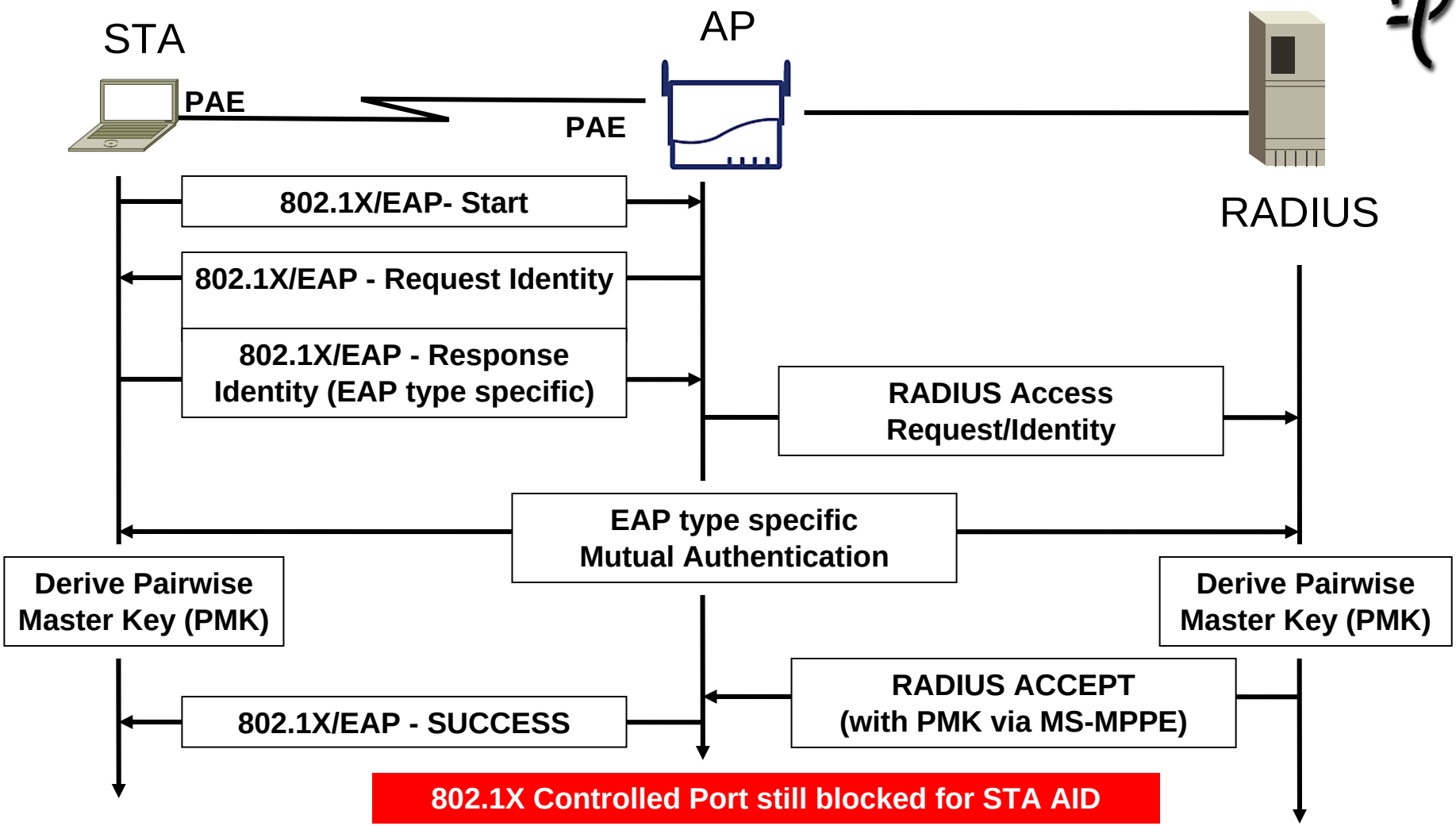


Element ID 0x30	Element Length	RSN Version 1	Group Cipher Suite	Pairwise Suite Count	Pairwise Cipher Suite List	Authentication Suite Count - n	Authentication Suite List	RSN Capabilities	PMK Count	PMK List
1 octet	1 octet	2 octet	4 octet	2 octet	4m octet	2 octet	4n octet	2 octet	2 octet	16n octet

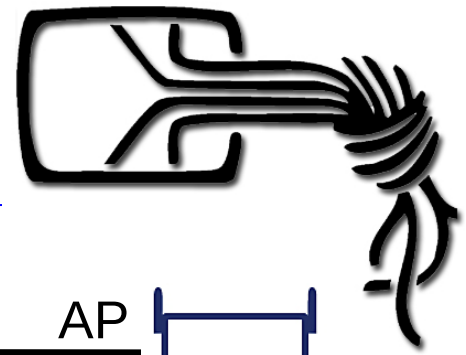
- Wird ein RSN-Packet gesendet müssen die ersten drei Felder enthalten sein.
- Angebotene Systeme für Gruppenschlüssel, Punkt-zu-Punkt Schlüsselsysteme, Unterstützung von den angebotenen Authentisierungssysteme und RSN-elemente sind optional.
- Die “Element ID” bestimmt die Art des Packets
  - 0x30 (48) steht für RSN ein RSN-Packet
  - 0xDD (221) steht für WPA
- “Length” steht für die Menge aller Elemente nach dem Längenelement.
- Bei WPA werden vor dem RSN Versionsfeld die vier Bytes 00:50:F2:01 eingebaut. Die PMK-Felder werden dann nicht benutzt.

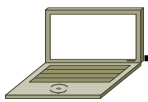
Phase 2 – Der 802.1x Austausch





Phase 3 – Der 4-Wege Austausch



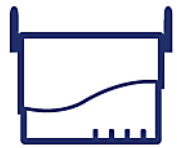


STA

PAE

AP

PAE



PMK

Derive SNonce

EAPoL-Key (Reply Required, Unicast, ANonce)

Derive PTK

EAPoL-Key (Unicast, SNonce, MIC, STA RSN IE)

EAPoL-Key (Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE, GTK)

Install Keys

EAPoL-Key (Unicast, MIC)

