WPA3 - 192bit Mode

Karsten Iwen

𝕏 @KarstenIwen

WPA3 - 192 bit Mode

WPA3-Enterprise: 192-bit cryptographic strength for networks transmitting sensitive data

The 192-bit security mode provides an added level of protection by specifying the configuration of **each cryptographic component**, ensuring that the **overall security of the network is consistent**. By design, WPA3-Enterprise 192-bit security mode does not allow a Wi-Fi network to be configured below the defined, high level of security. A Wi-Fi network in 192-bit security mode **requires all client devices** to operate in the same 192-bit security mode.

What's new in Wi-Fi® security?
by The Beacon, October 15, 2020

Security Level

Sicherheitsniveau (kryptographischer Verfahren) Ein kryptographisches Verfahren erreicht ein Sicherheitsniveau von n Bit, wenn mit jedem Angriff gegen das Verfahren, der das Sicherheitsziel des Verfahrens mit hoher Erfolgswahrscheinlichkeit bricht, Kosten verbunden sind, die zu 2^n Berechnungen der Verschlüsselungsfunktion einer effizienten Blockchiffre (zum Beispiel AES) äquivalent sind.

BSI TR-02102-1, Version 2024-01

Security Level

- BSI TR-02102-1, Version 2016-01
  Insgesamt erreichen alle in dieser Technischen Richtlinie angegebenen kryptographischen Verfahren mit den in den einzelnen Abschnitten geforderten Parametern ein **Sicherheitsniveau von mindestens 100 Bit**.

- BSI TR-02102-1, Version 2024-01
  Insgesamt erreichen alle in dieser Technischen Richtlinie angegebenen kryptographischen Verfahren mit den in den einzelnen Abschnitten genannten Parametern ein **Sicherheitsniveau von mindestens 120 Bits**.

Security Level

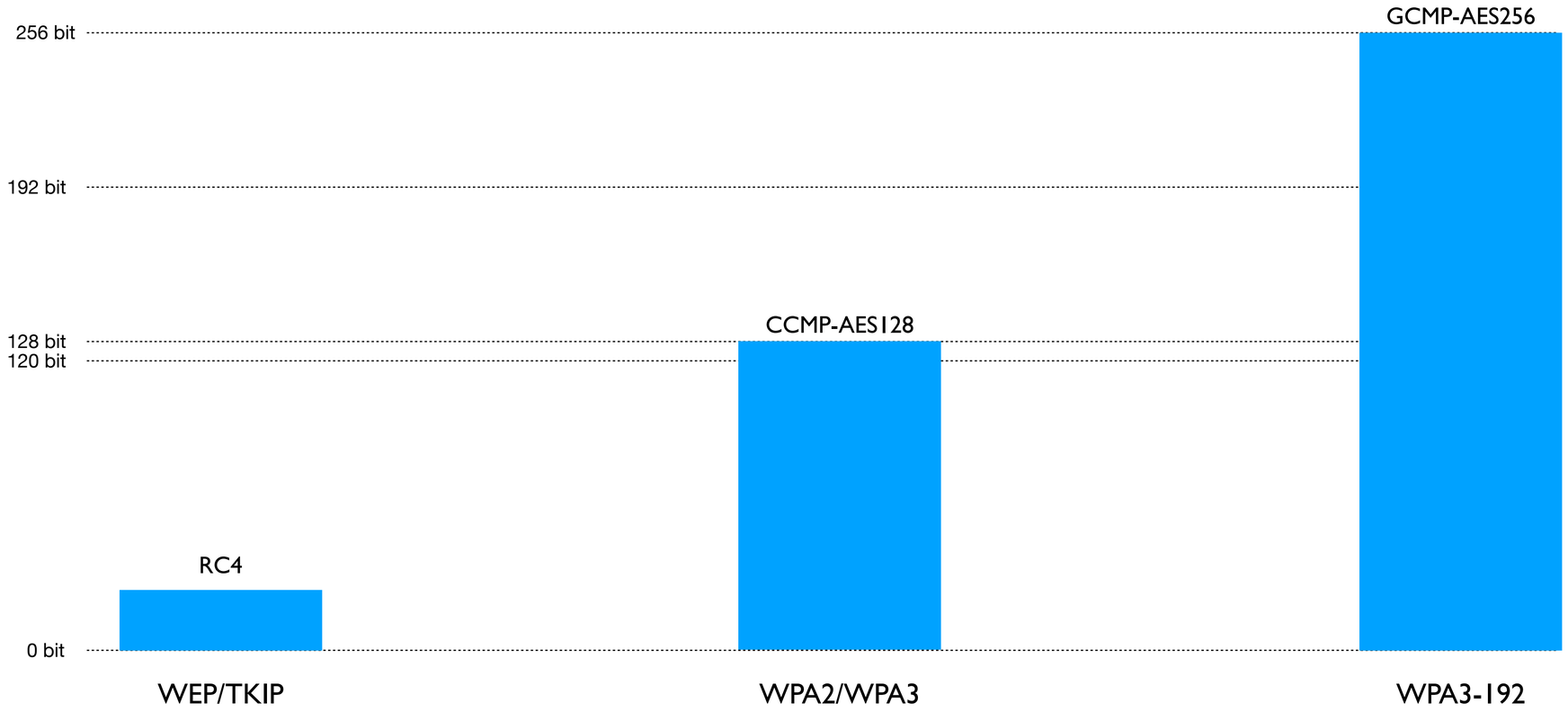
- NSA/NIST Suite B Cryptography (2005)
  - Security Level „Secret“: 128 Bit
  - Security Level „Top Secret“: 192 bit

