Wi-Fi Alliance® Wi-Fi® Security Roadmap and WPA3™ Updates

December 2020

Stephen Orr
Distinguished Architect
Cisco
sorr@cisco.com
@StephenMOrr

Dr. Thomas Derham
Principal Scientist
Broadcom

Session objective

High level overview of the Wi-Fi CERTIFIED WPA3™ program

Not intended to be a deep dive into the specific protocols, implementation details, or deployment models

Security and usability

There are always tradeoffs between usability and security

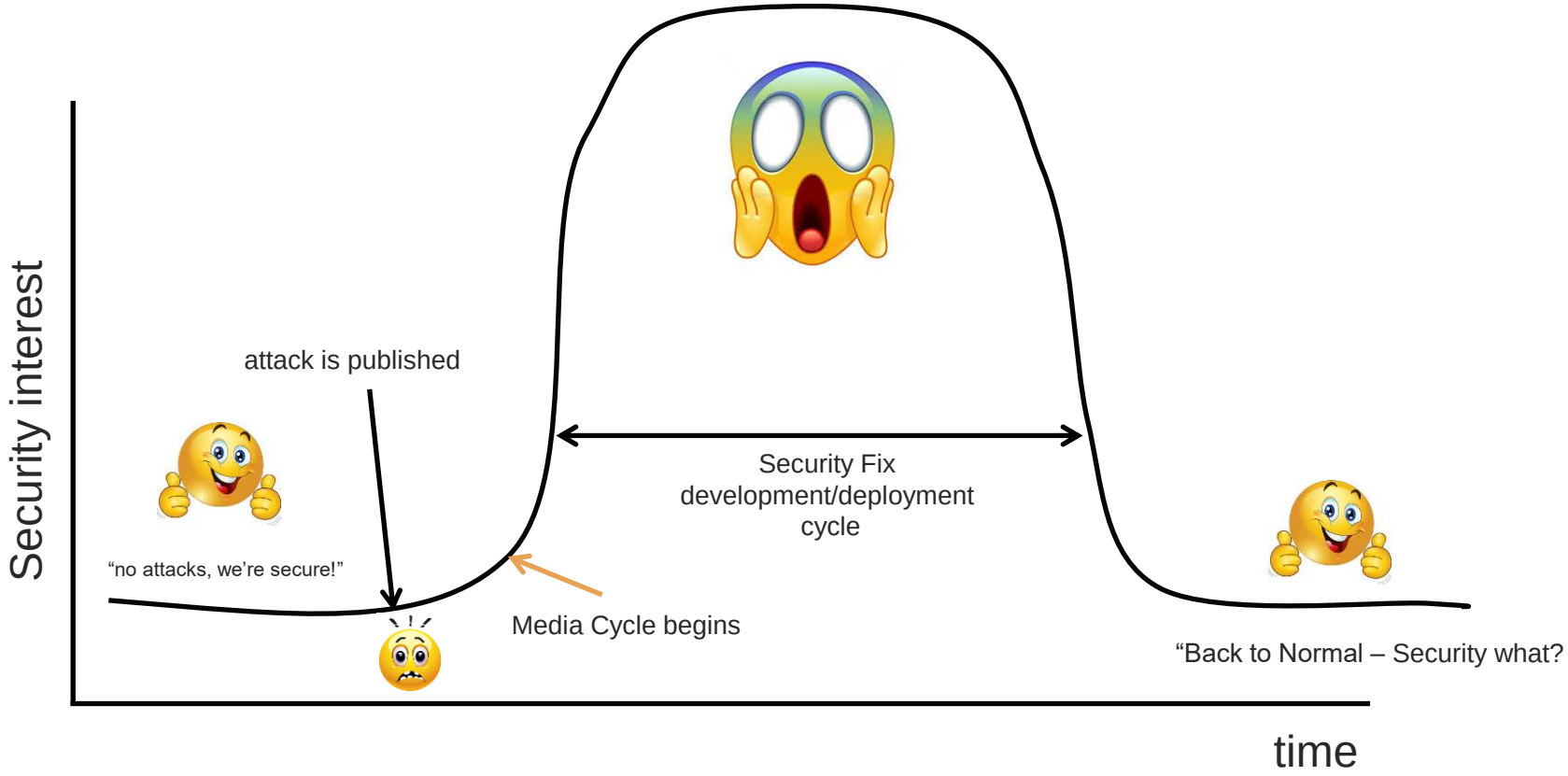
Over-rotating either way can cause challenges

Need to strike a balance between security and usability

Understand the tradeoffs when deploying security technologies and make sure they meet your security requirements