802.1X Controlled Port unblocked for STA AID

PMK

Derive ANonce

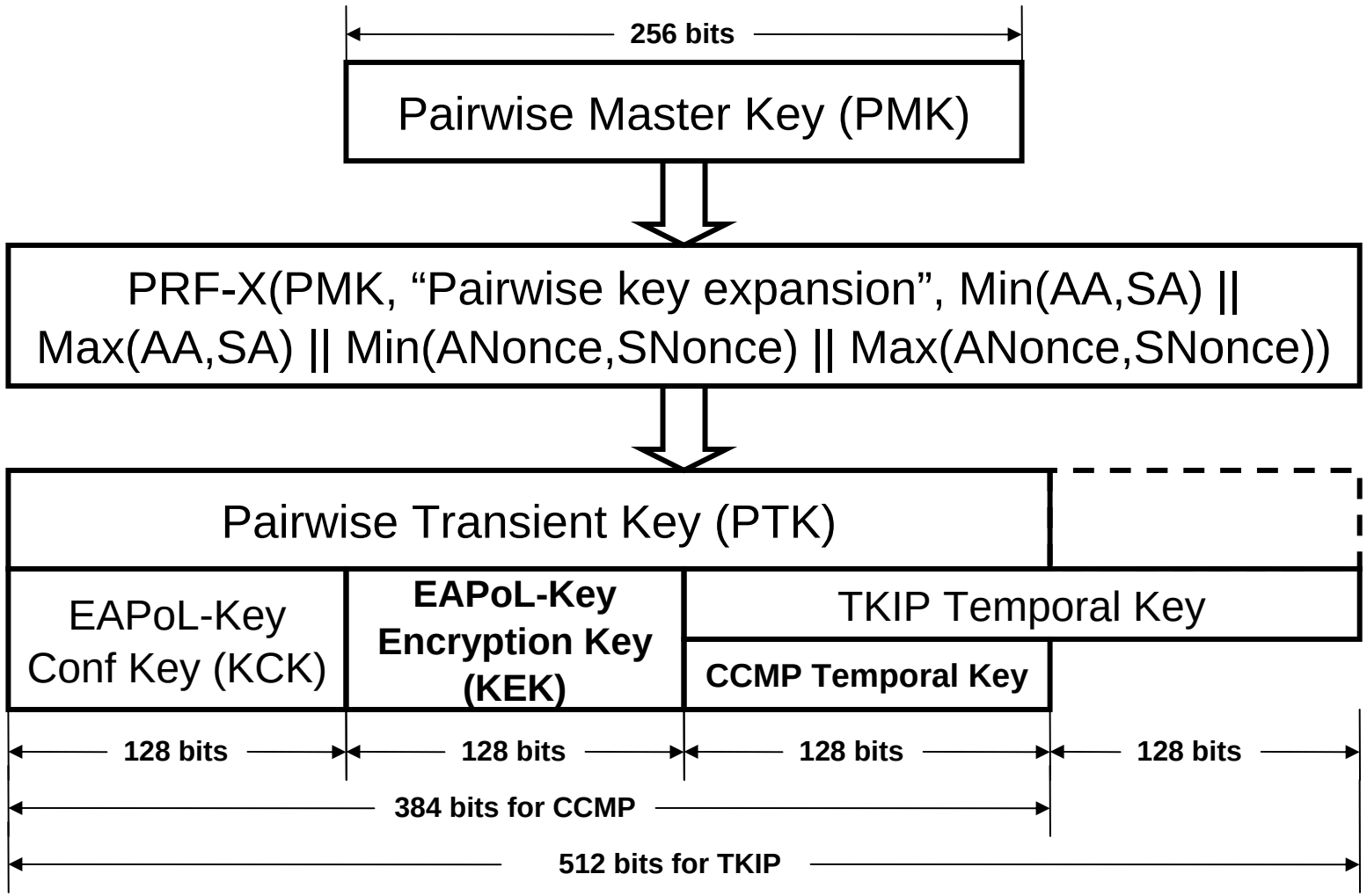
Derive PTK

Encrypt GTK

Install Keys

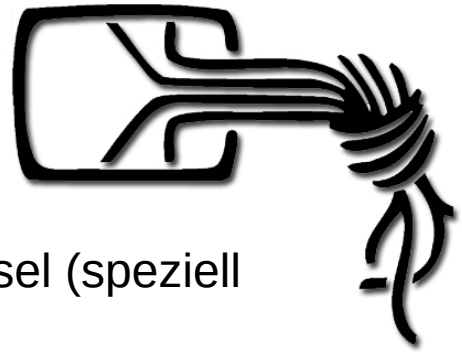
* Fields not noted are null

Die Schlüsselhirarchie



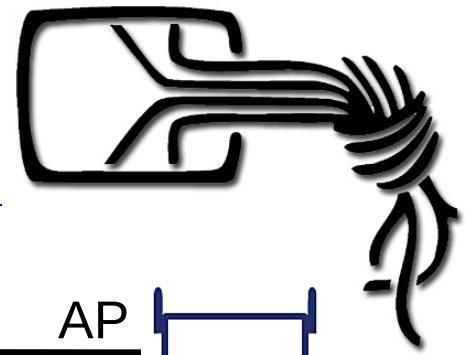
PMKID = HMAC-SHA1-128(PMK, "PMK Name" || Authenticator-MAC-Addr || Supplicant-MAC-Addr)

