

WLAN-Vorlesung

Teil-9

Inhalt

- Verschlüsselung
- Ziele
- WEP-Verschlüsselung / WEP-Desaster
- WPA / WPA2
 - ◆ Bauelemente der Verschlüsselung
 - ◆ Erzeugen der Transient Keys
 - ◆ Austausch der Nonce
- TKIP
 - ◆ Pairwise Key Hierarchie
 - ◆ Group Key Schlüsselhierarchie
 - ◆ TKIP Verschlüsselung / MPDU-Format / Entschlüsselung / MIC-Fehler
- CCMP
 - ◆ Pairwise Key Hierarchie
 - ◆ CTR-Code
 - ◆ Verschlüsselung / AAD-Aufbau / MIC-Berechnung / MAC-Frame / Entschlüsselung
- WPA3

Schutzziele

Bei der Übertragung von Daten sollten die folgenden Schutzziele erfüllt werden:

- Authentizität
- Datenintegrität
- Vertraulichkeit
- Verfügbarkeit
- Verbindlichkeit
- Anonymisierung

Erreichung der Schutzziele

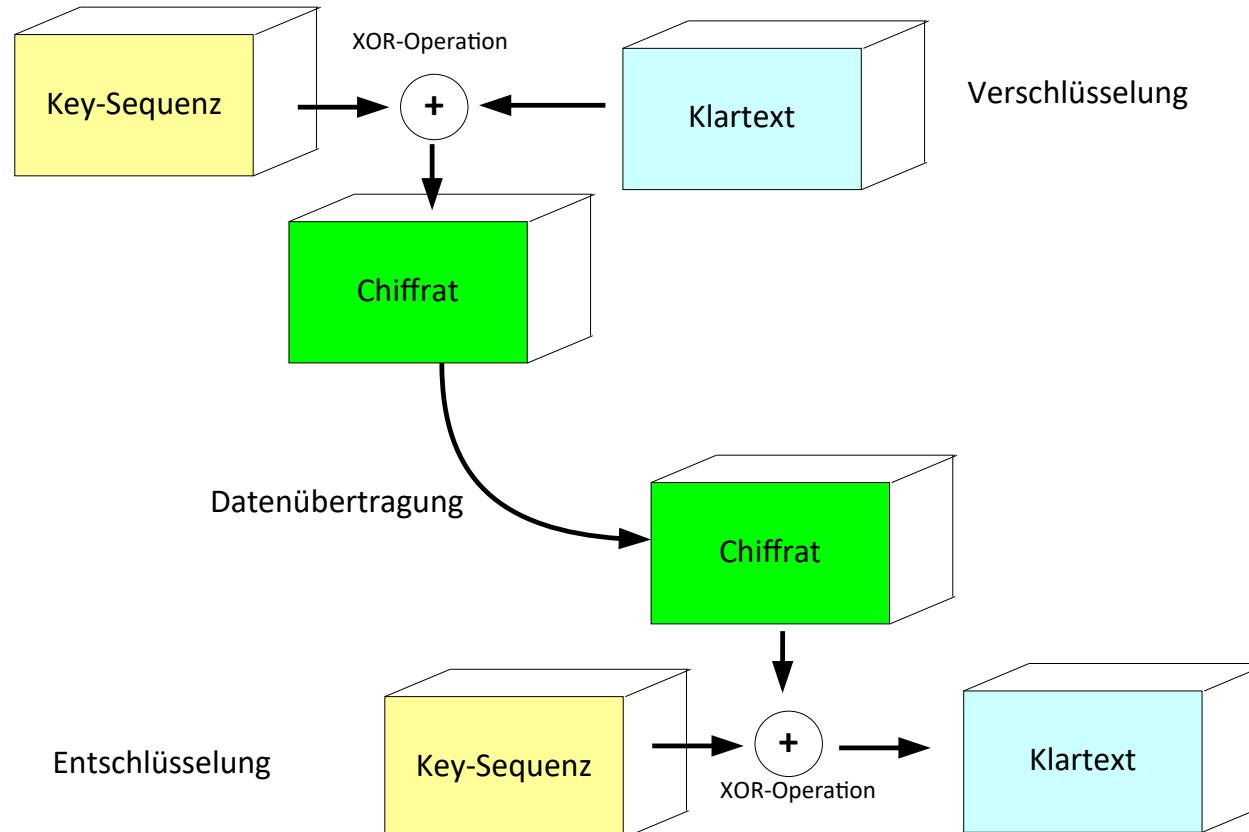
Die Schutzziele können mit unterschiedlichen Maßnahmen erreicht werden.
Allerdings ist dazu oft ein nicht unerheblicher Aufwand erforderlich.

In verkabelten Systemen sind die Schutzziele oft (aber nicht immer) einfacher zu realisieren.
Bei WLANs ist es schon allein durch das offene Medium Luft nicht einfach möglich die Schutzziele umzusetzen. Allein die Begrenzung der Reichweite eines WLANs ist nicht ohne weiteres möglich.

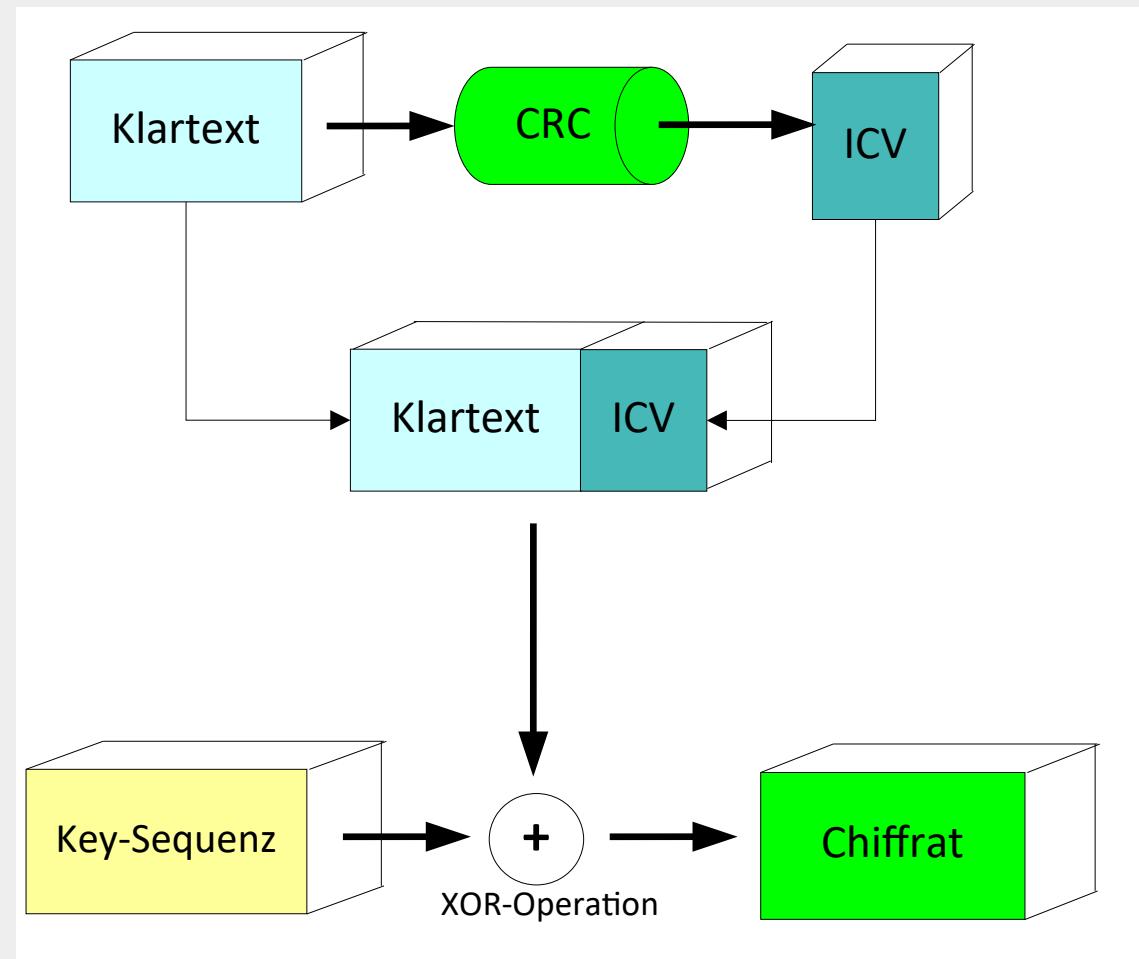
Mit den folgenden Maßnahmen soll trotzdem eine Sicherheit, die die einem verkabelten System entspricht, erreicht werden.

- Authentifizierung bei der Anmeldung
- Verschlüsselung bei der Datenübertragung
- Eindeutige Sequenznummern und Prüfsummen zum Schutz der Datenintegrität