- Personal vs Enterprise
- Transition modes
- EAP types
- Cryptographic strength

Interest in security technologies

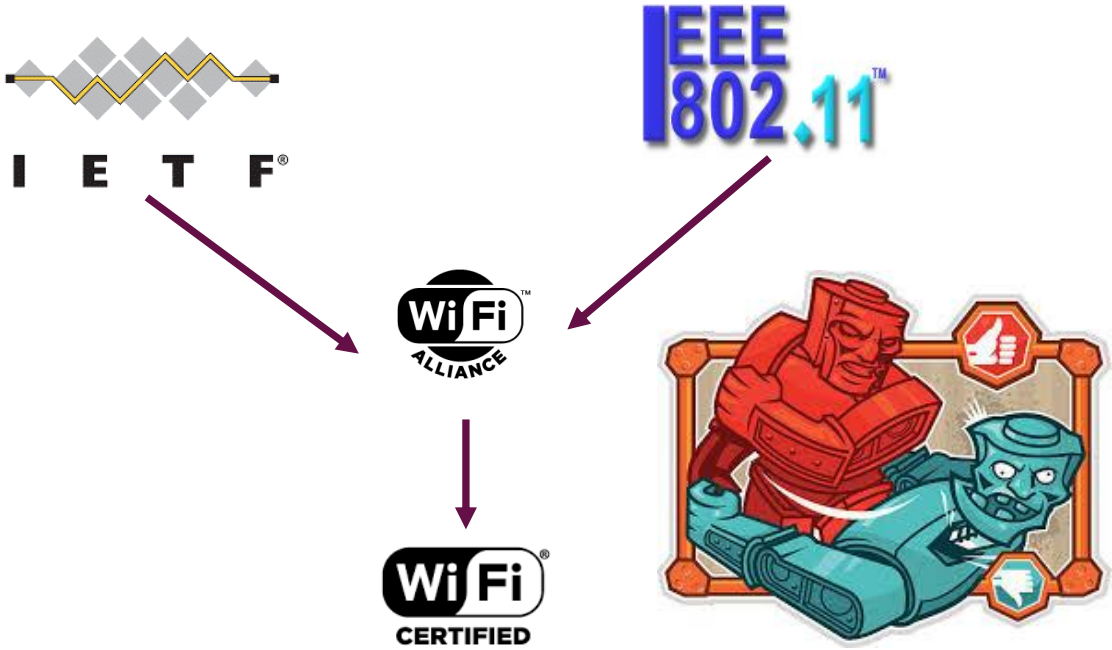


WPA3™

Mandatory as of 1 July 2020 for all new Wi-Fi CERTIFIED™ devices

Yes, it’s been a 5-year mission

The road to Wi-Fi Protected Access®



It’s all about compromise

Wi-Fi Alliance security program history

Security Enhancements have typically taken a reactive approach (something was broken and then we fixed it):

- **WEP – first exploits 2001**
- **WPA™ (2003)**
  - Attempted to bridge security gap from WEP to 802.11i
  - Beck-Tews attacks shows vulnerabilities in TKIP (compromises confidentiality) 2008
  - WPA-PSK brute force attacks (compromises network access and confidentiality)
- **WPA2™ (2004)**
  - Integrated security enhancements from 802.11i (added AES)
  - WPA2-Personal: brute force attacks still exist
  - Still maintains a TKIP only mode of operation
  - Inconsistent cryptography strength (SHA-1 <80 bits of security)
- **Wi-Fi Protected Setup™ (2006)**
  - Created for the consumer to easily adopt Security
  - 2011 – Brute force pin attack (compromises network access)
  - 2014 – Weak Random Number Generator implementations compromises WPS
- **KRACK (2017)**
- **WPA2 Security Enhancements (2018)**
- **WPA3™ (2018)**
- **Wi-Fi CERTIFIED Enhanced Open™ (2018)**
- **Dragonblood (2019)**
- **WPA3 (Dec 2019)**
- **WPA3 (Dec 2020)**

You are here

What comes next on this list?

Open networks get an upgrade: Wi-Fi CERTIFIED Enhanced Open™

Wi-Fi CERTIFIED Enhanced Open™: What problem are we trying to solve?

- Passive Eavesdropping – that's it!!
- Something better than Open Networks to provide privacy
- Similar End User Experience to Open but with encryption
- Privacy – not Security
- ***No, we do not claim Man-In-The-Middle prevention***

Wi-Fi Enhanced Open™ Transition mode

- When an Open SSID is enabled on a Wi-Fi Enhanced Open AP – it shall create a separate hidden BSS with the same properties as the Open BSS
- The Open BSS will include an OWE Transition Mode Element to direct Wi-Fi Enhanced Open capable STAs to the Wi-Fi Enhanced Open BSS
- Why did we do this???
  - Legacy STA behavior – some see a Wi-Fi Enhanced Open BSS as "Open, dot1x or PSK" leading to a poor user experience

Wi-Fi Enhanced Open Transition mode

Open SSID “Open”

```
▼ Tagged parameters (401 bytes)
  ▶ Tag: SSID parameter set: Open
  ▶ Tag: Supported Rates 12(B), 18, 24, 36, 48, 54, [Mbit/sec]
  ▶ Tag: DS Parameter set: Current Channel: 108
  ▼ Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
      Tag Number: Vendor Specific (221)
      Tag length: 17
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 28
      BSSID: Cisco_9f:54:29 (04:eb:40:9f:54:29)
      SSID length: 6
      SSID: E-Open
```

OWE Transition Mode Element

- Open network advertises BSS and SSID of Wi-Fi Enhanced Open Network
- Wi-Fi Enhanced Open network advertises BSS and SSID of Open Network

