Advanced Mobile Networks
Wi-Fi (IEEE 802.11 WLAN) Part 4

WS 2024/2025 Lecture

Max Riegel
(max.riegel@ieee.org)

WS 2024/2025 Wi-Fi Lecture topics overview

Part 0:

- Introduction and overview

Part 1:

- Wi-Fi Deployments
- Wi-Fi Network architecture
- Wi-Fi Stds & Certification
- Wi-Fi Spectrum
- Wireless Channel

Part 2:

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

+ PHY Exercises

Part 3:

- Wi-Fi MAC Layer
- Wi-Fi QoS
- Wi-Fi MAC Q&A

+ MAC Exercises

Part 4:

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

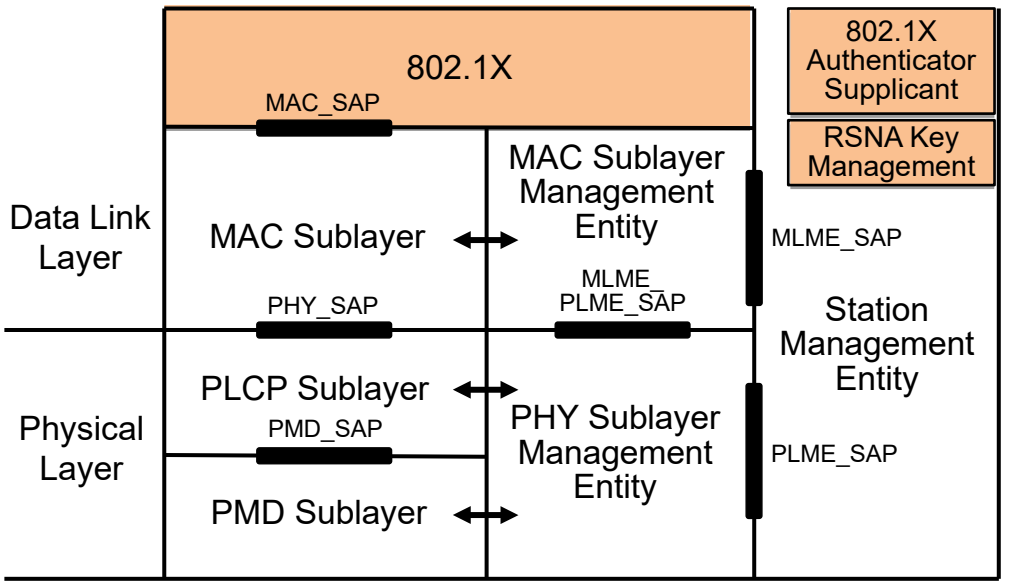
AMN – Wi-Fi Lecture dates and content (tentative)

Thu, Nov. 28	Part 0	Thu, Jan 16th	Part 3
Tue, Dec. 10th	Part 1	Tue, Jan 21st	||
Thu, Dec 12th	||	Thu, Jan 23rd	||
Thu, Dec 19th	Part 2	Thu, Jan 30th	Part 4
Tue, Jan 7th	||	Tue, Feb 4th	||(partial)
Thu, Jan 9th	||	Thu, Feb 6th	????

WI-FI SECURITY

IEEE802.11 Protocol architecture

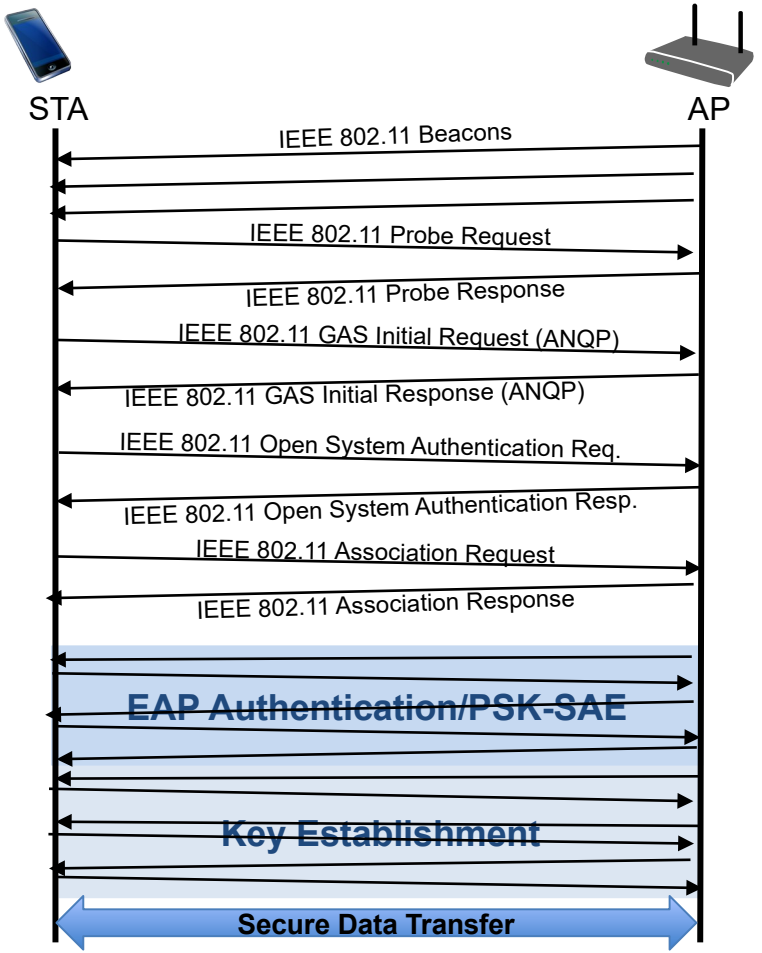
- 802.1X
  - Port Access Entity
  - Authenticator/Supplicant
- RSNA Key Management
  - Generation of Pair-wise and Group Keys
- Station Management Entity (SME)
  - interacts with both MAC and PHY Management
- MAC Sublayer Management Entity (MLME)
  - synchronization
  - power management
  - scanning
  - 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



