WPA3 - 192 bit Mode

Karsten Iwen

Only 10 minutes …
More details in an
upcoming Blog-post

@KarstenIwen https://www.linkedin.com/in/karsteniwen Blog: https://cyber-fi.net

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

Security Level (of Cryptographic Mechanisms) A cryptographic mechanism achieves a security level of n bits if there are costs associated with each attack against the mechanism that breaks the mechanism's security objective with a high probability of success, equivalent to 2^n calculations of the encryption function of an efficient block cipher (for example, AES).

German Federal Office for Information Security (BSI)
BSI TR-02102-1, Version 2024-01

Security Level

- BSI TR-02102-1, Version 2024-01
  Overall, all cryptographic mechanisms specified in this Technical Guideline achieve **a security level of at least 120 bits** …

- BSI TR-02102-1, Version 2016-01
  … **a security level of at least 100 bits**.

Security Level

H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

D5.4

Algorithms, Key Size and Protocols Report (2018)

Security Level

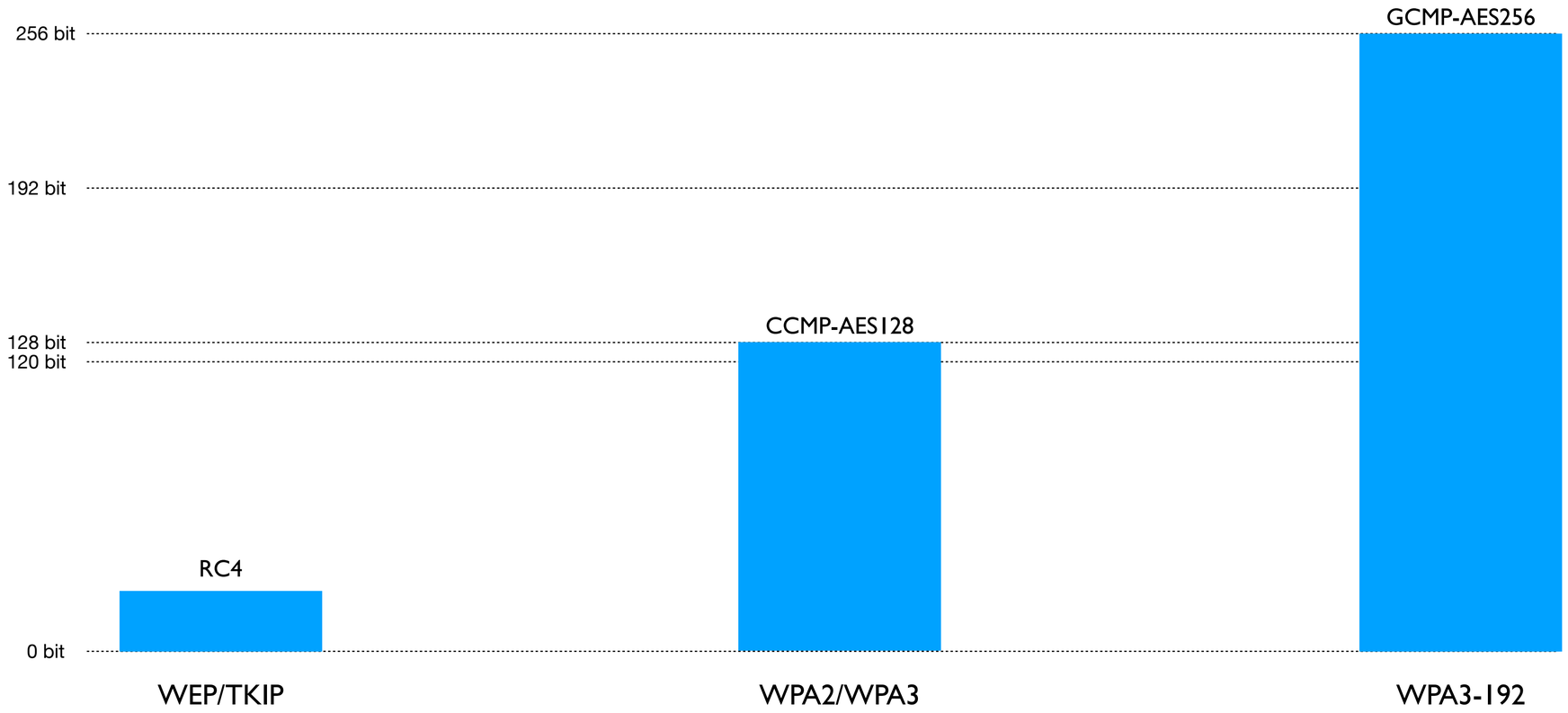
- NSA/NIST Suite B Cryptography (2005)
  - Security Level „Secret“: 128 Bit
  - Security Level „Top Secret“: 192 bit