Wi-Fi Enhanced Open SSID “E-Open”

```
▼ Tagged parameters (429 bytes)
  ▶ Tag: SSID parameter set: E-Open
  ▶ Tag: Supported Rates 12(B), 18, 24, 36, 48, 54, [Mbit/sec]
  ▶ Tag: DS Parameter set: Current Channel: 108
  ▼ Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
      Tag Number: Vendor Specific (221)
      Tag length: 15
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 28
      BSSID: Cisco_9f:54:2a (04:eb:40:9f:54:2a)
      SSID length: 4
      SSID: Open
```

What's the difference between WPA2™ and WPA3™

(it's a magic number)

- WPA3 is about continuous security development (multiple features over the last 3 years)
- Conformance as well as interoperability
- There is no Information Element that designates WPA3 (same as WPA2)
- WPA3 is defined by AKM/Cipher Suite/PFM combinations
- PMF must be negotiated (not optional)
- Mandatory for Wi-Fi 6 and now all new certifications

Level Set

WPA3 Modes: Because a mode is different than the brand

- WPA3-Personal
  - **WPA3-Personal only mode**
    - PMF Required
  - **WPA3-Personal Transition mode**
    - Configuration rules: On an AP, whenever WPA2-Personal is enabled, the WPA3-Personal Transition mode must also be enabled by default, unless explicitly overridden by the administrator to operate in WPA2-Personal only mode
- WPA3-Enterprise
  - **WPA3-Enterprise only mode**
    - PMF ***SHALL*** be negotiated for all WPA3 connections
  - **WPA3-Enterprise Transition mode**
    - PMF shall be negotiated for a WPA3 connection
    - PMF optional for a WPA2 connection
  - **WPA3-Enterprise “192-bit” mode (CNSA)**
    - More than just for the federal government
    - Consistent cryptographic cipher suites to avoid misconfiguration
    - Addition of GCM & ECC for crypto and better hash functions (SHA384)
    - PMF Required

WPA3 Transition modes:
Why did we do a transition mode for WPA2/WPA3?

WAIT – APs that support WPA3 should support Multiple BSSs – it's ***2020***

- Transition modes were created to preserve interoperability with WPA2 and help with end user experience

What did we inherit with a transition mode:

- ***Single BSS – for WPA2 and WPA3 certified devices***
  - WPA3-Personal
    - ***Same passphrase exists between WPA2-Personal and WPA3-Personal***
    - ***WPA2-Personal is still vulnerable to all the classic issues***
  - WPA3-Enterprise
    - Mix of Enterprise devices that have PMF negotiated (WPA3) and not (WPA2)

The upside

- WPA3-Personal
  - Connections are secure – knowing the passphrase gets that adversary access to the WLAN/Infrastructure not the ability to decrypt other users' sessions
- WPA3-Enterprise
  - All WPA3 devices will take advantage of PMF capabilities

If a WPA3 Transition mode does not meet the security requirements for a deployment, WPA3 and WPA2 should be deployed on individual SSIDs and logically separated/isolated network segments.

Important Wi-Fi Alliance security links

- Security topic page:
  - https://www.wi-fi.org/discover-wi-fi/security
- WPA3 Specification:
  - https://www.wi-fi.org/file/wpa3-specification
- WPA3 Specification Addendum:
  - https://www.wi-fi.org/file/wpa3-specification-addendum-draft
- WPA3 Security Considerations:
  - https://www.wi-fi.org/file/wpa3-security-considerations
- Security Development
  - https://www.wi-fi.org/security-development

Interesting stuff located here

Anyone can provide feedback on Security Specifications

WPA3
2019 Update

- Fast BSS Transition
- EAP Server Certificate Validation (SCV)

Fast BSS Transition (802.11r) for WPA3

Benefits

- Minimize connectivity outage and KPI degradation during roams
  - For transitions between bands, and for mobility roaming between APs
- Optimize for QoS-sensitive services, e.g. VoIP, gaming, video

Feature

- FT-SAE (WPA3-Personal), FT-EAP (WPA3-Enterprise)
  - Also includes FT-PSK (WPA2-Personal) and WPA3 transition modes
  - PMF enabled
- “Over-the-air” and “Over-the-DS” variants

Optional feature for Wi-Fi CERTIFIED WPA3

Fast BSS Transition (802.11r) for WPA3

AKM selection preference (STA)

When AP supports multiple FT and non-FT modes, highest security mode is always preferred by STA

Personal

1. FT-SAE (SHA256) 00-0F-AC:9
2. SAE (SHA256) 00-0F-AC:8
3. FT-PSK (SHA256) 00-0F-AC:4
4. PSK (SHA256) 00-0F-AC:6
5. PSK (SHA1) 00-0F-AC:2

Enterprise

1. FT-EAP (SHA256) 00-0F-AC:3
2. EAP (SHA256) 00-0F-AC:5
3. EAP (SHA1) 00-0F-AC:1

EAP Server Certificate Validation (SCV)

Benefits

- Ensure proper certificate validation with TLS-based WPA3-Enterprise
- *Protect against active evil-twin AP attacks on client devices*
  - Data traffic inspection, modification, etc.
  - Attacks on inner client authentication (e.g., dictionary attack) can compromise enterprise user credentials
- Address long-standing and well-documented issue in real-world WPA2-Enterprise deployments:
  - https://www.researchgate.net/publication/327005936_InSecure_Configuration_Practices_of_WPA2_Enterprise_Supplicants
  - https://www.securew2.com/blog/android-11-server-certificate-validation-error-solution