- Commercial National Security Algorithm Suite, CNSA (2018)
  - Advanced Encryption Standard with 256 bit keys
  - EC-DH and EC-DSA with curve P-384
  - SHA-2 with 384 bits
  - DH key exchange with a minimum 3072-bit modulus
  - RSA with a minimum modulus size of 3072

- Commercial National Security Algorithm Suite, CNSA, v2 (2022)

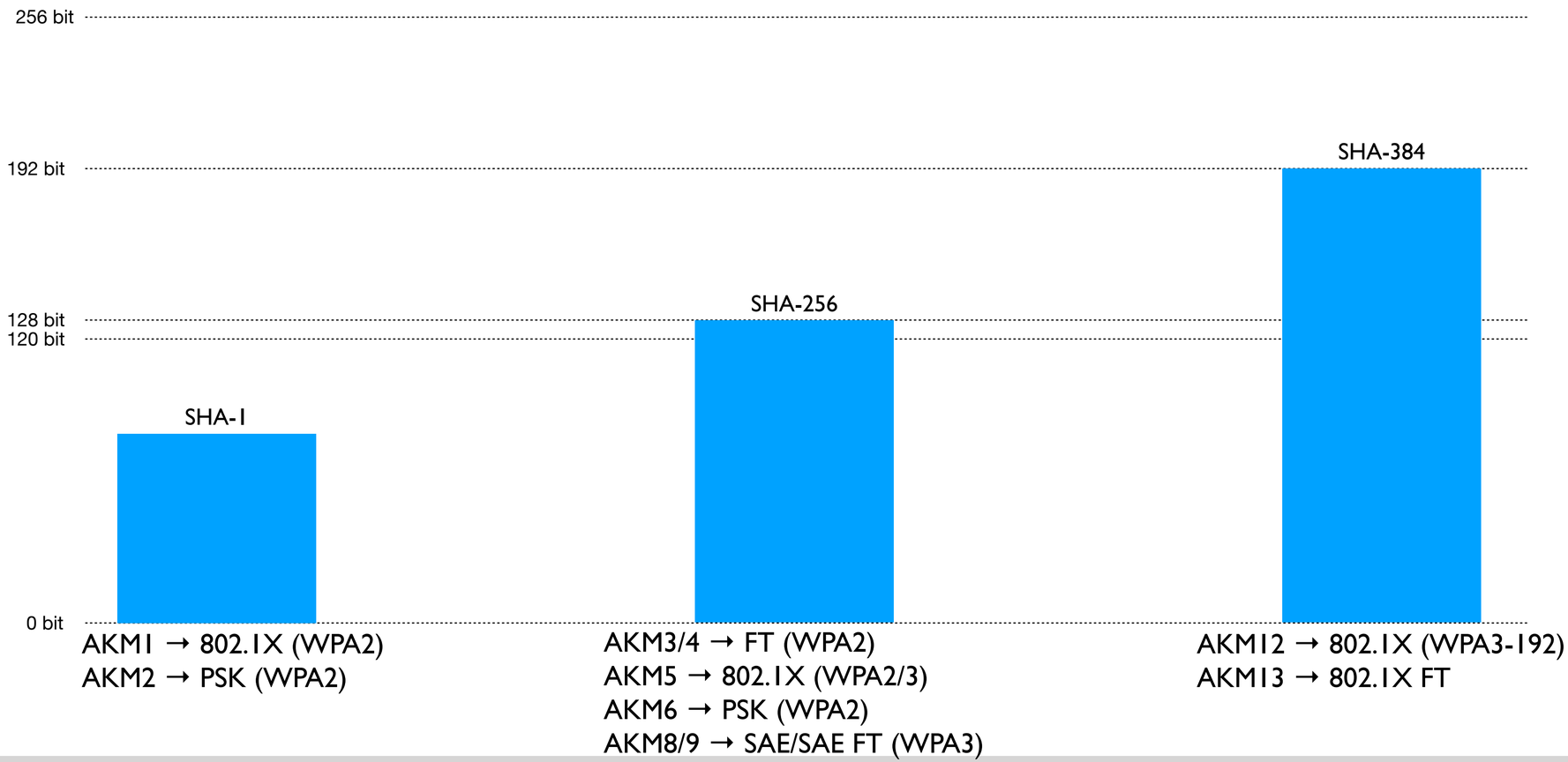
Security Level

Verschlüsselung



Security Level

PTK-Generierung



Security Level

Authentifizierung

256 bit

12.7.6.8 4-way handshake analysis

IEEE 802.11-2020

The following is an analysis of the 4-way handshake.

This subclause makes the trust assumptions used in this protocol explicit. The protocol assumes the following:

— The PMK is known only by the Supplicant's STA and the Authenticator's STA.

