Communication Systems
Wi-Fi (IEEE 802.11 WLAN) Part 4

WS 2025/2026@THI

Max Riegel
<max.riegel@ieee.org>

WS 2025/2026 Wi-Fi Lecture Topics

Part 1 (2025-11-25):

- Introduction
- Wi-Fi Architecture
- Wi-Fi Specifications
- Wi-Fi Spectrum
- Wireless Channel
- Wi-Fi PHY Evolution

Part 2 (2025-11-28):

- Wi-Fi PHY Layer
- Wi-Fi PHY Q&A

Part 3 (2025-12-02):

- Wi-Fi Medium Access
- Wi-Fi MAC Management
- Wi-Fi QoS
- Wi-Fi MAC Layer Q&A

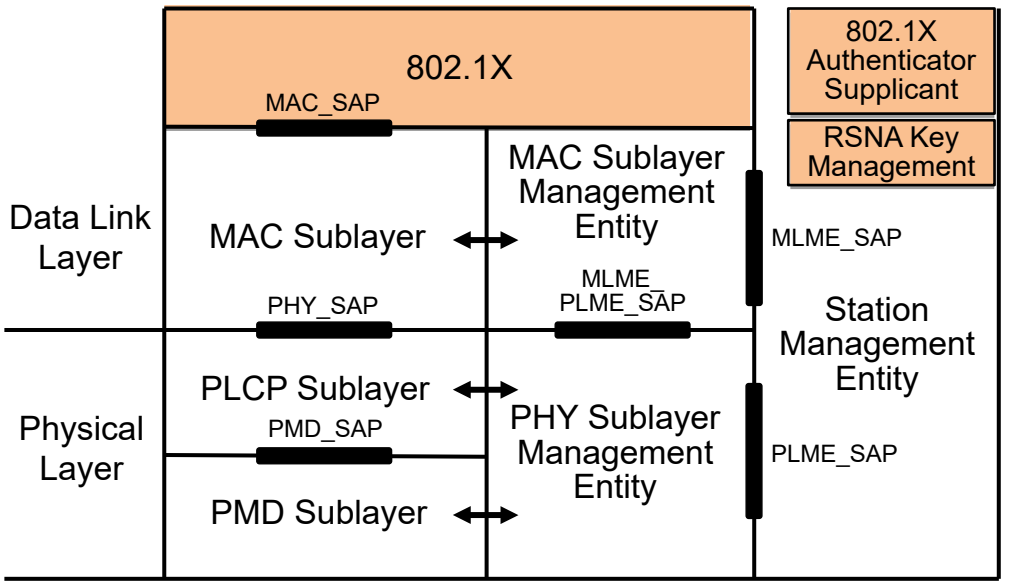
Part 4 (2025-12-05):

- Wi-Fi Security
- Wi-Fi Security Q&A

WI-FI SECURITY

IEEE802.11 Protocol architecture

- 802.1X
  - Port Access Entity
  - Authenticator/Supplicant
- RSNA Key Management
  - Generation of Pair-wise and Group Keys
- Station Management Entity (SME)
  - interacts with both MAC and PHY Management
- MAC Sublayer Management Entity (MLME)
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- MAC Sublayer
  - basic access mechanism
  - fragmentation
  - encryption
- PHY Sublayer Management Entity (PLME)
  - channel tuning
  - PHY configuration and monitoring
- Physical Sublayer Convergence Protocol (PLCP)
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- Physical Medium Dependent Sublayer (PMD)
  - modulation and encoding

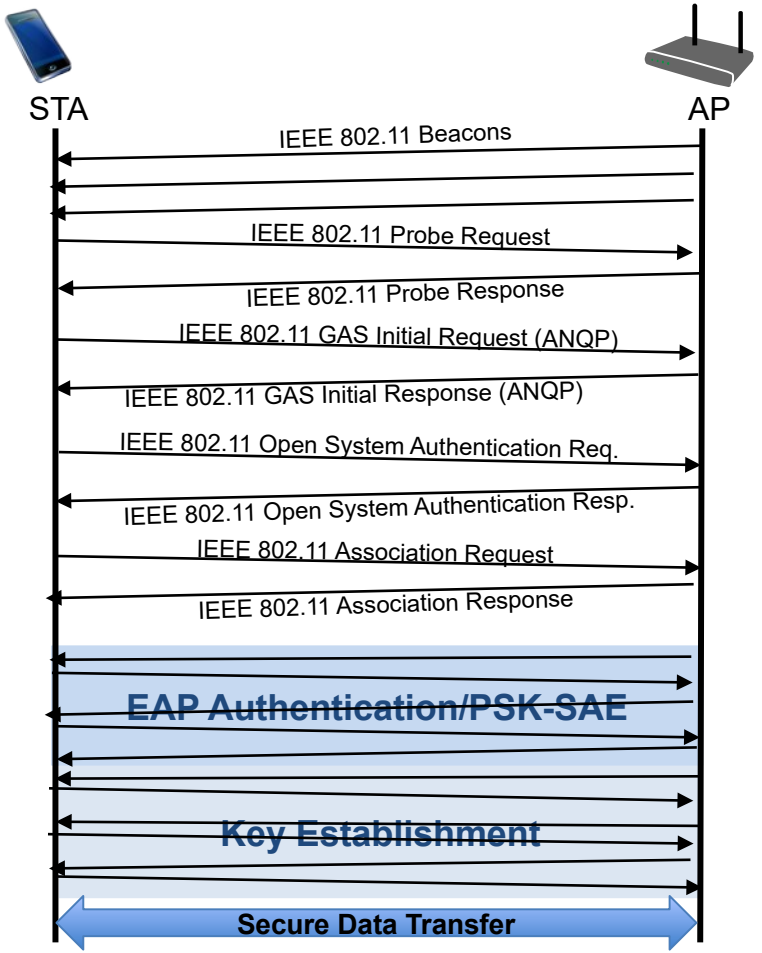


©Max Riegel, 2025

History of Wi-Fi/IEEE 802.11 security

- Initial goal was to provide “Wired Equivalent Privacy” (WEP)
  - Usable worldwide as there was strict export regulation at that time for any ‘strong’ security with more than 40bits keys
  - IEEE 802.11-1997 provided shared key authentication based on WEP privacy mechanism
    - RC4 algorithm with 40 bit secret key
  - WEP was completely insufficient
    - WEP unsecure by design, no user authentication, no mutual authentication, missing key management protocol
- IEEE 802.11i-2004 fixed weak security by “Robust Security Network”
  - 1. Transitional solution w/ TKIP for fixing bugs in existing hardware – now depreciated
    - Formerly known through WFA term WPA (TKIP)
  - 2. Conclusive solution w/ CCMP (AES) for new hardware
    - Meanwhile mainly known through WFA terms WPA2 (CCMP), WPA3 (CCMP, GCMP)
- WPA2 supported by all Wi-Fi hardware since about 2005
  - Updated in 2018 by WPA3 for increased security and operational reliability