- 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)

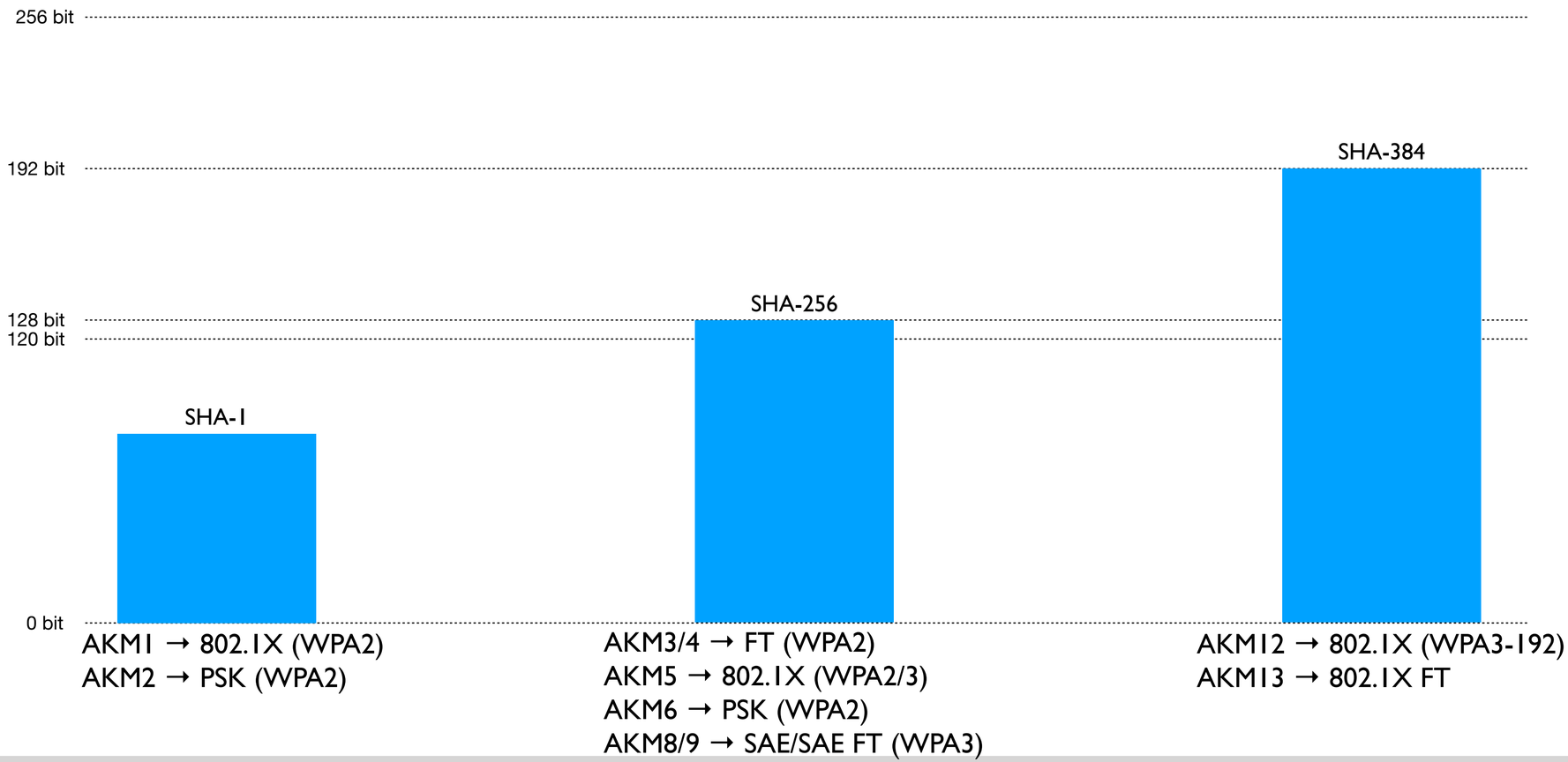
Security Level

Encryption



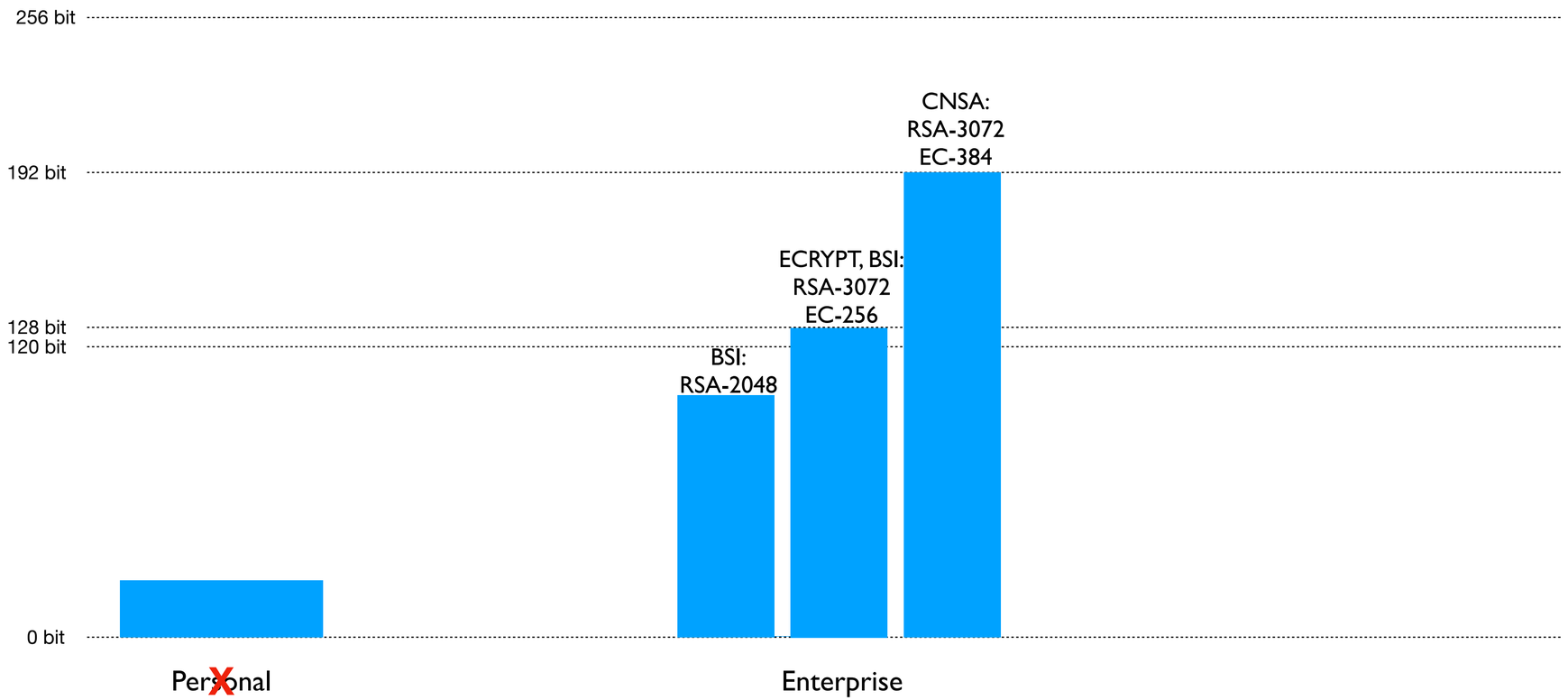
Security Level

PTK-Generation



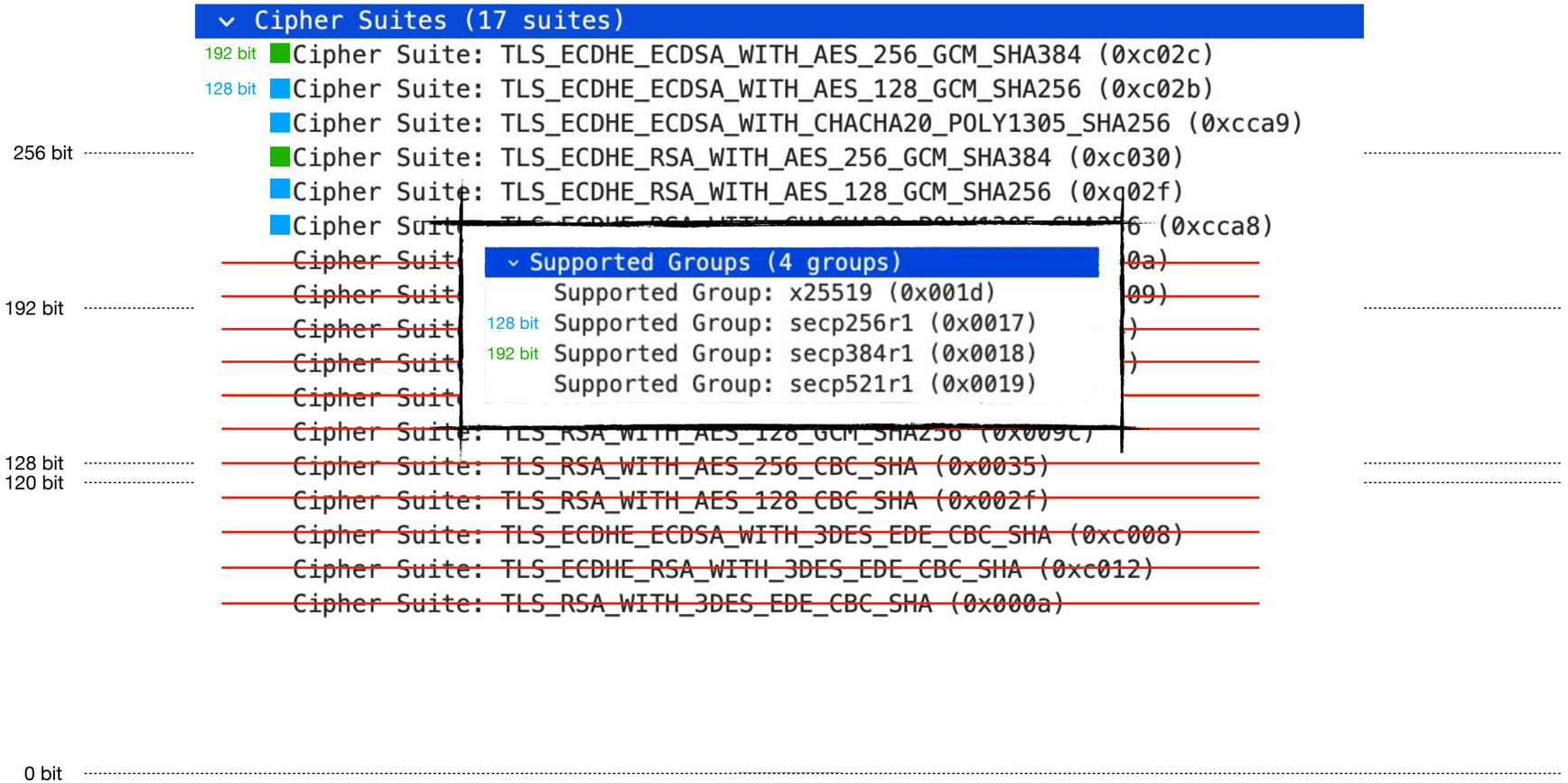
Security Level

Authentication



Security Level

Key Exchange



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 802.11-2020:

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

The AKM suite selector value **00-0F-AC:12** is used only with cipher suite selector values 00-0F-AC:9 (**GCMP-256**), 00-0F-AC:10 (**CCMP-256**), 00-0F-AC:13 (**BIP-CMAC-256**), and 00-0F-AC:12 (**BIP-GMAC-256**).