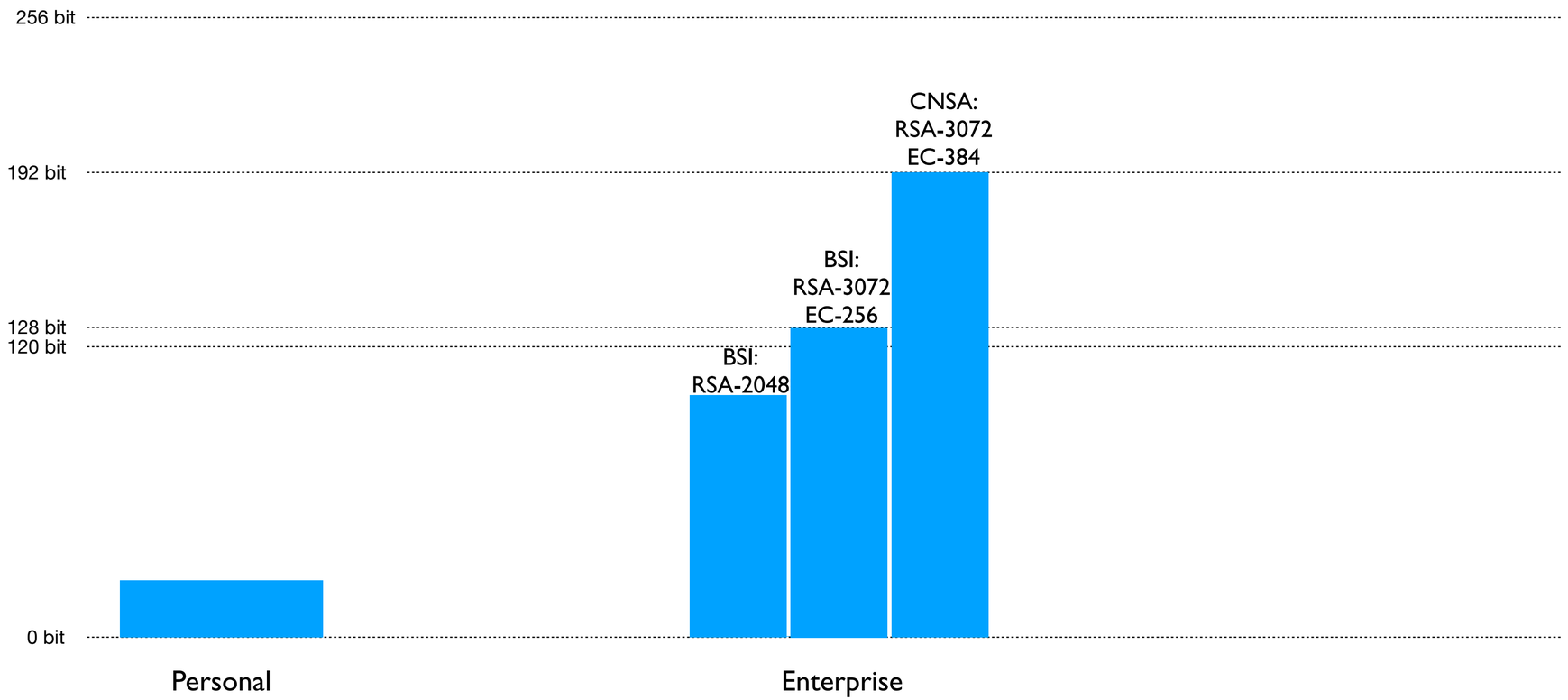
0 bit

Personal

Enterprise

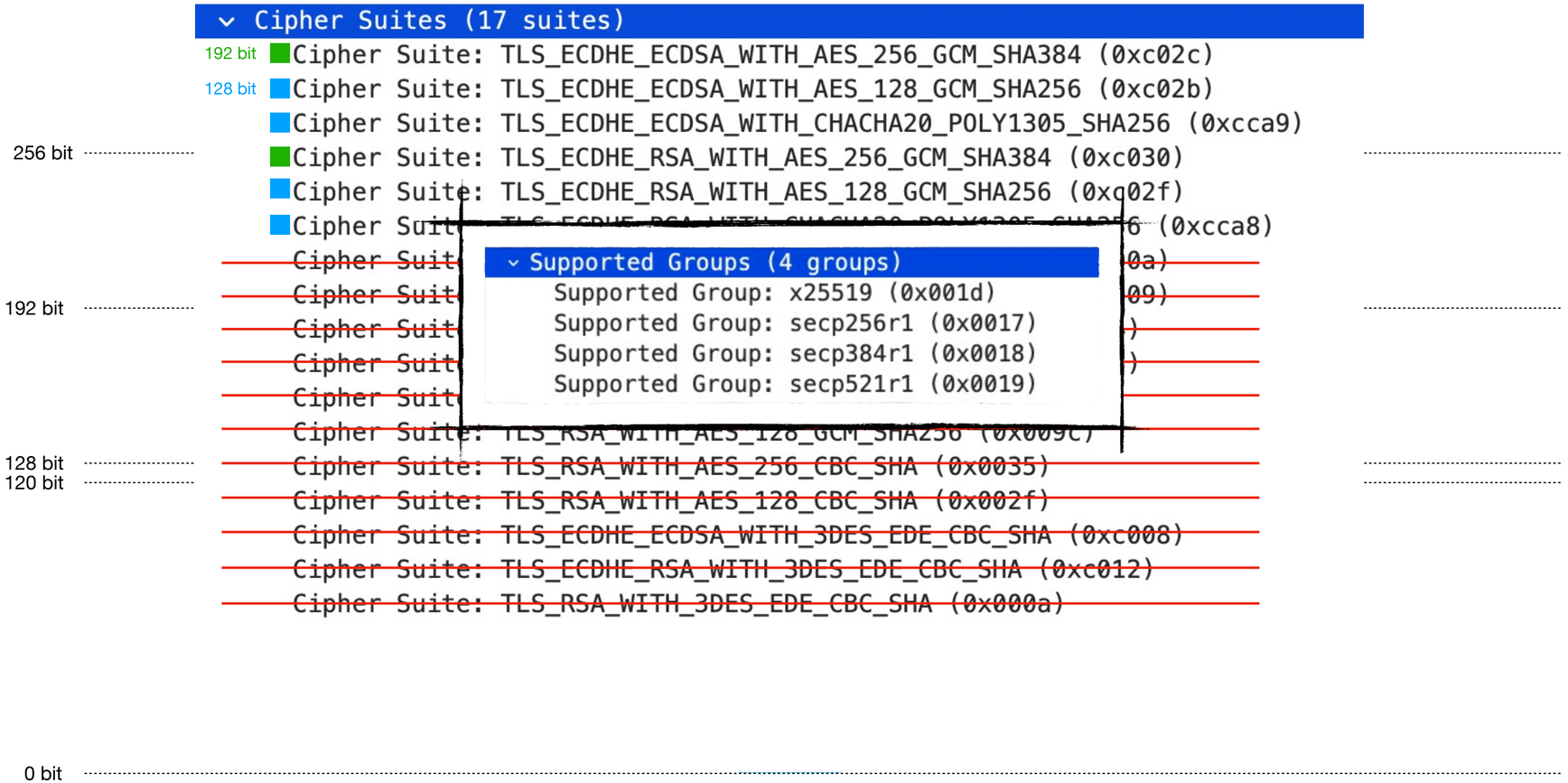
Security Level

Authentifizierung



Security Level

Schlüsselaustausch



WPA3 - 192 bit Mode

- WPA3 Specification, Version 3.3, 2024-02-16:
  - An AP's BSS configuration shall enable **AKM suite selector 00-0F-AC:12 (Suite B 192b)** and shall not enable any other AKM suite selector. Note: WPA3-Enterprise 192-bit mode does not interoperate with any other security mode.

IEEE Std 802.11-2016:

00-0F-AC	12	Authentication negotiated over IEEE Std 802.1X or using PMKSA caching as defined in 12.6.10.3 using a Suite B compliant EAP method supporting SHA-384	RSNA key management as defined in 12.7 or using PMKSA caching as defined in 12.6.10.3	Defined in 12.7.1.7.2 using SHA-384

IEEE Std 802.11-2020:

00-0F-AC	12	Authentication negotiated over IEEE Std 802.1X using a CNSA Suite compliant EAP method	RSNA key management as defined in 12.7	Defined in 12.7.1.6.2 using SHA-384	0 (open)

WPA3 - 192 bit Mode

- WPA3 Specification, Version 3.3, 2024-02-16:
  - An AP's BSS configuration shall be **PMF Required**, i.e., AP sets **MFPC to 1** and **MFPR to 1** in beacons and probe responses of the BSS.
  - **Permitted EAP cipher suites** for use with WPA3-Enterprise 192-bit mode are:
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
      - ECDHE and ECDSA using the 384-bit prime modulus curve P-384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
      - ECDHE using the 384-bit prime modulus curve P-384
      - RSA ≥ 3072-bit modulus
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
      - RSA ≥ 3072-bit modulus
      - DHE ≥ 3072-bit modulus

Und der RADIUS-Server?