Wi-Fi Security Establishment



- Scanning
  - Beacon
  - Probe Request/Response
- Network Selection
  - GAS (ANQP Request/Response)
- Authentication
  - Open System Authentication
- Association
  - Association Request/Response
- **Authentication/Authorization**
  - Either: IEEE 802.1X EAPoL for enterprise networks
    - Starts with controlled port blocked and uncontrolled port used for exchange of authentication messages
    - EAP protocol carries authentication method
  - Or: Pre-Shared Keys for small and residential networks
    - SAE to generate fresh pairwise master keys for each session
  - Authorization comprises configuration of data path and master key delivery to AP
- **Key establishment**
  - Four-way handshake for establishment of pair-wise transient keys and groups keys for broad-/multicasts
- **Secure data transfer**
  - Secure data transfer over controlled port commence once encryption keys are established

©Max Riegel, 2025

Robust Security Network Components

- Configuration
- PSK-SAE / IEEE 802.1X authentication
- Pre-shared keys / Key distribution by RADIUS
- Key management
- Data protection through CCMP
  - CTR/CBC-MAC Protocol (Counter mode/Cipher Block Chaining Message Authentication Code of AES)
  - Achieves both confidentiality and integrity

=> Establishes Robust Security Network Associations (RSNAs)

RSNA variations

WPA2/3-Personal	WPA2/3-Enterprise
RSN Capability identification from Beacon or Probe Response frames	
Open System authentication.	
Cipher suite negotiation during the association process	
Case of STA and AP supporting	
PSK/SAE	IEEE 802.1X authentication
Derive Pairwise Master Key from Pre-Shared Key	EAP authentication derive Pairwise Master Key
Establish temporal keys by executing 4-way key management algorithm for pairwise keys and group key management for broadcast keys	
Protect the data link by operation of ciphering and message authentication with keys generated above.	
If Protected Management Frame (PMF) is enabled, the temporal keys and pairwise cipher suite is used for protection of individually addressed robust management frames	

Wi-Fi Security

CONFIGURATION

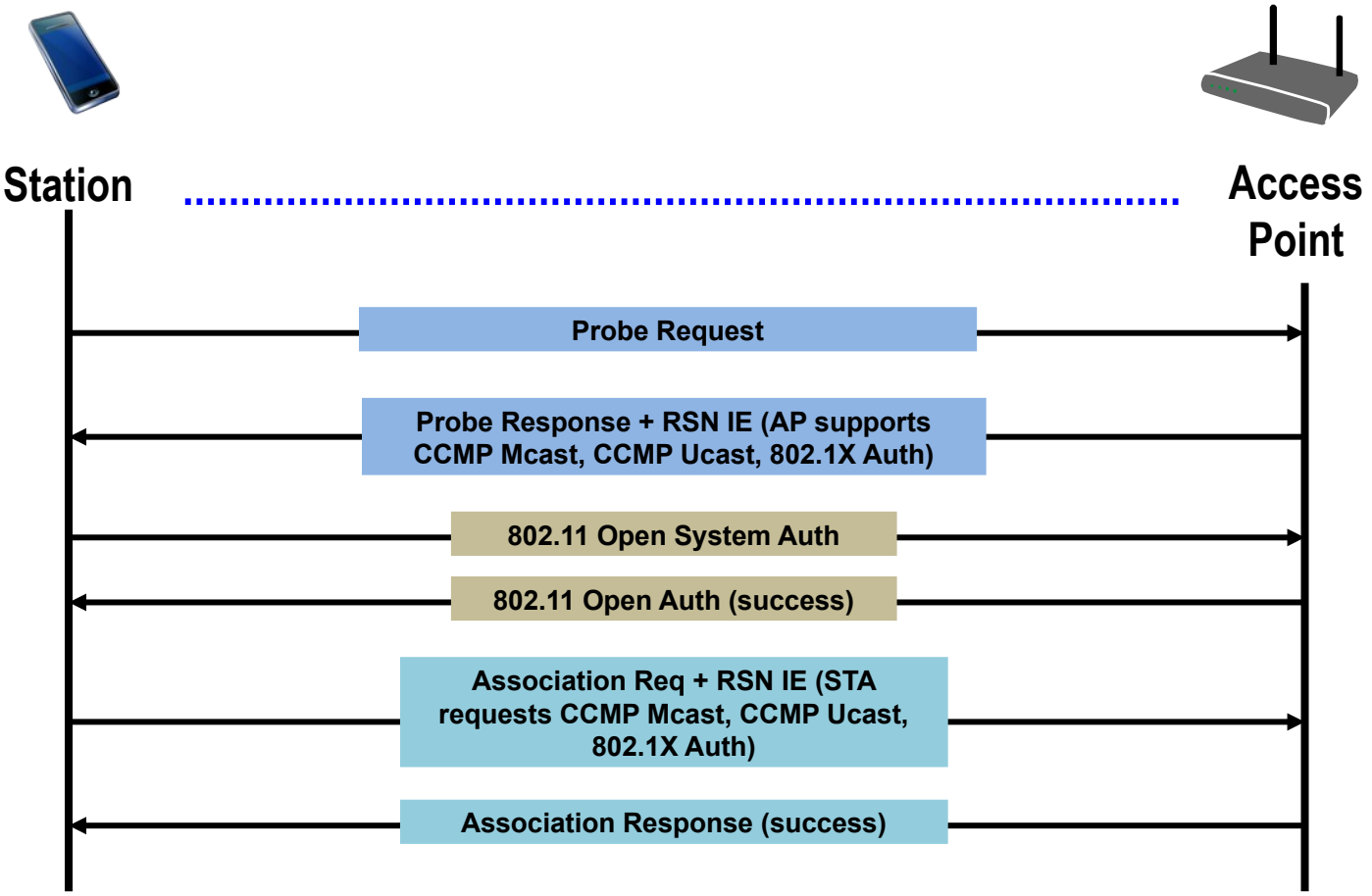
©Max Riegel, 2025

Configuration

- AP advertises capabilities in Beacon, Probe Response
  - SSID in Beacon, Probe provides hint for right authentication credentials
  - RSN Information Element advertises all enabled authentication suites, all enabled unicast cipher suites and multicast cipher suites
  - At the end of network discovery STA knows:
    - SSID of the network
    - Authentication and cipher suites of the network
    - The preferred choice of authentication and cipher suites
- STA selects authentication suite and unicast cipher suite in Association Request. When AP confirms authentication and cipher suite through Association Response:
  - STA and AP have an established link for exchanging user data
  - STA and AP authenticate each other through PSK-SAE or EAPoL