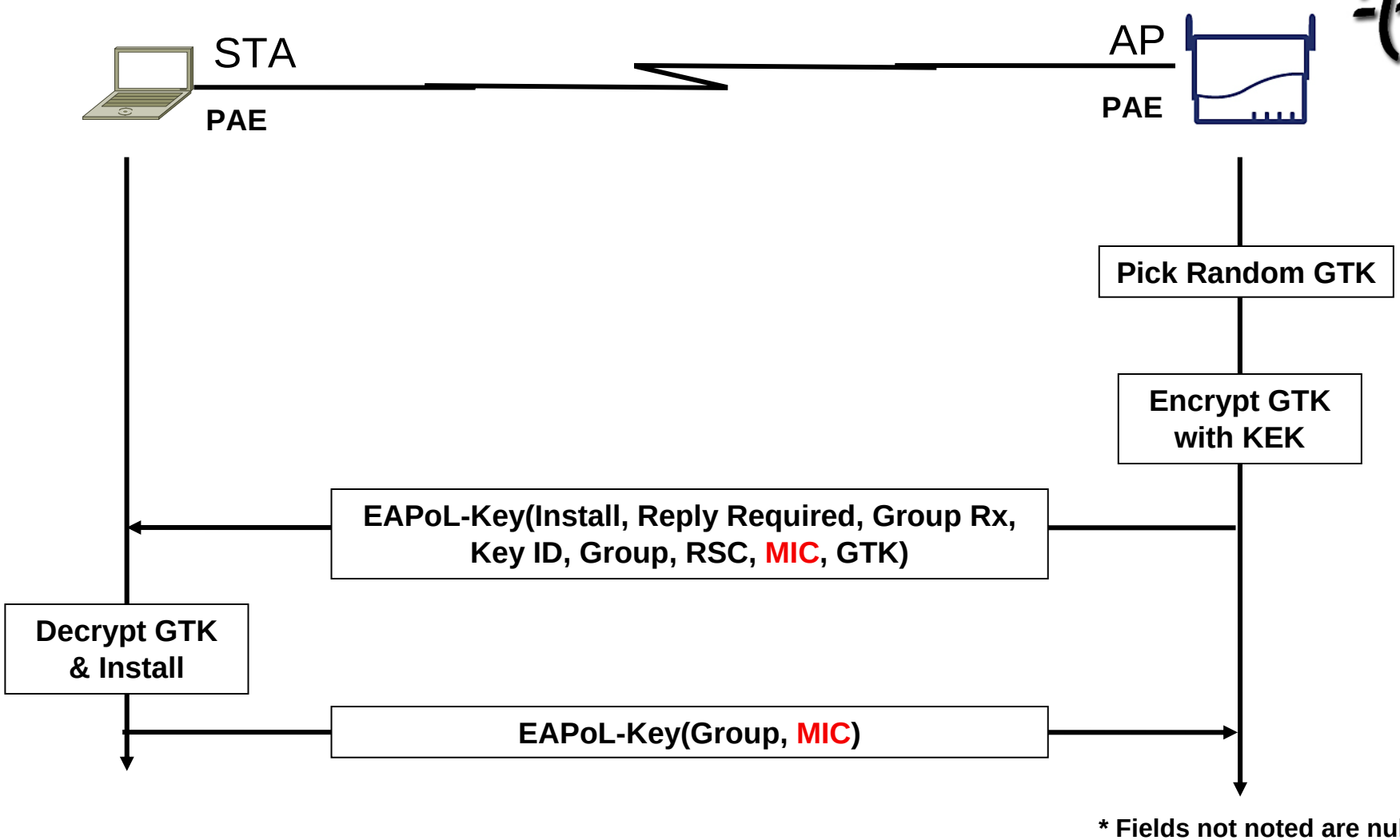
Wofür dient der 4-Wege Austausch



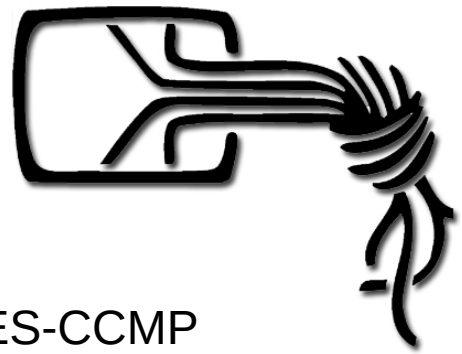
- Die PTK Erzeugung garantiert einen frischen Sitzungsschlüssel (speziell wenn Sie Pre-Shared-Key benutzen)
  - Da ANonce und SNonce zufällige 256bit Zeichen sind gibt es wenig statistische Wahrscheinlichkeiten, dass jemals derselbe PTK erzeugt wird.
- Die zweite Meldung demonstriert dem AP das der Client "lebt"; Meldung 3 sagt dem Client das der AP "lebt"
- Die PTK Erzeugung erzeugt eine einmalige Verbindung zwischen Client und AP aus der weiteres Schlüsselmaterial generiert werden kann.
- Meldungen 3 und 4 synchronisieren den erzeugten Temporären Schlüssel (TK)
- Meldung 3 lädt den Gruppenschlüssel (wird für Broadcastmeldungen benutzt) auf den Client
- Bei Meldung 2 wird durch Einbau des ausgehandelten RSN's ereicht das der Client dem AP gegenüber seine gewählten Sicherheitseinstellungen wiederholt. (Um Attacken mit schwachen Einstellungen zu vermeiden)
- Bei Meldung 3 signalisiert der AP noch mal dem Client gegenüber seine Sicherheitseinstellungen. (Angriffsvermeidung)

Erstellen eines Gruppenschlüssels



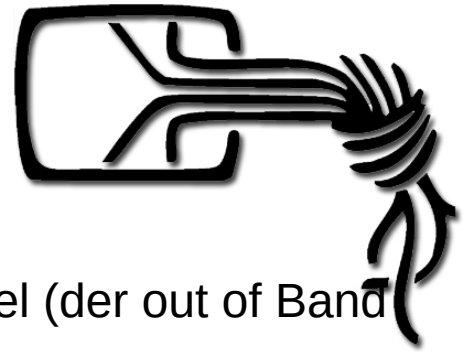


Unterschiede WPA, WPA2 und IEEE 802.11i



- Der alles umfassende Standard ist IEEE 802.11i.
  - In ihm sind die Verschlüsselungsprotokolle TKIP und AES-CCMP definiert.
  - Er definiert PSK (Pre-shared-Key) und EAP für die Authentisierung
  - Er definiert Zusatzprotokolle für schnelles Roaming und IBSS-Modus (Peer-to-Peer)
- WPA
  - Wurde von der Herstellerorganisation Wi-Fi.org vor der Fertigstellung von 802.11i veröffentlicht da man nicht mehr warten wollte.
  - Definiert TKIP, PSK und EAP
- WPA2
  - Definiert die noch fehlende Schnittmenge zum 802.11i Standard also:
    - AES-CCMP
    - Fast-Roaming
    - IBSS-Modus
- Achtung! Die Wi-Fi.org zertifiziert in ihren Standards meist nur kleinste gemeinsame Nenner die alle Hersteller erfüllen.