EAP Server Certificate Validation (SCV)

Feature

- STA must perform SCV whenever EAP-TLS, EAP-TTLS or EAP-PEAP is used
- Allowed trust anchors:
  - Server certificate, or CA root cert, pinned to network profile
  - CA in trust root store plus explicit domain name (partial or FQDN)
- Trust-on-First-Use (TOFU), aka “UOSC”, is allowed by default
  - See WPA3 specification for recommended dialog message for user to accept trust, e.g. based on cert fingerprint or (if CA is trusted) the domain name
- Operator can include Trust Override Disable (TOD) policy in server cert
  - Prevents user from subsequently overriding it
- SCV cannot be disabled (e.g. “Do not validate” option in UI is not allowed)

Mandatory for Wi-Fi CERTIFIED WPA3-Enterprise

WPA3
2020 Update

- SAE Hash-to-Element
- Transition Disable
- SAE Public Key (SAE-PK)
- Wi-Fi QR code
- Beacon Protection
- Operating Channel Validation
- Privacy Extension Mechanisms

SAE Hash-to-Element (H2E)

Benefits

- Computationally efficient technique to mitigate side-channel attacks
  - Original “hunting-and-pecking” technique requires large number of loop iterations
  - Based on crypto best practice (see IETF draft-irtf-cfrg-hash-to-curve)
- Intermediary key (PT) is derived from password offline (one-time, per group)
  - Further reduces potential side-channel attack vectors

Protocol support

- Defined in 802.11REVmd; AKMs remain the same (SAE and FT-SAE)
  - H2E advertised in RSNXE, negotiated in SAE exchange; also includes group downgrade protection
- STA falls back to hunting-and-pecking if AP does not support H2E

Mandatory feature for Wi-Fi CERTIFIED WPA3

Also, for SAE in 6 GHz band, only H2E is used (hunting-and-pecking disallowed)

Transition Disable Indication

Benefits

- Provides protection against Transition mode downgrade attacks on STAs
- Configurable policy on AP (e.g. by network operator)
  - For example, when all APs in the network support a higher security mode, STAs no longer need to enable lower-security modes for that network

Feature

- When configured, AP sends Transition Disable indication to STAs at association
  - Protected in 4-way handshake
- The STA disables the indicated Transition modes in its network profile for subsequent connections to that network (SSID)
- Currently supports the following Transition modes (also disables WEP/TKIP):
  - WPA3-Personal Transition mode
  - SAE-PK in transition with WPA2/3-Personal
  - WPA3-Enterprise Transition mode
  - Wi-Fi Enhanced Open Transition mode

Mandatory feature for Wi-Fi CERTIFIED WPA3

SAE Public Key (SAE-PK)

Benefits

- Better security for “small” public networks that cannot deploy EAP authentication
  - Use cases where, today, a WPA2/WPA3-Personal password is shared on signage in a cafe/restaurant, meeting venue, etc.
- Avoids evil-twin AP attacks by attacker who knows the password
  - Data traffic inspection, modification, etc.
  - Social engineering attacks, such as:
    - Fake login portal (compromises other credentials, credit card, ...)
    - Accept trust in malicious HTTPS proxy cert
  - Exploit client device vulnerabilities

SAE Public Key (SAE-PK)

Feature

- Extension to SAE protocol (same AKM)
  - SAE-PK advertised in RSNXE, negotiated in SAE exchange
  - Authentication results in pairwise PMK with same properties as SAE
  - Network access control based on knowledge of password
- SAE-PK network is configured with EC public key pair
  - Secrecy of private key provides protection against evil-twin AP attacks even when password is known by attacker
- Password is specially generated, embeds base32 fingerprint of public key
  - Example password: *a2bc-de3f-ghi4*
  - Design provides resistance against second preimage attacks and “blackboard” attacks
- During SAE authentication, AP signs the SAE transcript, and STA validates the signature using the trusted fingerprint decoded from the password
  - Authentication fails if public key or signature not validated by STA

Optional feature for Wi-Fi CERTIFIED WPA3

Wi-Fi QR code

- Formalized “WIFI” URI definition
  - Registered with IANA: https://www.iana.org/assignments/uri-schemes/prov/wifi
  - Typically used in Wi-Fi QR codes
    - Easy way for a STA (with a camera) to connect to a new network
- Backward-compatible with current de-facto standard WIFI URI format
  - As supported by many major client operating systems
- Adds support for WPA3 features, including:
  - Transition Disable
  - SAE-PK
  - Non-ASCII passwords (percent-encoded)

Beacon Protection and Operating Channel Validation (802.11 REVmd)

Beacon Protection

- Provides integrity protection of Beacon frames using a key that is known only by devices in the network
- Protects against attacks where Beacon frame content is manipulated, e.g. denial-of-service “quiet” attack and WMM parameter set attack, Transmit Power Control limit attack
- See: https://papers.mathyvanhoef.com/wisec2020.pdf