WLAN-Pairwise-Cipher	00:0f:ac:09
WLAN-Group-Cipher	00:0f:ac:09
WLAN-AKM-Suite	00:0f:ac:0c
WLAN-Group-Mgmt-Cipher	00:0f:ac:0c

RFC 7268 - RADIUS Attributes for IEEE 802 Networks

Quantum Computer?

- Commercial National Security Algorithm Suite, CNSA, v2.0 (2022)

Table II: CNSA 2.0 symmetric-key algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.

U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

Quantum Computer?

- Commercial National Security Algorithm Suite, CNSA, v2.0 (2022)

Table III: CNSA 2.0 quantum-resistant public-key algorithms

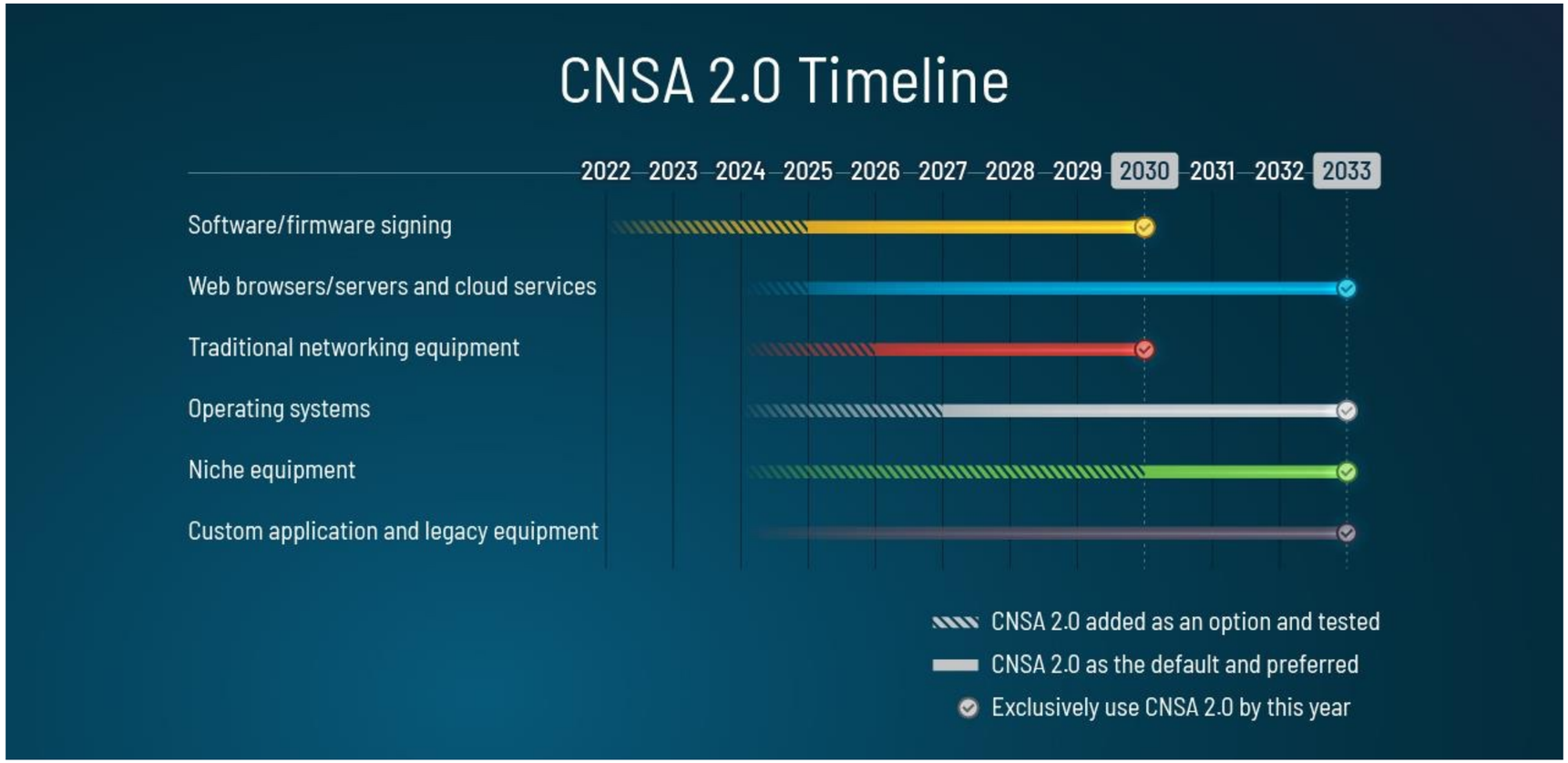
Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.