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 through 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

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	IEEE Std 802.1X-2004 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	

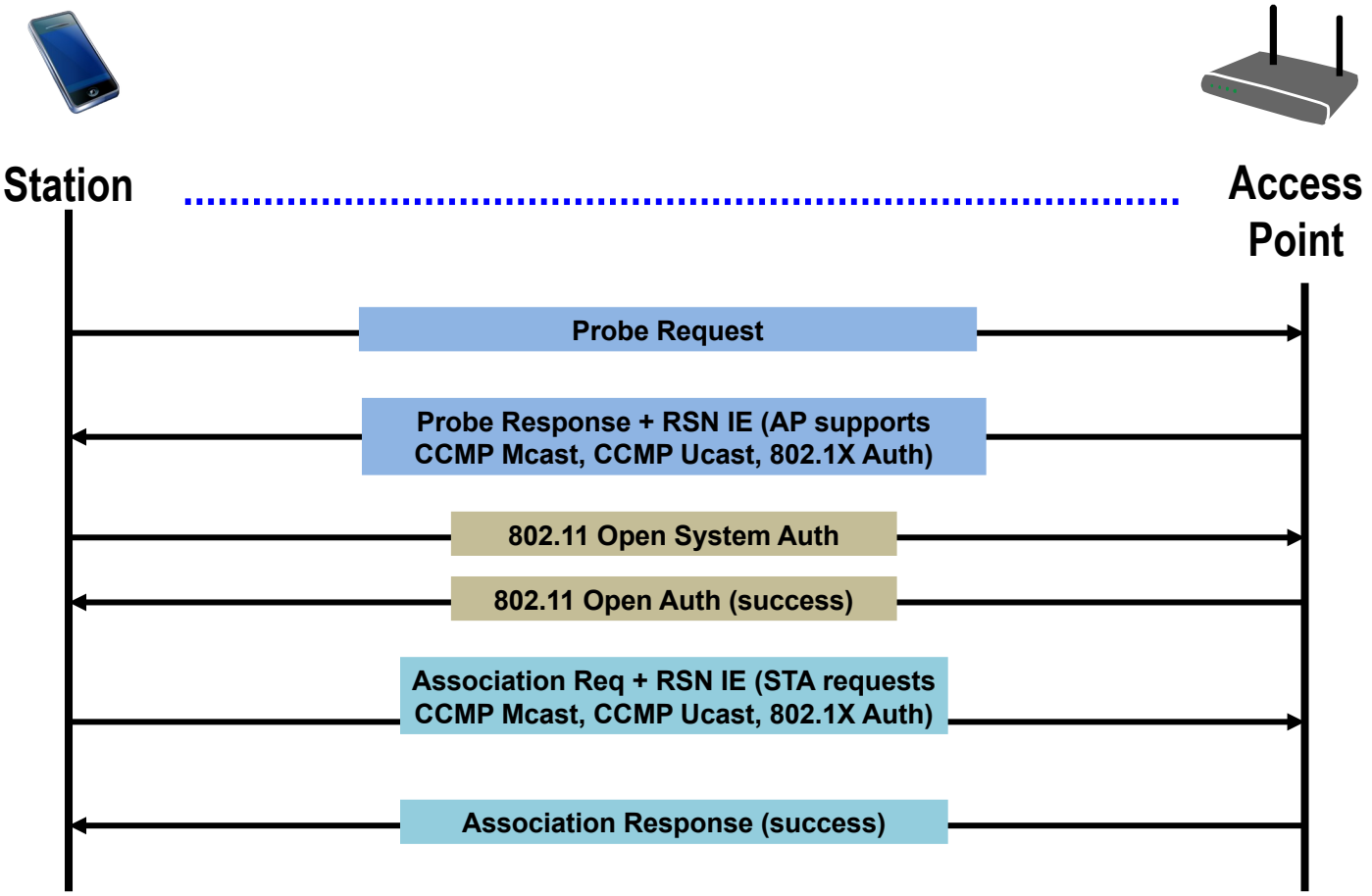
Wi-Fi Security

CONFIGURATION

Configuration

- Security requires networks with “right” characteristics
- 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 IEEE 802.1X EAPoL

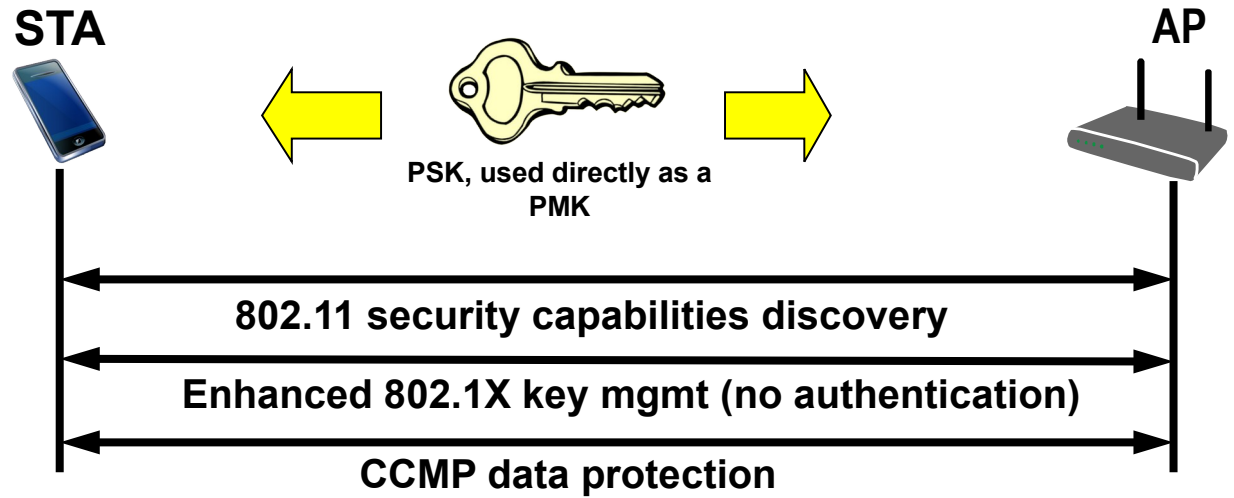
