# Referat: Bluetooth, Wlan und NFC

Inhalt

[Referat: Bluetooth, Wlan und NFC 1](#_Toc530310187)

[WLAN 1](#_Toc530310188)

[Allgemeines 1](#_Toc530310189)

[Geschichtliche Entwicklung 1](#_Toc530310190)

[1980: Gründung der IEEE 802 Normen (Netzwerk) 1](#_Toc530310191)

[IEEE-Norm 1](#_Toc530310192)

[Geschwindigkeit 2](#_Toc530310193)

[Verwendete Technologien 2](#_Toc530310194)

[FHSS (Frequence Hoping Spread Spectrum) 2](#_Toc530310195)

[DSSS (Direct Sequenz Spread Spectrum) 2](#_Toc530310196)

[Sicherheit 2](#_Toc530310197)

[WEP (Wired Equivalent Privacy) 2](#_Toc530310198)

[WPA (Wi-Fi Protected Access) 3](#_Toc530310199)

[WPA2 (Wi-Fi Protected Access 2) 4](#_Toc530310200)

[TKIP und CCMP – Was steckt dahinter 4](#_Toc530310201)

[TKIP (Temporal Key Integrity Protocol) 4](#_Toc530310202)

[CCMP (Counter-Mode/CBC-MAC Protocol) 5](#_Toc530310203)

[Welche WLAN Verschlüsselung ist die sicherste Wahl? 5](#_Toc530310204)

[Bluetooth 5](#_Toc530310205)

[NFC 5](#_Toc530310206)

# WLAN

## Allgemeines

WLAN steht für „Wireless Local Area Network“ und wurde 1963 durch die Verbindung zwischen American Institute of Electronical Engineers (AIEE) und Institute of Radio Engineers (IRE) erfunden. Dadurch wurde der Zusammenschluss zwischen Elektrotechnikern und Informatikern garantiert.

# IEEE-Norm

Begonnen wurde mit der Erstellung von der IEEE-Norm 802.11. Herausgeber ist das [Institute of Electrical and Electronics Engineers](https://de.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers). Die Definition der [IEEE-802-Normen](https://de.wikipedia.org/wiki/IEEE_802), die zunächst ganz allgemein den Netzwerkzugriff beschreiben, begann im Februar 1980, daher wurde die Bezeichnung 802 gewählt.

Die heute verwendeten Normen sind: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac. Die neueste Norm ist 802.11ay die 2019 herauskommen wird.

## Geschwindigkeit

Theoretische Übertragungsraten:

Nach 802.11 b 🡪 11 Mbit/s

Nach 802.11 a/g 🡪 54 Mbit/s

Übertragungsraten in der Praxis:

Nach 802.11 b 🡪 5 Mbit/s

Nach 802.11 a/g 🡪 23 Mbit/s

Im Schnitt wird die Hälfte der angegeben Übertragungsrate erreicht.

Gründe dafür:

* Dämpfung, Reflektionen, Beugung
* Mehrwegsausbreitung
* Störung
* Verschlüsselungen

Außerdem ist das WLAN nur höchstens so schnell wie die langsamste Komponente.

## Verwendete Technologien

### FHSS (Frequence Hoping Spread Spectrum)

Sender und Empfänger wechseln zyklisch die Frequenz

### DSSS (Direct Sequenz Spread Spectrum)

* Schmalbandiges Signal wird in ein Breitband-Signal umgewandelt
* 13 überlappende Kanäle mit einer Bandbreite von 22 MHz
* Jedes Datenbit wird mit einem 11 Bit Barker Code XOR verknüpft

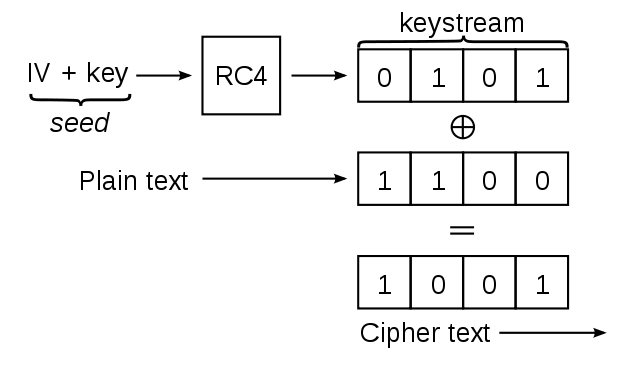
## Sicherheit

Am Anfang der IEEE-Standards war der Zugang zum Wlan offen und die Datenpakete nicht verschlüsselt.