Wie funktioniert die Pre-Shared-Key Methode

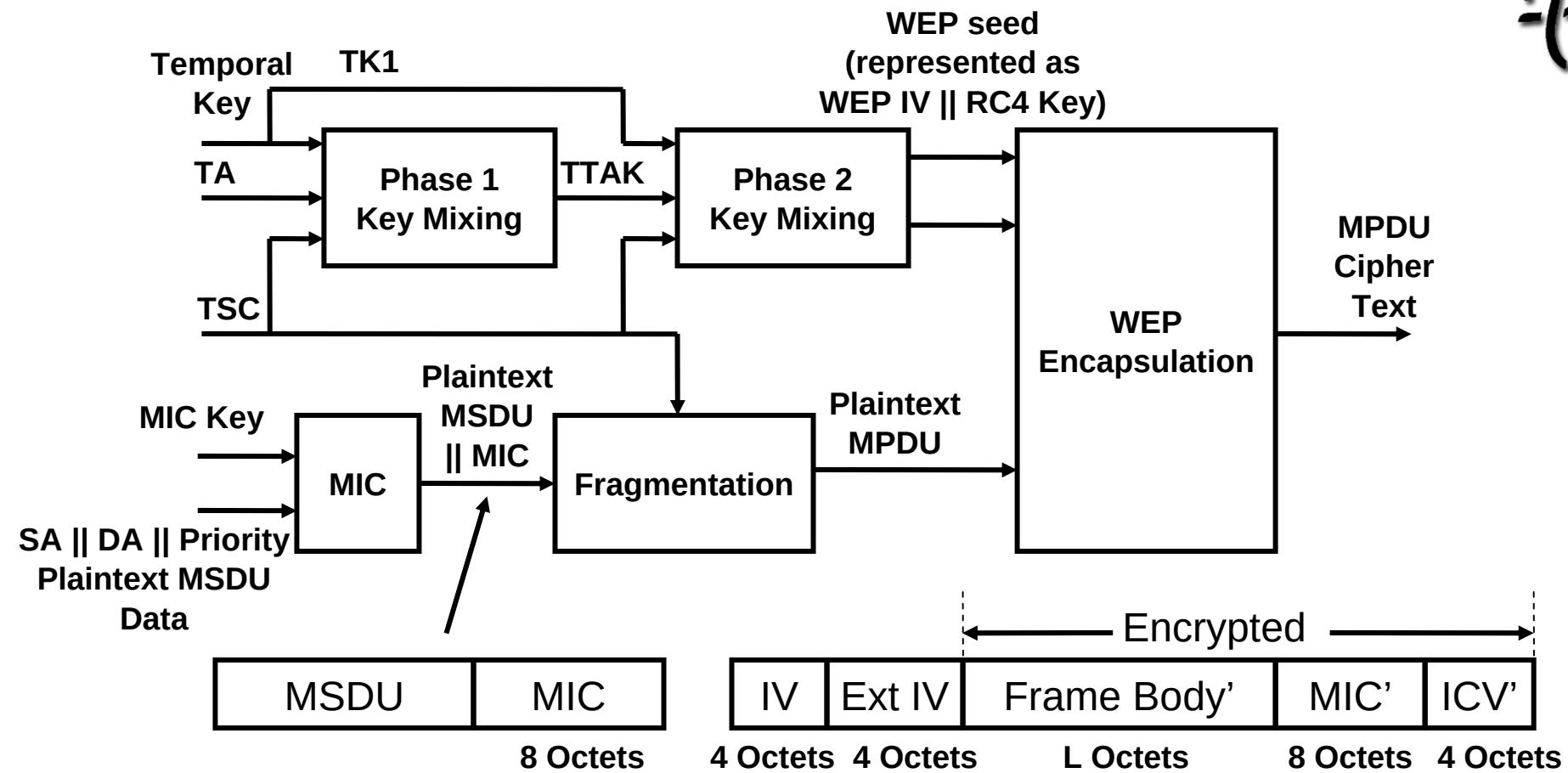


- Funktionsweise:
  - Client und AP kennen einen geheimen Gruppenschlüssel (der out of Band ausgetauscht werden muß).
  - Der geheime Guppenschlüssel wird mit öffendlich übertragenen Anteilen wie SSID, Länge der SSID verknüpft und per HASH-Funktion wird daraus der PMK gebildet (4096* Durchlauf durch Hash oder direkeingabe).
- Vorteile:
  - Es wird kein Authentisierungsserver benötigt
  - Gute Sicherheit/Authentisierung für kleine Netzwerke
  - Sehr schnell wenn Roaming kritisch ist (z.B. VoWLAN)
- Nachteile:
  - Durch den öffendlichen Anteil und das HASH verfahren sind pro Byte Gruppenschlüssel nur ca. 2 Bit aktiv an der security beteiligt. Daher erst “sicher” wenn Gruppenschlüssel mehr als 20 Zeichen lang.
  - Wortbuchattacken auf nachlässig gewählte Passphrase möglich
  - PMK ist kompromitiert wenn jemand die Gruppe verlässt.
  - Keine Authorisierung der Teilnehmer. Wer den PSK kennt kann das Netz nutzen.
  - Traffic kann entschlüsselt werden wenn PSK kompromitiert und 4-Wayhandshake bekannt ist.

Temporal Key Integrity Protocol (TKIP)

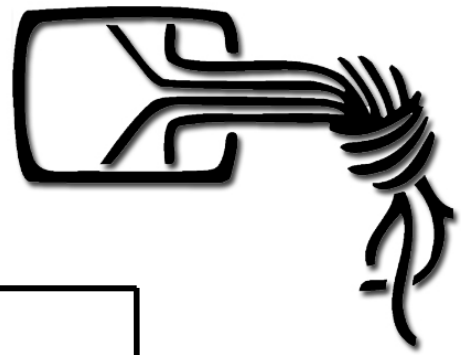
- Schlüsselerzeugung unter Ableitung aus dem PMK (siehe Schlüsselhirarchie)
- Längerer initialisierungs Vector (IV) als bei WEP (48bit)
- Feste Vorschrift zur Inkrementierung der IV's (verhindert Replay Attacken)
- WEP wird noch für die Verschlüsselung der Packete benutzt aber dafür für jedes Packet ein neuer Schlüssel (verhindert die Attacken auf statische WEP Schlüssel)
- Michael MIC (Message Integrity Check) statt einfacher CRC
- Wurde so definiert das er als Software update in bestehende Clients / AP‘s integriert werden kann ohne die Hardware zusätzlich zu überlasten. (Dabei mussten natürlich auch Kompromisse geschlossen werden.)