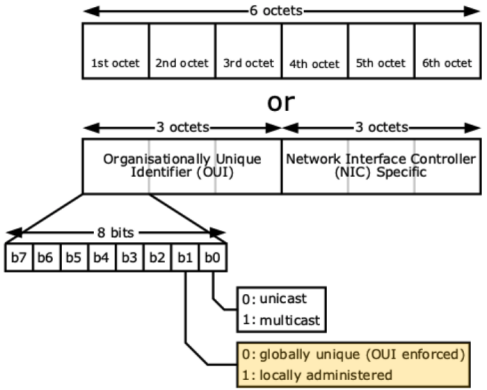
Operating Channel Validation

- Provides mutual verification between peers (e.g., AP and STA) of the current operating channel during security-related exchanges and channel switches
- Generic protection to harden against channel-based man-in-the-middle attacks
- See: https://papers.mathyvanhoef.com/wisec2018.pdf

Optional features for Wi-Fi CERTIFIED WPA3

Privacy Extension Mechanisms

- Goal is to establish consistent implementation guidelines and use cases for MAC Address randomization
  - based on 802.11aq privacy enhancements, updated in 802.11REVmd
  - critical to protect user privacy
- In addition, protects against exposure of certain other information that may lead to Personally Identifiable Information (PII) leakage
  - STA shall construct a uniquely randomized MAC address per SSID, unless saved Wi-Fi network profile explicitly requires to use its globally unique MAC address. The STA may construct a new randomized MAC address for an SSID at its discretion.
  - During Active Scanning while not associated to a BSS
  - For each ANQP exchange while not associated to a BSS



Optional feature for Wi-Fi CERTIFIED WPA3
enabled by default (out-of-box) if supported

What’s next?

High level – what's on the horizon: 6 GHz, 60 GHz and others

In new greenfield MAC/PHY/Bands

- **WPA3 is the starting point**
  - WPA3-Personal required
  - WPA3-Enterprise and WPA3-Enterprise 192-bit optional
  - Legacy WPA2/WPA shall not be supported (Personal or Enterprise)
- **Open Networks - eliminated**
  - If open access without authentication is needed, Wi-Fi Enhanced Open must be used
- **The following transition modes will not be supported**
  - WPA3-Personal Transition mode
  - Wi-Fi Enhanced Open Transition mode
- **WEP and TKIP shall not be supported**

2020 and beyond

- What do we focus on?
- Security is an obscure technology
  - Better UX/UI to inform users?
  - Consistent crypto?
  - Focus 3-5 years out?
- Opportunity to make your voice heard