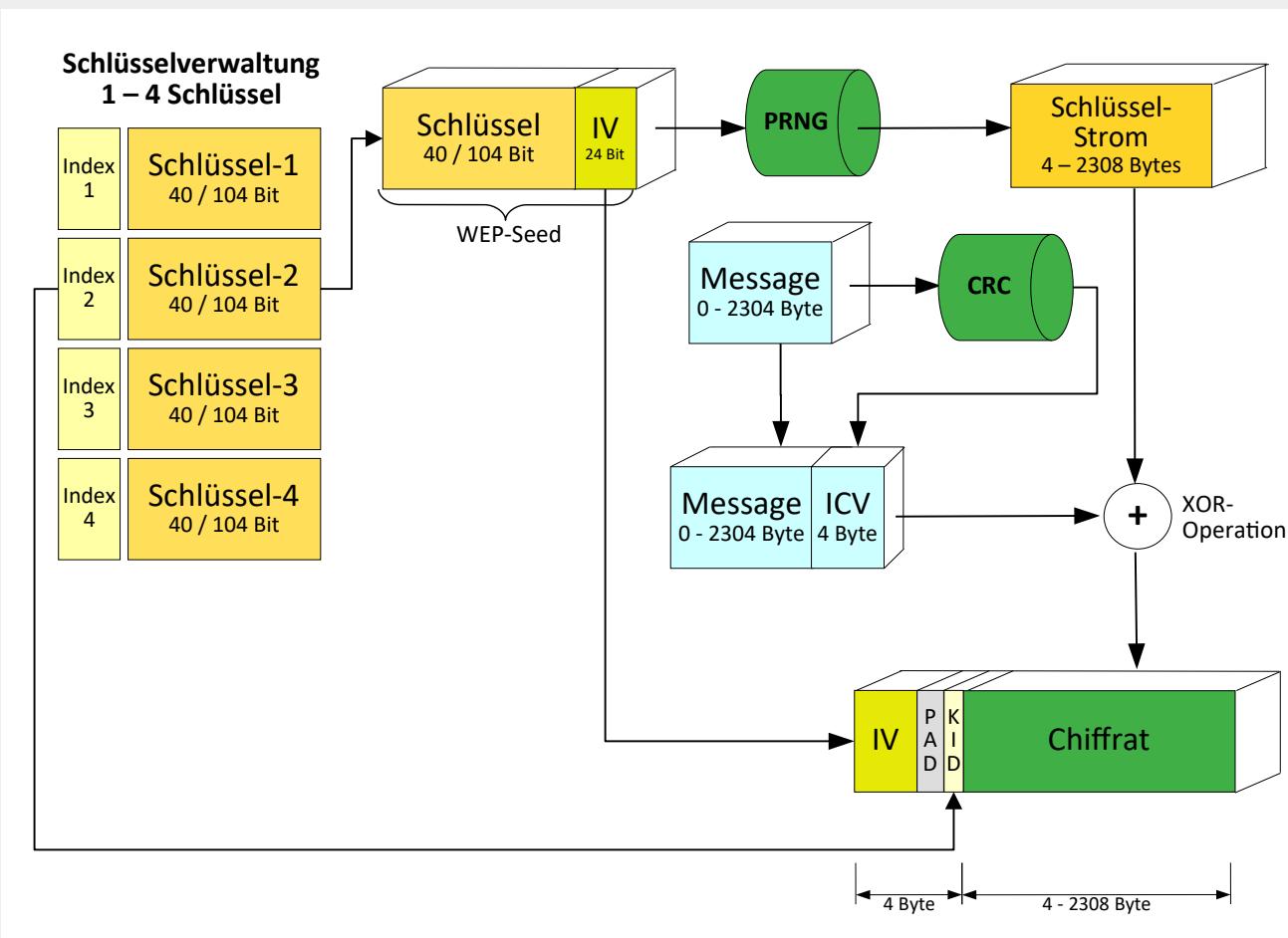
Verschlüsselung



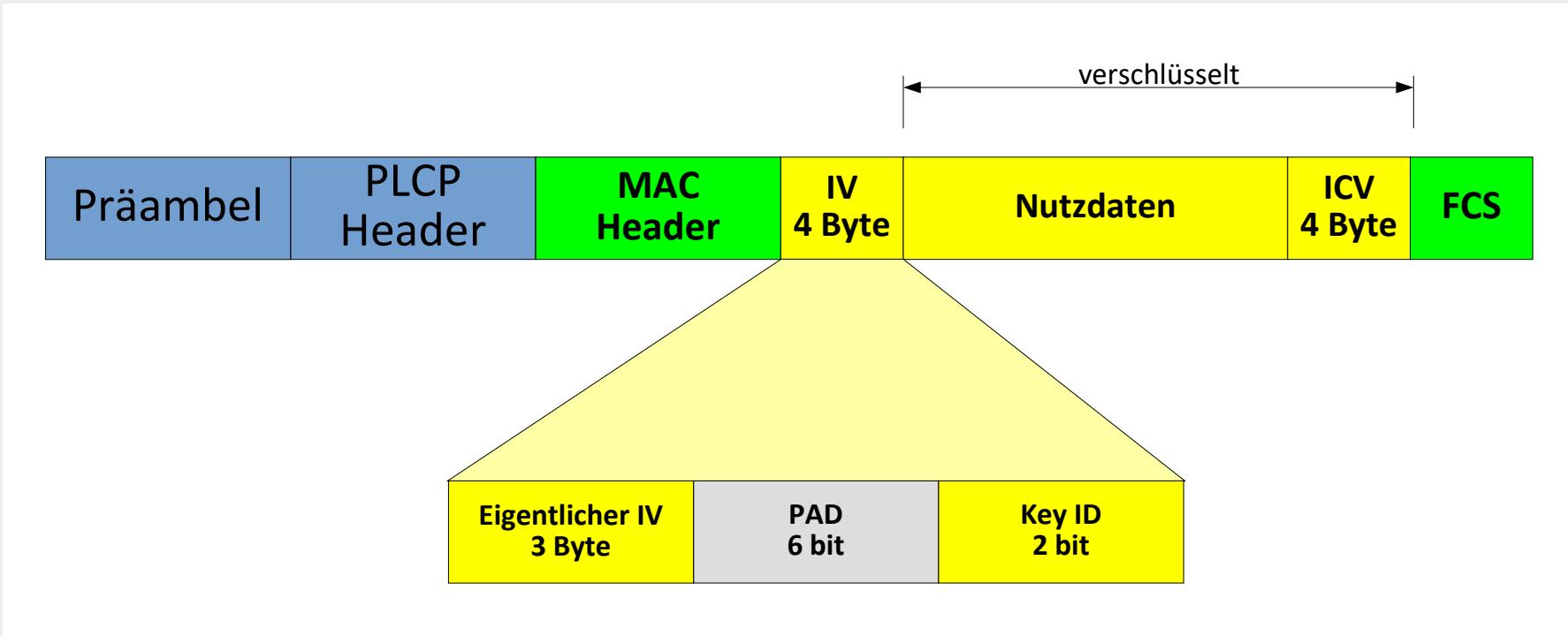
WEP-Verschlüsselung



WEP-Verschlüsselung



Frame-Aufbau mit WEP-Verschlüsselung

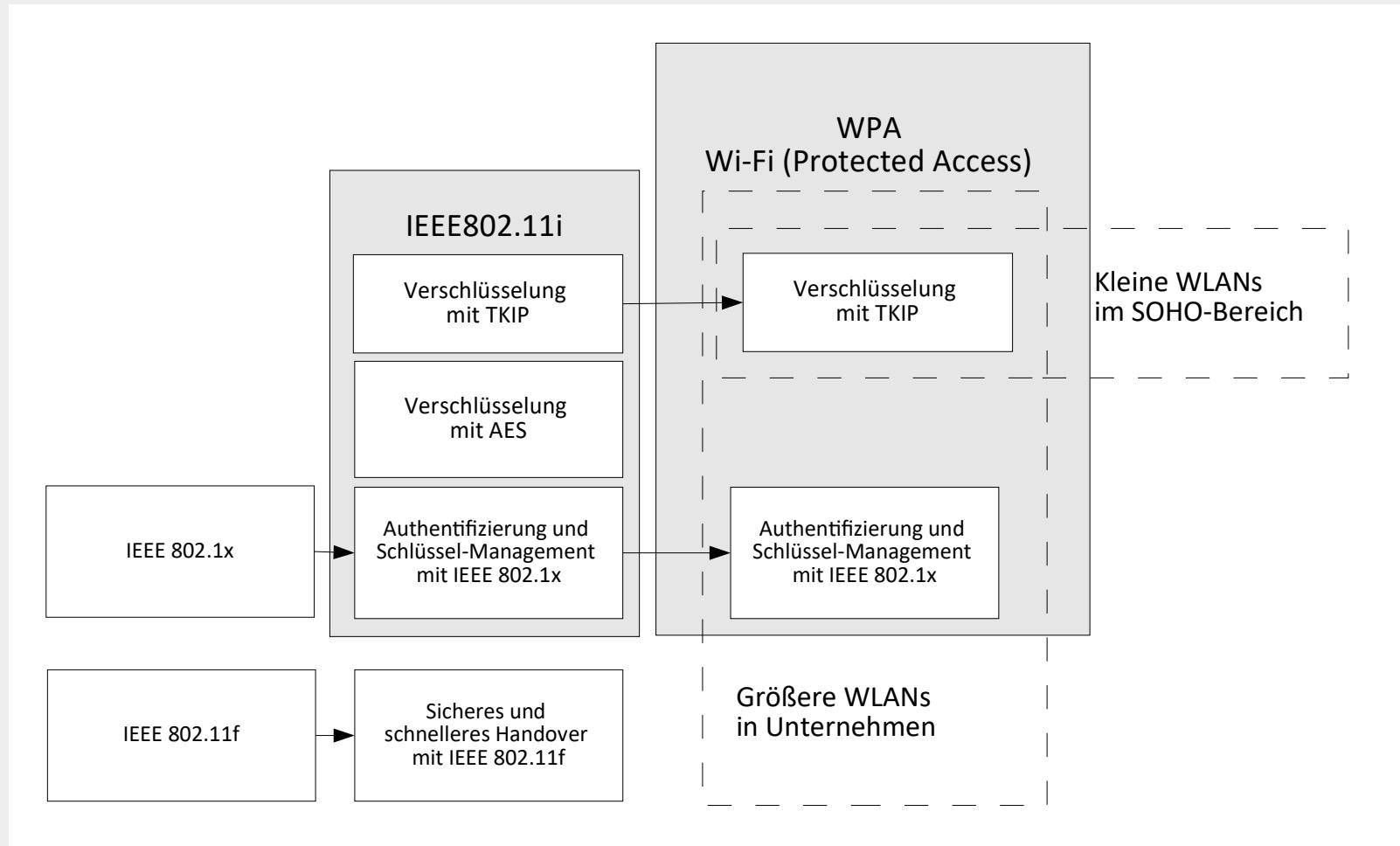


WEP-Desaster

Die mit der Wired Equivalent Privacy (WEP) erzeugte Sicherheit hat viele Schwachstellen

- Der Initialisierungsvektor ist mit 24 Bit zu kurz
- Die Schlüssellänge ist mit 40 oder 104 Bit zu kurz
- WEP hat ein Symmetrisches Verschlüsselungsverfahren jedoch kein Schlüssel-Management
- Das Authentifizierungsverfahren kann geknackt werden
- Das Authentifizierungsverfahren authentifiziert keinen Benutzer sondern einen Adapter
- Der für die Integritätskontrolle verwendete Algorithmus kann problemlos modifiziert werden
- Die Frame-Inhalte können wegen der schwachen Integritätskontrolle trotz einem unbekannten WEP-Schlüssel verändert werden

WPA-Modi



WPA2

WPA-Variante		WPA	WPA 2
Personal-Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP / MIC	AES-CCMP
Enterprise-Mode	Authentifizierung	IEEE 802.1x	IEEE 802.1x
	Verschlüsselung	TKIP / MIC	AES-CCMP

Bauelemente der Verschlüsselung mit WPA

Mehrstufige Schlüsselhierarchie mit paarweisen Schlüsseln

- Master-Key
- Transient Key
- Keys für Schlüsselübertragung und Datenübertragung

Schlüsselarten

- Unicasts mit eigener paarweiser Schlüsselhierarchie für jede Verbindung
- Multicasts / Broadcasts mit Schlüsselhierarchie für Gruppen

Bauelemente der Verschlüsselung

- Pseudo Random Number Generator (PRNG)
- Pseudo Random Function (PRF)

$$\text{PRF} - n(K, A, B) = \text{PRF}(K, A, B, n)$$

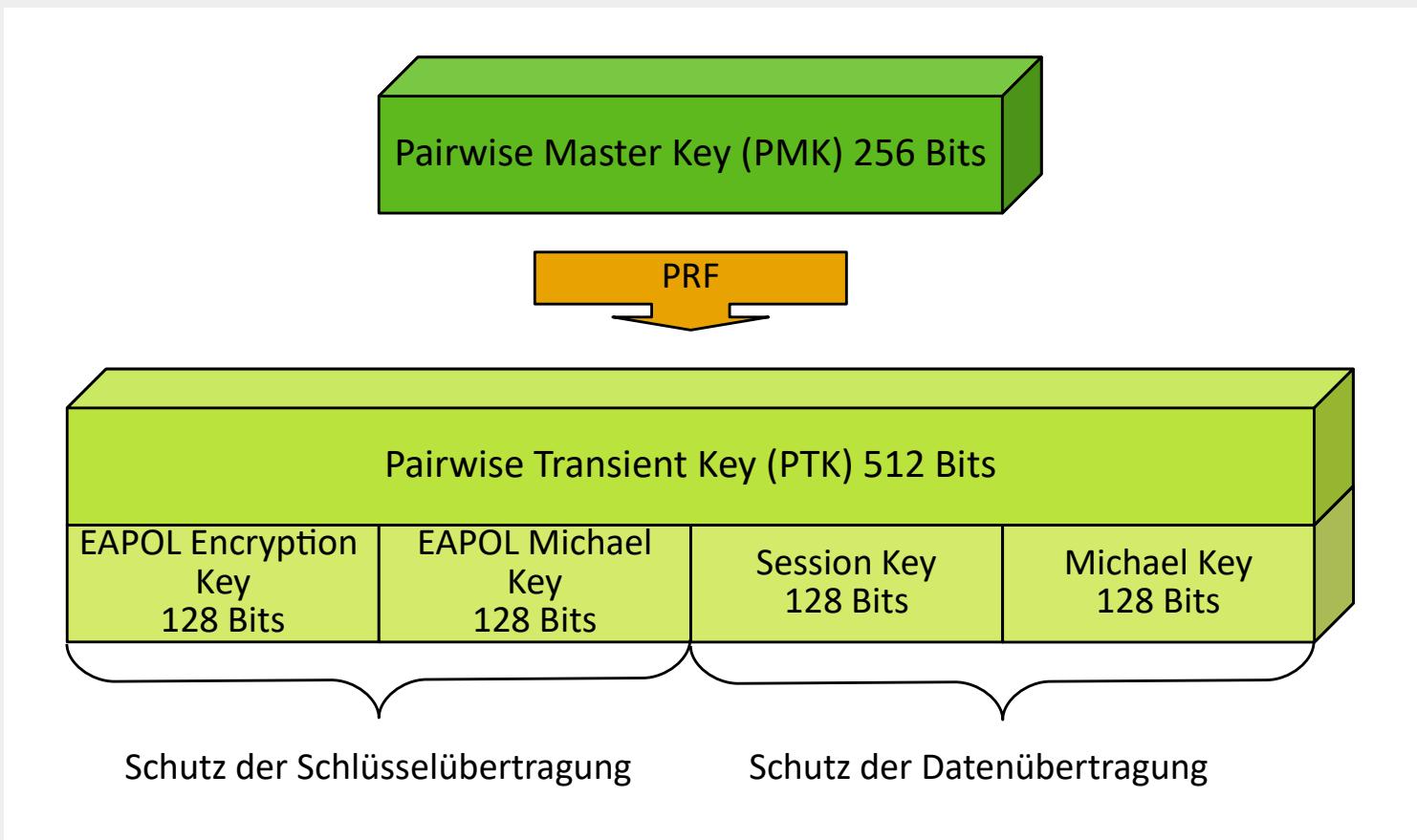
Geheimer Schlüssel (K) , oder ersatzweise ein Zufallswert

Beschreibung (A) der Funktion, für die der Aufruf der PRF dient. (Z. B. „Pairwise key expansion“)

Bytefolge, bestehend aus MAC-Adresse und Zeit-Rahmen

Gewünschte Länge (n)

TKIP Pairwise Key Hierarchie



PTK = PRF-512(PMK, "Pairwise key extension", MAC1 || MAC2 || Nonce1 || Nonce2)

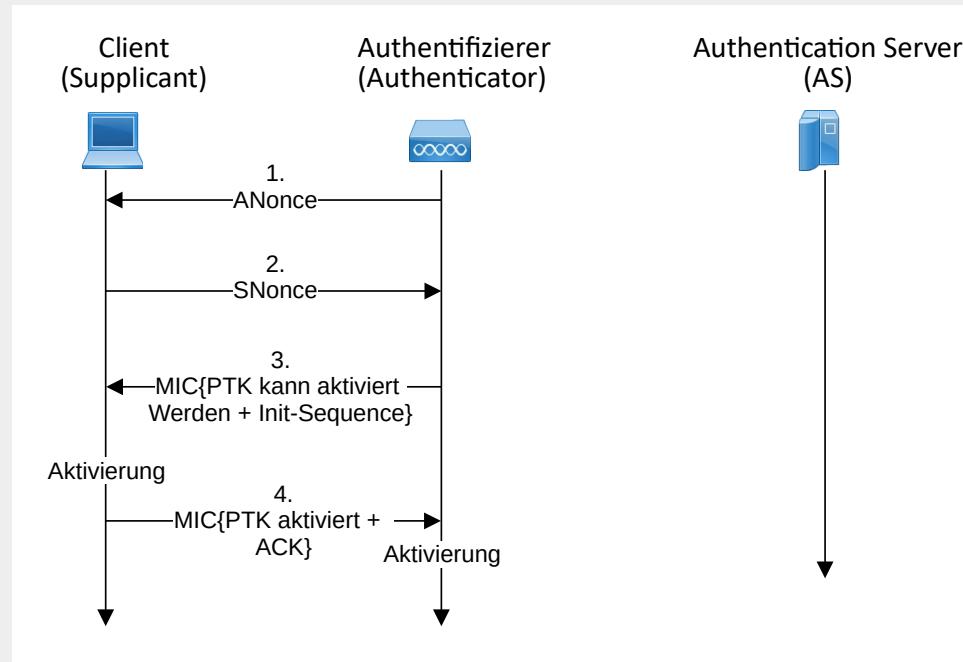
Erzeugen der Transient Keys

Der Pairwise Transient Key (PTK) wird mit einer PRF aus folgenden Komponenten erzeugt:

- PMK
- MAC-Adresse des Authenticators
- MAC-Adresse des Supplicants
- Nonce (Zufallszahl) des Authenticators
- Nonce des Supplicants

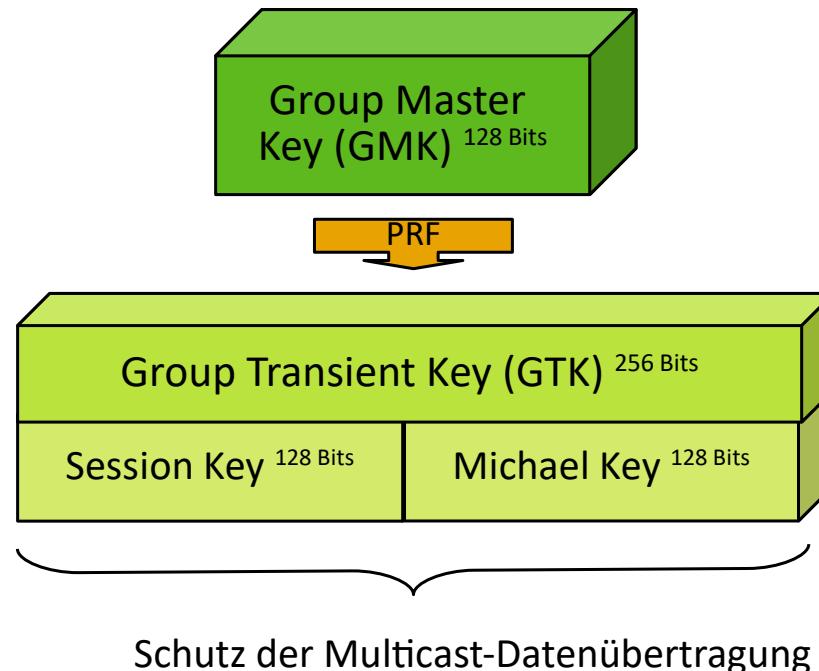
$\text{PTK} = \text{PRF-n}(\text{PMK}, \text{"Pairwise key extension"}, \text{MAC1} \parallel \text{MAC2} \parallel \text{Nonce1} \parallel \text{Nonce2})$