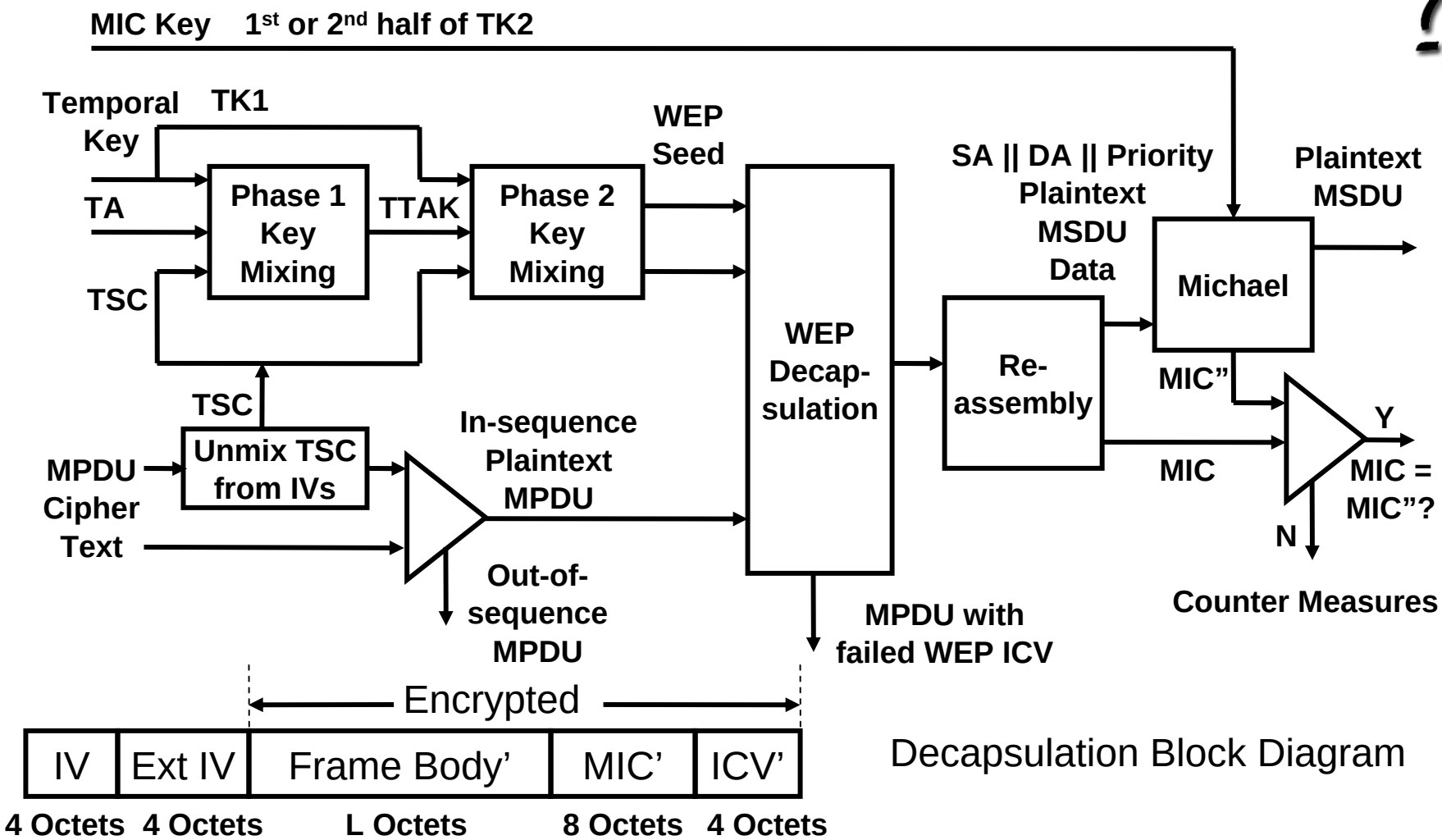
TKIP Verschlüsselungsdiagramm



Encapsulation Block Diagram

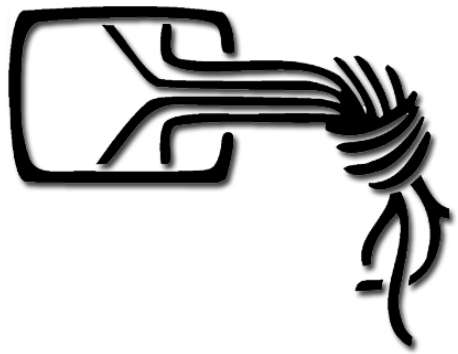
TKIP Entschlüsselungsdiagramm





Decapsulation Block Diagram

Aufbau des Michael MIC



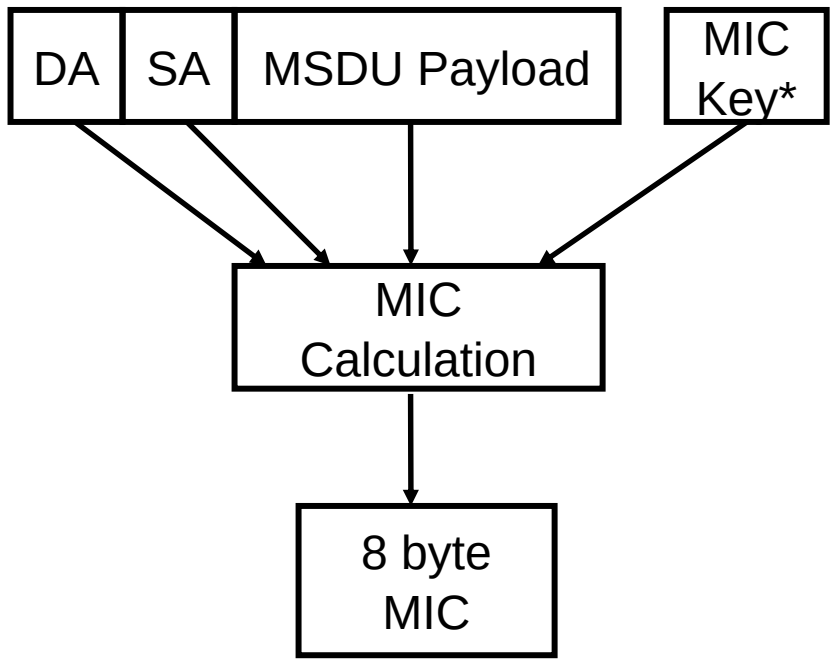
Schützt gegen Manipulation der Prüfsumme. (Richtige Prüfsumme kann nur errechnet werden wenn man auch in der Lage ist das Packet zu entschlüsseln)

Wird gebildet unter Einbeziehung der beiden MAC-Adressen (Client/AP) und der Payload.

Nutzt pro Richtung eigene (64bit) Schlüssel

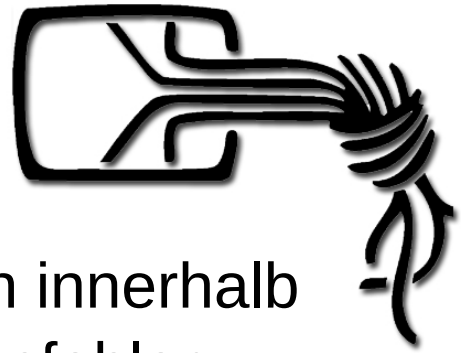
Nutzt kaum die CPU ca. 5 Zyklen/Byte
- 3 - 4 Zyklen/Byte auf ARM7 (2.7 – 3.6 MHz)
- 5 - 6 Zyklen/Byte auf i486 (4.5 – 5.4 MHz)

Vergleichsweise schwach ~30bits an Sicherheit



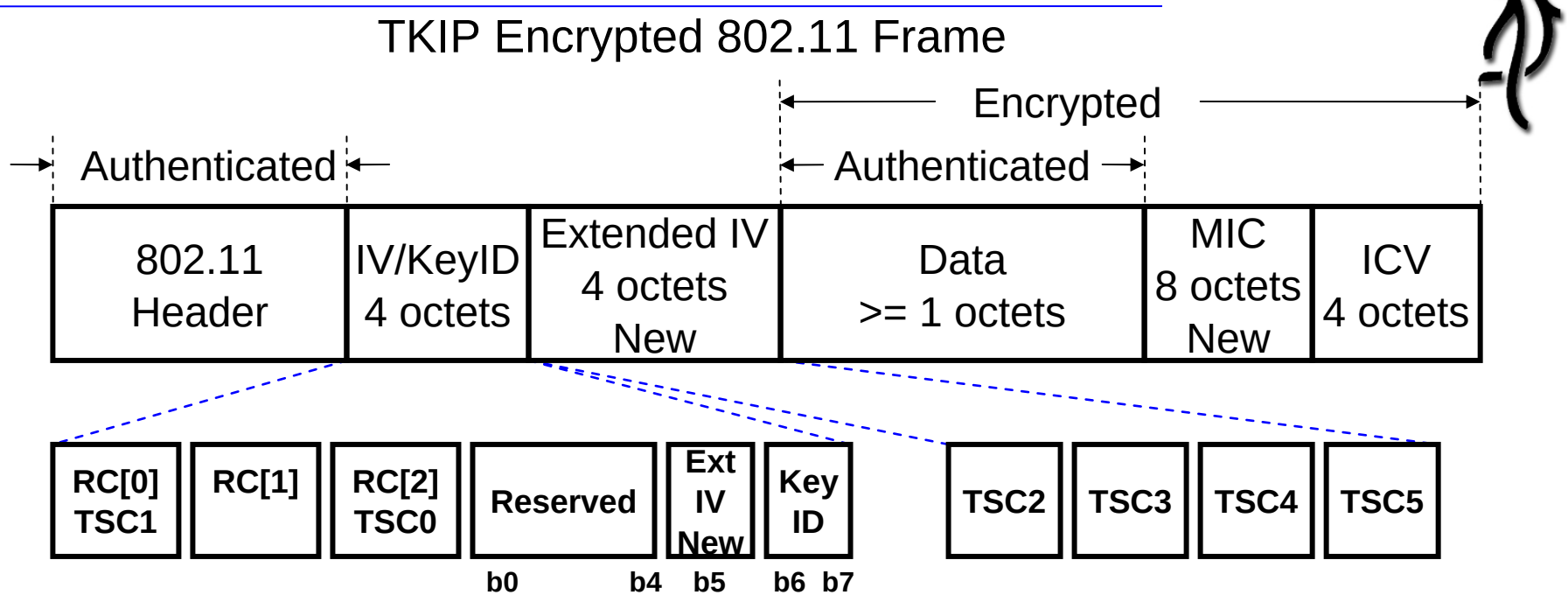
* Der MIC Schüssel wird aus dem Pairwise Transient Key (PTK) abgeleitet. Der PTX wird aus dem 4-Wege Handshake von dem benutzten PMK generiert. Der PMK wiederum entscheht aus der 802.1x Authentisierung.

