BENEFITS OF WPA3, ENHANCED OPEN & EASY CONNECT

WLPC PRAGUE 2018

PHILIPP EBBECKE, LANCOM SYSTEMS

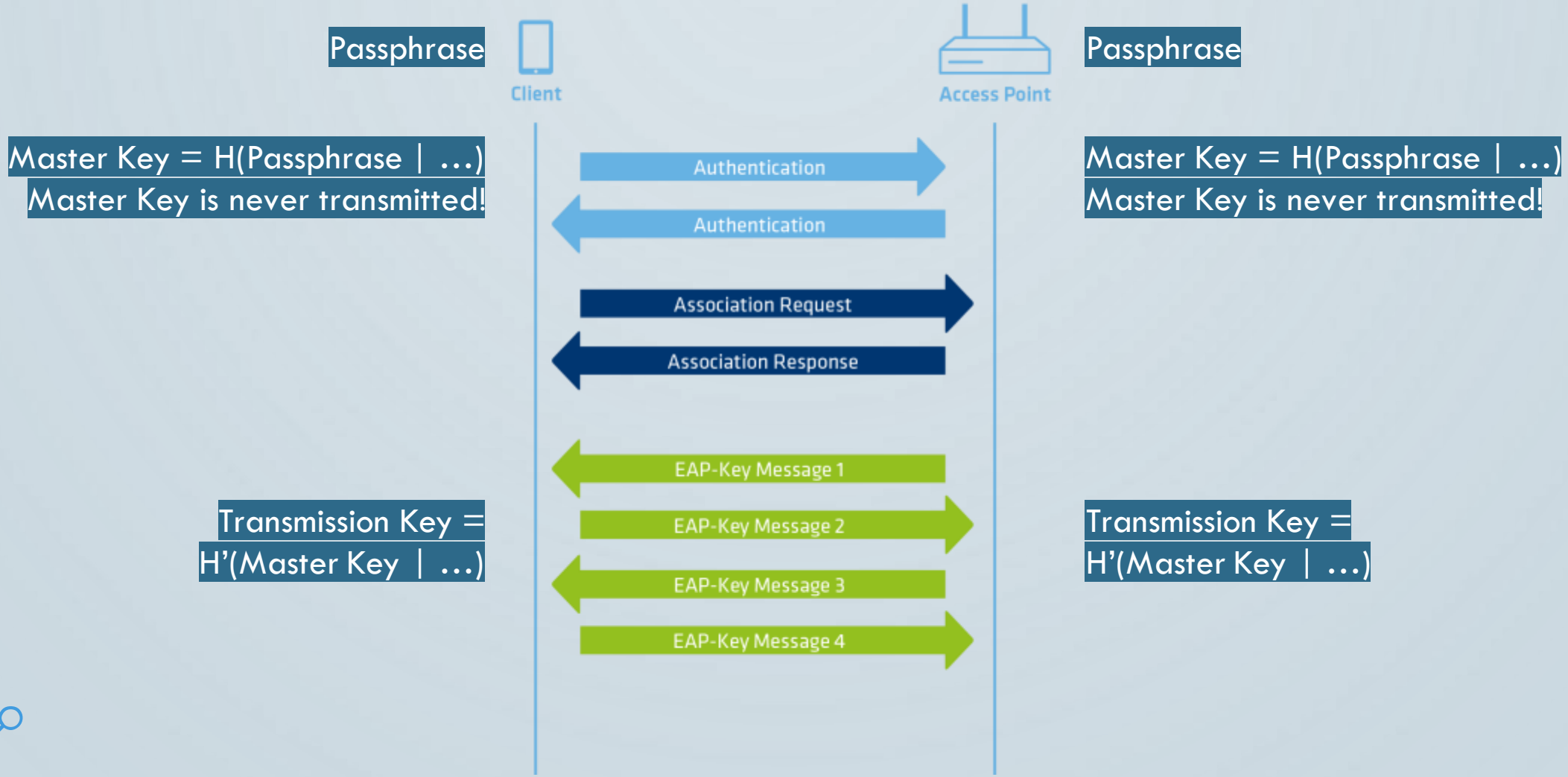
PERRY CORRELL, AEROHIVE

TABLE OF CONTENT

INTRODUCTION: WPA HISTORY

- Security Enhancements have typically taken a reactive approach:
  - **WEP** – first exploits 2001
  - **WPA (2003)**
    - attempted to bridge security gap from WEP to 802.11i
    - 2008 – Beck-Tews attacks shows vulnerabilities in TKIP (compromises confidentiality)
    - WPA-PSK brute force attacks (compromises network access and confidentiality)
  - **WPAv2 (2004)**
    - Integrated security enhancements from 802.11i (added AES)
    - WPA2-PSK: brute force attacks still exist
    - Still maintains a TKIP only mode of operation
    - Inconsistent cryptography strength (SHA-1 <80 bits of security)
  - **WPS (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