Austausch der Nonce

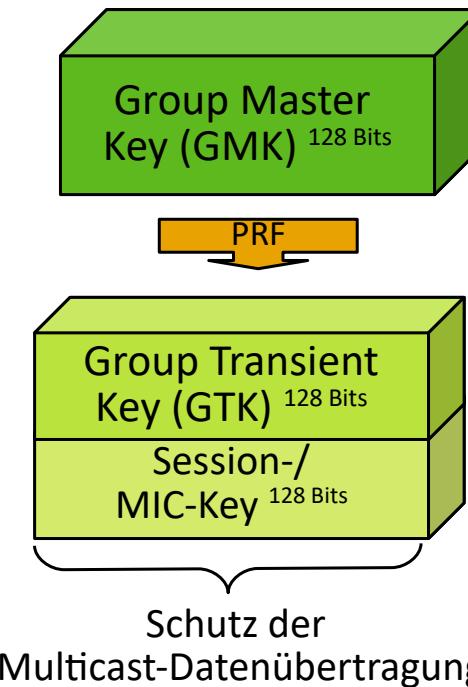


Group Key Schlüsselhierarchie

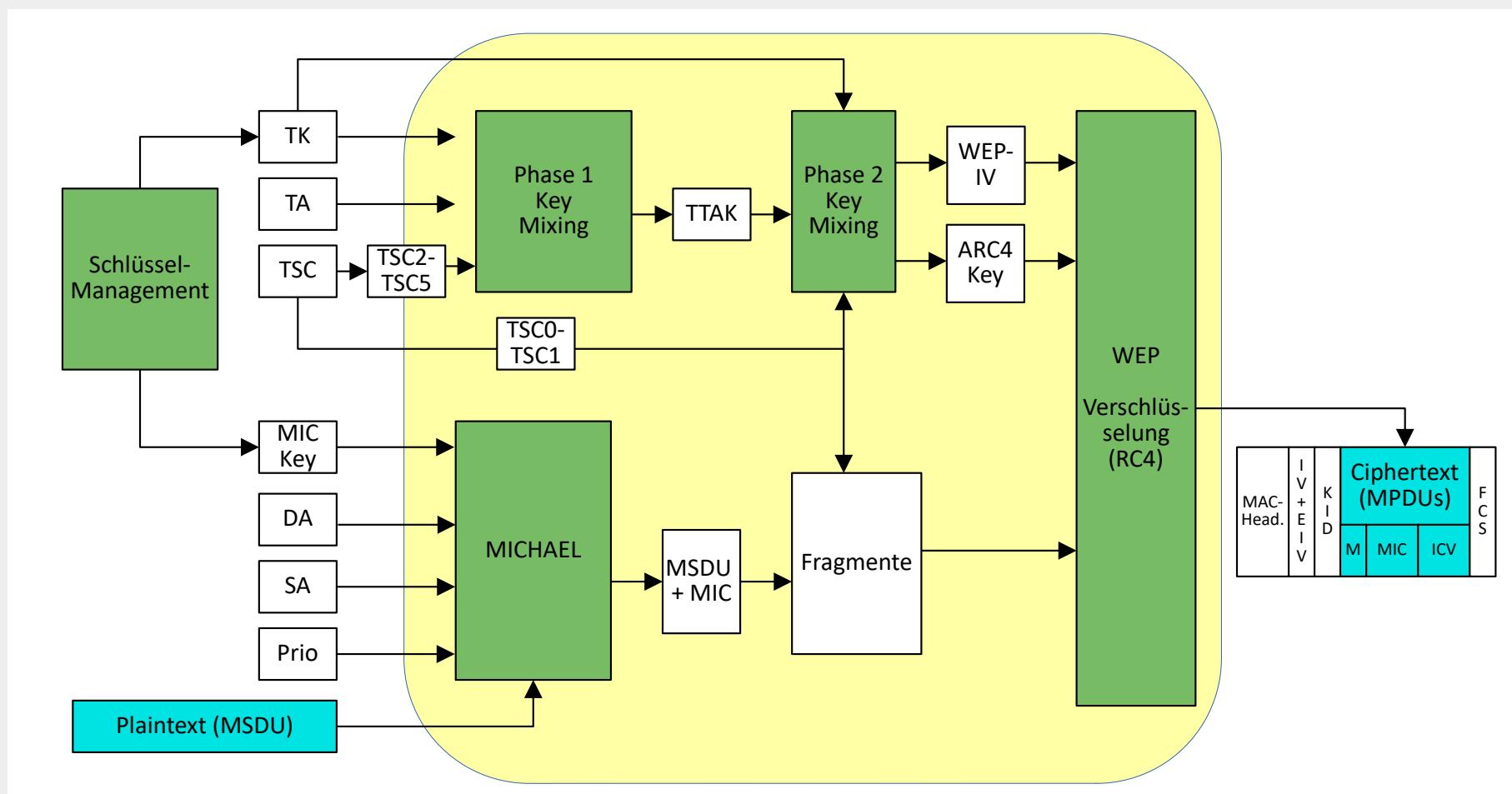
TKIP: Group Key-Schlüsselhierarchie



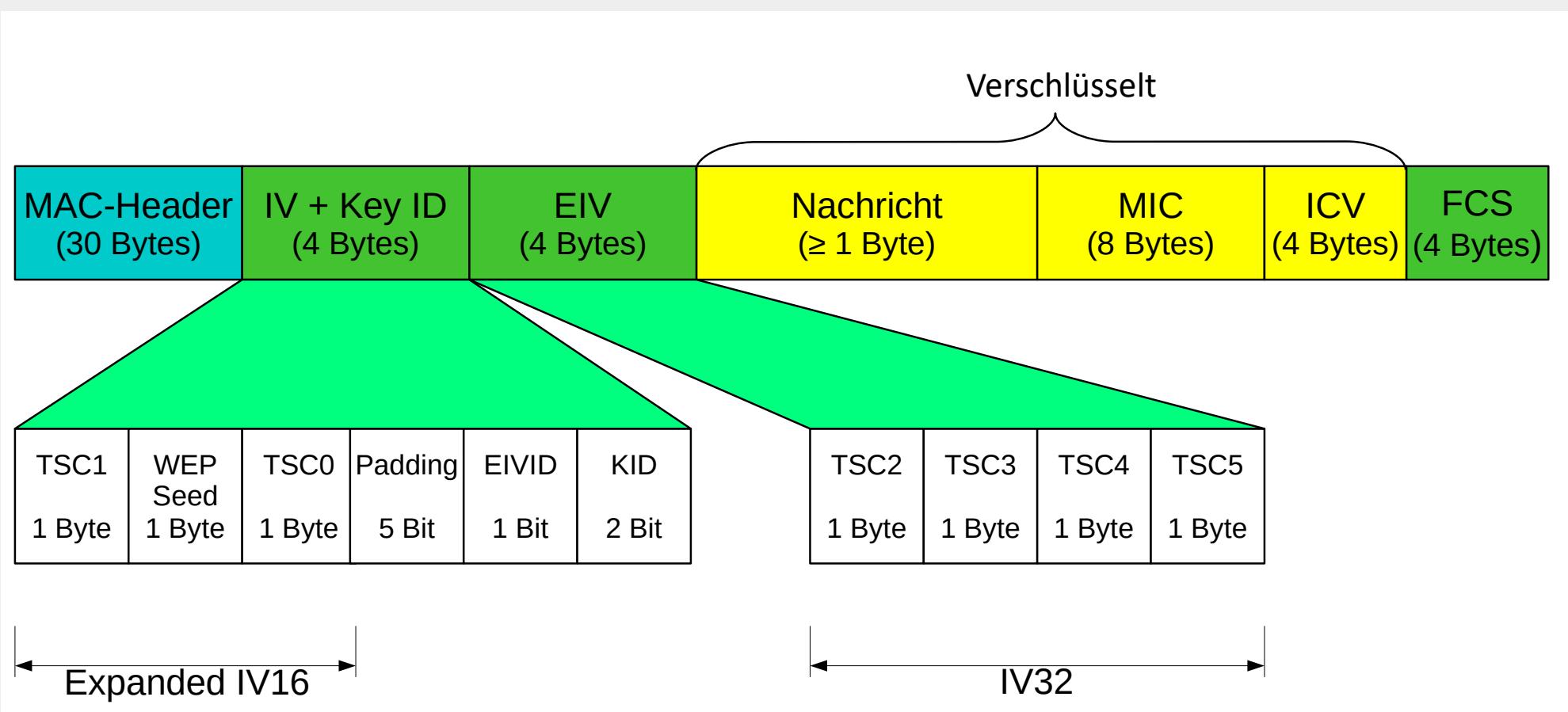
CCMP: Group Key-Schlüsselhierarchie



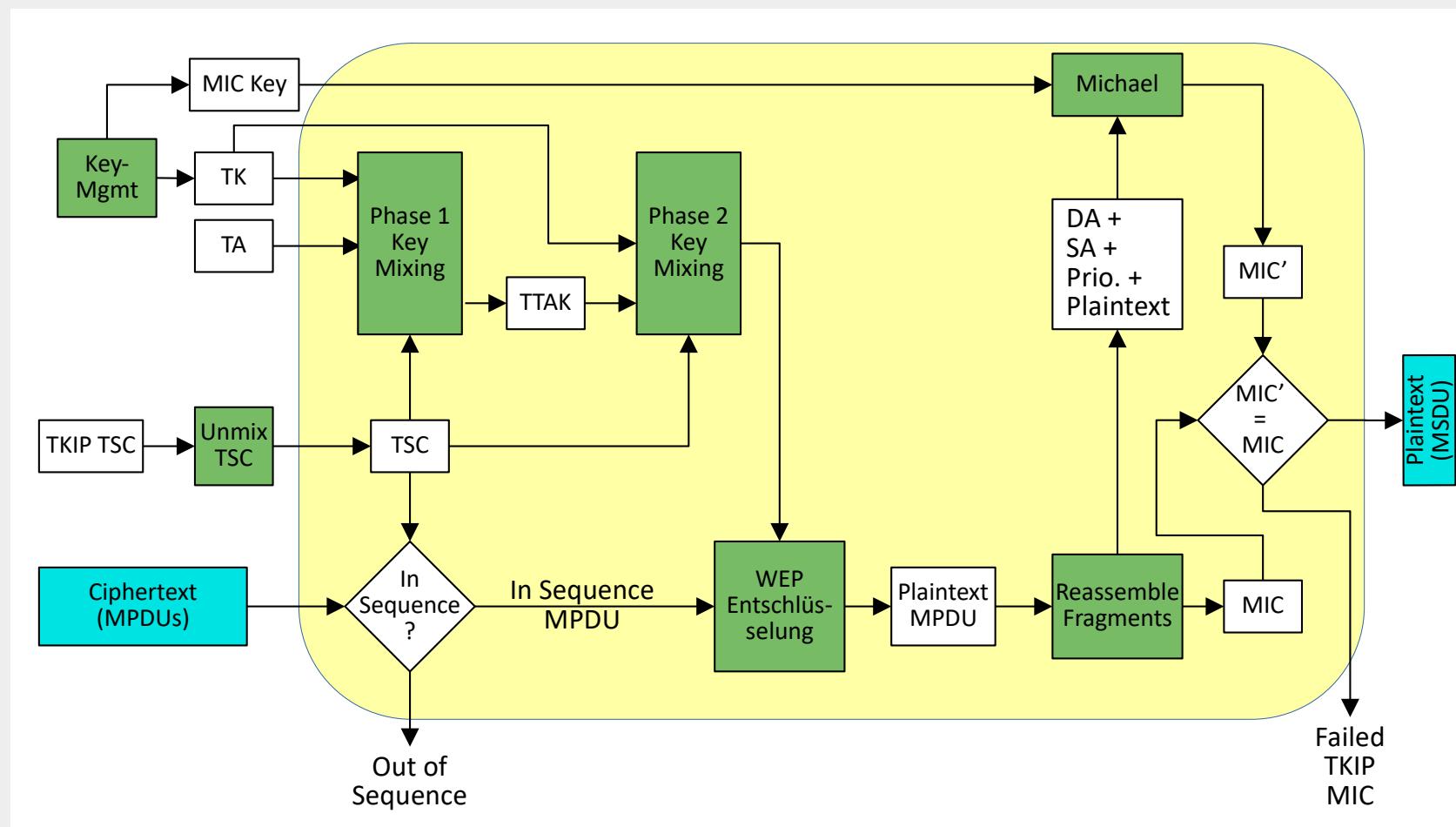
TKIP Verschlüsselung



TKIP-MPDU-Format



TKIP Entschlüsselung



MIC-Fehler

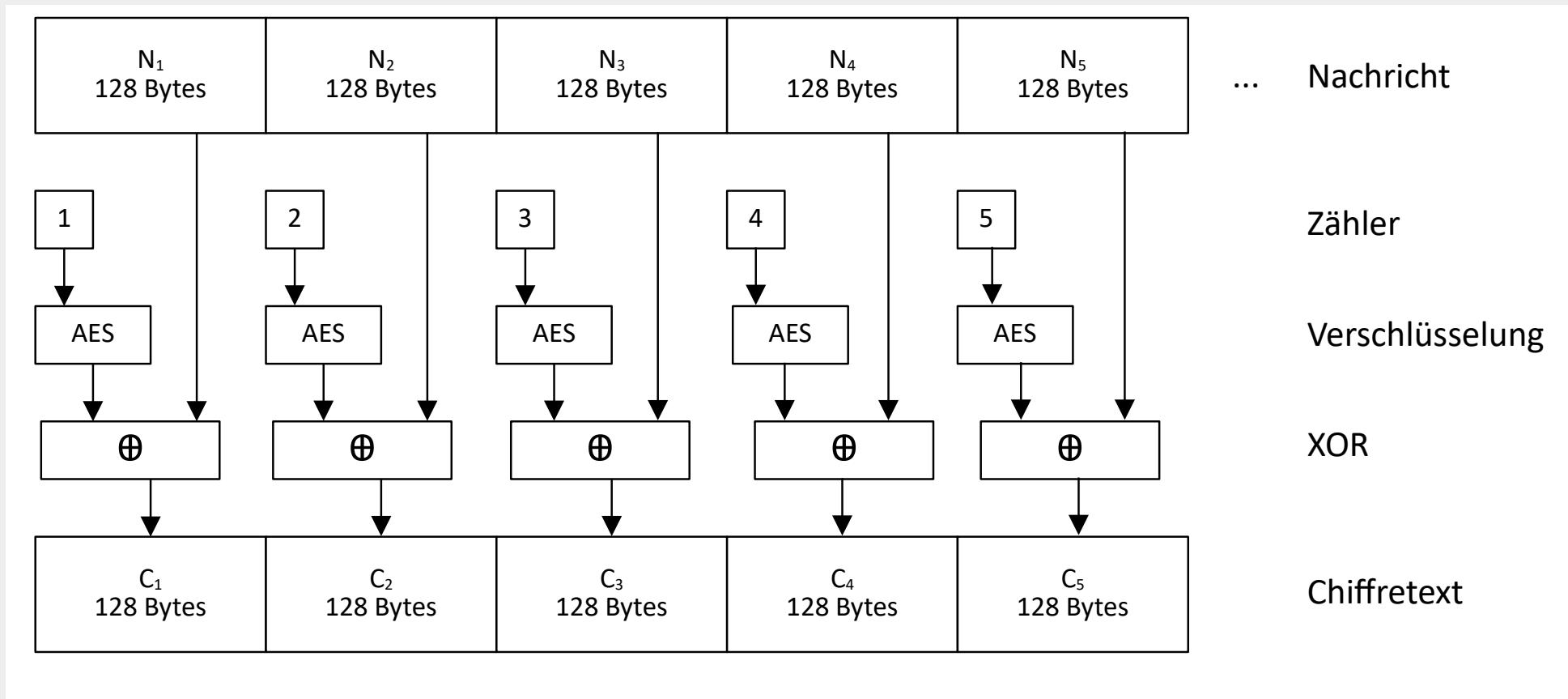
Wird innerhalb von 60 Sekunden mehr als ein MIC-Fehler erkannt, wird eine Attacke angenommen und es deassoziiieren sich die Stationen oder der AP deassoziiert die betroffene Station. Das ist abhängig von der Senderichtung und somit von dem Gerät, das die MIC-Fehler erkennt.

