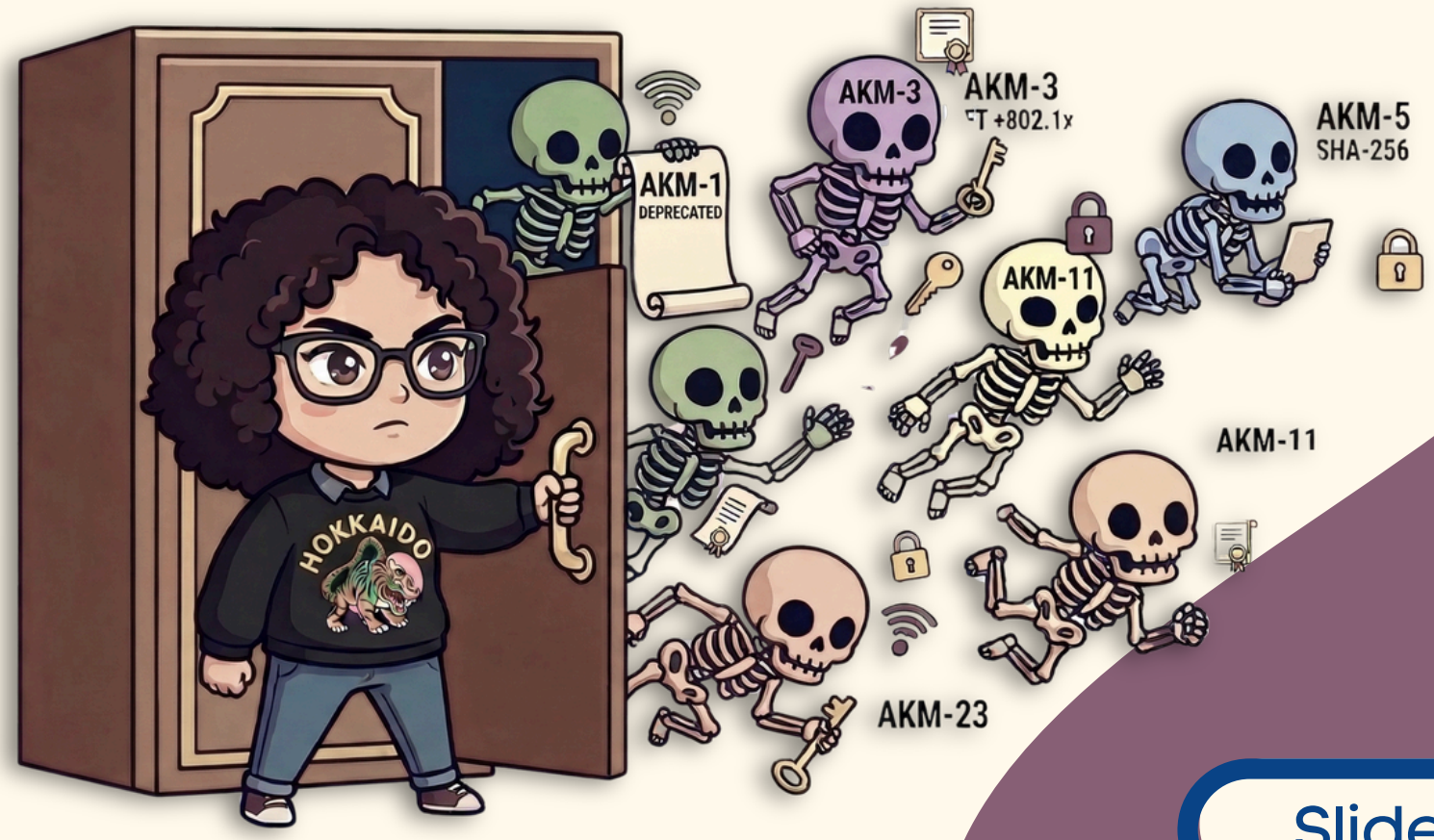
The Killer AKMs And Their Security Skeletons