WPA2-PERSONAL CONNECTION PROCESS



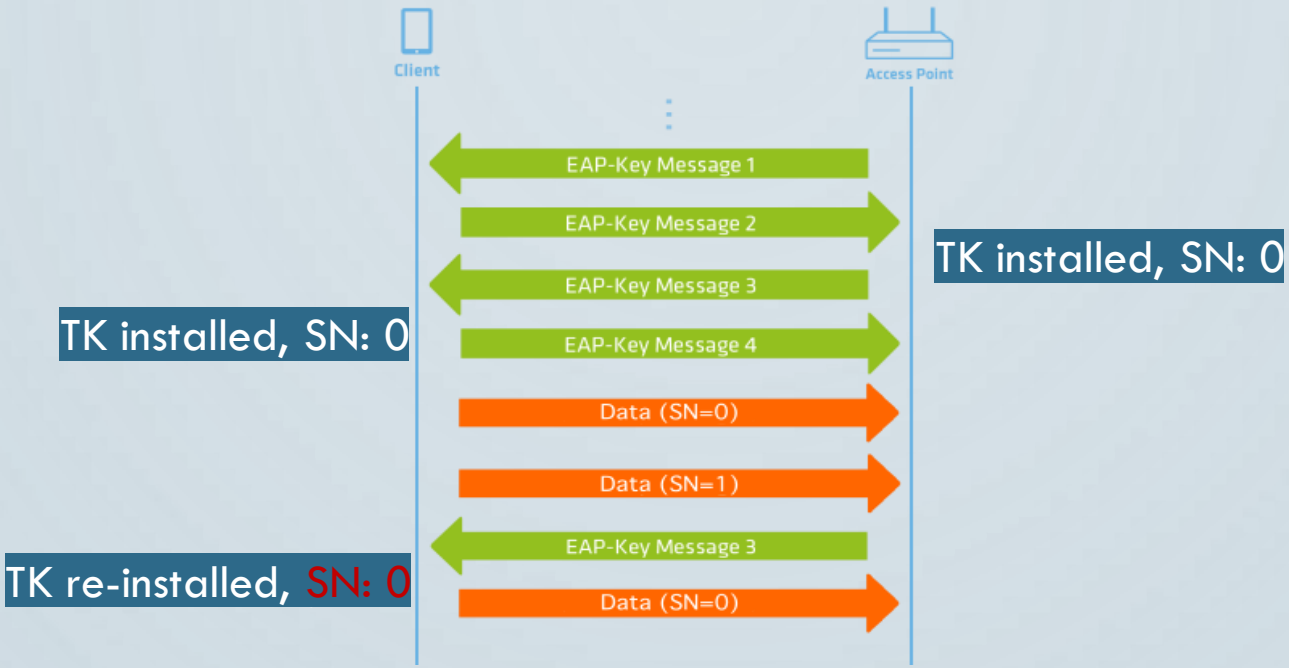
WPA2-PERSONAL: DEEPER DIVE

- Attacker can record EAP 4-Way handshake => Transmission $Key_{recorded}$ (TK)
- H and H' are known functions
- Offline:
  - Try out passphrase => Master $Key_{attacker}$
  - Generate new Transmission $Key_{attacker}$ based on Master $Key_{attacker}$
  - Check if Transmission $Key_{attacker}$ = Transmission $Key_{recorded}$
    - YES: Decrypt traffic and access network
    - NO: Try next passphrase

A LOOK BACK: PROTECTED MANAGEMENT FRAMES

- Protected Management Frames (PMF)
  - Disassociate Frames
  - Deauthenticate Frames
  - Action Frames
- Prevent ”Spoofed Disconnect” Attacks
- Prevent any disturbance of connections
- Works for WPA, WPA2 and WPA3

A LOOK BACK: THE KRACK-ATTACK



- NONCE: Number only used ONCE
- NONCE for Transmission(s):
  - Transmission Key (TK) + Sequence Number (SN)
- Attack: Keep TK but reset Sequence Number
- Counter-Measurement: Never reset SN for the same TK

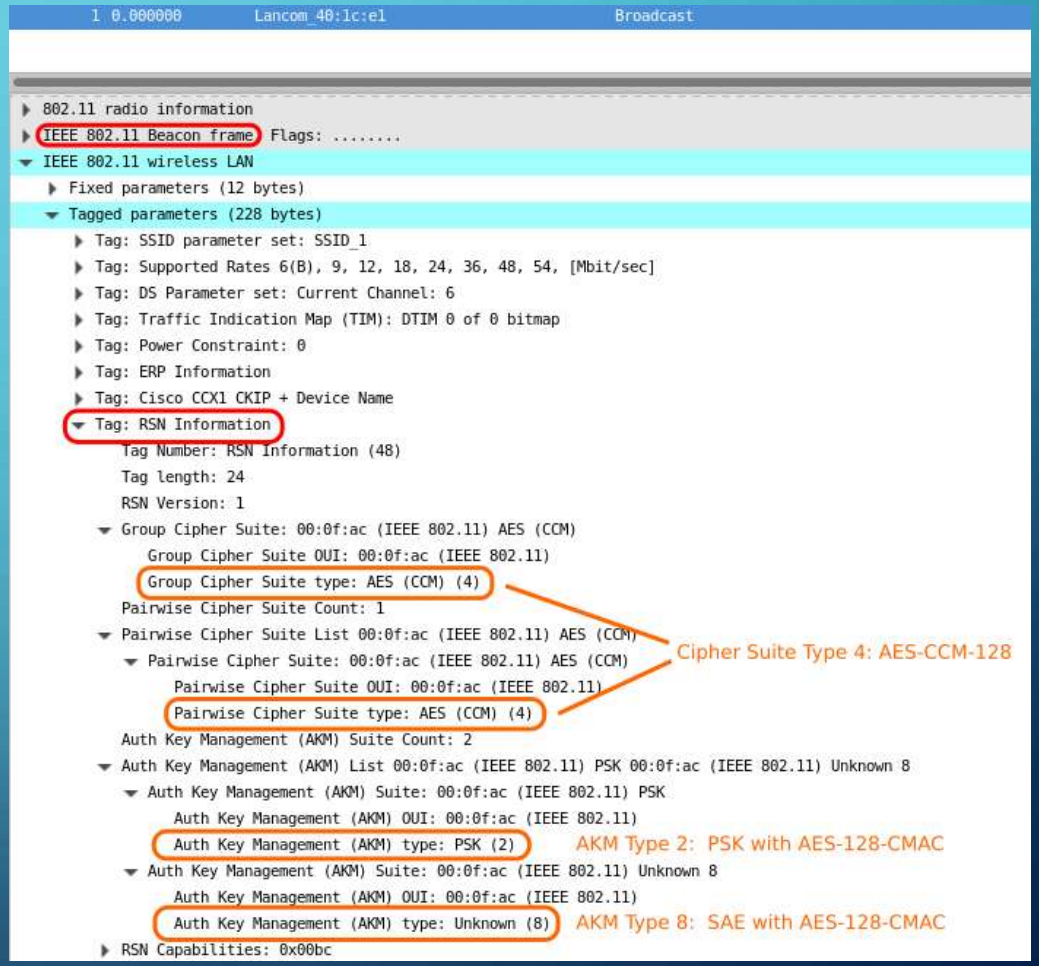
WI-FI CERTIFIED WPA3™ TECHNOLOGY OVERVIEW