https://pq-crystals.org/

U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

Quantum Computer?

- Commercial National Security Algorithm Suite, CNSA, v2.0 (2022)



U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

(Fast) Roaming

00-0F-AC	12	Authentication negotiated over IEEE Std 802.1X using a CNSA Suite compliant EAP method	RSNA key management as defined in 12.7	Defined in 12.7.1.6.2 using SHA-384	0 (open)
00-0F-AC	13	FT authentication negotiated over IEEE Std 802.1X	FT key management as defined in 12.7.1.6	Defined in 12.7.1.6.2 using SHA-384	2 (FT) for FT protocol reassociation as defined in 13.5 0 (open) for FT Initial Mobility Domain Association over IEEE Std 802.1X or PMKSA caching

IEEE Std 802.11-2020
Table 9-151—AKM suite selectors

(Fast) Roaming

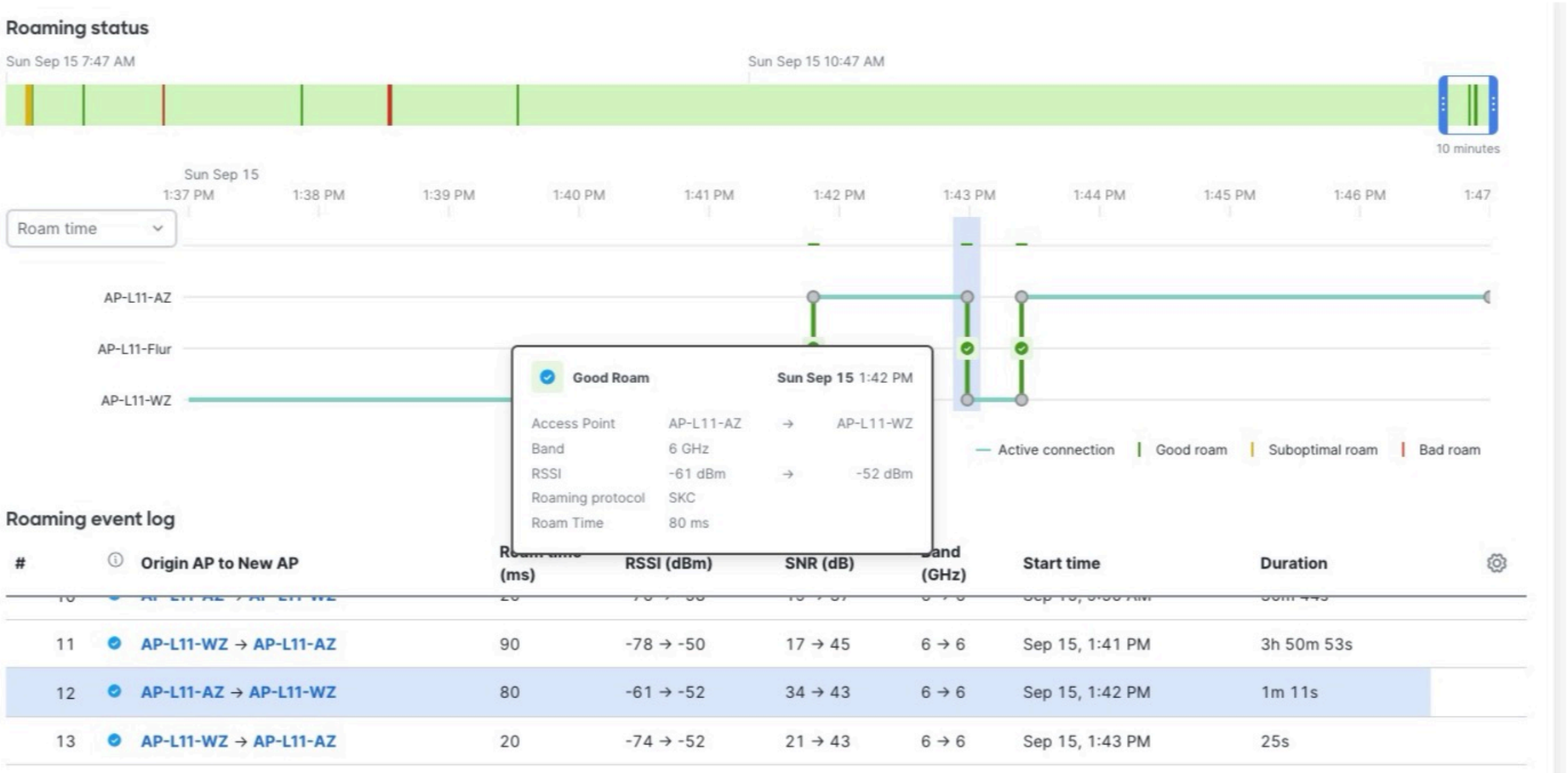
360 View | General | QOS Statistics | ATF Statistics | **Mobility History** | Call Statistics