©Max Riegel, 2025

Configuration process



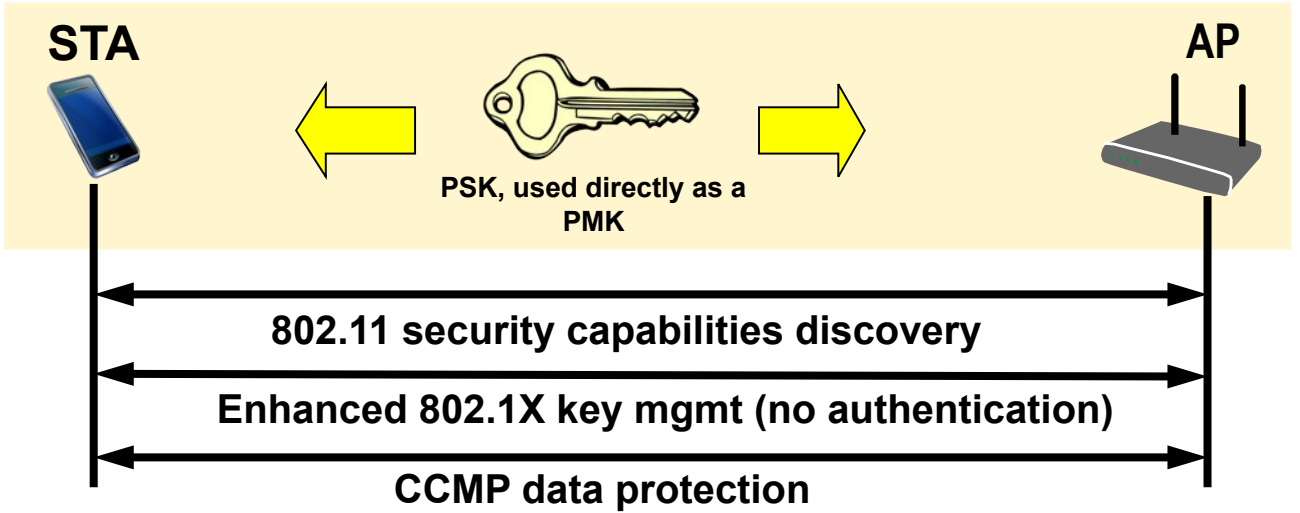
©Max Riegel, 2025

Wi-Fi Security

PSK/SAE AUTHENTICATION (WPA2/3-PERSONAL)

©Max Riegel, 2025

Legacy PSK Authentication (WPA2-Personal)

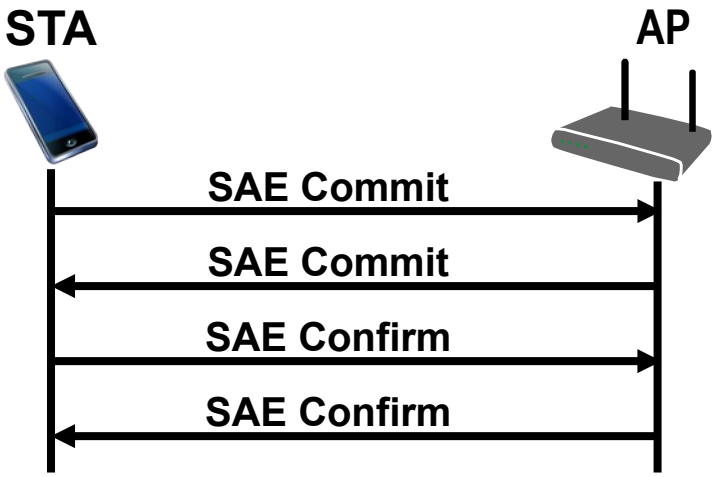


- Reason to provide PSK-Mode:
  - Home users might configure passwords, but will never configure keys
- Password-to-Key Mapping
  - Uses PKCS #5 v2.0 PBKDF2 (RFC2898; Public Key Cryptography Specification #5 v2.0, Password Based Key Derivation Function #2), to generate a 256-bit PSK from an ASCII password
  - Quality of PSK security depends on quality of ASCII password!

WPA3-Personal deploys SAE for key generation

- Replacement of legacy PSK password-to-key mapping through Simultaneous Authentication of Equals (SAE)
  - SAE has been made available in IEEE 802.11 through IEEE 802.11s amendment for authentication and encryption among mesh partners.
  - Resistant to offline dictionary attacks to determine the network password
    - Requires repeated active attacks for each guess of the password
  - Provides forward secrecy
    - Property of secure communication protocols in which compromise of long-term keys does not compromise past session keys.
  - Retains the ease-of-use and system maintenance associated with WPA2-Personal
- WPA3-Personal Transition Mode allows for gradual migration while maintaining interoperability with WPA2-Personal devices

Simultaneous Authentication of Equals (SAE)



- SAE is based on a Dragonfly handshake as defined in RFC 7664
  - Mutually authenticates two peers using only a password.
  - Creates a shared secret between the two peers that is stronger than the passwords.
- The SAE handshake negotiates a fresh Pairwise Master Key (PMK) per client
  - PMK used in a traditional Wi-Fi four-way handshake to generate session keys.
- Neither the PMK nor the password credential used in the SAE exchange can be obtained by a passive attack, active attack, or offline dictionary attack.