WPA3 VISION

- Retain WPA3-Personal and WPA3-Enterprise split
  - Personal retains passwords
  - Enterprise interacts with other security systems
- Prevent the use of old technology
  - WPA3 would not allow WEP or TKIP (WPAv1)
  - Revisit EAP methods – remove unsecure EAP methods and utilize EAP methods with stronger ciphers
- Add new technology with improved security (even if not readily visible to user)
  - Replace WPA-PSK with SAE
  - Add 192-bit mode (Suite B) for high-grade encryption (optional)
  - PMF enabled by default
  - Utilize consistent cryptographic algorithms/hashing across all aspects of encryption/key generation/authentication

SECURITY IMPROVEMENTS

- WPA2+WPA3: Test for KRACK-Vulnerability
- Robust Security Network Element (RSNE) robustness
  - Unexpected RSNE termination
  - Unexpected values
  - Multiple AKM support
- Clients only:
  - Unknown root Certificate Authority (CA) detection
  - Replay protection on unicast + group addressed frames



WPA3-PERSONAL: CRYPTO BASICS

- Generator: a number, e.g. 3
- Prime numbers: 1, 3, 5, 7, 11, 13, …
- Modulo: 5 modulo 3 = 2
- Exponentiation: $5^3 = 5 * 5 * 5 = 25 * 5 = 125$
- Rules for Exponentiation:
  - $(5^3)^2 = (125)^2 = 15625$
  - $(5^2)^3 = (25)^3 = 15625$
- Discrete logarithm problem: $5^x \bmod 3 = 2$, determine the x!