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
AP-MD-9162-1	70bc.480d.9a4f	1	09/17/2024 17:00:20	0	Local	324	802.11i Slow
AP-MD-9162-2	70bc.480d.982f	1	09/17/2024 16:55:51	0	Local	232	802.11i Slow
AP-MD-9162-1	70bc.480d.9a4f	1	09/17/2024 16:55:31	0	Local	249	802.11i Slow
AP-MD-9162-2	70bc.480d.982f	1	09/17/2024 16:55:10	0	Local	239	802.11i Slow
AP-MD-9162-1	70bc.480d.9a4f	1	09/17/2024 16:54:49	0	Local	265	802.11i Slow
AP-MD-9162-2	70bc.480d.982f	1	09/17/2024 16:54:11	0	Local	5698	N/A

Cisco CW9162, v17.15.1, iPhone 15 Pro Max, v17.6.1

(Fast) Roaming



Roaming event log

#	Origin AP to New AP	Roam time (ms)	RSSI (dBm)	SNR (dB)	Band (GHz)	Start time	Duration
11	AP-L11-WZ → AP-L11-AZ	90	-78 → -50	17 → 45	6 → 6	Sep 15, 1:41 PM	3h 50m 53s
12	AP-L11-AZ → AP-L11-WZ	80	-61 → -52	34 → 43	6 → 6	Sep 15, 1:42 PM	1m 11s
13	AP-L11-WZ → AP-L11-AZ	20	-74 → -52	21 → 43	6 → 6	Sep 15, 1:43 PM	25s

Meraki CW9166, v30.7, iPhone 15 Pro Max, v17.6.1

Endgeräte

- **Apple iOS/iPadOS**
  … allen iPhone 11-Geräten (oder neuer), allen iPad-Geräten ab der 7. Generation und … unterstützt.

- **Apple macOS**
  … allen Mac-Computern mit Apple Chips unterstützt.

- **Android v12**

- **Windows 10/11**

Wann mit der WPA3-192 Implementierung anfangen?

Jetzt!