CCMP

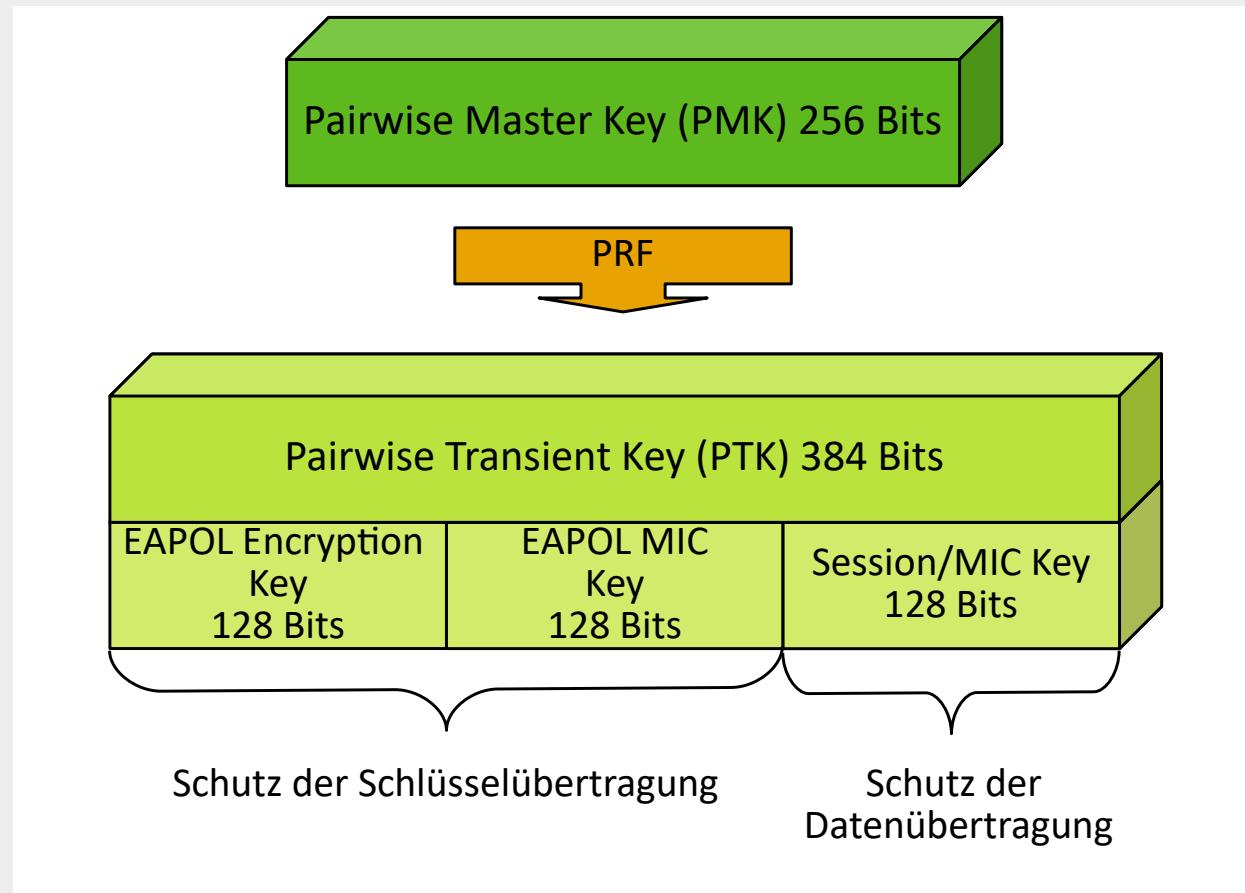
Es wird der Advanced Encryption Standard (AES) verwendet.

Das ist ein Block-Chiffre, der unterschiedliche Längen verschlüsseln kann.
Für WLANs wurde die Blocklänge auf 128 oder 256 Bit festgelegt.