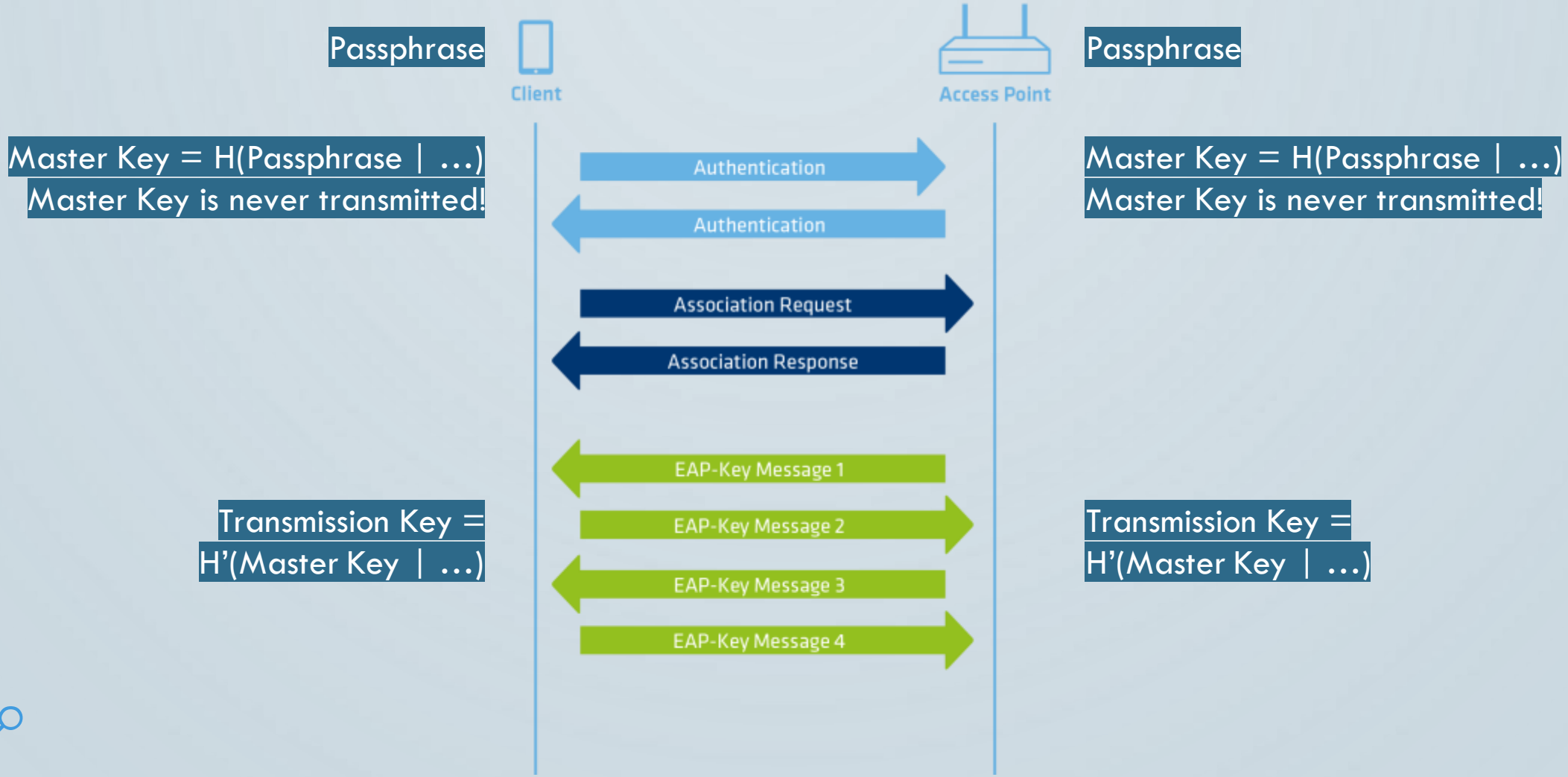
WPA3-PERSONAL: DH KEY EXCHANGE

Source: https://www.youtube.com/watch?v=M-0qt6tdHzk

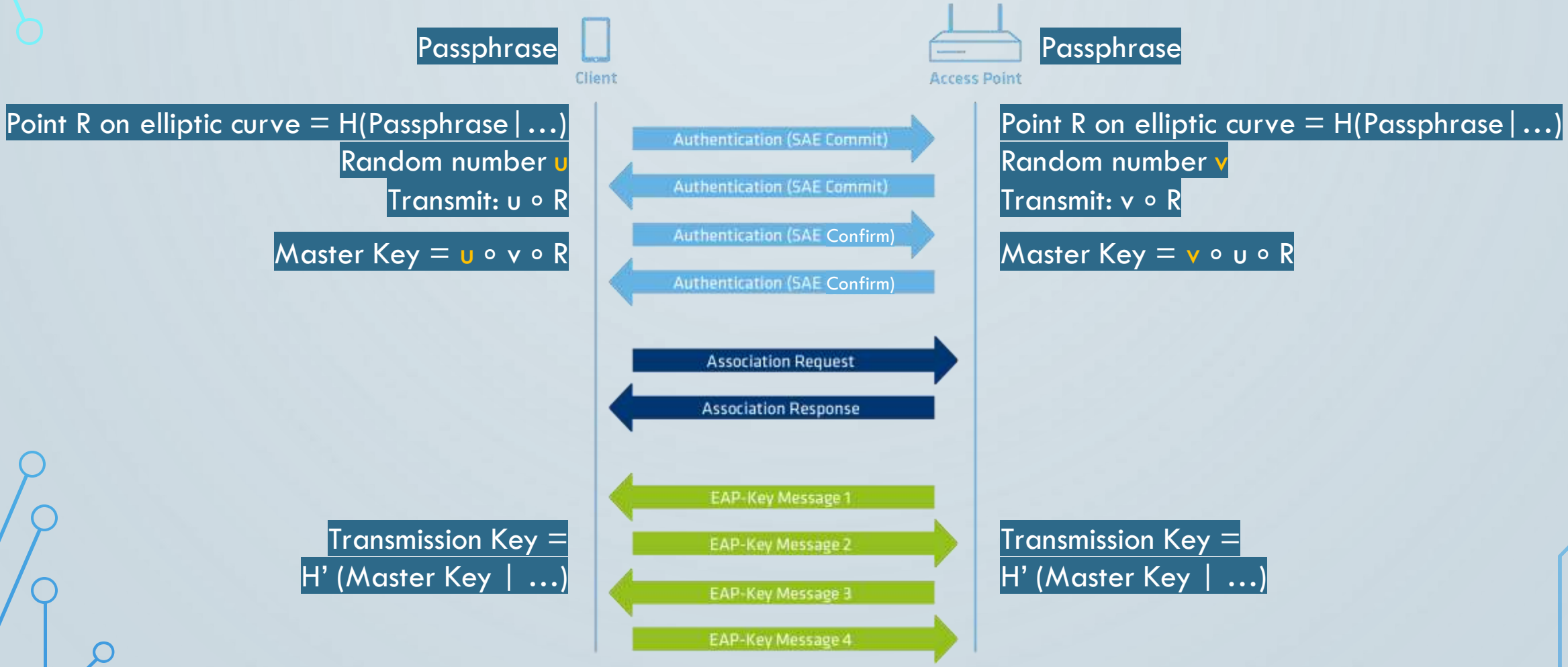
WPA3-PERSONAL

- Disallows WEP & TKIP protocols
- Requires the use of Protected Management Frames
- Replaces PSK with SAE (Simultaneous Authentication of Equals)
  - SAE is already used in IEEE 802.11s (Mesh)
  - Elliptic curve cryptography
  - Password is never shared during the key exchange protocol
    - Uses ‘Zero knowledge proof’
  - Resistant to dictionary attacks
    - Master key no longer based on Passphrase
    - Only one guess per network access attempt
- Transition Mode (WPA2-PSK + WPA3-SAE)

WPA2-PERSONAL CONNECTION PROCESS



WPA3 CONNECTION PROCESS



WPA3-ENTERPRISE

- Simple: WPA2-Enterprise + Protected Management Frames (PMF)
  - PMF is mandatory
- Real Improvement, but optional:
  - 192-bit mode for EAP-TLS (Suite B)
- Downside(s):
  - No real update to WPA2
  - 192-bit mode requires RADIUS and clients with EAP-TLS 192-bit support

WPA3-ENTERPRISE: 192-BIT MODE

- WPA2-Enterprise offers a lot of options, not all combinations are secure:
  - Diffie-Hellmann or RSA key exchange
  - RSA: 1k or 2k keys
  - Different TLS versions possible
- WPA3-Enterprise with 192-bit mode: 192-bit mode enforces EAP-TLS, 256 bit encryption and SHA384
  - RSA keys > 3K or elliptic curve P-384
  - TLS v1.2
  - Quantum resistant
- EAP server enforces policy via RADIUS attributes
- 4-Way Handshake uses SHA384 with 192-bit AKM

WI-FI CERTIFIED ENHANCED OPEN™ TECHNOLOGY OVERVIEW

ENHANCED OPEN: VISION

- WFA certification program designed to preserve the convenience of open networks, while reducing risks associated with accessing an unsecured network
- Provide unauthenticated individual data encryption to users
  - Protection against insider type attacks (ARP Spoofing) by isolating clients and filtering
- Network Service providers can:
  - Retain the user experience in open networks without requiring users to enter passwords
  - Provide data and management frame protection for the end user (PMF)
  - Maintain simplicity of deployment because there are no network credentials to maintain or share
  - Preserve interoperability with legacy open networks, including those using a captive portal