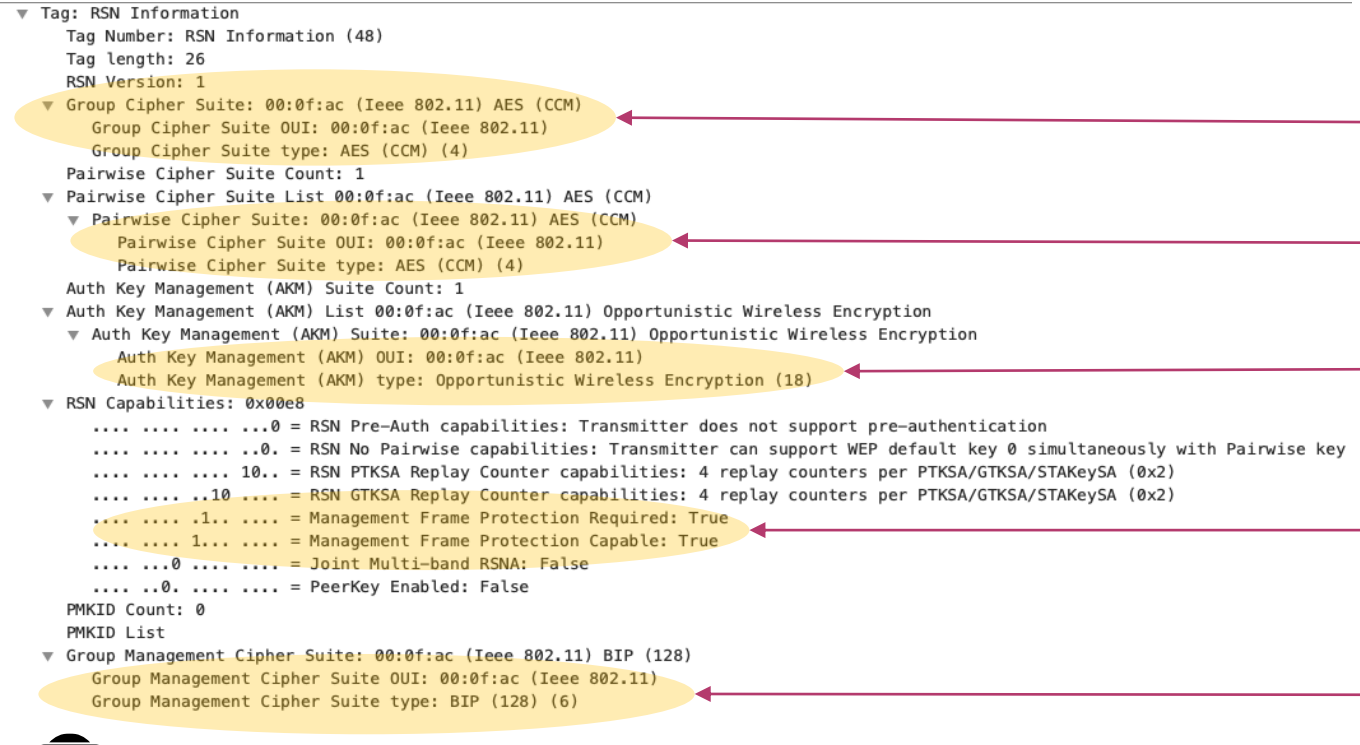
Additional information

WPA3 and Wi-Fi Enhanced Open decoder ring

Feature	2.4/5 GHz	6 GHz
Wi-Fi Enhanced Open	Optional	Optional
Wi-Fi Enhanced Open Transition mode	Required if Wi-Fi Enhanced Open is supported	Disallowed
WPA3-Personal	Required	Required (H2E only)
WPA3-Personal Transition mode	Required	Disallowed
WPA3-Enteprise	Optional	Optional
WPA3-Enterprise Transition mode	Optional	Disallowed
EAP Server Certificate Validation (SCV)	Required with WPA3-Enterprise	Required with WPA3-Enterprise
WPA3-Enterprise 192-bit security	Optional	Optional
Fast BSS Transition	Optional	Optional
SAE-PK	Optional	Optional
Beacon Protection	Optional	Optional
Operating Channel Validation	Optional	Optional
Privacy Extension Mechanisms	Optional	Optional

Wi-Fi Enhanced Open – only mode

Beacon Frame



Group Cipher AES-CCM-128

Pairwise Cipher AES-CCM-128

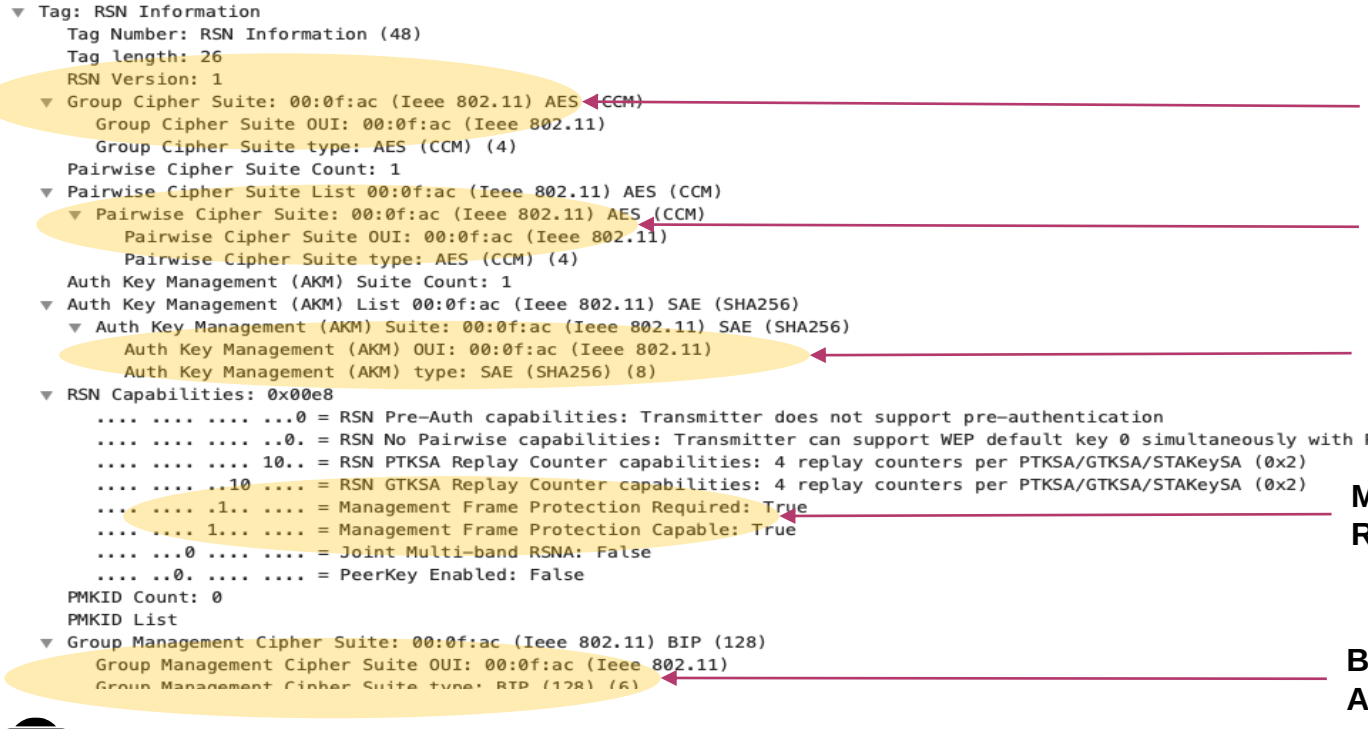
AKM 00:0f:ac:18 (OWE)