### WEP (Wired Equivalent Privacy)

Die erste Form der WLAN Verschlüsselung war der Standard WEP. Er ist immer noch in vielen [aktuellen Routern](https://www.only4gamers.de/bester-wlan-router/) und Geräten implementiert, wobei seine Entwicklung auf das Jahr 1999 zurückgeht und die technischen Gegebenheiten dieser Ära wiederspiegelt. Damals schien sich dieses Protokoll als sicher zu erweisen, doch schon bald wurden viele Nutzer eines besseren belehrt. Seit dem Jahr 2001 gilt WEP als geknackt und die Routinen zur [Verschlüsselung](http://www.was-ist-malware.de/it-sicherheit/verschluesselung-definition-ziele-funktionsweise-und-verfahren/) sind inzwischen allgemein bekannt. Somit handelt es sich bei dieser WLAN Verschlüsselung um eine veraltete Technologie, die nicht mehr eingesetzt werden sollte.

Die Schwäche von WEP liegt vor allem in der Art des verwendeten Verschlüsslungs-Algorithmus. Dieser zeigte sehr schnell seine Lücken, denn die Anzahl der möglichen Code-Kombinationen beschränkt sich auf eine für Computer, durchaus überschaubare Zahl. Da nur 16.777.216 Möglichkeiten existieren, wiederholt sich der Schlüssel in heutigen Systemen relativ schnell. Ein Cracker kann also den WLAN-Verkehr mitsniffen und erhält mittels technischer Beschleunigungsverfahren innerhalb weniger Minuten den gesuchten WLAN-Code. Damit hat er Zugriff auf die übertragenen Daten und könnte sogar [Schadsoftware auf Ihren Computer](http://www.was-ist-malware.de/allgemein/schadsoftware/) installieren.

[](http://www.was-ist-malware.de/wp-content/uploads/2017/06/wlan-verschluesselung-wep.png)

### WPA (Wi-Fi Protected Access)

Als WEP im Jahre 2001 als absolut unsicher eingestuft wurde, sahen sich die Entwickler im Zugzwang. Eine neue Technik musste her, die nicht die Fehler der alten Methode wiederholte. So wurde WPA entwickelt und im Jahre 2003 mit der Zertifizierung begonnen.

Dabei unterscheidet sich die Funktionsweise von WPA nicht sonderlich von der des vormals verwendeten WEP. Es kommt auch bei diesem Standard immer noch die gleiche [RC4-Stromchiffre](https://www.kryptographiespielplatz.de/index.php?aG=5651c3bab8f2a5a60cc93b8e2a7e6a377eb26a34) zum Einsatz. Allerdings besitzt diese keinen festen 48-Bit Verschlüsselungs-Algorithmus mehr. Diese WLAN Verschlüsselung verwendet für jedes neue Datenpaket einen eigenen Key, sodass quasi jeder Block separat entschlüsselt werden muss. Diese Methode nennt sich Temporal Key Integrity Protocol – kurz TKIP (siehe weiter unten). Durch dieses Prinzip werden dynamische Keys erstellt, die ein Auslesen durch reines „Mithören“ unmöglich machen.

Allerdings bieten sich auch bei WPA Optionen, wie der Key herausgefunden werden kann. So können Brutforce-Angriffe durchaus zum Erfolg führen, denn hierbei werden alle möglichen Kombinationen ausprobiert, bis ein korrektes Passwort für den Router ermittelt werden konnte. Daher hängt es allein von der Komplexität des Passwortes ab, wie lange es dauert, bis WPA von einem Cracker umgangen wurde.

### WPA2 (Wi-Fi Protected Access 2)

Als die Schwachstellen von WPA bekannt wurden und somit das Sicherheitsrisiko wieder beim User lag – er musste ein komplexes Passwort wählen – wurde eine Weiterentwicklung in Angriff genommen. Aus diesem Prozess ging dann WPA2 hervor, welches im Jahre 2005 auf den Weg gebracht wurde.

WPA2 setzt ausschließlich auf [AES (Advanced Encryption Standard)](http://www.was-ist-malware.de/it-sicherheit/advanced-encryption-standard-aes/). So kann diese WLAN Verschlüsselung bis zu 256-Bit verwenden, um die eingegebene Passwort-Phrase zu verbergen. Zudem wird der verwendete Schlüssel asymmetrisch genutzt. Dies bedeutet, dass für die Verschlüsselung des Klartextes nicht immer der ganze Schlüssel zum Einsatz kommen muss, sondern auch nur Teile von diesem in unterschiedlichen Permutationen angewendet werden können. Ein Auslesen dieser Daten, ohne das dabei der Originalschlüssel bekannt ist, ist auch nach fast 17 Jahren immer noch nicht möglich.

Allerdings gibt es auch bei WPA2 Schwachstellen, die es zu berücksichtigen gilt. Zum einem kommt immer noch das schon im WEP verwendet TKIP-Verfahren zum Einsatz, was bei dieser WLAN Verschlüsselung wiederum ein Einfallstor für Cracker sein könnte. Allerdings soll dieser Umstand bald der Vergangenheit angehören, denn als neuer Standard ist langfristig CCMP (Counter-Mode/CBC-MAC Protocol) geplant.