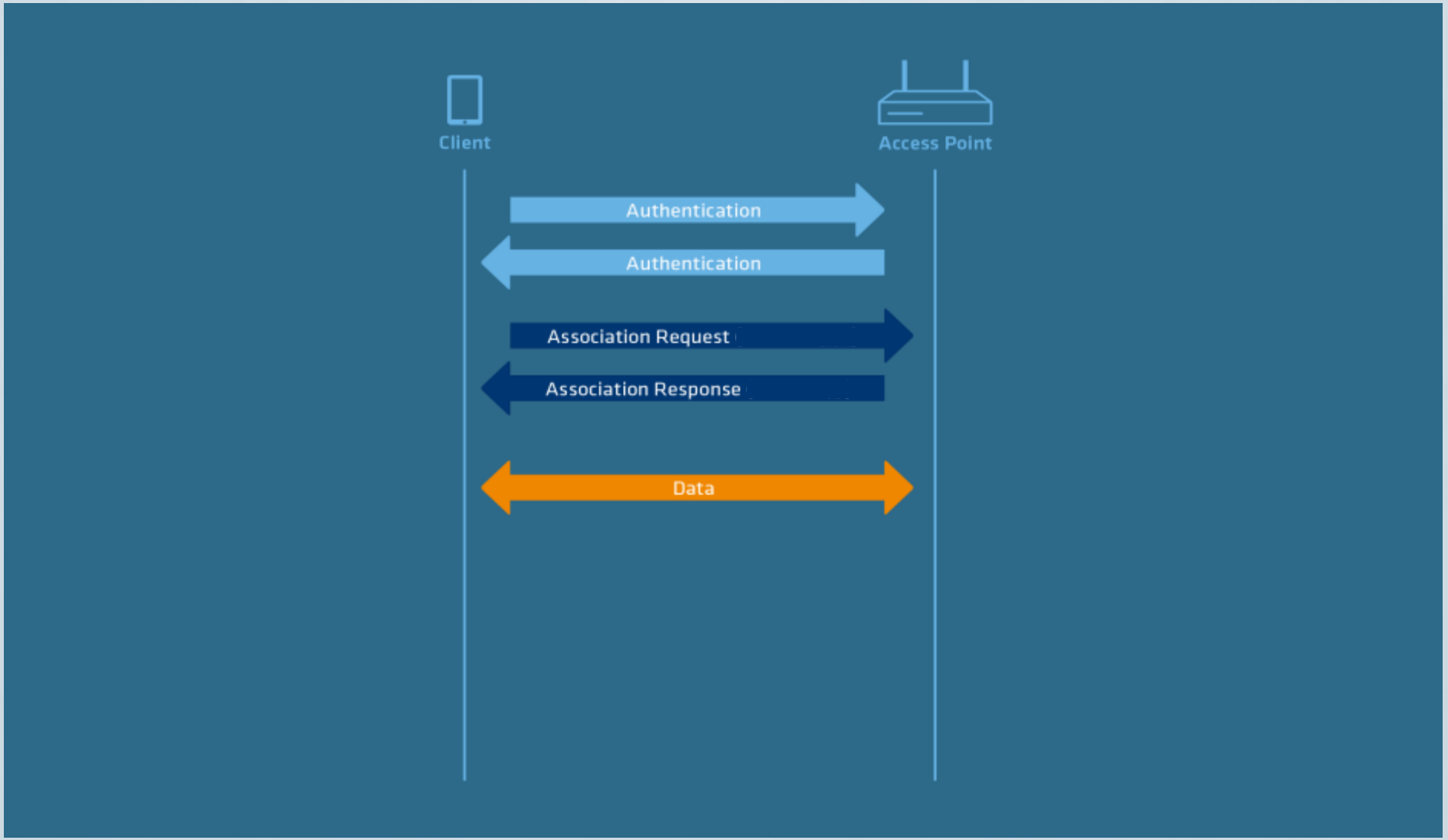
ENHANCED OPEN

- Open network – but encrypted
  - Like HTTPS: No user interaction necessary
  - Transition Mode (Open + Enhanced Open supported on same BSS)
- Mechanism: Opportunistic Wireless Encryption (OWE) – IETF RFC 8110
- Downsides:
  - No Authentication (MITM still works)
  - Second BSS for Transition Mode required
    - One new OWE BSS per open BSS
- WFA: separate and optional certification program (not part of WPA3)

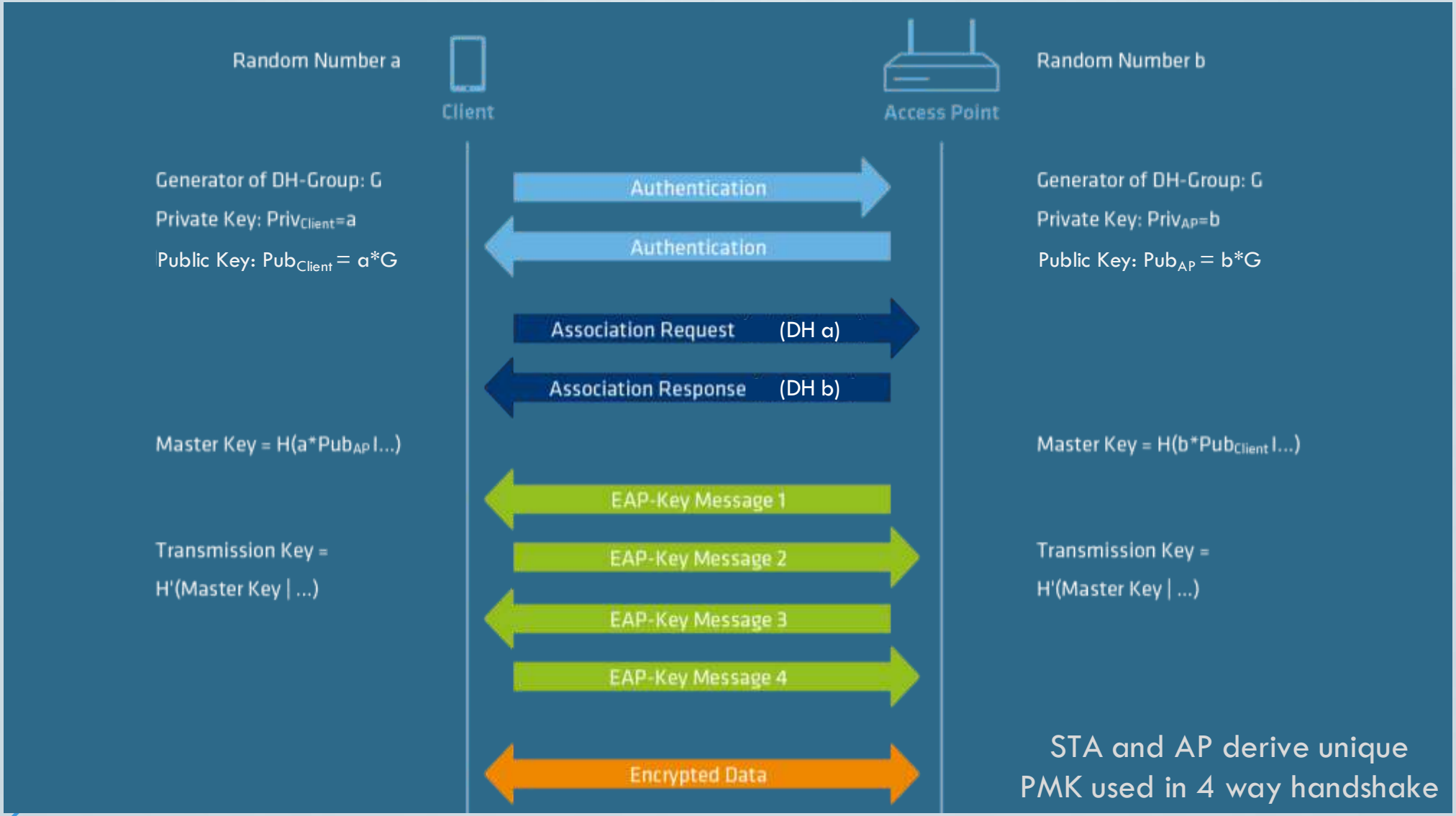
ENHANCED OPEN: TECHNICAL

- Performs unauthenticated Diffie-Hellman Key Exchange during association
- Only AES supported– no WEP, no TKIP
- Supports PMK-Caching
- RSN IE:
  - Group & Pairwise Cipher Suite: AES CCM (4)
  - Authentication Key Management: OWE (18)
  - PMF Required / Optional (Transition Mode)
- New IE (Tag no. 32): ECDH number
- Bridging, Multicast and Broadcasting between is allowed and vendor specific