Management Frame Protection Required

Broadcast Integrity Protocol (BIP) AES-CMAC-128

WPA3-Personal only

Beacon



Group Cipher AES-CCM-128

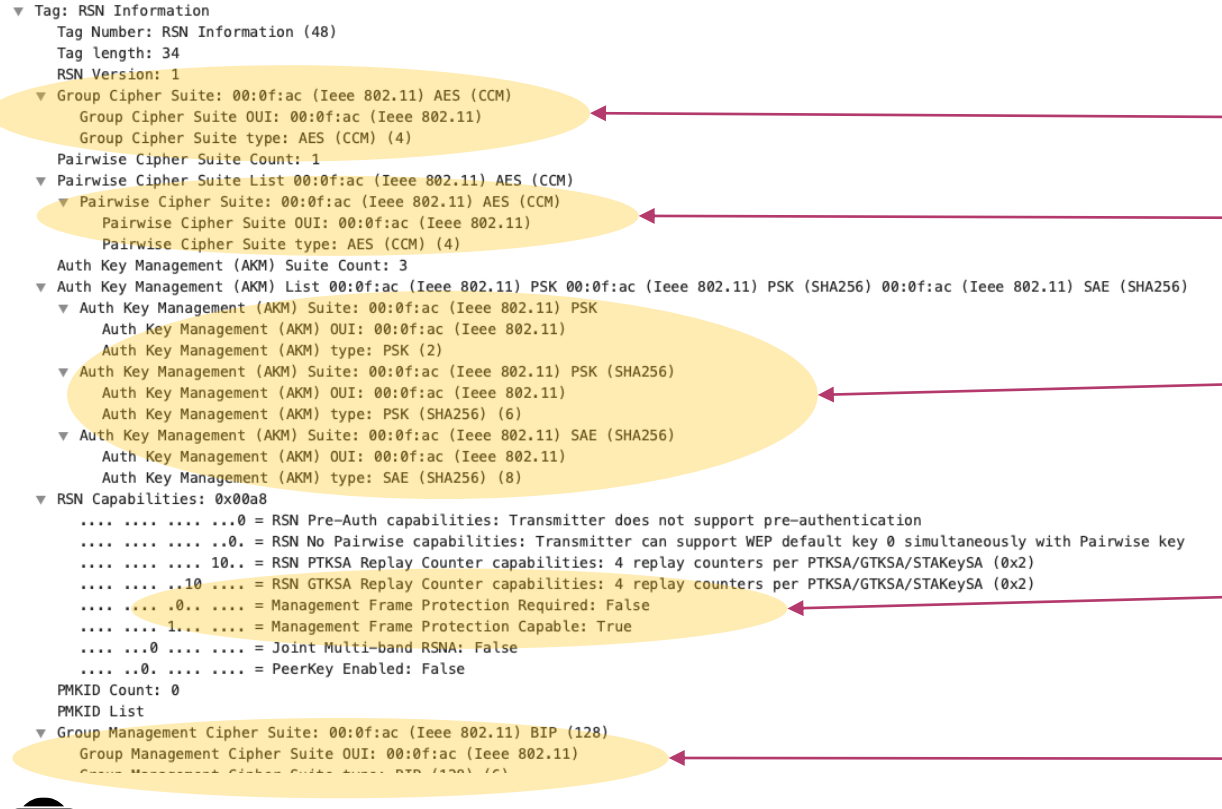
Pairwise Cipher AES-CCM-128

AKM 00:0f:ac:08 (SAE)