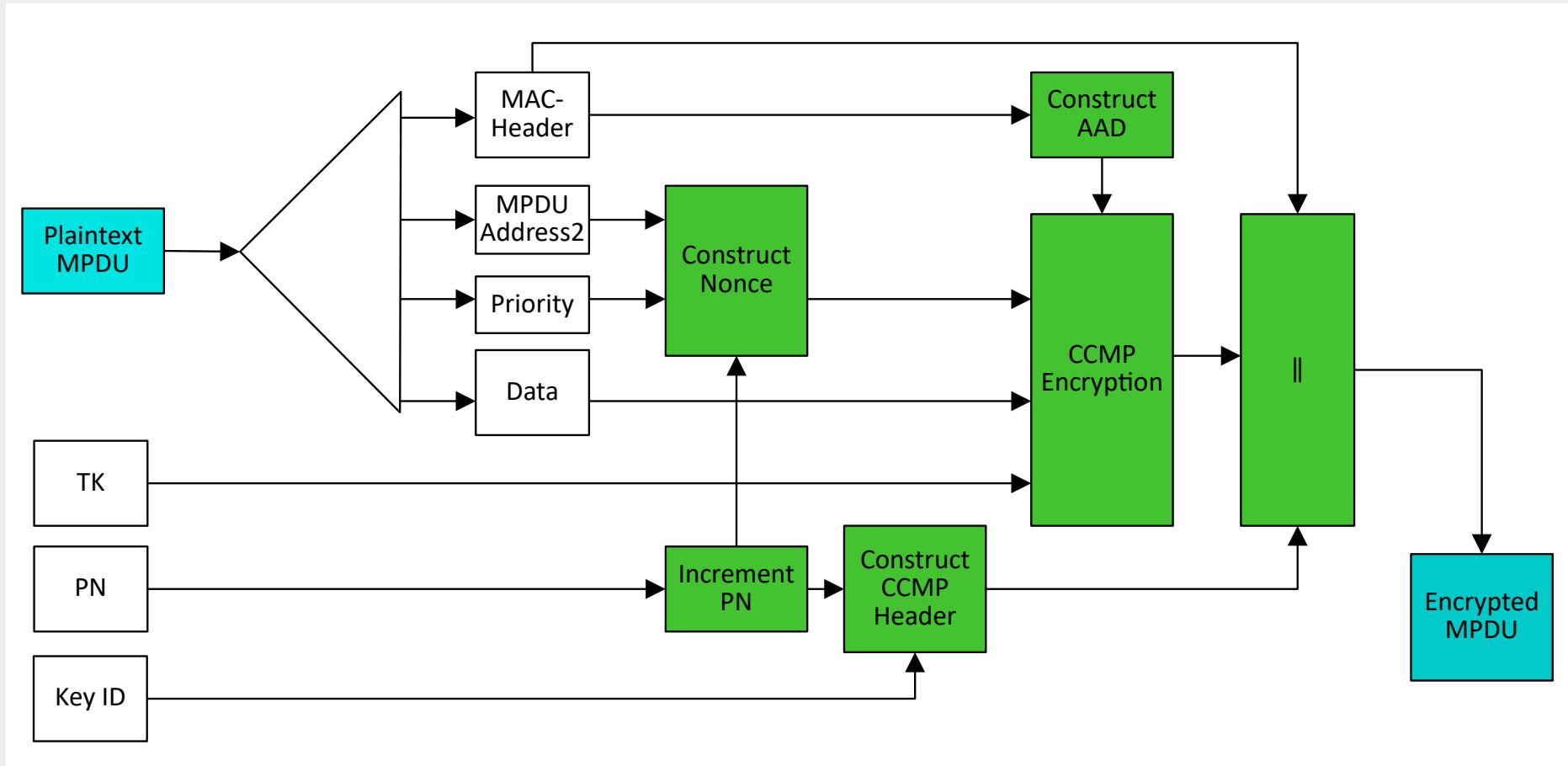
CCMP-CTR-Code



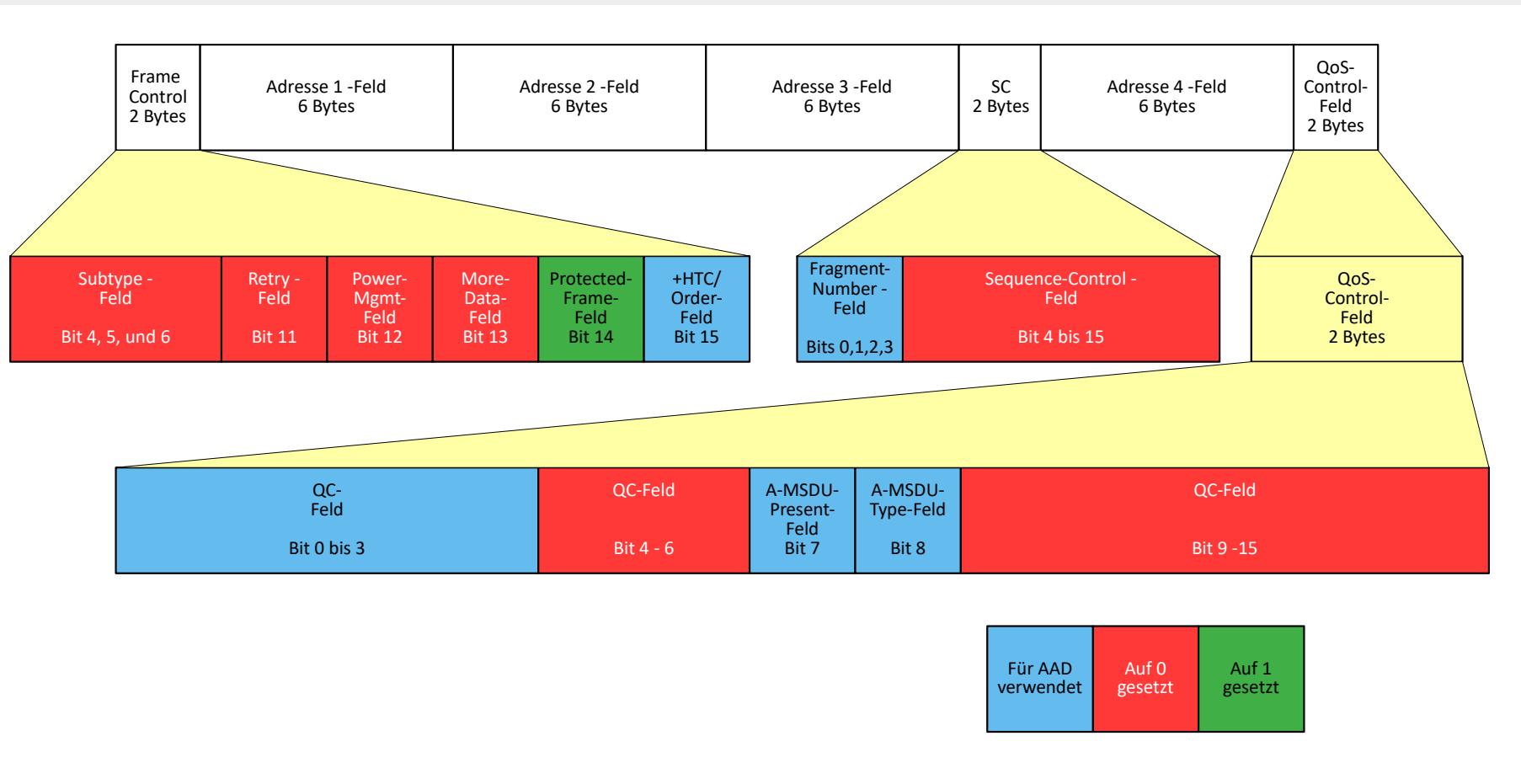
CCMP Pairwise Key Hierarchie



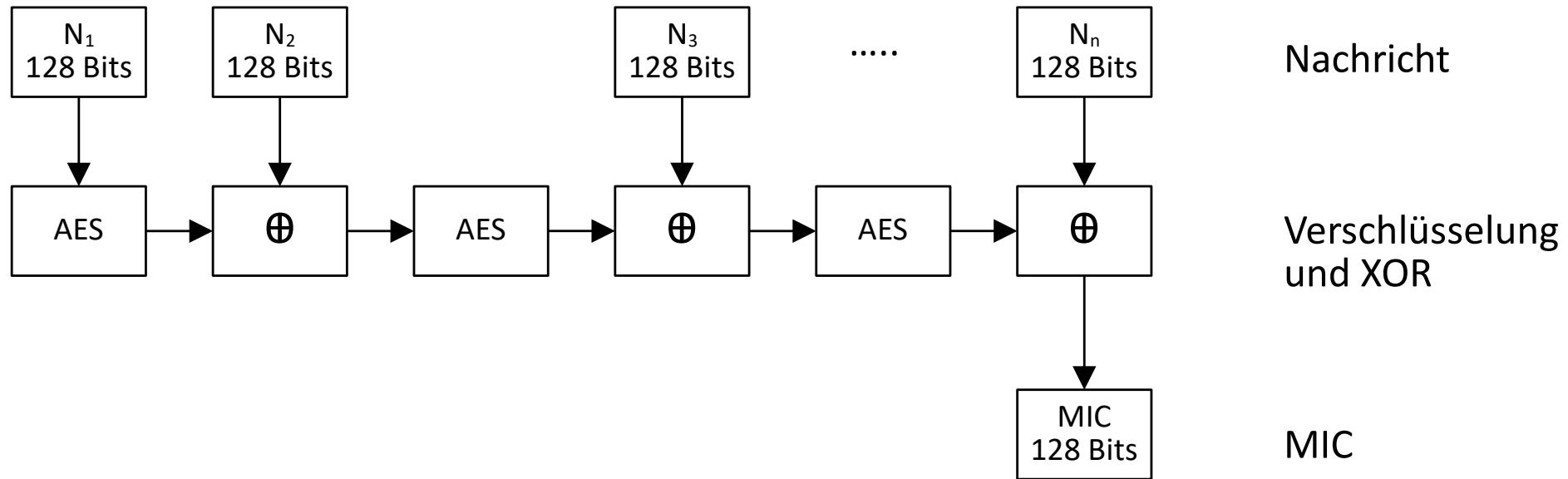
CCMP-Verschlüsselung



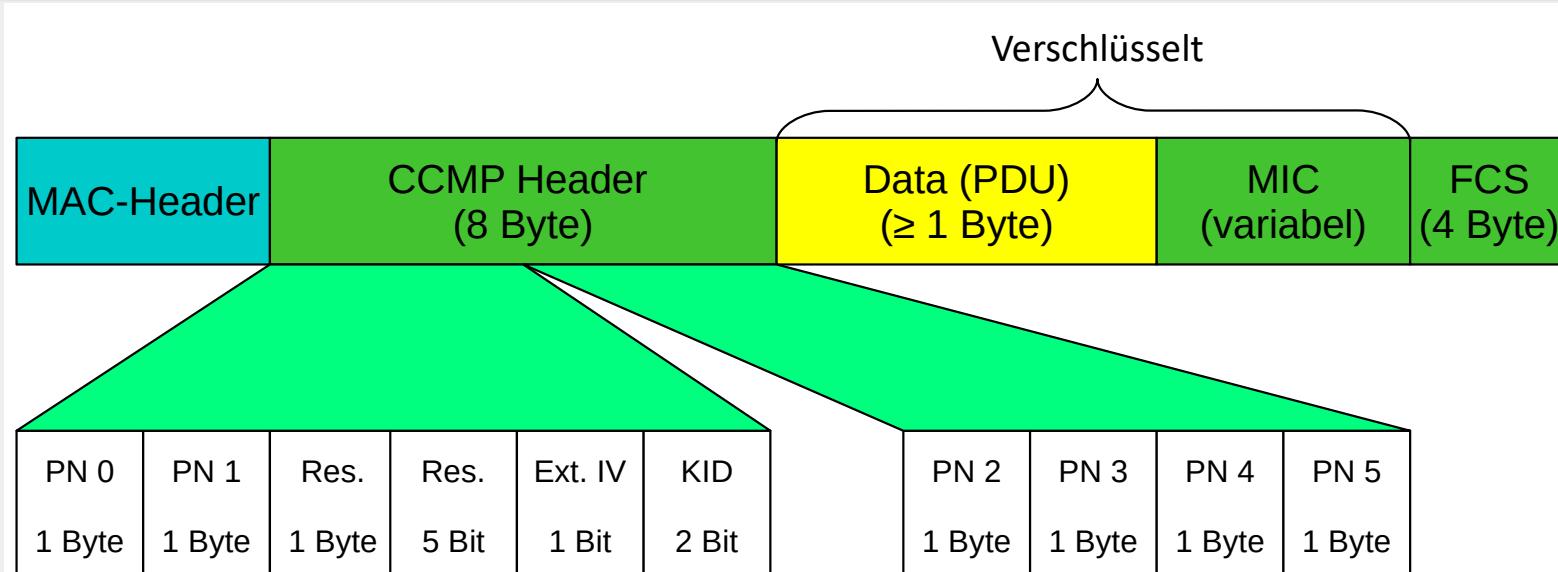
MPDU-Header für den Aufbau der AAD



CCMP-MIC-Berechnung

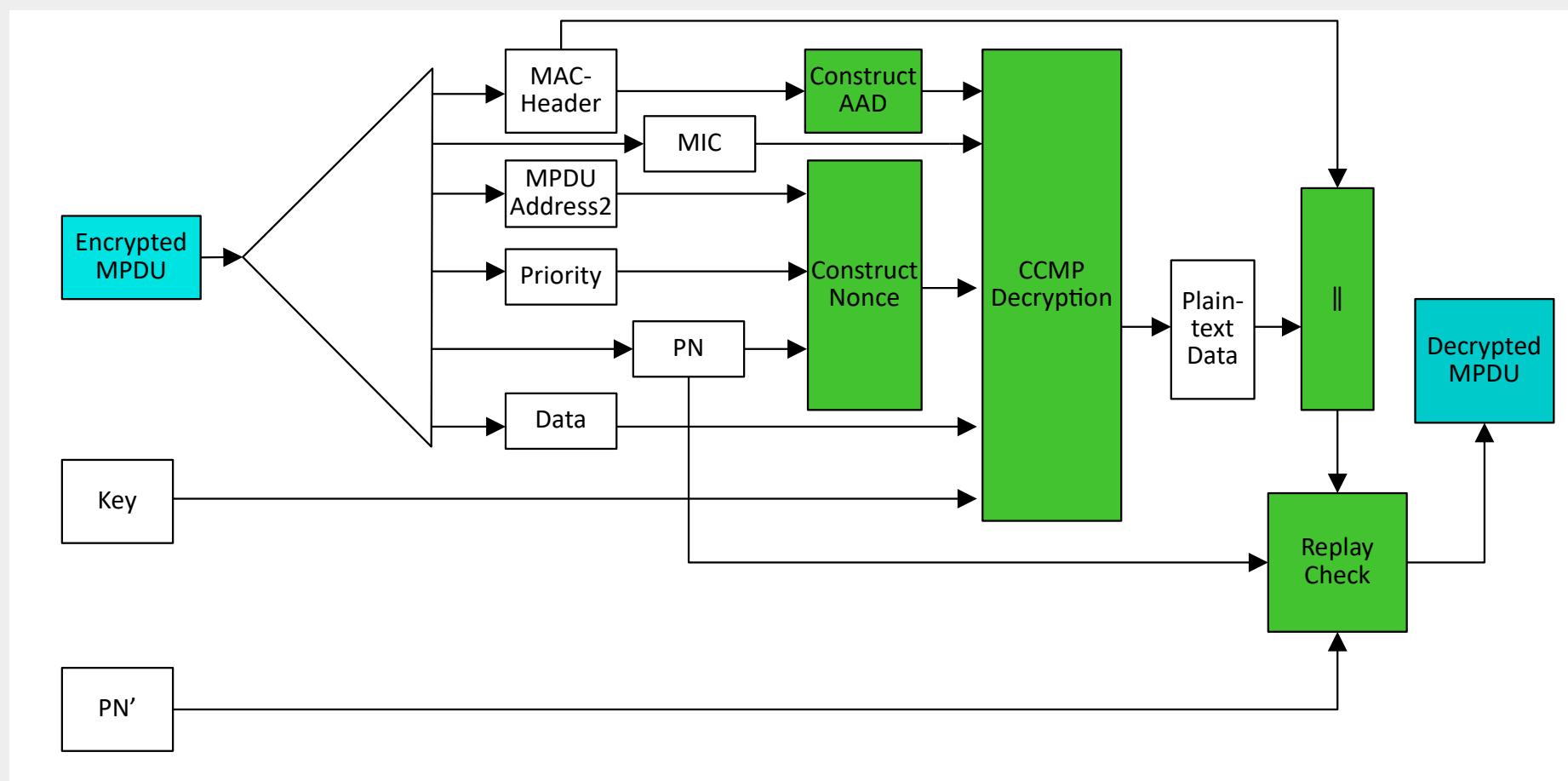


CCMP-MAC-Frame

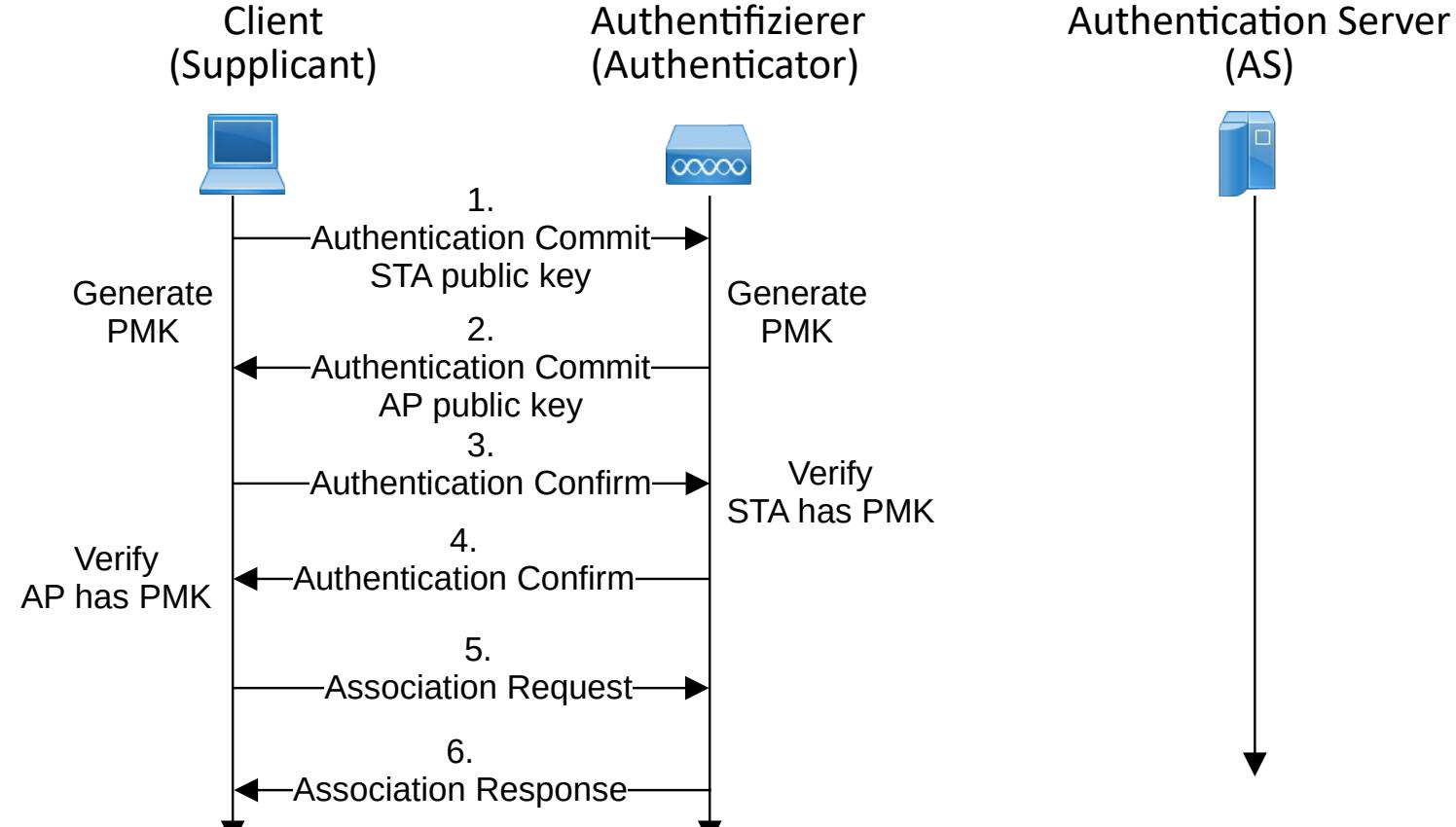


	Parameter					
CCM-Version	M			L		
CCM-128	8 = MIC hat eine Länge von 8 Bytes				2 = MPDU-Längen-Feld ist 2 Bytes groß	
CCM-256	16 = MIC hat eine Länge von 16 Bytes				2 = MPDU-Längen-Feld ist 2 Bytes groß	

CCMP-Entschlüsselung



WPA3



Inhalt

- Verschlüsselung
- Ziele
- WEP-Verschlüsselung / WEP-Desaster
- WPA / WPA2
 - ◆ Bauelemente der Verschlüsselung
 - ◆ Erzeugen der Transient Keys
 - ◆ Austausch der Nonce
- TKIP
 - ◆ Pairwise Key Hierarchie
 - ◆ Group Key Schlüsselhierarchie
 - ◆ TKIP Verschlüsselung / MPDU-Format / Entschlüsselung / MIC-Fehler
- CCMP
 - ◆ Pairwise Key Hierarchie
 - ◆ CTR-Code
 - ◆ Verschlüsselung / AAD-Aufbau / MIC-Berechnung / MAC-Frame / Entschlüsselung

WLAN-Vorlesung Teil-9

- Verschlüsselung
- Ziele
- WEP-Verschlüsselung / WEP-Desaster
- WPA / WPA2
 - ◆ Bauelemente der Verschlüsselung
 - ◆ Erzeugen der Transient Keys
 - ◆ Austausch der Nonce
- TKIP
 - ◆ Pairwise Key Hierarchie
 - ◆ Group Key Schlüsselhierarchie
 - ◆ TKIP Verschlüsselung / MPDU-Format / Entschlüsselung / MIC-Fehler
- CCMP
 - ◆ Pairwise Key Hierarchie
 - ◆ CTR-Code
 - ◆ Verschlüsselung / AAD-Aufbau / MIC-Berechnung / MAC-Frame / Entschlüsselung
- WPA3

Bei der Übertragung von Daten sollten die folgenden Schutzziele erfüllt werden:

- Authentizität
- Datenintegrität
- Vertraulichkeit
- Verfügbarkeit
- Verbindlichkeit
- Anonymisierung

Authentizität entspricht der Echtheit / Glaubwürdigkeit, die anhand einer Identität oder charakteristischen Eigenschaft überprüfbar sein muss.

Datenintegrität ist gewährleistet, wenn es nicht möglich ist die zu übertragenden Daten unautorisiert zu manipulieren (Löschen, Hinzufügen, Ändern, Wiederholen, ..)

Vertraulichkeit bedeutet, dass es keine Möglichkeit gibt unautorisiert an die übertragenen Daten zu kommen

Verfügbarkeit bedeutet, dass berechtigte Benutzer nicht in der Wahrnehmung ihrer Rechte beeinträchtigt werden dürfen.

Verbindlichkeit bedeutet, dass es im Nachhinein nicht möglich sein darf abzustreiten dass die Daten von einem bestimmten User gesendet wurden.

Anonymisierung stellt sicher, dass anhand der übertragenen Information nicht auf natürliche Personen zurückgeschlossen werden kann.

Die Schutzziele können mit unterschiedlichen Maßnahmen erreicht werden.
Allerdings ist dazu oft ein nicht unerheblicher Aufwand erforderlich.

In verkabelten Systemen sind die Schutzziele oft (aber nicht immer) einfacher zu realisieren.
Bei WLANs ist es schon allein durch das offene Medium Luft nicht einfach möglich die Schutzziele umzusetzen. Allein die Begrenzung der Reichweite eines WLANs ist nicht ohne weiteres möglich.

Mit den folgenden Maßnahmen soll trotzdem eine Sicherheit, die die einem verkabelten System entspricht, erreicht werden.

- Authentifizierung bei der Anmeldung
- Verschlüsselung bei der Datenübertragung
- Eindeutige Sequenznummern und Prüfsummen zum Schutz der Datenintegrität

Authentizität → Authentifizierung bei der Anmeldung

Datenintegrität → Verschlüsselung, Sequenznummern

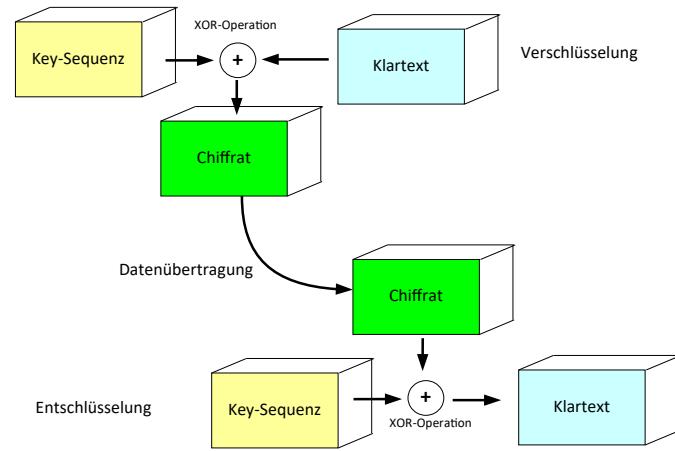
Vertraulichkeit → Verschlüsselung

Verfügbarkeit →

Verbindlichkeit →

Anonymisierung → Usernamen (Pseudomisierung)

Verschlüsselung



Eine oft angewandte Verschlüsselung ist die symmetrische Verschlüsselung.

Dabei wird ein Klartext mit einer Key-Sequenz zu einem Chiffrat mittels einer XOR-Operation verschlüsselt.

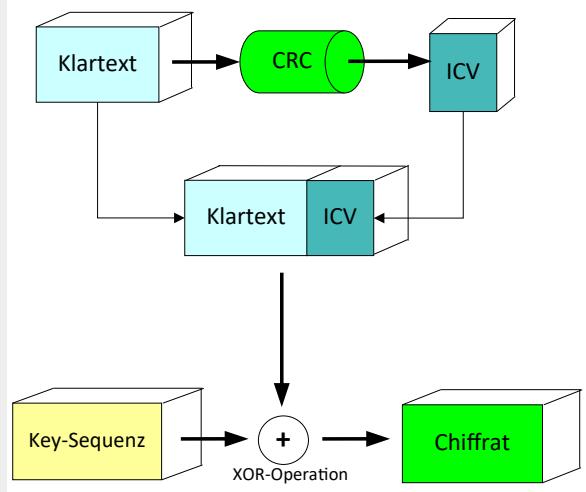
Das Chiffrat kann dann über einen Kanal transportiert werden, da aus ihm keine Rückschlüsse mehr auf den Inhalt des Textes gezogen werden können.

Auf der Empfängerseite wird die gleiche XOR-Operation mit dem gleichen Schlüssel durchgeführt um den Klartext wieder herzustellen.

Nachteil der symmetrischen Verschlüsselung ist, dass der gleiche Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln vorliegen muss.

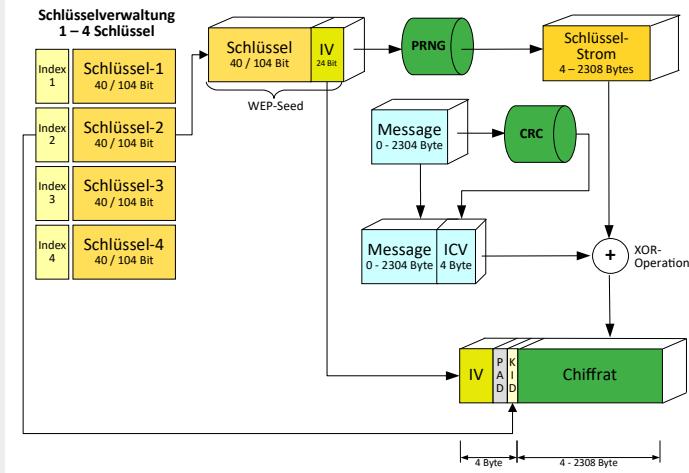
Gelangt ein Angreifer an ein Chiffrat und einen Klartext kann durch die XOR-Operation der Schlüssel erzeugt werden.