OPEN NETWORK: TECHNICAL



ENHANCED OPEN: TECHNICAL



ENHANCED OPEN: TRANSITION MODE REQUIREMENTS

- A Wi-Fi Enhanced Open AP in Transition Mode uses two different, related SSIDs: one for Wi-Fi Enhanced Open and one for a traditional open network.
- The open basic service set (BSS) advertises an OWE Transition Mode element to communicate the basic service set identifier (BSSID) and SSID of the paired Wi-Fi Enhanced Open BSS.
- A Wi-Fi Enhanced Open client device suppresses the display of the Wi-Fi Enhanced Open BSS SSID on a Wi-Fi Enhanced Open AP by listing only the SSID for the open BSS.
- The Wi-Fi Enhanced Open client device seamlessly associates to the Wi-Fi Enhanced Open network, which is linked to the open network that the user selected.
- An AP operating in Wi-Fi Enhanced Open Transition Mode may bridge broadcast or multicast traffic between the open and Wi-Fi Enhanced Open networks to support network management goals, such as discovery of devices while in Wi-Fi Enhanced Open Transition Mode.
- An AP in Wi-Fi Enhanced Open Transition Mode uses the same operating policies, for example client isolation, for both the Wi-Fi Enhanced Open and open SSIDs.
- When Wi-Fi Enhanced Open penetration has reached a sufficient level amongst their user base, network managers should disable Wi-Fi Enhanced Open Transition Mode.

WI-FI ENHANCED OPEN: SUMMARY

- Wi-Fi Enhanced Open technology is based on Opportunistic Wireless Encryption (OWE), defined in the Internet Engineering Task Force (IETF) RFC8110
- OWE overlays an Elliptic-curve Diffie-Hellman (ECDH) key exchange on top of association to a Wi-Fi network
- OWE does not provide authentication, and does not guard against man-in-the-middle attacks that lure clients to connect to a rogue AP
- OWE does protect against passive eavesdropping, as well as unsophisticated packet injection such as deauthentication storm attacks or layer-2 injection of data into insecure HTTP sessions
- Network managers must remain vigilant in monitoring for rogue APs and active attackers that modify information being transmitted on a network
- Certain types of "insider" attacks, such as ARP spoofing, might be mitigated on Wi-Fi Enhanced Open networks by configuring the network to isolate clients

ENHANCED OPEN: USE CASES

Areas where it is not convenient or useful to require authentication

- Hotspots in coffee shops, bars, restaurants that want to offer encryption without the need of authentication (former WPA2-PSK)
- Guest network with captive portals in airports, stadiums, arenas

Wi-Fi CERTIFIED Easy Connect™ Technology Overview

EASY CONNECT

- Setting up Wi-Fi devices must be simple to the user
  - It's the first experience after a consumer opens the package for a new device
  - Adding headless devices to a network (e.g. IoT devices) must be easy
  - There is a need to enhance security while delivering a better user experience.
  - Replacement for WPS

- DPP at a glance:
  - Mobile devices are used to setup and manage Wi-Fi provisioning/connectivity
  - A newly enrolled device will connect and operate without further user interaction
  - Initial focus is on Infrastructure network connectivity – solution can be applied to technologies such as P2P and NAN in future.

WFA EASY CONNECT

- Simplifies process of adding Wi-Fi devices with limited or no display interface to Wi-Fi network
- Enables the utilization of device with more robust interface to easily provision and configure devices
- Use smartphone or tablet to scan product QR code (other) to add devices to a Wi-Fi network
- Provides standardized, consistent method for onboarding IoT devices
- Supports WPA2 and WPA3 networks

EASY CONNECT: OVERVIEW

Process (QR Code Example)

- The user utilizes the camera on the configurator device to scan the QR code displayed by the enrollee device.
  - Note that the QR code could be displayed using a sticker or card.
- After the configurator reads and decodes the QR code, it automatically discovers and sets up a secure Wi-Fi communication link with the device.
- The configurator uses the secure channel to configure the Wi-Fi network information on the enrollee device.
- Once configured, the enrollee device uses the Wi-Fi network information delivered by the configurator to discover, select, and connect to the Wi-Fi network without the need for human intervention.

DPP: ROLES

- Configurator
  - Main device in a Wi-Fi Easy Connect network is designated as a configurator. It is the central point of configuration for all devices on the network, including the initial network AP.
  - Configurator can be on any trusted device within the Wi-Fi network.
    - Mobile device: Likely the most common model, a device such as a smartphone or tablet may be the configurator, initiating the Wi-Fi Easy Connect protocol through an application on the device.
    - AP accessed through a web interface - the user logs into the Wi-Fi Easy Connect AP administration screen and runs the configurator, initiating the protocol to provision a new enrollee.
    - AP accessed through an application, instead of APs web interface to initiate the protocol.
- Enrollee
  - Devices that administrator wants to connect to the network, includes APs, smart appliances, computers, printers, TVs, …. Essentially any Wi-Fi device can be an enrollee.

EASY CONNECT: ESTABLISHING THE NETWORK

- Access point Configuration
  - ***Configurator*** runs the Wi-Fi Alliance Device Provisioning Protocol to provision an initial enrollee -AP.
  - During the initial enrollment process, the network administrator uses a mobile device as the 'configurator' to configure the AP, the enrollee. This configuration establishes the Wi-Fi Easy Connect network.

EASY CONNECT TECHNICAL: BOOTSTRAPPING

Every Wi-Fi Easy Connect device ships with an identity. These identities are contained in a QR code or human-readable string (PKEX), either printed or digitally available, in the form of public and private keys.