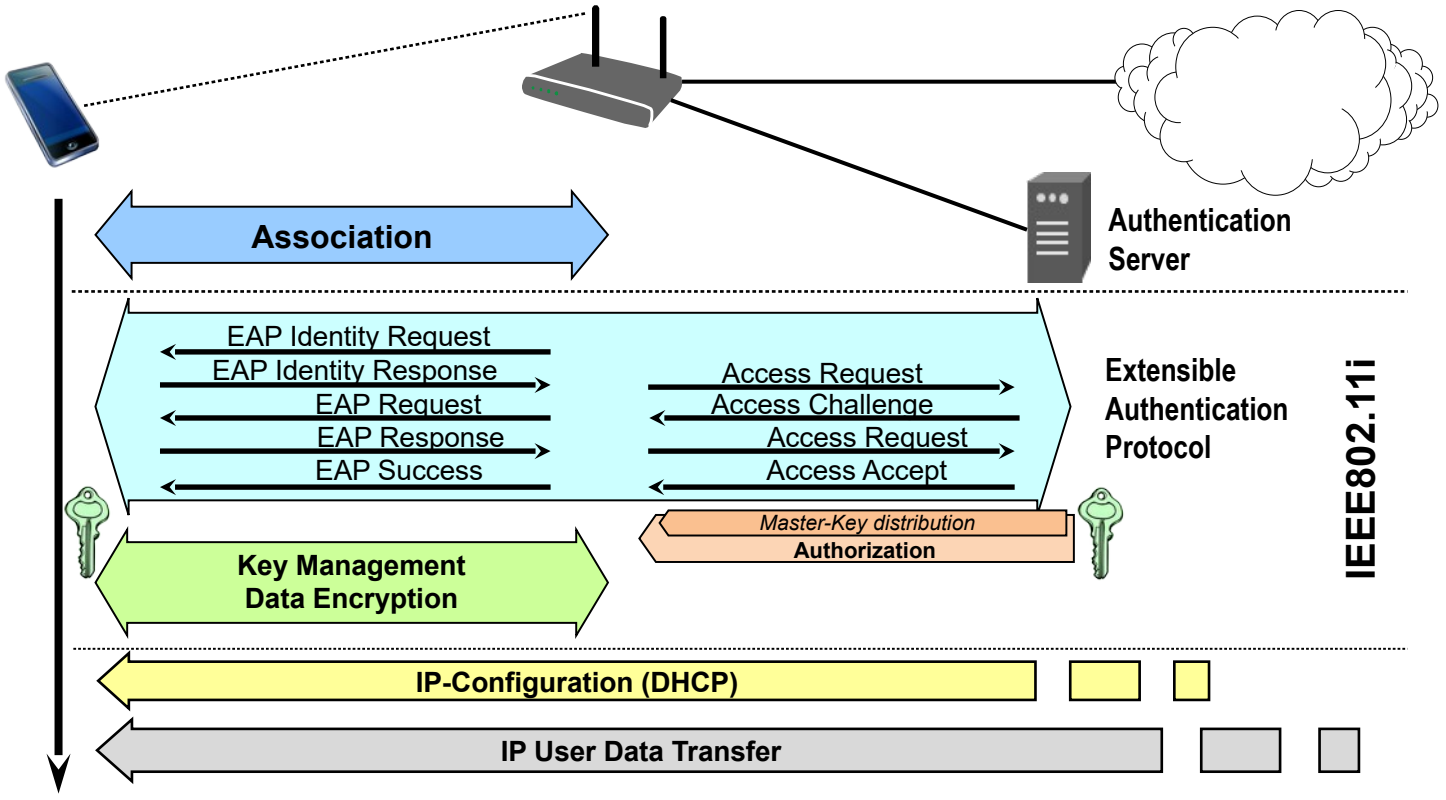
Wi-Fi Security

IEEE 802.1X AUTHENTICATION (WPA2/3-ENTERPRISE)

©Max Riegel, 2025

WPA 2/3-Enterprise Wi-Fi access control

IEEE 802.1X access authentication was introduced as part of RSN

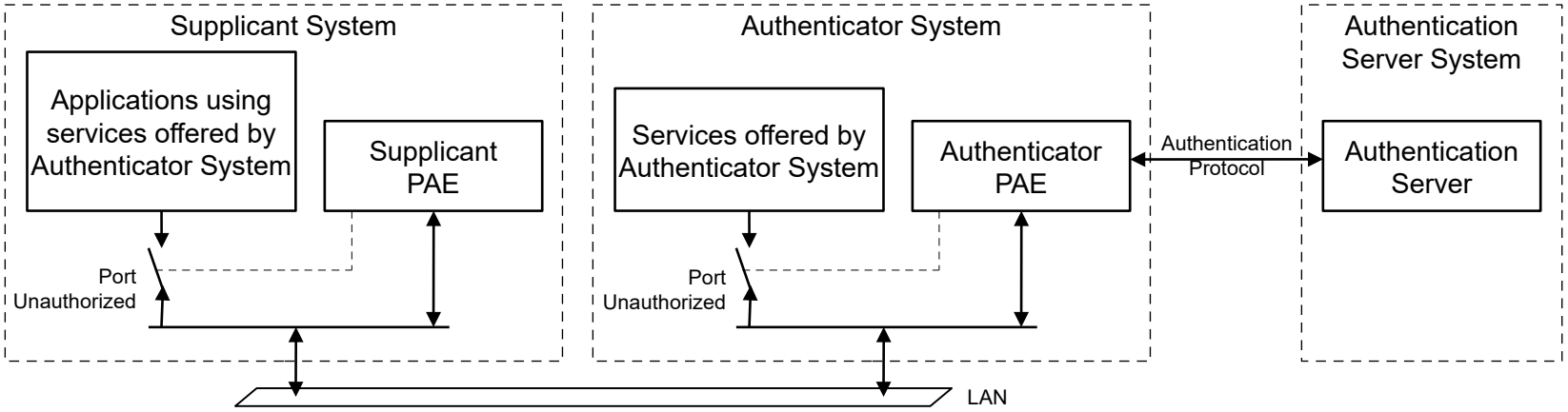


IEEE 802.1X (EAP over LAN) authentication

- Purpose: Establishment of a mutually authenticated session key between Authentication Server (AS) and STA
  - At the begin of session => key is fresh
  - Mutually authenticated => bound only to AS and STA
- The applied EAP authentication method has to provide protection against eavesdropping, man-in-the-middle attacks, forgeries, replay, dictionary attacks against either party.
- At the end of authentication:
  - The AS and STA have established a session bound to a mutually authenticated Master Key
  - Master Key has to be generated and provided by EAP method
    - Authentication Server forwards PMK to the AP
- Identity protection (privacy) not provided
  - MAC addresses are not hidden
  - However, identities can protected by random MAC addresses and tunneled EAP methods

IEEE 802.1X aka EAPoL (EAP over LAN) architecture

- Inherits EAP architecture (RFC 3748, RFC 5247)
  - “Authenticator” located in AP, “Supplicant” located in STA
  - Transport for EAP messages over IEEE 802 LANs