WPA3 - 192 bit Mode

- WPA3 Specification, Version 3.3, 2024-02-16:
  - An AP's BSS configuration shall be **PMF Required** …
  - **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

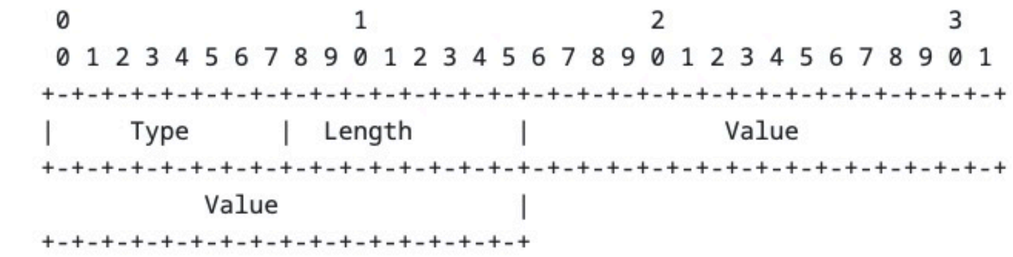
The RADIUS-Server?

2.16. WLAN-AKM-Suite

Description

The WLAN-AKM-Suite Attribute contains information on the authentication and key management suite used to establish the robust security network association (RSNA) between the AP and mobile device. A WLAN-AKM-Suite Attribute MAY be included within Access-Request and Accounting-Request packets.

A summary of the WLAN-AKM-Suite Attribute format is shown below. The fields are transmitted from left to right.



Type

188

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

(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

End Devices

- **Apple iOS/iPadOS**
  … on all iPhone 11 or later models and all iPad models, starting with the iPad (7th generation).

- **Apple macOS**
  … All Mac-Computers with Apple Chips …

- **Windows 10/11**

- **Android v12**

When to start with the WPA3-192 Implementation?

Now!