Optional information may include MAC and channel to connect on

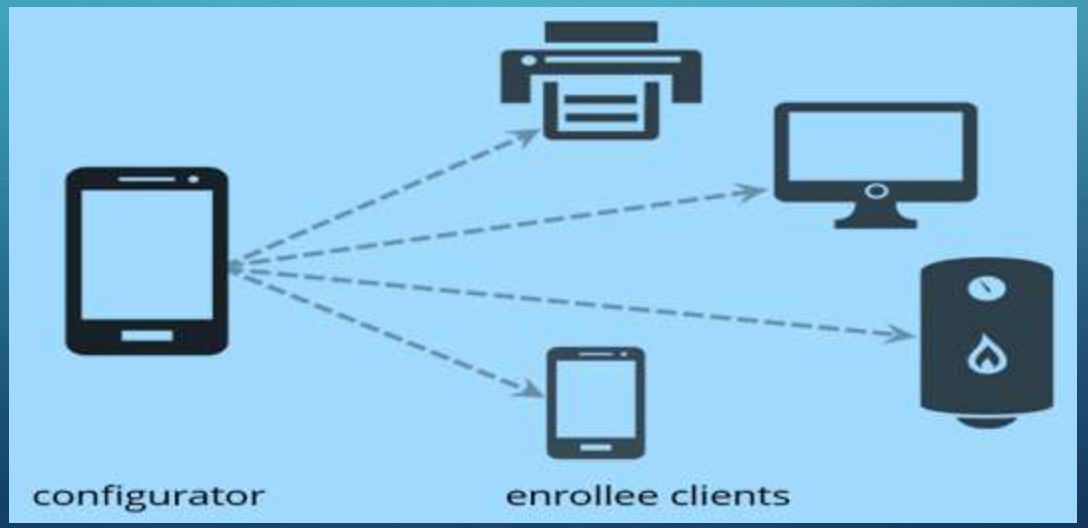
During this process the configurator and enrollee establish a trust relationship that allows them to authenticate and establish a secure connection..

For example, this QR code includes a public key as well as operating channels of 1 and 36. :

DPP:C:81/1,115/36;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;;

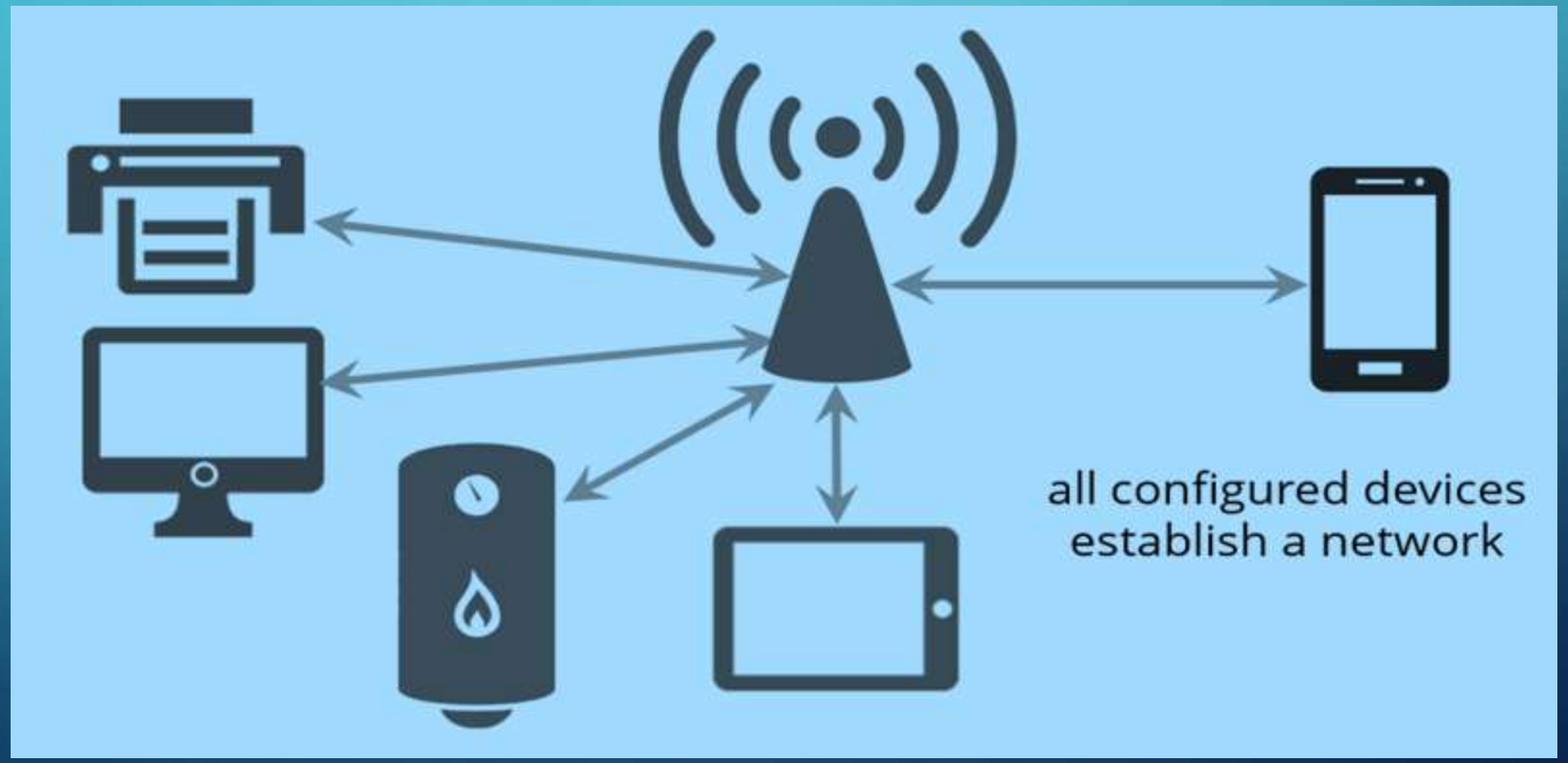
EASY CONNECT: ENROLLING DEVICES

- Provisioning Client Devices
  - With Wi-Fi Easy Connect network established, administrator can begin enrolling devices. Each candidate device (enrollee), obtains its own configuration, enabling it to join the target Wi-Fi Easy Connect network.
  - Configuration process produces security credentials unique to that network and device resulting in a mutually trusted connection to the Wi-Fi network.