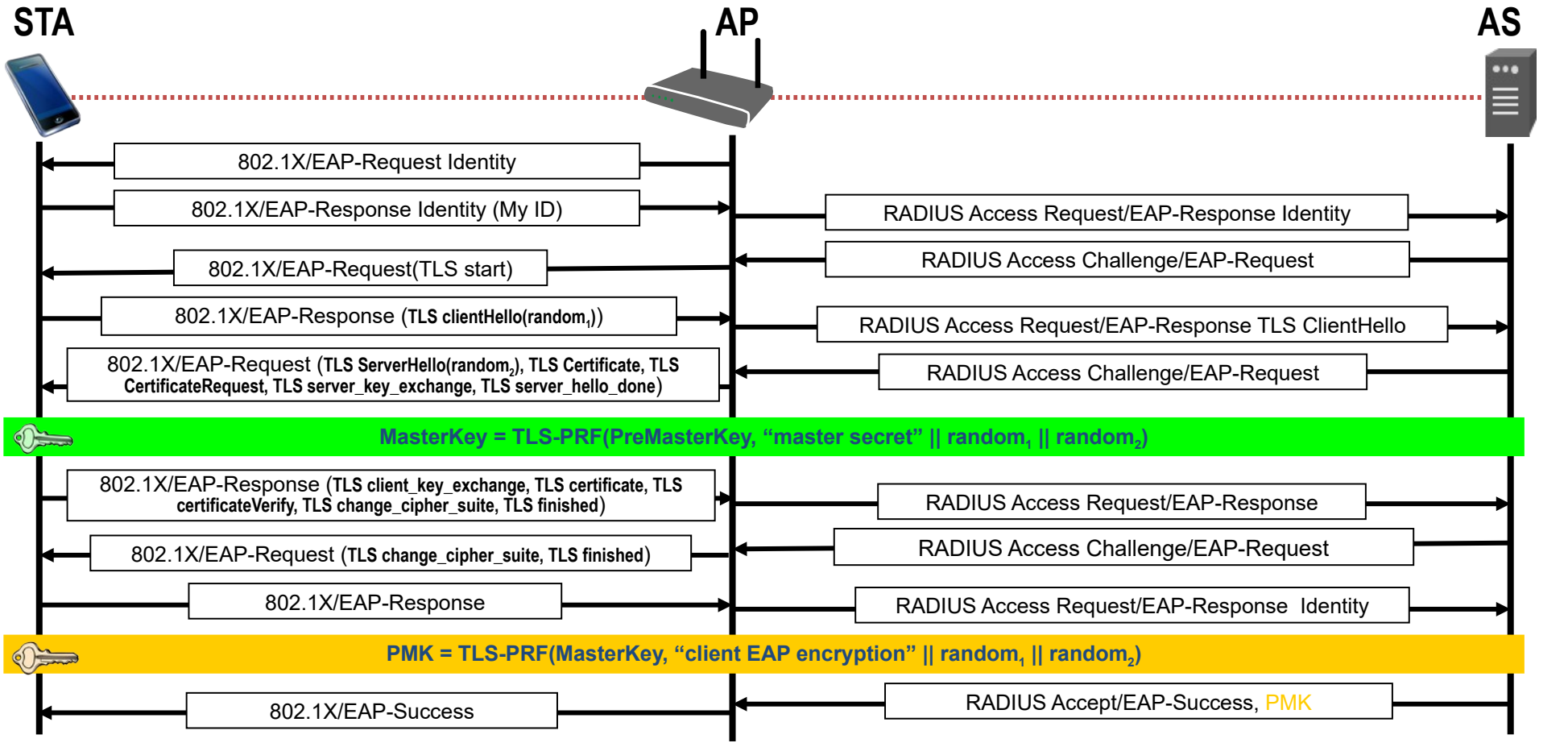


- Port Authentication Entity (PAE) with uncontrolled and controlled port.
- IEEE 802.1X/EAP provides no cryptographic protections
  - No defense against forged EAP-Success. It relies on EAP method to detect all attacks
  - “Mutual” authentication and binding must be inherited from EAP method

EAP Menthods, e.g. EAP-TLS

- EAP-TLS = TLS Handshake over EAP
  - EAP-TLS defined by RFC 5216, TLS initially defined by RFC 2246
  - Provides the capability to verify the identity of the peer and to generate a Master Key (MK) that can be used for encryption.
  - Requires deployment of public key infrastructure
    - Mutual authentication in EAP-TLS requires X.509 certificates for both, STA and Authentication Server
  - First standardized EAP method, that could be used for RSN
- No particular EAP method mandated by RSN
  - Any method with the ability to derive a Master Key from authentication can be used.
  - WFA certification covers an extended set of appropriate EAP methods, e.g EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA

IEEE 802.1X authentication with EAP-TLS



Wi-Fi Security

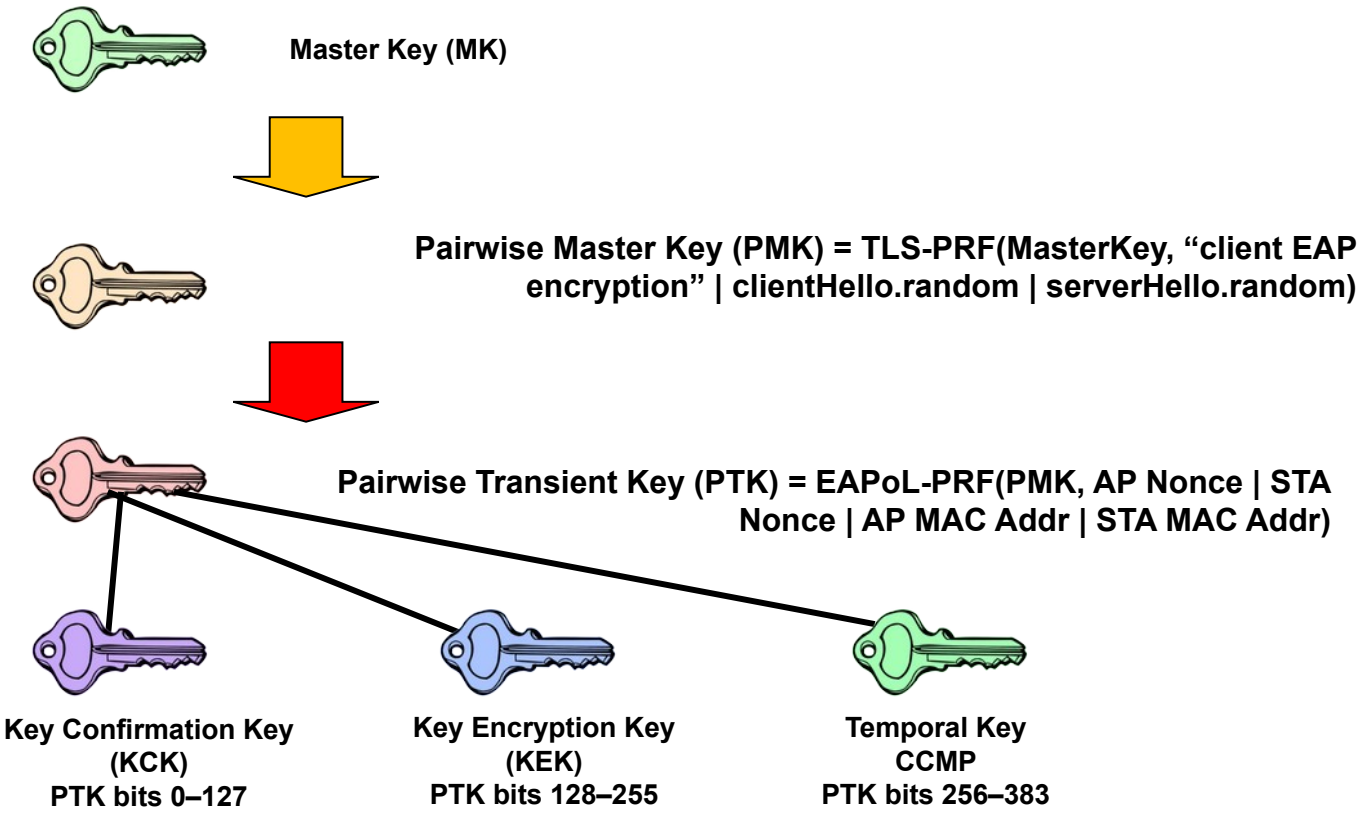
KEY MANAGEMENT

©Max Riegel, 2025

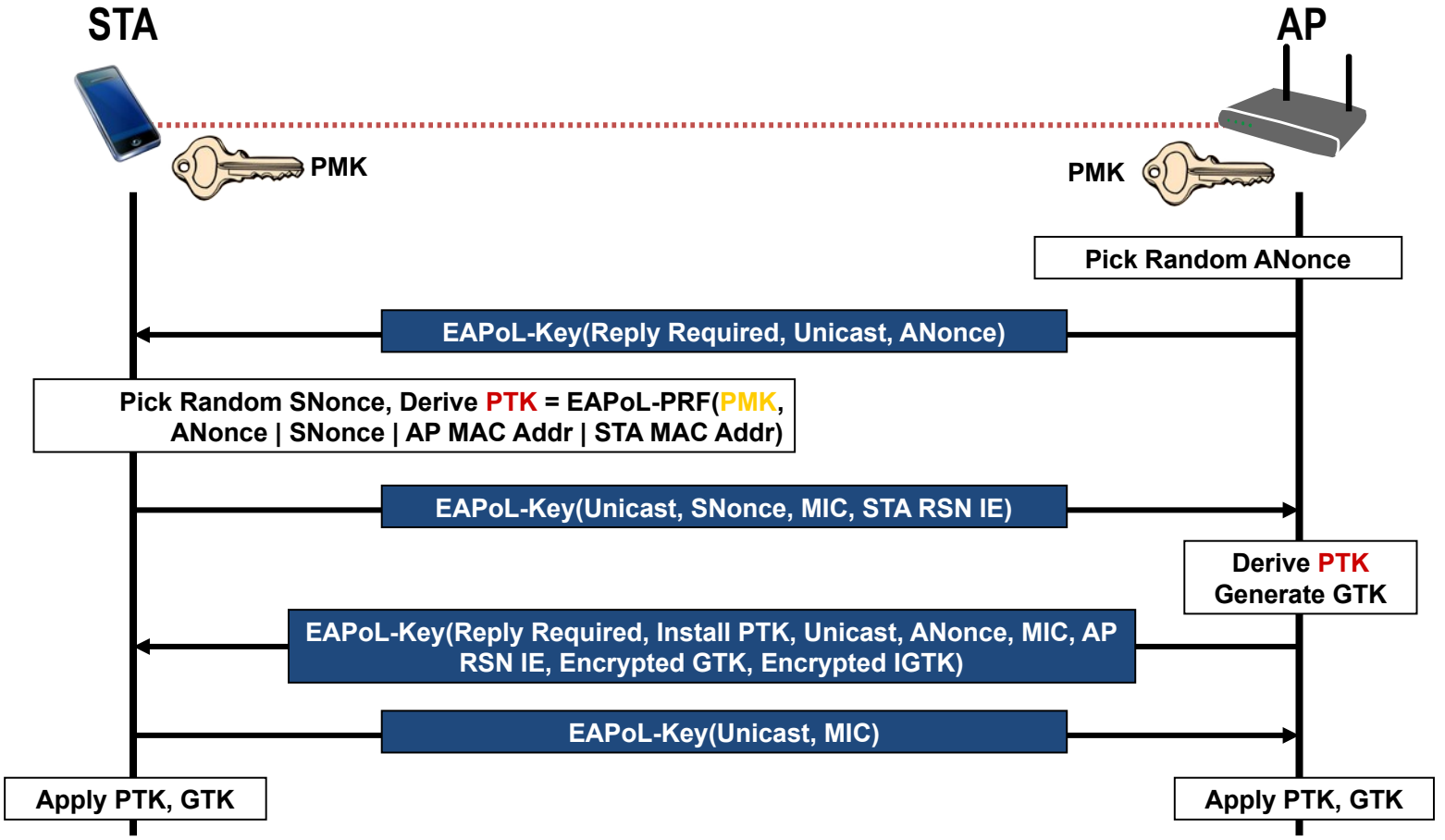
Key Management

- Redesigned through IEEE 802.11i to fix original 802.1X key management
  - Based on availability of a Pairwise Master Key (PMK)
  - AP and STA use PMK to derive Pairwise Transient Key (PTK)
  - PTK used to protect the data link
- Limitations:
  - No explicit binding to preceding association, authentication
  - Keys are only as good as back-end allows
- 4-Way Handshake
  - Establishes a fresh pairwise key bound to STA and AP for this session
  - Proves liveliness of peers
  - Demonstrates there is no man-in-the-middle between PTK holders if there was no man-in-the-middle holding the PMK
  - Synchronizes pairwise key use
  - Piggybacked Group Key provisioning to STA