Die hauptsächliche Schwachstelle von WPA2 ist aber darin zu sehen, dass die gesamte WLAN Verschlüsselung als eine nicht-lineare Gleichung verstanden werden kann, die sich im Grunde mit entsprechend hoch entwickelter Software auflösen lässt. Allerdings hat dieser Faktor für den alltäglichen Einsatz derzeit noch keine Bedeutung.

## TKIP und CCMP – Was steckt dahinter

Bei einer WLAN Verschlüsslung ist immer wieder von den Begriffen TKIP und CCMP die Rede. Für den normalen Verbraucher handelt es – sofern nicht erweiterte technische Kenntnisse im Hintergrund stehen – dabei um kryptische Zeichenfolgen. Doch tatsächlich ist das Ganze einfacher erklärt, als es im ersten Moment erscheinen mag.

### TKIP (Temporal Key Integrity Protocol)

TKIP wurde eigentlich geschaffen, um bei der Umstellung von WEP auf WPA behilflich zu sein. Durch diesen Sicherheitsstandard musste die Hardware nicht vollständig ausgetauscht werden – die Methode konnte einfach in die bestehenden Router per Software-Update implementiert werden.

Das Protokoll stellt quasi den RC4-Algorithmus für die Codierung des WLAN-Keys zur Verfügung und verfügt gleichzeitig über eine 64-bit Hashkomponente welcher die Prüfsumme bereitstellt. Dabei wird jedem Datenpaket ein eigener Key zugewiesen, der auch noch die MAC-Adresse des jeweiligen Clients enthält. Am einfachsten ausgedrückt stellt TKIP die mathematische Basis, für die Verschlüsselung der Informationen dar.

### CCMP (Counter-Mode/CBC-MAC Protocol)

CCMP ist der nächste Schritt bei den Verschlüsselungsprotokollen. Dieser Algorithmus basiert nur noch auf AES und liefert einen 128-Bit langen Schlüssel, welcher jeweils über 48-Bit lange Initialisierungsvektoren verfügt. Dabei kommt eine Mischung aus verschiedenen Verschlüsselungen zum Einsatz, sodass der Key kaum noch auszulesen ist.

## Welche WLAN Verschlüsselung ist die sicherste Wahl?

Doch welche WLAN Verschlüsselung ist nun die sicherste Wahl für den Endkunden? Natürlich kann hier nur zu WPA2 AES mit CCMP geraten werden. Diese Methode ist so gut wie undurchdringbar und es wird vermutlich genauso lang wie bei WPA dauern, bis diese WLAN Verschlüsselung die ersten Schwachstellen preisgibt.

Allerdings kann auch noch auf WPA2 mit AES und TKIP gesetzt werden. Diese WLAN Verschlüsselung ist ebenfalls noch ungeknackt, selbst wenn sich im Laufe der Zeit einige Makel offenbart haben. Wer gegenwärtig diesen Standard verwendet, kann sich also als sicher betrachten.

Einzig WEP sollte als WLAN Verschlüsselung absolut gemieden werden. In den aktuellsten Geräten aus dem jetzigen Jahrgang ist diese Technik auch nicht mehr verfügbar, sie kann aber aufgrund von Kompatibilitäsproblemen durchaus noch nachinstalliert werden.http://vg01.met.vgwort.de/na/d8b801bf8ba74f62a20c962fb85c5910

# Bluetooth

Bluetooth dient zur schnellen Datenübertragung. Bluetooth sendet im 2,5 GHz Bereich und arbeitet mit Frequenzy-Hopping. Dies bedeutet, dass nach jedem gesendeten Paket das Modul in eine andere Frequenz wechselt. Dies dient dazu um Störungen vorzubeugen.

Bluetooth arbeitet mit zwei Verbindungstypen:

* Synchronous Connection Oriented (SCO), wird für Voice-Verkehr eingesetzt
* Asynchronous Connectionless (ACL), für Datenverkehr im symetrischen und asymetrischen Verkehr verwendet

Beide Verbindungstypen verwenden ein Zeitmultiplexverfahren für Duplex-Datenübertragung.

So ist es möglich mehrere Kanäle für eine Verbindung zu verwenden, indem jedem ein unterschiedlicher Zeitintervall (Slot) zugeteilt wird.

/ Bei synchronen Datenpackten können mehrere Slots reserviert werden, wobei ein Datenpacket bis  
/ zu fünf Slots beanspruchen kann

Bluetooth ist in der Lage ein Point-to-Point oder ein Point-to-Mulitpoint Netzwerk aufzubauen.

Die Geräte sind dabei in der selben Hopping-Frequenz synchronisiert, haben eine identische Implementation

# NFC