WEP-Verschlüsselung



Eine Maßnahme zur Sicherung der Datenintegrität ist, dass aus dem Klartext mit einem Cyclic Redundancy Check eine Prüfsumme (Integrity Check Value = ICV) erzeugt wird, die dem zu übertragenden Text vor der Verschlüsselung angehängt wird.

WEP-Verschlüsselung



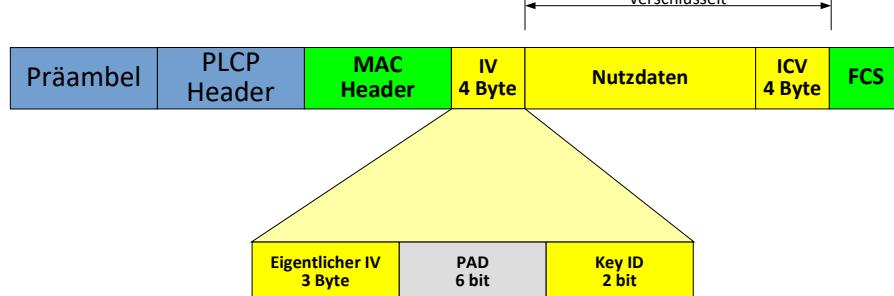
Für die Verschlüsselung steht ein Pool von bis zu vier Schlüsseln zur Verfügung, aus dem einer für die Übertragung ausgewählt wird. Der Schlüssel-Pool muss natürlich sowohl auf der Senderseite als auch auf der Empfangsseite zur Verfügung stehen.

Aus dem verwendeten Schlüssel wird zusammen mit einem 24 Bit-Initialisierungsvektor mittels einem Pseudo Zufallszahlengenerator (Pseudo Random Number Generator = PRNG) ein Schlüsselstrom generiert.

Mit dem Schlüsselstrom wird dann der Klartext mitsamt der Prüfsumme zum Chiffrat verschlüsselt.

Dem Chiffrat wird im Frame der Initialisierungsvektor sowie der Schlüsselindex im Klartext vorangestellt.

Frame-Aufbau mit WEP-Verschlüsselung



Damit ergibt sich der in der Folie dargestellte Frameaufbau.

Der 3 Byte (24 Bit) große Initialisierungsvektor (IV) muss nach 2^{24} Verschlüsselungen wiederholt werden, was evtl. ein Problem darstellen kann.

Die mit der Wired Equivalent Privacy (WEP) erzeugte Sicherheit hat viele Schwachstellen

- Der Initialisierungsvektor ist mit 24 Bit zu kurz
- Die Schlüssellänge ist mit 40 oder 104 Bit zu kurz
- WEP hat ein Symmetrisches Verschlüsselungsverfahren jedoch kein Schlüssel-Management
- Das Authentifizierungsverfahren kann geknackt werden
- Das Authentifizierungsverfahren authentifiziert keinen Benutzer sondern einen Adapter
- Der für die Integritätskontrolle verwendete Algorithmus kann problemlos modifiziert werden
- Die Frame-Inhalte können wegen der schwachen Integritätskontrolle trotz einem unbekannten WEP-Schlüssel verändert werden

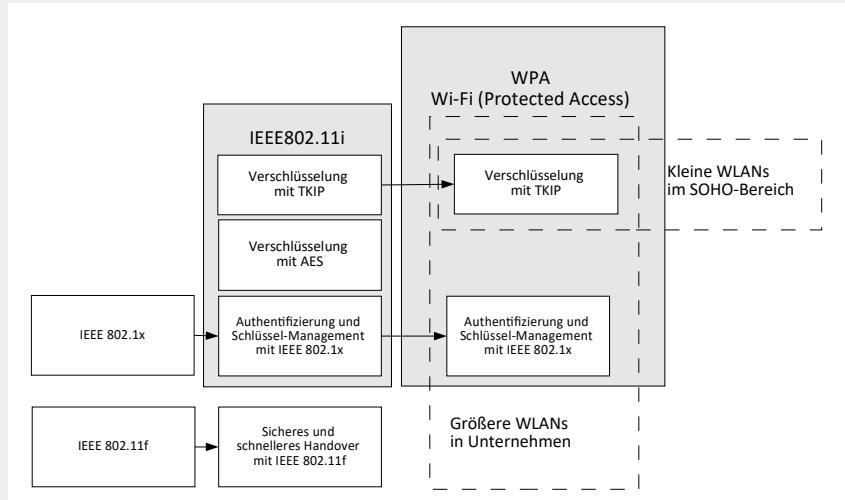
Für die meisten Punkte gibt es gleich mehrere Angriffsszenarien.

Beispiel:

Die Schlüssel enthalten bei einer Länge von 64Bit einen 24Bit langen Initialisierungsvektor und sind damit nur 40 Bit lang.

Bei einer Länge von 128Bit enthält der Schlüssel auch einen 24Bit langen Initialisierungsvektor und sind damit nur 104 Bit lang

WPA-Modi



Als erste Reaktion auf das WEP-Desaster wurden mit WPA für zwei Bereiche unterschiedliche Modi eingeführt:

Enterprise-Mode (für den Einsatz in Firmen)
IEEE802.1x zur Authentifizierung

Temporal Key Integrity Protocol (TKIP)
sowie der Message Integrity Check (MIC) zur Verschlüsselung

Personal-Mode (für SoHo-Lösungen)
Preshared Keys zur Authentifizierung

Temporal Key Integrity Protocol (TKIP)
sowie der Message Integrity Check (MIC) zur Verschlüsselung

WPA-Variante		WPA	WPA 2
Personal-Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP / MIC	AES-CCMP
Enterprise-Mode	Authentifizierung	IEEE 802.1x	IEEE 802.1x
	Verschlüsselung	TKIP / MIC	AES-CCMP

Bei der WPA2-Lösung wurde TKIP und MIC durch AES-CCMP ersetzt.

Die in IEEE802.11i vorgestellte Sicherheitsarchitektur war komplett neu und wird als **Robust Security Network** (RSN) bezeichnet.

Die wichtigsten Elemente der RSN-Sicherheitsarchitektur sind die Mechanismen zur Verschlüsselung, Integritätssicherung und Authentifizierung.

Mehrstufige Schlüsselhierarchie mit paarweisen Schlüsseln

- Master-Key
- Transient Key
- Keys für Schlüsselübertragung und Datenübertragung

Schlüsselarten

- Unicasts mit eigener paarweiser Schlüsselhierarchie für jede Verbindung
- Multicasts / Broadcasts mit Schlüsselhierarchie für Gruppen

Vom Master Key werden alle anderen Schlüssel abgeleitet. Deshalb ist auf ihn besondere Sorgfalt zu legen. Er soll so selten wie möglich genutzt werden und nach Möglichkeit auch nie übertragen werden.

Die Transient Keys werden in Echtzeit erzeugt und in die einzelnen Keys, die zu unterschiedlichen Zwecken genutzt werden, aufgeteilt.

Auf der Art des Datenaustauschs beruht die Aufteilung in:

Unicasts

Die Keys werden hierbei aus den Transient Keys entnommen. Für Jede Verbindung ist ein Pairwise Key zu verwenden. Jede Station verwaltet einen Pairwise Key, während jeder AP für jede angebundene Station einen Pairwise Key verwaltet.

Multicasts/Broadcasts

Die Groupwise Keys werden mit den Transient Keys erzeugt und gelten für alle an einen AP angebundenen Stationen bei der Verwendung von Multicasts und Broadcasts.

- Pseudo Random Number Generator (PRNG)

- Pseudo Random Function (PRF)

PRF - $n(K, A, B) = PRF(K, A, B, n)$

Geheimer Schlüssel (K) , oder ersatzweise ein Zufalls Wert
Beschreibung (A) der Funktion, für die der Aufruf der PRF dient. (Z. B. „Pairwise key expansion“)
Bytefolge, bestehend aus MAC-Adresse und Zeit-Rahmen
Gewünschte Länge (n)

Die benötigten Zufallszahlen werden mit einem Pseudo Random Number Generator (PRNG) erzeugt. Diese arbeiten deterministisch, was bedeutet, dass bei gleichen Eingangswerten immer die gleichen Ausgangswerte erzeugt werden. Damit kommt dem Startwert eine große Bedeutung zu. Er sollte aus möglichst vielen zufallsabhängigen Daten erzeugt werden um eine ausreichende Zufälligkeit zu erzeugen.

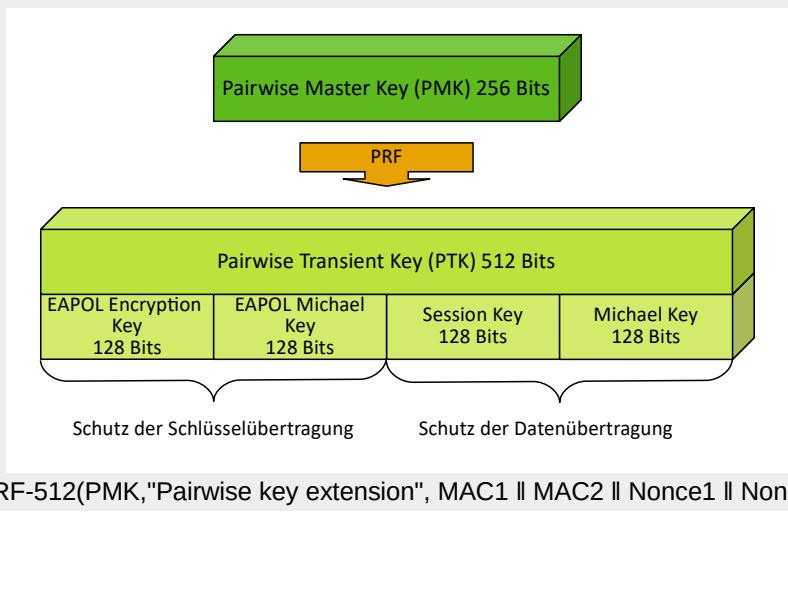
Mit der Pseudo Random Function kann ein n-Bit langer zufälliger Ausgangswert erzeugt werden.

Zweck dieser Funktion ist einen pseudozufälligen Wert mit vorgegebener Länge zu erzeugen, der unabhängig von der Länge der Eingabewerte ist und von dem nicht auf die Eingabewerte geschlossen werden kann.

Verwendet wird dafür der Hashed Message Authentication Code (HMAC) in Kombination mit dem Secure Hash Algorithmus (SHA)-1 kurz HMAC SHA-1. Damit kann ein 20 Byte langer Hashwert erzeugt werden.

Werden längere Werte benötigt wird der Algorithmus mit einem jeweils um 1 inkrementierten Eingabewert mehrfach angewendet. Am Ende wird die Zufallszahl (Z) aus den ersten n Bits, die durch diese Funktion erzeugt wurde, verwendet.

TKIP Pairwise Key Hierarchie



Grundlage für das Temporal Key Integrity Protokol (TKIP) ist die Pairwise Key Hierarchie.

An oberster Stelle steht der Pairwise Master Key (PMK) mit einer Länge von 256 Bits.

Der PMK ist im Vorfeld manuell auf den Systemen einzutragen, oder über ein Key-Management (z. B. IEEE802.1x) zu verteilen.

Aus dem PMK werden die 512Bit langen Pairwise Transient Keys (PTK) mit der Pseudo Random Function (PRF) in Echtzeit erzeugt.

Die 512 Bits der PTKs werden in vier 128 Bit große Schlüssel aufgeteilt, die zur Hälfte zur Schlüsselübertragung und zur Datenübertragung genutzt werden .

Der Pairwise Transient Key (PTK) wird mit einer PRF aus folgenden Komponenten erzeugt:

- PMK
- MAC-Adresse des Authenticators
- MAC-Adresse des Supplicants
- Nonce (Zufallszahl) des Authenticators
- Nonce des Supplicants

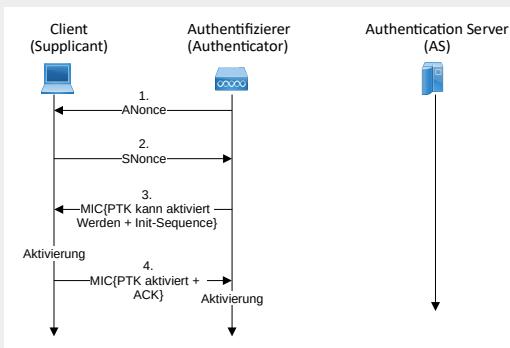
$\text{PTK} = \text{PRF-n}(\text{PMK}, \text{"Pairwise key extension"}, \text{MAC1} \parallel \text{MAC2} \parallel \text{Nonce1} \parallel \text{Nonce2})$

Der Trancient Key wird aus mehreren Bestandteilen mittels der Pseudo Random Function (PRF) zusammengesetzt.

Dazu zählen

- Pairwise Master Key
- MAC-Adressen der der Kommunikationspartner
- ANonce (Nonce des Authenticators)
- SNonce (Nonce des Supplicants)

Austausch der Nonce



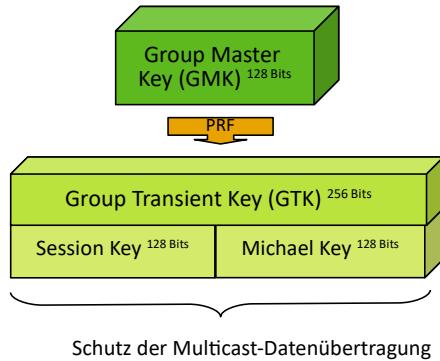
1. Zuerst sendet der Authenticator den Authenticator Nonce (ANonce) an den Supplicant. Dies erfolgt im Klartext. Damit kann der Client seinen PTK zusammenbauen und verwenden.
2. Danach sendet der Supplicant den Supplicant Nonce (SNonce) an den Authenticator. Dies erfolgt wiederum unverschlüsselt jedoch erfolgt mit Hilfe des zuvor berechneten EAPOL MIC-Schlüssels vorher ein Integritätscheck.
3. Der Authenticator sendet nun eine mit MIC verschlüsselte Nachricht „Aktivierung der PTKs kann vorgenommen werden“ + Sequenznummer der künftigen MPDUs
4. Der Supplicant bestätigt mit einer MIC-verschlüsselten Nachricht an den Authenticator die erfolgreiche Schlüsselerzeugung und aktiviert ihn.

Nach dem Empfang und MIC-Prüfung der Nachricht aktiviert der Authenticator ebenfalls seinen PTK.

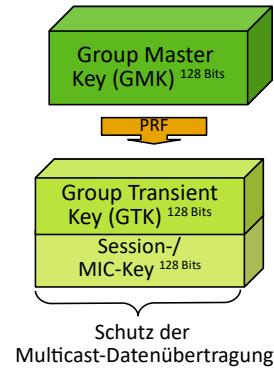
Nach dem erfolgreichen Ablauf des 4-Wege-Handshakes haben die Teilnehmer die erforderlichen temporären Schlüssel (PTKs) aktiviert. Der Standard bezeichnet diesen Status auch als Pairwise Transient Key Security Association (PTKSA) und Group Transient Key Security Association (GTKSA).