Gegenmaßnahmen bei Attacken auf Michael



- Sobald eine aktive Attacke erkannt wird (wenn innerhalb von 60 Sekunden zwei oder mehr Prüfsummenfehler erkannt werden):
  - Neue Schlüssel generieren und die alten löschen.
  - Limitierung der neuen Schlüsselerzeugung auf einen pro Minute. (Dadurch das der Access Point für 60 Sekunden ausgeschaltet wird.)
- Überprüfung von FCS, ICV und TSC bevor die Prüfsumme des MIC getestet wird.
  - Macht es unwahrscheinlich das zufällig eine aktive Attacke auf Micheal erkannt wird obwohl einfach nur Bits bei der Übertragung gekippt sind.

Packetformat eines TKIP-Packets



- Initialisiere den 48 bit IV mit 1 wenn der Temporäre Schlüssel (TK) erzeugt wurde.
- Erhöhe den IV bei jedem Packet um eines (Sequenzregel)
- Ignoriere alle Packte die einen IV haben der kleiner ist als der zuletzt emfangene.

AES Verschlüsselung mit CCMP

- Der Rijndael genannte Algoritmus wurde als Ablösung des bisherigen DES Standart vom National Institute of Standards and Technology, NIST, 2001 gewählt.

- Rijndael (nach seinen Erfindern Vincent Rijmen & Joan Daemen), ist ein relativ simpler Blockziffer Algorithmus mit unterschiedlichen grössen (128/192/256 Bits).

- Operationen auf Byte-basis wie Tabellensuche, XORs, Multiplikationen, Byteweisen verschiebungen machen ihn einfach zu implementieren.

- Wiederholungen dieser Operationsvorschriften mehrfach hintereinander (10 Runden bei 128Bit) machen ihn zu einem sehr starken Verschlüsselungsalgorithmus.

- Rijndael wurde von Cryptoanalysten, der freien Welt, sehr genau unter die Lupe genommen und von diesen "erwählt".

- AES wird von WPA2 nicht in Reinform verwendet. Er wird mit Verfahren wie CBC und Counter Mode verbunden um gleichzeitig auch die Bildung von starken Prüfsummen zu ermöglichen. Dieses führt zu AES-CCMP

Counter Mode/CBC MAC Protokoll (CCMP)

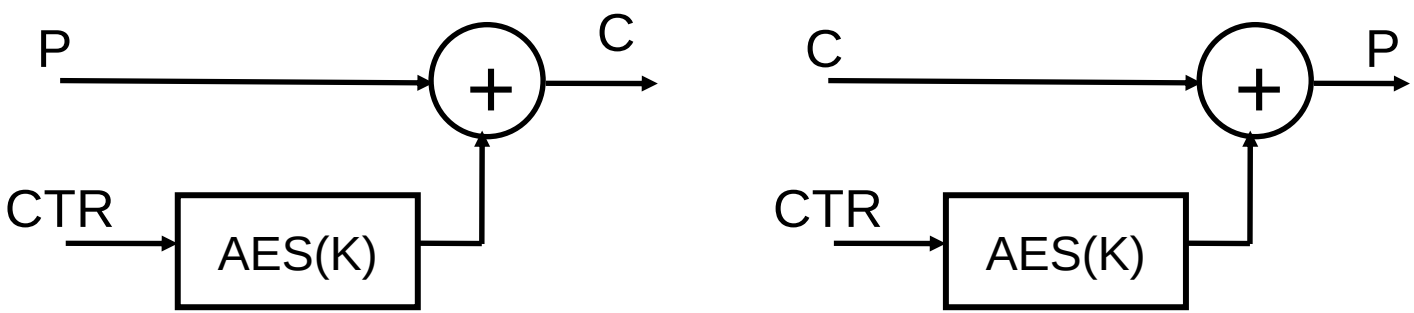
- CCMP bietet:
  - Benutzt AES (Advanced Encryption Standard)
    - Dieser erfordert allerdings auch „stärkere“, neue Hardware eventuell mit spezial Chips.)
  - Schlüsselerzeugung wird vom PMK abgeleitet (Schlüsselhirarchie)
  - 48bit grosse Packet Nummer (PN)
  - Regel für die Erhöhung der Packet Nummer (um eins pro Packet)
  - Counter Mode und CBC (Chiper Block Chaining) MAC müssen zusammen benutzt werden.