Pairwise Key Hierarchy

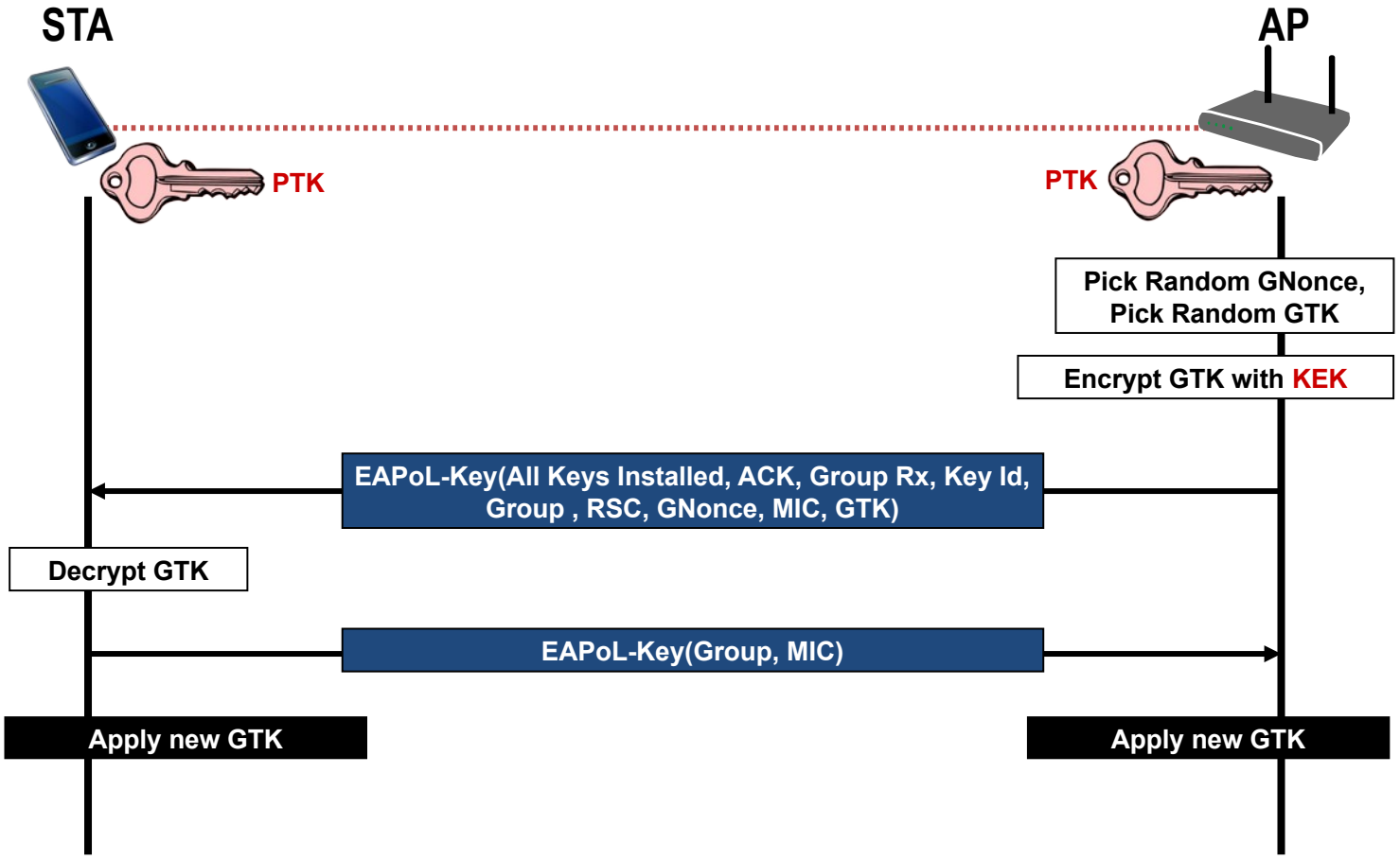


4-Way Handshake to establish Temporal Keys



©Max Riegel, 2025

Optional Group Key handshake to refresh GTK



©Max Riegel, 2025

Wi-Fi Security

DATA PROTECTION

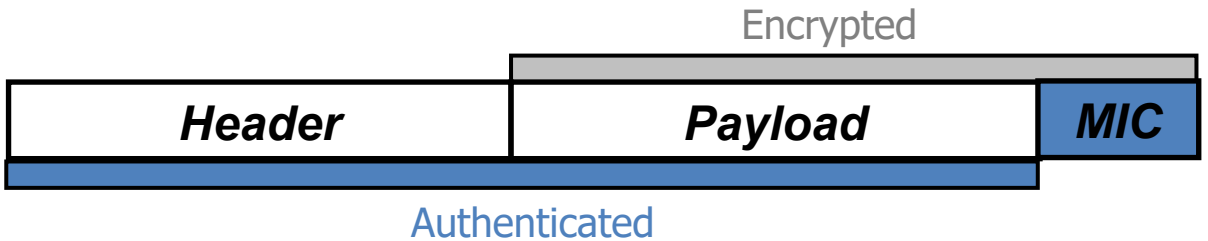
©Max Riegel, 2025

General data protection requirements

- Never send or receive unprotected packets
- Authenticate message origin
  - Forgeries prevention
- Sequence packets
  - Replay detection
- Avoid re-keying
  - 48 bit packet sequence number
- Protect source and destination addresses
- Use strong cryptography
  - For both, confidentiality and integrity

CCMP (CTR with CBC-MAC Protocol)

- CounTeR mode with Cipher-Block Chaining Message Authentication Code (CCM) is specified in IETF RFC 3610
  - Especially designed for IEEE 802.11i
  - Encrypt packet data payload
  - Protect packet selected header fields from modification



- CBC-MAC used to compute a MIC on the plaintext header, length of the plaintext header, and the payload
- CTR mode used to encrypt the payload and the MIC using 128bit-AES
- Same 128-bit temporal key for encryption and message authentication at both AP and STA
  - Generated and established through 4-way handshake

Stronger cryptography through WPA3-Enterprise

- Introduces an enhanced 192-bit security mode
- Replaces 128-bit CCMP through 256-bit GCMP (Galois/Counter Mode Protocol)
  - GCMP was introduced to IEEE 802.11 through IEEE 802.11ad (WigGig)
  - 256-bit GCMP was used instead of 192-bit GCMP because of broader adoption in industry
- In addition:
  - More secure key derivation and key confirmation through 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
  - More secure key establishment and authentication through Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
  - Used security algorithms are known as ‘Suite B’
- Mandatory support of Protected Management Frames required
- No need for transition mode, but considerations given for interoperability between WPA2-Enterprise and WPA3-Enterprise

Wi-Fi Security

WPA3 OPERATIONAL ENHANCEMENTS

©Max Riegel, 2025

WPA3 Operational Enhancements

- EAP Server Certificate Validation (SCV)
  - Mandatory for Wi-Fi CERTIFIED WPA3-Enterprise
- SAE Hash-to-Element (amendment to SAE avoiding hunting-and-peeking algorithm)
  - Mandatory for Wi-Fi CERTIFIED WPA3
- Transition Disable
  - Mandatory for Wi-Fi CERTIFIED WPA3
- SAE Public Key (SAE-PK)
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Wi-Fi QR code
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Beacon Protection
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Operating Channel Validation
  - Optional feature for Wi-Fi CERTIFIED WPA3
- Privacy Extension Mechanisms
  - Optional feature for Wi-Fi CERTIFIED WPA3

Some optional WPA3 enhancements briefly explained...