Group Key Schlüsselhierarchie

TKIP: Group Key-Schlüsselhierarchie



CCMP: Group Key-Schlüsselhierarchie

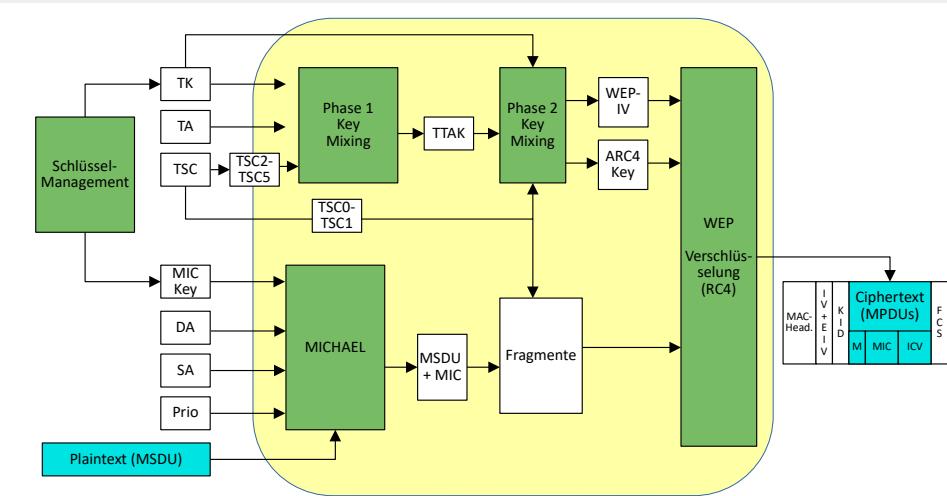


Der Authenticator (AP) übernimmt die Erstellung der Gruppenschlüssel. Das gestaltet sich nun einfacher da bereits eine sichere Verbindung besteht.

Verlässt ein Client ein Netzwerk, teilt er das dem AP mit, der daraufhin das Senden an den Client einstellt und den paarweisen Schlüssel für den Client löscht. Auf Clientseite ist keine Aktivität erforderlich.

Problematisch wird es hingegen beim Gruppenschlüssel. Auch nach dem Abmelden des Clients kann er ihn noch nutzen. Deshalb muss er vom AP neu erstellt und an die Clients verteilt werden. Da dies zentral vom AP gemacht wird hält sich der Aufwand in Grenzen. Allerdings kann bei erhöhter Fluktuation von Clients ein Problem entstehen. Solange die Gruppenschlüssel verteilt werden können die Clients keine Multicasts und Broadcasts empfangen. Erst wenn der letzte Client den neuen Gruppenschlüssel hat, können alle Clients wieder mit dem neuen Gruppenschlüssel arbeiten. Dieses Problem wird mit einer alten WEP Eigenschaft gelöst, bei der bis zu 4 Schlüssel mittels einer Key-ID (KID) verwaltet werden konnten. Der auf dem Client gespeicherte Gruppenschlüssel hat die KID = 0. Damit sind 3 weitere Gruppenschlüssel möglich. Während der AP die neuen Gruppenschlüssel verteilt sendet er Multicasts und Broadcasts noch mit dem alten Gruppenschlüssel. Sobald der neue Gruppenschlüssel verteilt ist, sendet er mit dem neuen Schlüssel und deaktiviert den alten Gruppenschlüssel bei sich und den Clients. Dies sorgt dafür, dass vor allem bei Audio- und Videostreaming Diensten keine Beeinträchtigungen erfolgen.

TKIP Verschlüsselung



Das Schlüsselmanagement stellt den Michael Key (MIC Key) und den Session Key (TK) zur Verfügung. Der Michael Key dient zur Sicherung der Datenintegrität während der TK der Datenverschlüsselung dient. Die zu übertragenden Daten werden in Form der MSDU zugeführt. Mithilfe der Source-MAC-Adresse (SA), der Destination-MAC-Adresse (DA) IUND der Priorität wird zusammen mit dem Michael Key mittels der Michael-Hash-Funktion der TKIP Message Integrity Code (MIC) errechnet und an die MSDU angehängt. Der MIC verlängert die MSDU um 8 Bytes, was zu einer zusätzlichen Fragmentierung führen kann.

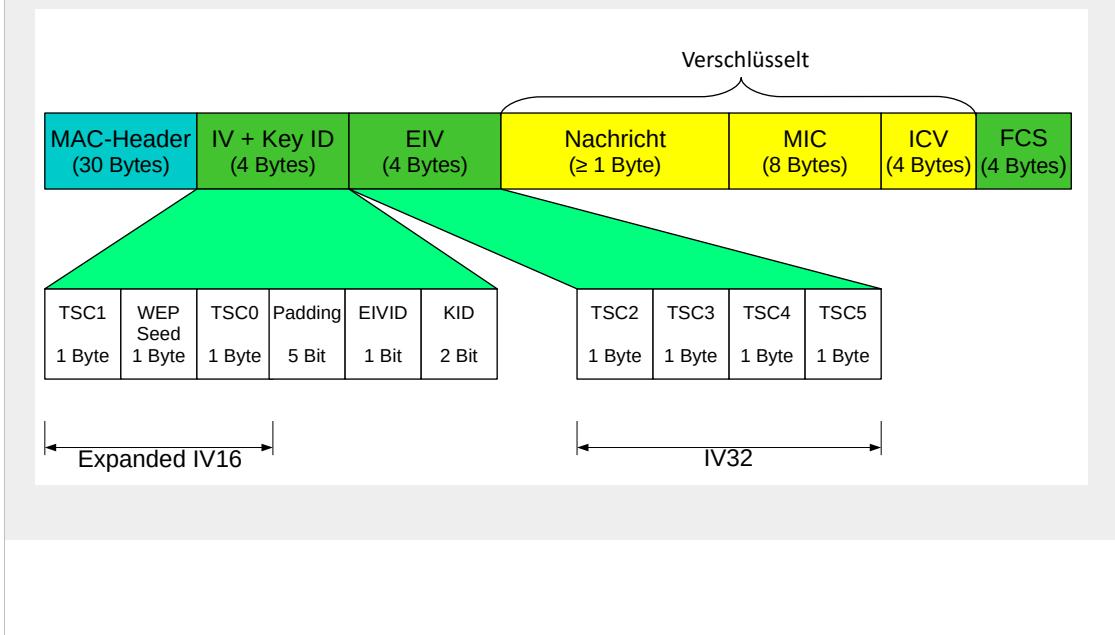
TKIP sorgt mit dem 6 Byte großen TKIP Sequence Counter (TSC) dafür, dass die Fragmente eine aufsteigende Reihenfolge haben. Damit kann dem Einfügen von Paketen durch Angreifer entgegengewirkt werden. Der TSC wird im Header im Klartext im IV und im EIV gesendet.

Die Erstellung des Schlüssels erfolgt in zwei Phasen.

In der ersten Phase wird aus dem Session Key (TK), der Transmitter Adresse (TA) und dem IV32-Teil (höherwertiger Teil) des TSC ein Zwischenschlüssel mit 80 Bits ($5 * 16$ Bit) namens TKIP-mixed transmit address and key (TTAK) erzeugt. Der TTAK Zwischenschlüssel kann bis zum Ende der Session beibehalten werden. Es gibt jedoch auch Gründe für eine Neuberechnung.

Für jede zu erzeugende MPDU wird in einer zweiten Phase ein eigener Schlüssel, der so genannte Per Packet Key (PPK) erstellt, der sich aus dem PRNG-ARC4-Key und dem IV16-Teil des TSC zusammensetzt. Da zur Erzeugung des ARC4-Key nur der IV16-Teil (niederwertiger Teil) des TSCs inkrementiert wird, kann er auf Vorrat errechnet und zwischengespeichert werden. Bei einem Überlauf ist der höherwertige Teil TSC zu inkrementieren.

TKIP-MPDU-Format



Bei TKIP wird der IV (IV16) um einen Extended IV (EIV) mit 32 Byte ergänzt (IV32), der zwischen dem IV und der verschlüsselten MPDU eingefügt wird.

Zusätzlich ist im verschlüsselten Teil der 8 Byte große Message Integrity Code (MIC) zwischen Nachricht (MSDU) und dem Integrity Check Value (ICV) eingefügt.

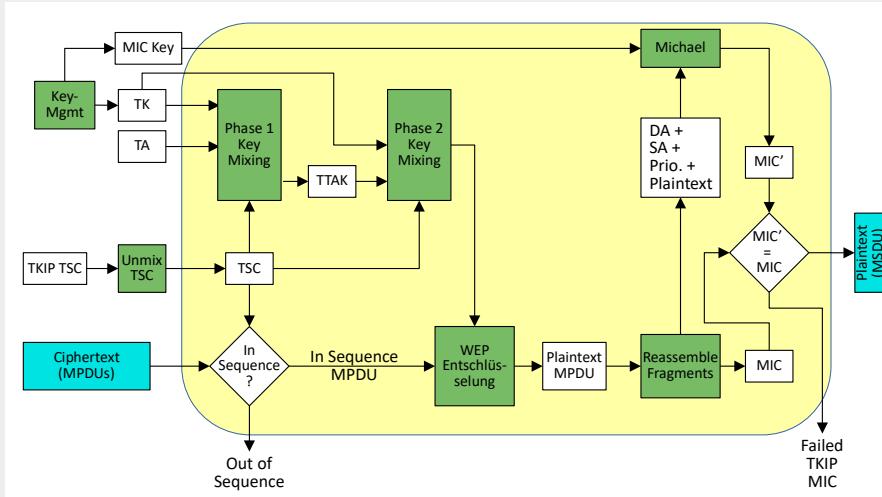
Um zu erkennen, ob ein EIV eingefügt wurde, musste eine Kennung dafür geschaffen werden. Dafür wurde aus dem 6 Bit großen Padding ein Bit namens EIVID spendiert. Ist es auf 1 gesetzt, ist ein EIV eingefügt. Hat die EIVID den Wert 0, handelt es sich um einen mit WEP verschlüsselten Frame.

Ist der Wert der Key-ID (KID) = 0 handelt es sich um ein pairwise verschlüsselten Frame für einen Unicast. Bei den Werten 1 bis 3 handelt es sich um Gruppenschlüssel.

Das erste und dritte Byte des IV sowie die vier Bytes des EIV werden zur Übermittlung des TSC verwendet. Dabei werden die 6 Bytes des TSC nach steigender Signifikanz der Bits eingefügt. Nur TSC0 und TSC1 werden im IV getauscht um schwachen RC4-Schlüsseln entgegen zu wirken.

Das zweite Byte im IV (WEP Seed) wird nicht für Erstellung des TSC verwendet und ist nur eine Kopie von TSC1 bei der Bit B0 immer auf 0 und Bit B6 immer auf 1 gesetzt werden. WEP-Seed = (TSC1 | 0x20) & 0x7F.

TKIP Entschlüsselung



Zuerst wird aus dem IV und dem EIV der TSC ermittelt und überprüft ob er aufsteigend ist. Bei Unstimmigkeiten wird der Frame verworfen.

Wie bei der Verschlüsselung wird bei der Phase 1 aus dem Session Key (TK), der Transmitter Adresse (TA) und dem TKIP Sequence Counter (TSC) der TKIP MIXED Transmit Address and Key (TTAK) erzeugt.

Das Ergebnis der Phase 2 ist der WEP Seed (WEP IV und ARC4 Key). Der WEP Seed wird zusammen mit der MPDU für die Entschlüsselung verwendet. Das Entschlüsselungs-Ergebnis sind MPDUs die evtl. noch fragmentiert sind. Deshalb schließt sich eine evtl. erforderliche Reassemblierung an.

Die Reassemblierten Frames (DA, SA, Priorität und der der Plaintext MSDU) werden im Michael-Verfahren zusammen mit dem MIC Key zu einem MIC'.

Am Ende vergleicht die MIC-Überprüfung den MIC aus den reassemblierten Daten und den MIC'. Sind beide gleich, werden die Daten als MSDU an die überlagerte Schicht übergeben. Sind MIC und MIC' ungleich werden die Daten verworfen.

Wird innerhalb von 60 Sekunden mehr als ein MIC-Fehler erkannt, wird eine Attacke angenommen und es deassoziiieren sich die Stationen oder der AP deassoziiert die betroffene Station.
Das ist abhängig von der Senderichtung und somit von dem Gerät, das die MIC-Fehler erkennt.

Wurde ein MIC-Fehler von einer Station erkannt, sendet sie einen MIC-Failure-Report-Frame an den AP.

Wurden wiederholte MIC-Fehler vom AP erkannt, werden die PTK und der GTK verworfen.

Damit müssen sich alle Stationen neue authentifizieren!

Der neue GTK wird erst nach 60 Sekunden wieder freigegeben.

Nun kann es jedoch sein, dass es tatsächlich Übertragungsfehler gab, die als MIC-Fehler interpretiert werden.

Um das auszuschließen, werden vor der MIC-Überprüfung die FCS, der ICV und der TSC einer MPDU überprüft.

Sind bereits hierbei Fehler erkennbar, handelt es sich um einen Übertragungsfehler und es wird kein MIC-Fehler registriert.

Leider kann mit der forcierten Erzeugung von MIC-Fehlern ein DoS-Angriff durchgeführt werden.

Wer es schafft den TSC richtig zu inkrementieren und zusätzlich einen MIC-Fehler zu erzeugen,
kann den Zugriff auf einen AP für 60 Sekunden zu unterbinden. (Die TSC-Überprüfung läuft vor der MIC-Überprüfung)

Es wird der Advanced Encryption Standard (AES) verwendet.

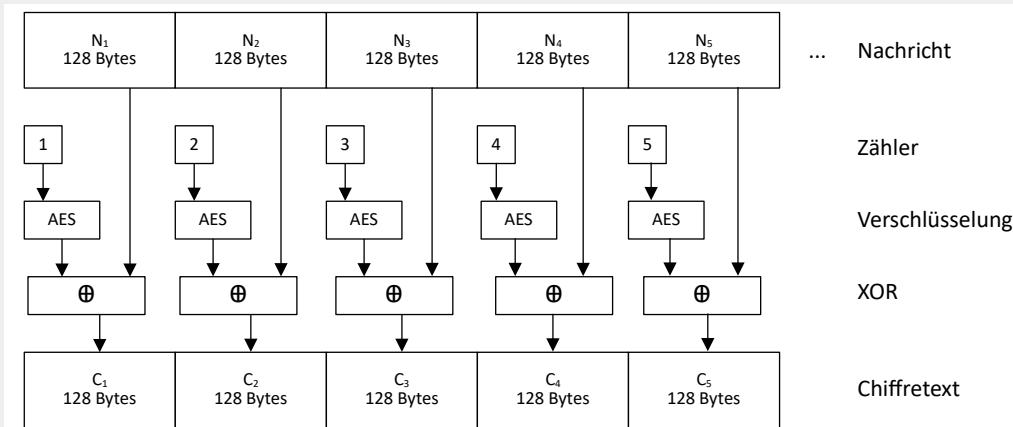
Das ist ein Block-Chiffre, der unterschiedliche Längen verschlüsseln kann.
Für WLANs wurde die Blocklänge auf 128 oder 256 Bit festgelegt.

Die Daten die bei WLANs zu verschlüsseln sind haben eine Länge zwischen 64 und 1500 Bytes. Daher müssen die Daten vor der Verschlüsselung in Blöcke aufgeteilt werden. Dazu gibt es wiederum verschiedene Modi.

Die für WLANs festgelegte Modi sind der Counter-Modus (CTR) zusammen mit dem Cipher Block Chaining – Message Authentication Code (CBC-MAC) für die Integritätssicherung kurz CCM-Mode festgelegt. CCM ist im RFC 3610 beschrieben.