- Was kann (braucht CCMP) nicht:
  - Schlüsselerzeugung für jedes Packet
    - AES ist stark genug
    - Durch CBC muss man auch die Vorgeschichte kennen/entschlüsselt haben
  - Gegenmassnahmen auf Prüfsummen-Attacken
    - Das Design (durch den CBC) ist resistent dagegen

AES, alleine und mit Counter Mode

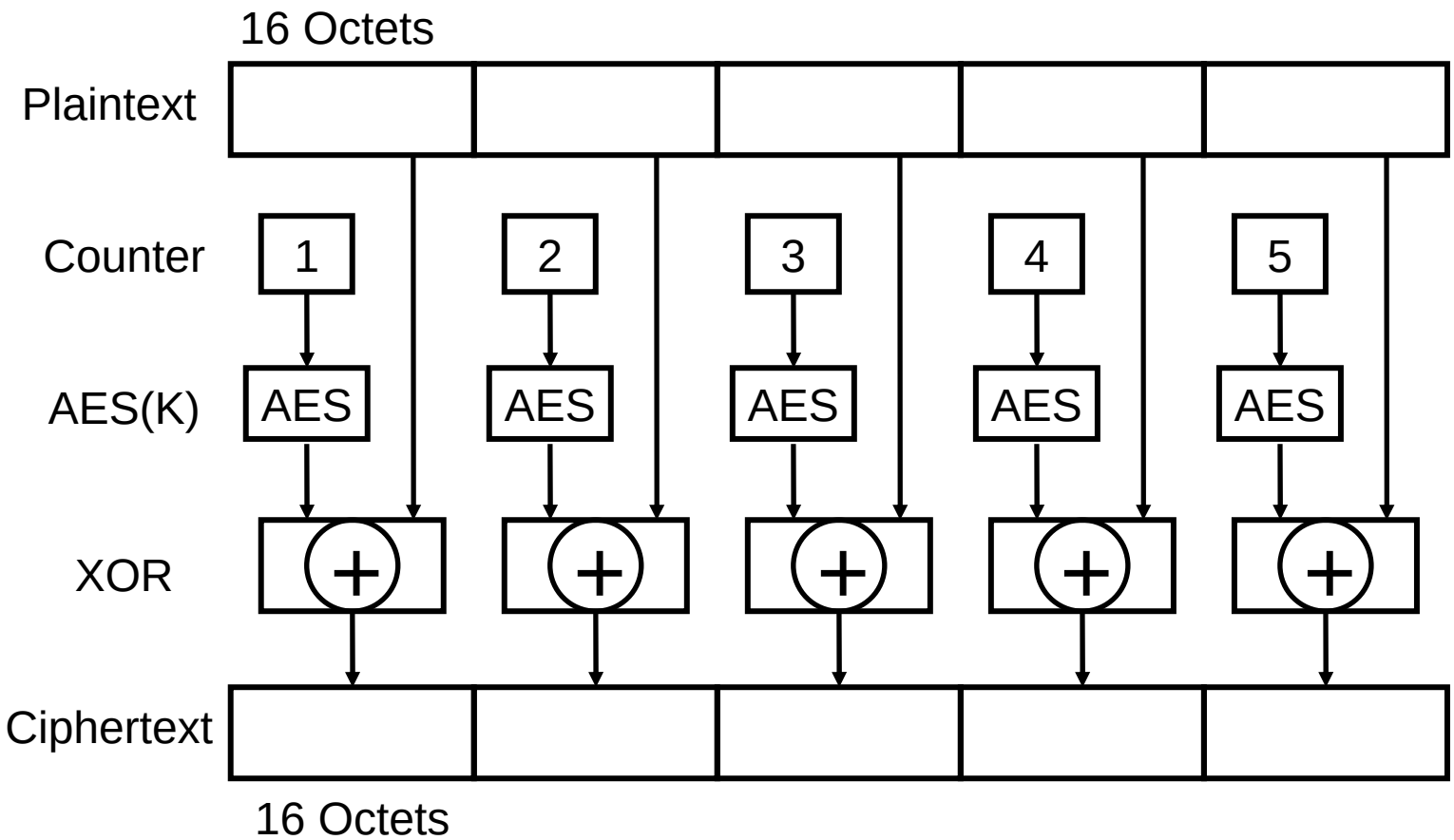
AES Block Cipher/Decipher

AES in Counter Mode Cipher/Decipher

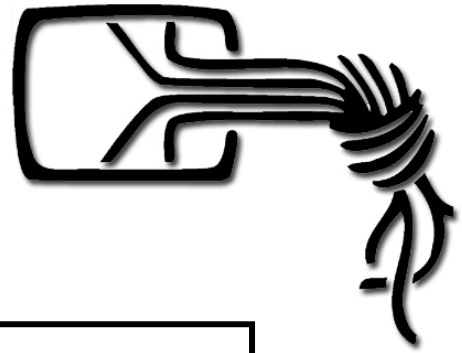


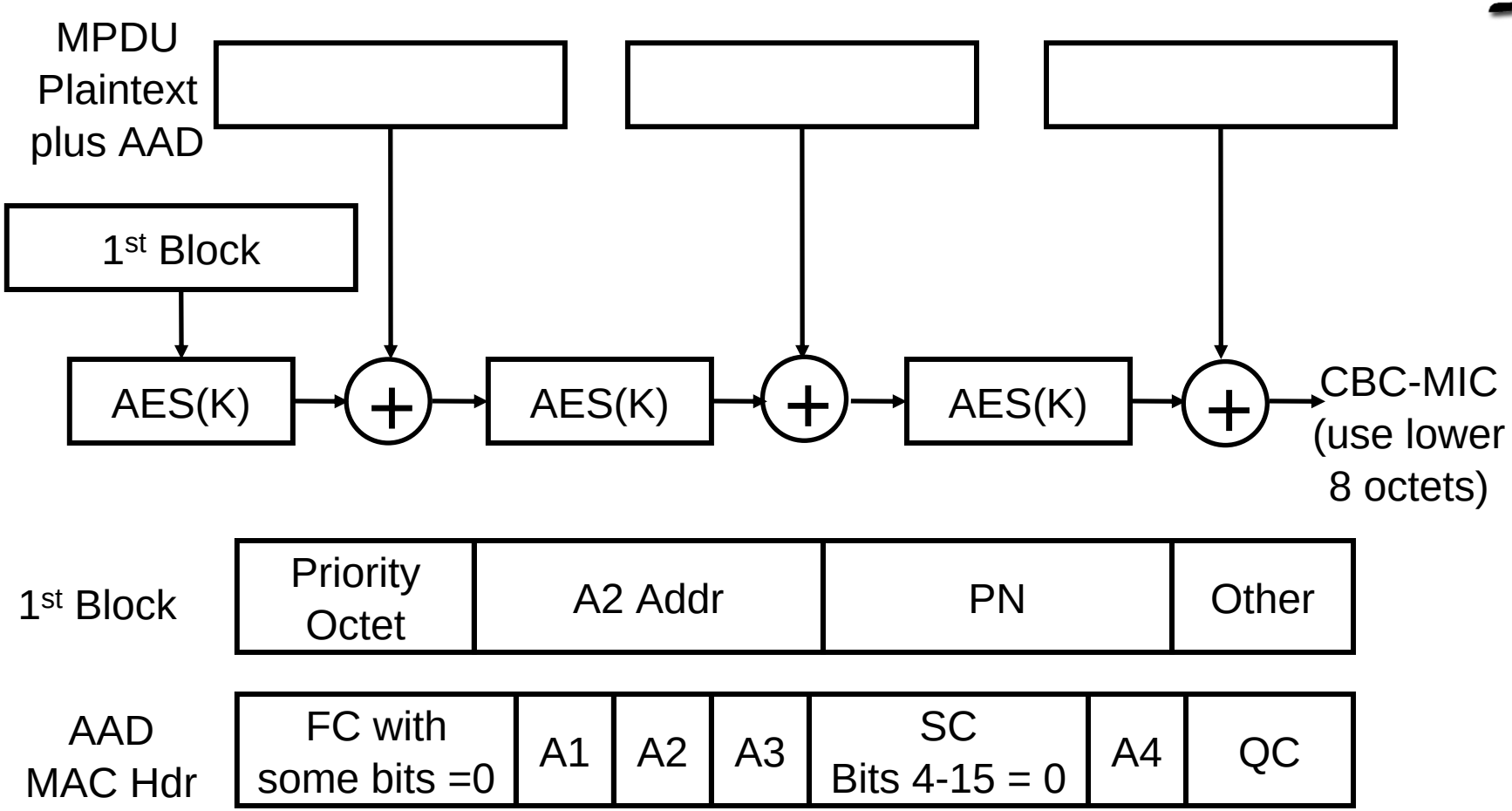
- IV_ccm = PKT_CTR || TA_MAC_ADDR
- CTR = IV_CCM++ for each 16 byte block