- SAE Public Key (SAE-PK)
  - 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
  - Extension to SAE protocol, but password is especially generated,
    - embeds base32 fingerprint of public key
    - Example password: a2bc-de3f-ghi4
  - During SAE authentication, AP signs the SAE transcript, and STA checks the signature using the trusted fingerprint decoded from the password
    - Authentication fails if public key or signature not validated by STA

- Wi-Fi QR code
  - Formalized “WIFI” URI definition according https://www.iana.org/assignments/uri-schemes/prov/wifi
  - Easy way for a STA (with a camera) to connect to a new network
  - Backward-compatible with current de-facto standard WIFI URI format
  - Adds support for WPA3 features, including Transition Disable, SAE-PK, and non-ASCII passwords (percent-encoded)

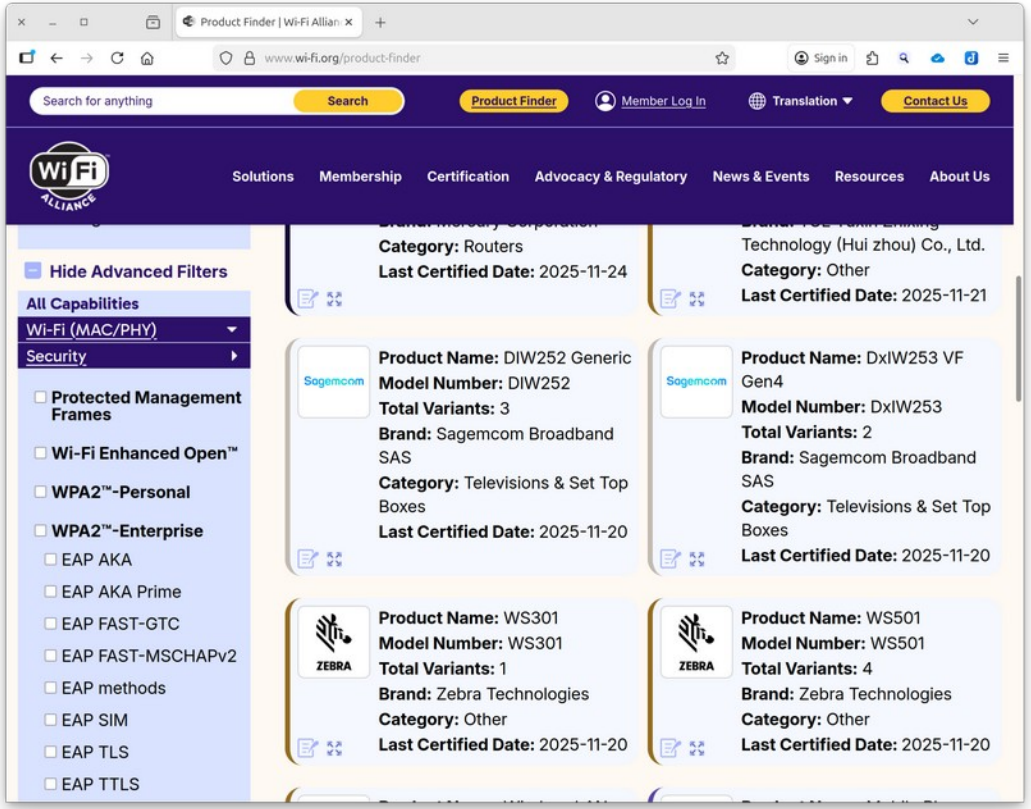
Wi-Fi Security

SUMMARY

Steps of Wi-Fi security establishment

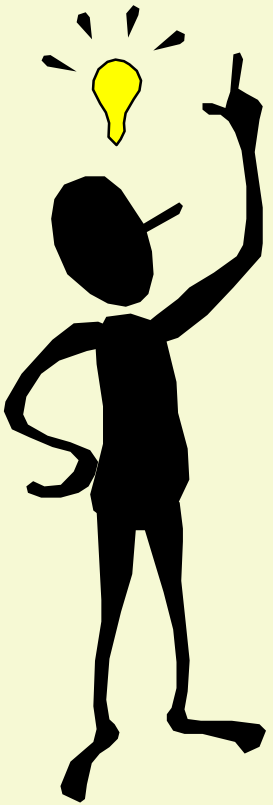
- **Security negotiation**
  - Determine promising parties with whom to communicate
  - AP advertises network security capabilities to STAs
- **Authentication based on IEEE 802.1X**
  - Centralize network admission policy decisions at the Authentication Server
  - Mutually authenticate STA and Authentication Server representing AP
  - Generate Master Key as a side effect of authentication
  - Use master key to generate session keys = authorization token for access by STA
- **RADIUS-based key distribution**
  - Authentication Server moves (not copies) session key (PMK) to STA's AP
- **Key management by 4-way handshake**
  - Bind PMK to STA and AP and confirm both AP and STA possess PMK
  - Generate fresh operational keys (PTK) and communicate group keys (GTK, IGTK)
  - Prove each peer is live and synchronize PTK and GTK, IGTK use
- **Data Protection**
  - Encrypt data by CTR (AES)
  - Authenticate data by CBC-MAC (AES) {or GMAC (AES) for WPA3-Enterprise}

WPA3 product support



- https://www.wi-fi.org/product-finder provides more details about the supported security features of certified products.

Questions and answers



Security questions…

1) What does RSN mean?
2) What is the function of IEEE 802.1X?
3) What kind of authentication is supported by RSN?
4) Which name is used by Wi-Fi Alliance to denote the certification of latest IEEE 802.11 security?
5) Which method does WPA3-Personal use for authentication and key generation?
6) What is the difference between WPA3-Enterprise and WPA3-Personal authentication?
7) Which authentication protocols are used in the Robust Security Network?
8) What is the outcome of the configuration phase in the Robust Security Network?
9) What are the peer entities of the EAP protocol in IEEE 802.11?
10) How is the master key transferred from the AAA server to the AP?
11) What is the mandatory data encryption protocol of RSN?

More security questions…

12) Where is the supplicant located used in WPA3-Enterprise?
13) What is the function of the PAE in IEEE 802.1X?
14) What kind of credentials are used in EAP-TLS to identify the peers?
15) Why was the SAE method introduced in WPA3?
16) Which key is used as input to start the 4-way handshake in RSN?
17) What is the purpose of the group key in IEEE 802.11?
18) Which default key length is used in RSN for AES?
19) Why is it important that CCMP protects but does not encrypt the header part of a WLAN frame?

THE END

Questions and remarks