Das damit realisierte Protokoll heißt CCM Protocol (CCMP)
(Ausgeschrieben CTR/CBC-MAC Protocol)

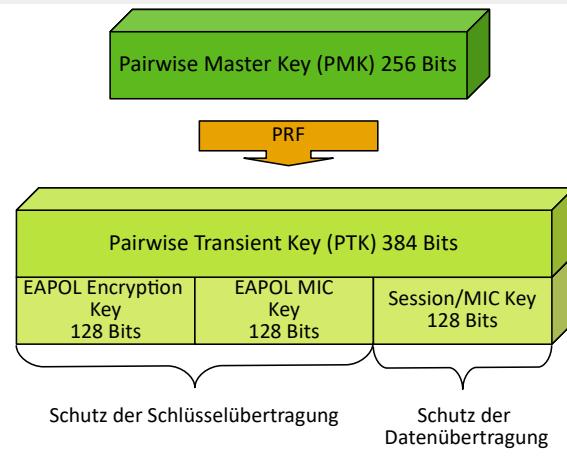
CCMP-CTR-Code



Der CTR-Mode hat seinen Namen von einem Zähler (Counter) auf den die AES-Verschlüsselung angewendet wird. Es wird also nicht die Nachricht mit AES verschlüsselt, sondern ein Zähler. Das Ergebnis der Verschlüsselung wird dann mit einem Nachrichten-Block mit XOR-Verknüpft. Der Zähler wird mit einemNonce-Wert initialisiert.

Das Chiper-Block-Chaining übernimmt die Aufgabe des Message Authentication Code (MAC). Bei IEEE802.11i wurde allerdings aus MAC, um eine Verwechslung mit einer MAC-Adresse zu vermeiden, der Message Integrity Code (MIC).

CCMP Pairwise Key Hierarchie

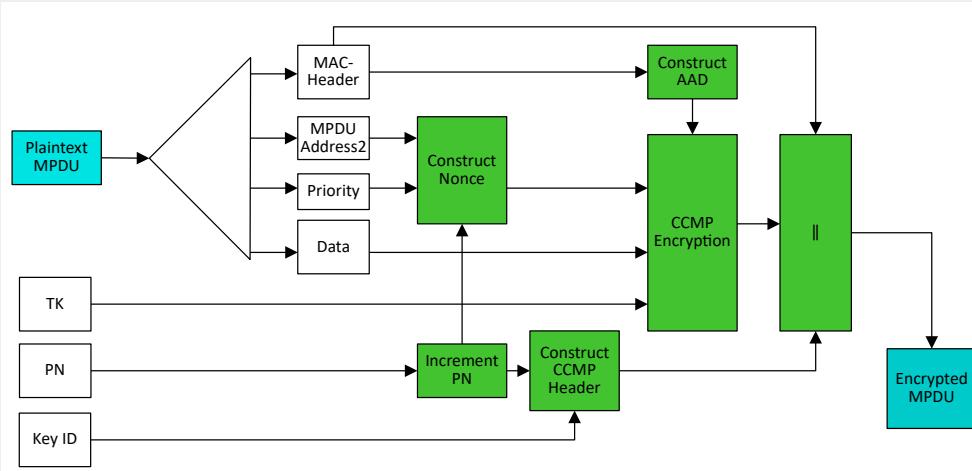


Auch beim CTR with CBC-MAC Protocol (CCMP) gibt es eine Schlüsselhierarchie mit einem Pairwise Master Key (PMK) an der Spitze.

Allerdings wird daraus ein nur 384Bit großer Pairwise Transient Key (PTK) mit einer Pseudo Random Function (PRF) erzeugt.

Aus dem PTK werden 3 Schlüssel erzeugt, von denen 2 für den Schlüsselaustausch und einer für den Datenaustausch genutzt wird.

CCMP-Verschlüsselung



Im Gegensatz zu TKIP wird die Verschlüsselung nicht auf MSDU-Ebene sondern auf MPDU-Ebene durchgeführt. Deshalb muss eine evtl. erforderliche Fragmentierung vorher durchgeführt werden.

Es gibt nur einen Schlüssel für Datenverschlüsselung und Datenintegrität. Um den sicherheitstechnischen Nachteil auszugleichen wird ein 13Byte großer Nonce-Wert zusätzlich bei der Verschlüsselung verwendet. Er wird aus der Sender-MAC-Adresse der Priorität und einer Sequenznummer der Packet Number (PN) gebildet.

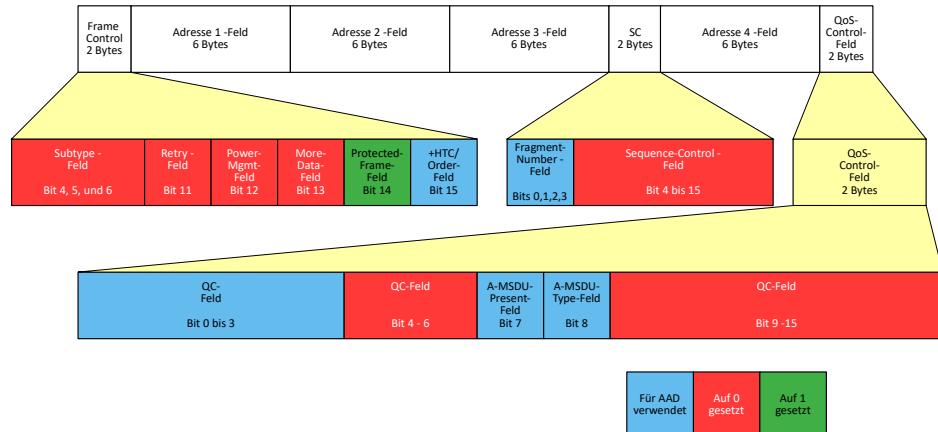
Ablauf der Verschlüsselung

Packet-Number-Counter (PN) wird für jede MPDU inkrementiert.
Erstellung des Additional Authentication Data (AAD) für das CCM-Verfahren. (Siehe unten)

Erstellung des Nonce-Blocks aus der Sender-MAC-Adresse, der Priorität und dem PN.

Erstellung des CCMP-headers aus dem PN und der Key-ID (KID).
Aus dem temporären Schlüssel (TK), der AAD, dem Nonce und den MPDU Daten wird der Ciphertext und der MIC mit der CCMP Encryption erzeugt.
Aus dem Original-MPDU-Header, dem CCMP-Header und den verschlüsselten Daten wird die verschlüsselte MPDU erzeugt.

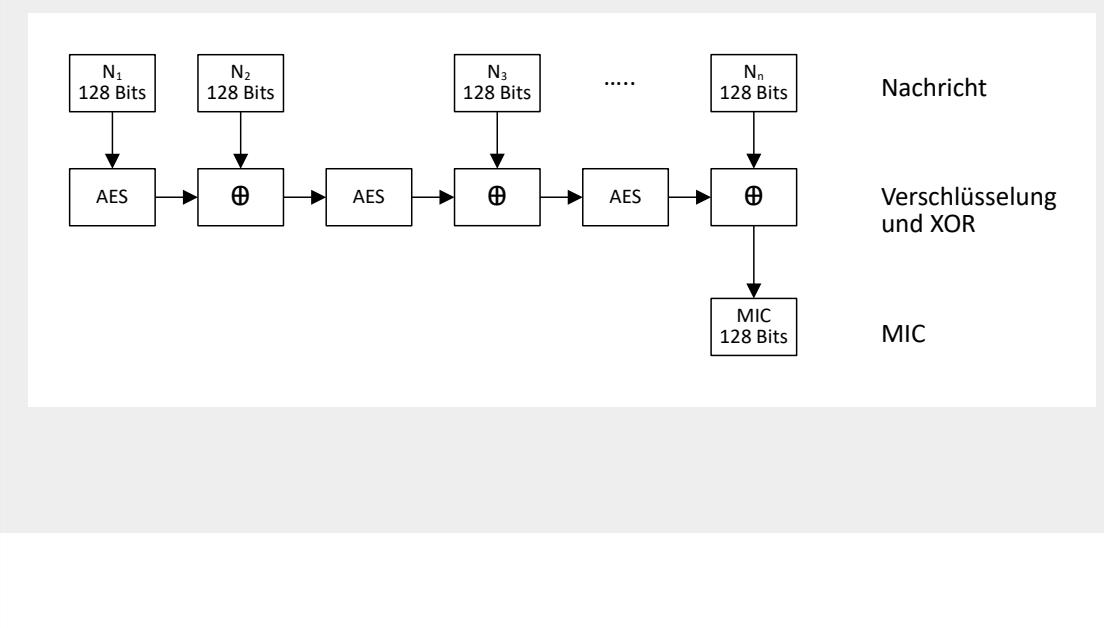
MPDU-Header für den Aufbau der AAD



Die MIC-Berechnung erfolgt mit dem Cipher-Block-Chaining (CBC-MAC)-Verfahren. Dazu werden die Daten in 128 Bit lange Blöcke aufgeteilt. Teile des MPDU-Headers werden vorher zu den Additional Authentication Data (AAD) zusammengesetzt und bei der MIC-Berechnung berücksichtigt. Mit den AAD wird die Authentizität der MPDU sichergestellt. Die Teile des MPDU-Headers, die sich bei einer wiederholten Frame-Übertragung ändern würden werden auf 0 gesetzt.

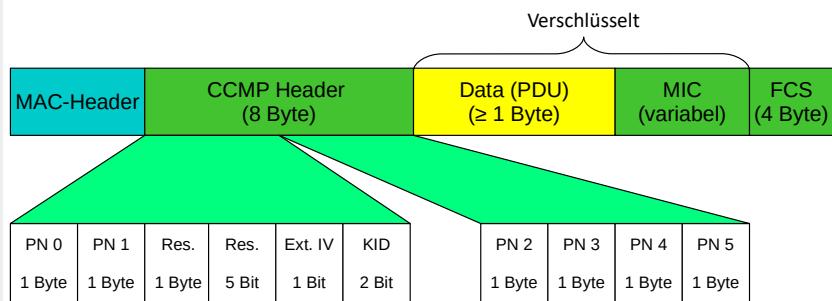
Die Folie zeigt, welche Teile des MPDU-Headers für die AAD verwendet werden. Je nachdem, welche Felder Verwendung finden, hat die AAD eine Länge von 22 bis 28 Bytes.

CCMP-MIC-Berechnung



Die MIC-Berechnung erfolgt, indem der erste Block mit AES verschlüsselt wird. Das Ergebnis wird mit dem zweiten Block XOR-verknüpft. Danach wird das mit AES verschlüsselt und so weiter.

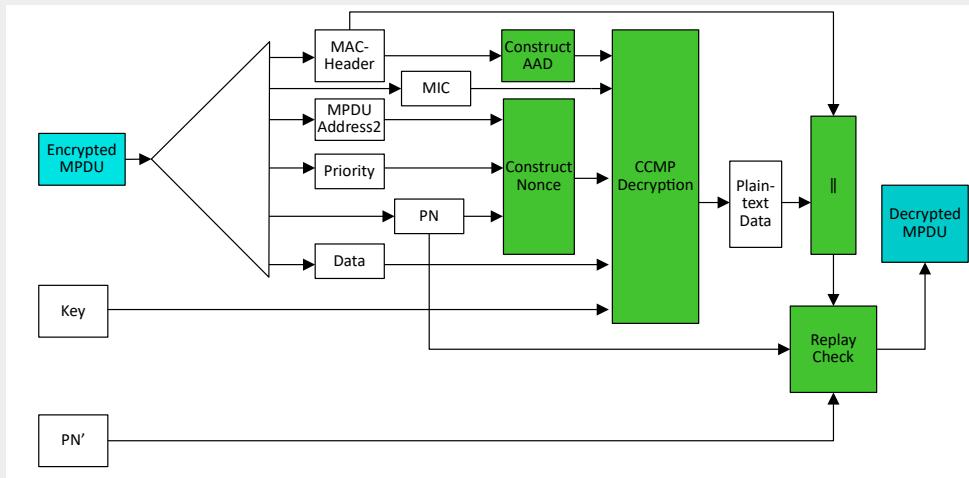
CCMP-MAC-Frame



CCM-Version	Parameter									
	M					L				
CCM-128	8 = MIC hat eine Länge von 8 Bytes					2 = MPDU-Längen-Feld ist 2 Bytes groß				
CCM-256	16 = MIC hat eine Länge von 16 Bytes					2 = MPDU-Längen-Feld ist 2 Bytes groß				

Je nachdem welche CCM-Verschlüsselung vorgenommen wurde, hat das MIC-Feld eine Länge von 8 oder 16 Bytes.

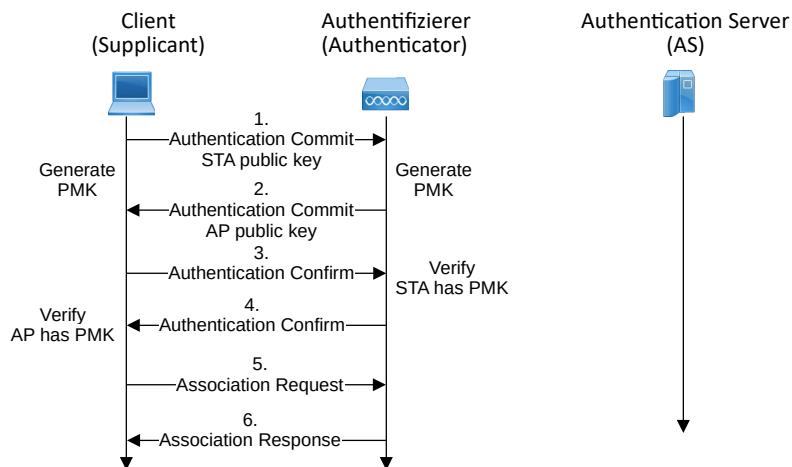
CCMP-Entschlüsselung



Der Ablauf der Entschlüsselung ist folgender:

- 1) Aus der verschlüsselten MPDU werden die AAD, der Nonce, der MIC und die PN ermittelt.
- 2) Bei der CCMP-Entschlüsselung wird der Plaintext ermittelt sowie der Integrity-Check durchgeführt.
- 3) Danach wird der MAC-Header vorangestellt.
- 4) Am Ende findet mit dem PN und dem selbst verwalteten PN' ein Replay-Check statt.
- 5) Verläuft der Replay-Check erfolgreich werden die MPDU ausgeliefert.

WPA3



2018 wurden als Folge von KRACK mit WPA3 eine weitere Verbesserung von WPA eingeführt. Alle Wi-Fi-6 Geräte müssen WPA3 implementiert haben.

Im Personal-Mode wurde der Preshared Key (PSK) durch die simultaneous authentication of equals (SAE) ersetzt.

Im Enterprise Mode wurde die Authentifizierung durch einen 192-Bit Verschlüsselung ergänzt.

Die SAE-Authentifizierung nutzt den Elliptic Curve Diffie Hellman (ECDH) Algorimus, also eine asymmetrische Verschlüsselung, um den PMK für den AP und die STA zu erstellen.

Zur Verschlüsselung wurde optional mit einem 256-Bit-Schlüssel das AES Galois Counter Mode Protocol (GCMP) eingeführt. GCMP benötigt für das gleiche Security-Level nur halb so viele Security-Operations.

- Verschlüsselung
- Ziele
- WEP-Verschlüsselung / WEP-Desaster
- WPA / WPA2
 - ◆ Bauelemente der Verschlüsselung
 - ◆ Erzeugen der Transient Keys
 - ◆ Austausch der Nonce
- TKIP
 - ◆ Pairwise Key Hierarchie
 - ◆ Group Key Schlüsselhierarchie
 - ◆ TKIP Verschlüsselung / MPDU-Format / Entschlüsselung / MIC-Fehler
- CCMP
 - ◆ Pairwise Key Hierarchie
 - ◆ CTR-Code
 - ◆ Verschlüsselung / AAD-Aufbau / MIC-Berechnung / MAC-Frame / Entschlüsselung