EASY CONNECT: CONNECTING TO THE NETWORK

- Device Association - Once a Wi-Fi device has been enrolled, it uses its configuration to discover and connect to the network through a Wi-Fi Easy Connect AP.



EASY CONNECT: PUBLIC KEY-BASED IDENTITIES

- Devices have an identity out-of-the box
  - Wi-Fi Easy Connect uses public key cryptography for authentication between Configurator and a new device (Enrollee)
  - All devices have their own key pair
  - Every device has a unique identity based on the public key that can be authenticated using the public/private key pair
  - Public keys are shared with everyone; Private keys are kept secret
  - Messages encrypted using a public key can only be decrypted with the associated private key
  - Wi-Fi Easy Connect does not rely on certificates for authentication; trust is established via the bootstrapping mechanisms

EASY CONNECT: USE CASE

- Adding Devices to an existing DPP network
  - User buys a large number of DPP enabled bulbs and wants to replace his old bulbs.
  - He scans the QR code on the DPP enabled bulbs with his Smartphone/PC and then screws in the bulbs.
  - When the bulb is turned on, the bulb connects to the Smartphone/PC, is provisioned by the smart phone, and then connects to the user 's home network
  - User can use the bulb's application to control the bulb.

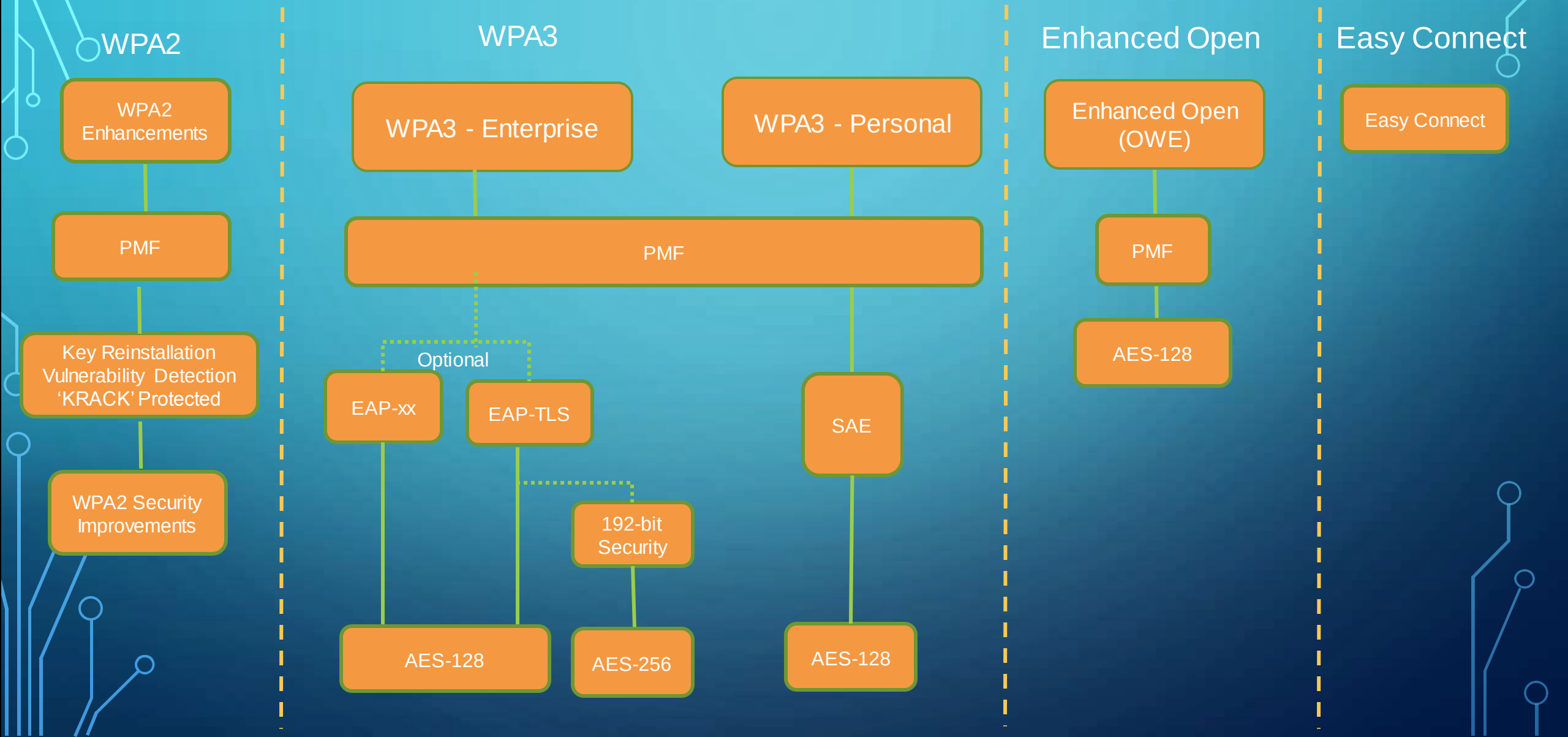
EASY CONNECT: USE CASE

- The user registers at a hotel and enters their room. The TV is on and displays a QR-code and network access instructions.
- User scans the QR code with his smartphone and the phone establishes a secure link with the TV and the TV, acting as the Configurator, provisions the phone.
- The Smartphone then successfully connects to the hotel AP.
- The Smartphone credentials are configured to expire when the user checks out.

Phone uses application to scan QR Code gain Network Access

The QR code displayed on the TV changes on check-out

WFA SECURITY PROGRAMS



DEMO – WPA3 AND ENHANCED OPEN

FUTURE OUTLOOK FOR SECURITY IMPROVEMENTS

- What do you expect for further security topics?
  - Fast Roaming with WPA3/Enhanced Open
  - “Private PSK” for WPA3-Personal
  - TLS v1.3
  - OCSP
  - EAP-PWD
  - Enhanced Open Transitional Mode on single SSID

SUMMARY

- Encryption everywhere, with no additional complexity
- No more active/passive/dictionary attacks
- Mandatory: Protected Management Frames
- Quantum-resistant WPA3-Enterprise 192-bit mode