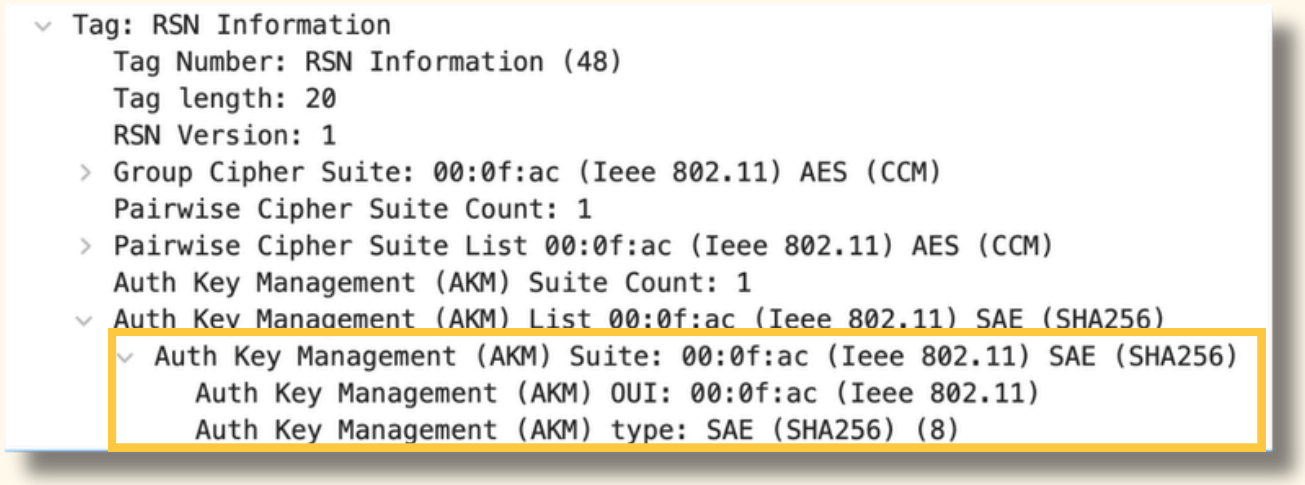
linkedin.com/santoseva

Slide

What's an AKM?

The Authentication Key Management (AKM) List Field defines the authentication used by an AP or client.

You'll see this field in the **RSN IE** in management frames such as beacons and probe requests/responses.



This field begins with **00:FC:AC:##** where the last byte (##) indicates the authentication type.

Above, the example shows SAE (00:FC:AC:08) in use.

Slide >

The Basic AKMs

AKM 1 802.1x with SHA-1

Used in WPA# Enterprise modes permitting SHA-1 hashes

AKM 2 PSK with SHA-1

Used in WPA# Personal modes permitting SHA-1 hashes

SHA-1 = Secure Hash Algo version 1
It yields a 160 bit hash.
SHA-1 is widely considered deprecated.

AKM 5 802.1x with SHA-256

Used in WPA# Enterprise modes permitting SHA-256 hashes

AKM 6 PSK with SHA-256

Used in WPA# Personal modes permitting SHA-256 hashes

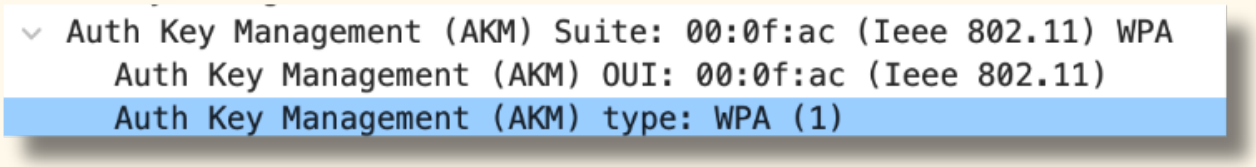
SHA-256 =. Secure Hash Algo, 256 bit
Part of SHA-2 family.
Output hash is 256 bits.

Fun Fact: AKM 0 (00-0F-AC:0) is reserved in IEEE 802.11-2024, Table 9-190—AKM suite selectors