Hintereinanderschaltung des AES CM

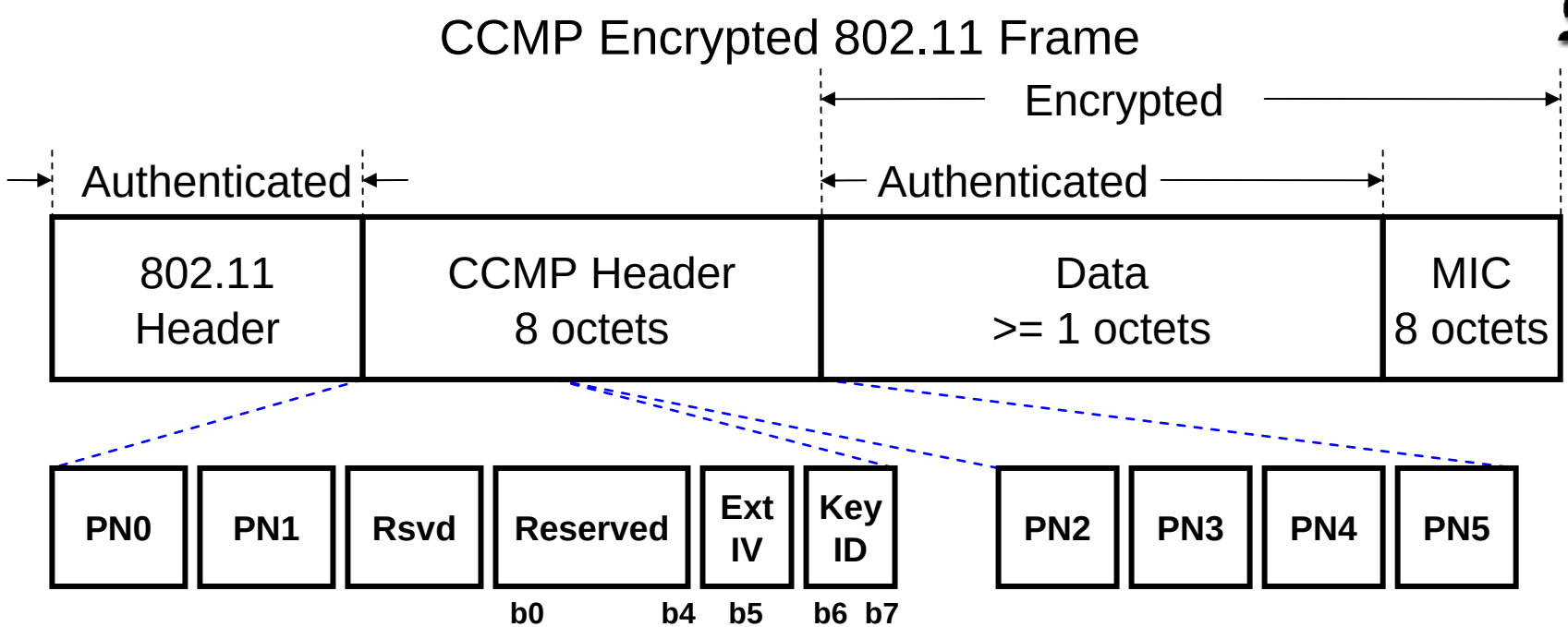


CBC Modus (Cipher Block Chaining) & Bildung von Prüfsummen (Message Integrity Code)



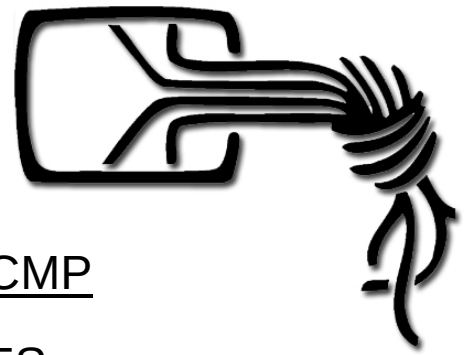


Packetformat eines AES-CCMP-Packets



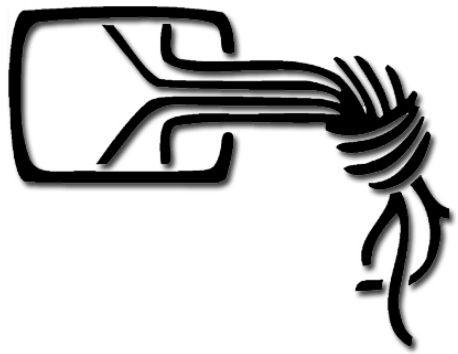
- Erhöung des PN um einen (Sequenzregel)
- Verwerfe alle Packete deren PN kleiner ist als der vorherige

Gegenüberstellung WEP, TKIP und AES-CCMP



	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits encryption,	128 bits 64 bit auth
Key Life	24-bit IV, wrap	48-bit IV	48-bit PN
Packet Key	Concat.	Mixing Function	Not Needed
Integrity Data Header	 CRC-32 None	 Michael Michael	 CCM CCM
Replay	None	Use IV	Use PN
Key Mgmt Way	None	802.11i 4-Way Handshake	802.11i 4-Handshake

Verweise



- IEEE Standarts für 802.11*

  http://standards.ieee.org/getieee802/802.11.html

- Wi-Fi Hersteller Organisation

  http://www.wi-fi.org

  http://certifications.wi-fi.org/wbcs_certified_products.php?TID=2

- Grundlagen der Kryptografie

  Buch: Applied Cryptography von Bruce Schneier

- Godzilla Crypto Tutorial

  http://www.cs.auckland.ac.nz/~pgut001/tutorial/index.html

- Linksammlung zu Test-Tools

  http://www.corecom.com/html/wlan_tools.html

- Backtrack Security Live CD

  http://www.remote-exploit.org/backtrack.html

- Sicherheitsfibel für Wireless LAN

  http://www.mms-ag.de/ftp/pdf/systems/WLAN_Sicherheitsbroschuere.pdf