Management Frame Protection Required

Broadcast Integrity Protocol (BIP) AES-CMAC-128

WPA3-Personal Transition mode



Group Cipher AES-CCM-128

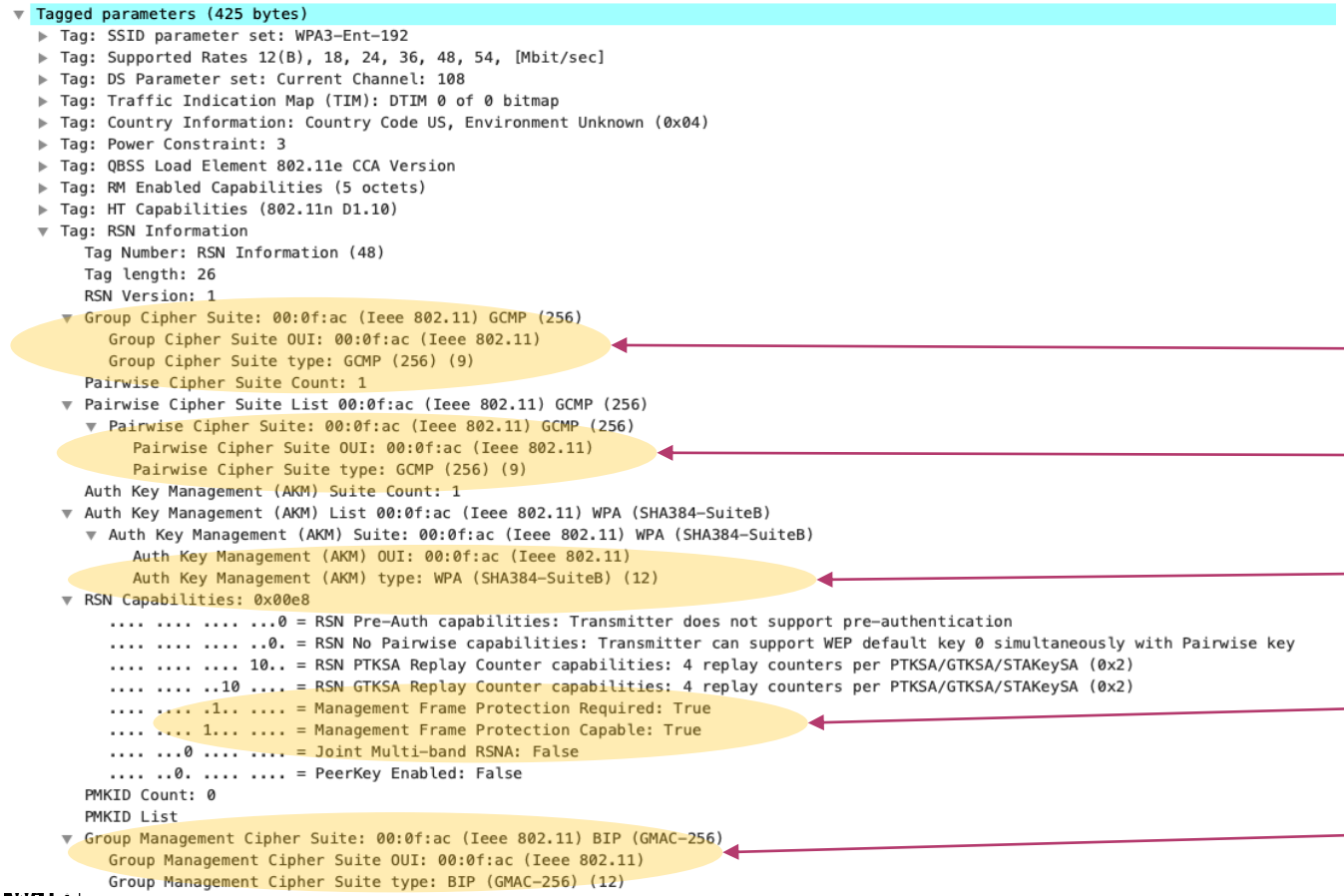
Pairwise Cipher AES-CCM-128

Multiple AKMs:
AKM 00:0f:ac:2 PSK
AKM 00:0f:ac:6 PSK (SHA256)
AKM 00:0f:ac:8 (SAE)

Management Frame Protection *Capable*

Broadcast Integrity Protocol (BIP) AES-CMAC-128

WPA3-Enterprise 192-bit security



Group Cipher AES-GCMP-256

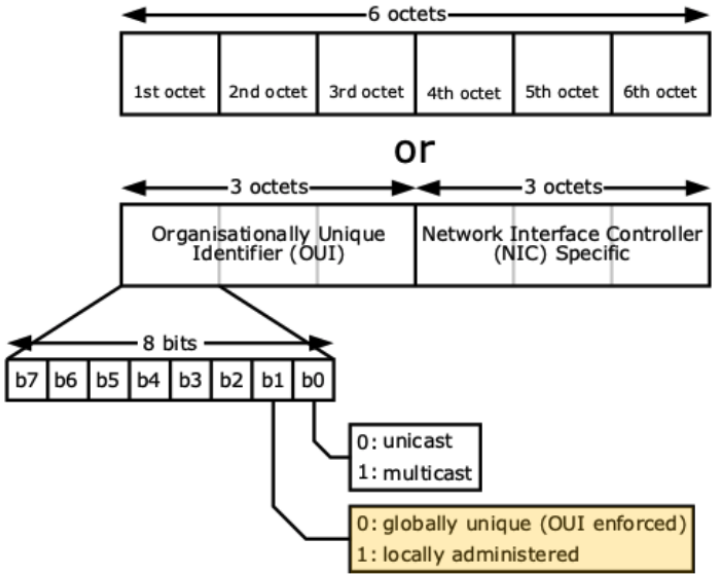
Pairwise Cipher AES-GCMP-256

AKM 00:0f:ac:12 SHA384

Management Frame Protection Required

Broadcast Integrity Protocol (BIP) AES-GMAC-256

MAC Randomization – locally administered



- b1 set to 1 (locally administered)
- based on the rule, all of the numbers below would qualify as a random MAC address. For a simple rule, any MAC address' first octet that ends 2,6,A,E would be a random MAC address.

- 32-28-6D-51-13-AF
- 56-EF-68-F6-0D-30
- 0A-13-A8-8E-B5-EF
- AE-83-37-55-A7-22

02-	32-	62-	92-	C2-	F2-
06-	36-	66-	96-	C6-	F6-
0A-	3A-	6A-	9A-	CA-	FA-
0E-	3E-	6E-	9E-	CE-	FE-
12-	42-	72-	A2-	D2-	
16-	46-	76-	A6-	D6-	
1A-	4A-	7A-	AA-	DA-	
1E-	4E-	7E-	AE-	DE-	
22-	52-	82-	B2-	E2-	
26-	56-	86-	B6-	E6-	
2A-	5A-	8A-	BA-	EA-	
2E-	5E-	8E-	BE-	EE-	