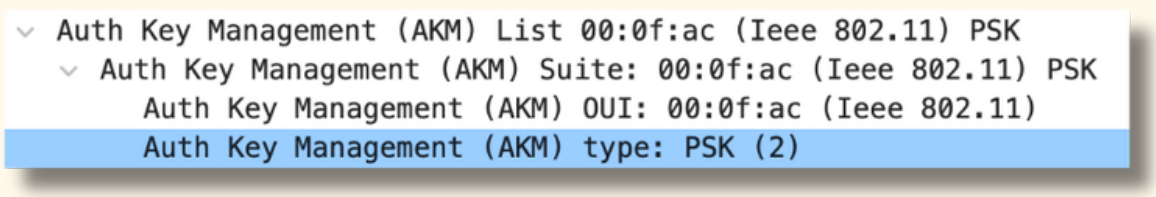
Slide >

Practically speaking,

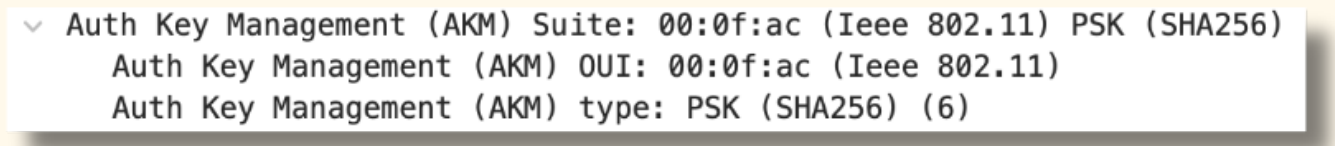
for WPA2-Enterprise networks not using 802.11r, you'll probably see **AKM 1.**



For WPA2-Personal networks not using 802.11r, you'll probably see **AKM 2.**



You may come across **AKM 6** on its own or advertised in WPA3-Personal Transition mode SSIDs



Slide >

“Gotta go Fast” AKMs

Generally speaking, FT versions of authentication modes will have their own AKMs.

AKM 3 FT with 802.1x with SHA-256

Used in WPA# Enterprise modes permitting SHA-256 hashes and fast transition (802.11r)

AKM 4 FT with PSK with SHA-256

Used in WPA# Personal modes permitting SHA-256 hashes and fast transition (802.11r)

Note: You’ll see **AKM 3** often in WPA2-Enterprise SSIDs.

However, **AKM 4** is probably not common. Fast Transition is meant for shortening roams on Enterprise SSIDs with longer re-auth times.

There are other FT AKMs, which we’ll get to...

Slide

WPA3-Personal AKMs

(Not Wi-Fi 7)

AKM 8 SAE, **AKM 9** FT with SAE

These AKMs were introduced to replace PSK authentication. **AKM 9** is the fast transition variant.

Non-Wi-Fi 7 SSIDs using WPA3-Personal will use **AKM 8 or 9.**
WPA-3 Personal Transition will use **AKM 8.**

6 GHz STAs cannot use **AKM 2,4 or 6.**
(IEEE 802.11-2024, 12.12.2)

WPA3-Personal also must support Wi-Fi 7 **AKM 24** and optionally **AKM 25**.

Slide >

WPA3-Enterprise AKMs

Non-192-bit

You'll likely see **AKM 5** or **AKM 3** in use.
Notably, **AKM 1** is not allowed in WPA3-Enterprise mode and only allowed in WPA3-Enterprise Transition.

192-bit

AKM 12 802.1X with SHA-384

SHA-384 = Secure Hash Algo, 384 bit
It yields a 384 bit hash.
This complies with NSA Commercial National Security Algorithm (CNSA) requirements

Used in WPA3-Enterprise modes requiring Suite B cryptography

AKM 23 (FT with 802.1x with SHA384) is also defined but allowed in the WPA3 Standard for WPA3-Enterprise 192-bit

As a result, there's no fast roaming for the 192-bit mode.

Slide >

New AKMs on the Block (Wi-Fi 7)

AKM 24 SAE using GDH

AKM 25 FT with SAE using GDH

GDH = Group-Dependent Hash

For WPA3-Personal SSIDs with Wi-Fi 7 STAs, the STAs can only use **AKM 24 or 25 for EHT (802.11be) operation.**

AKMs 22 and 23 were introduced in 802.11be, but aren't part of Wi-Fi Alliance certification currently.

Slide >

Conclusion?

AKM comprehension will only get more important.

Wi-Fi 7 has its own AKMs for Personal mode. SuiteB 192-bit encryption comes with its own caveats. Legacy AKMs should be continually phased out.

With every generation, there's more AKMs to keep track of and comply with.

Slide >

Find this helpful?

Eva Santos
<- Likes Wi-Fi
WiFrizzy.com

Repost Follow

linkedin.com/santoseva

Share