Configuration process



Wi-Fi Security

PSK/SAE AUTHENTICATION (WPA2/3-PERSONAL)

Legacy PSK Authentication (WPA2-Personal)

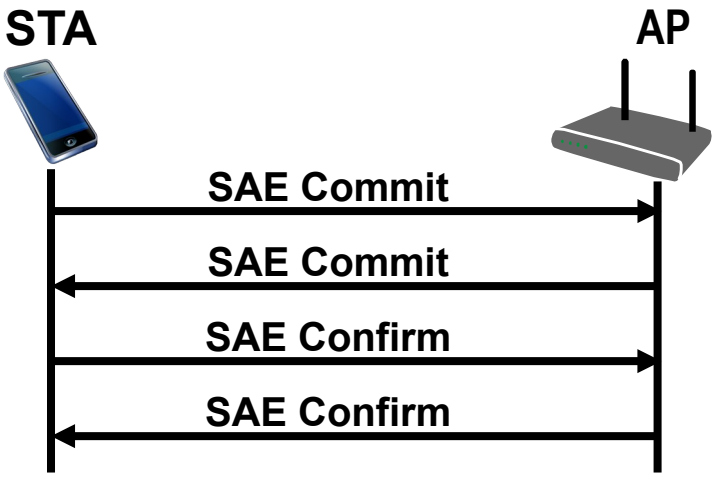


- Reason to provide PSK-Mode:
  - Home users might configure passwords, but will never configure keys
- Password-to-Key Mapping
  - Uses PKCS #5 v2.0 PBKDF2 (RFC2898; Public Key Cryptography Specification #5 v2.0, Password Based Key Derivation Function #2), to generate a 256-bit PSK from an ASCII password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



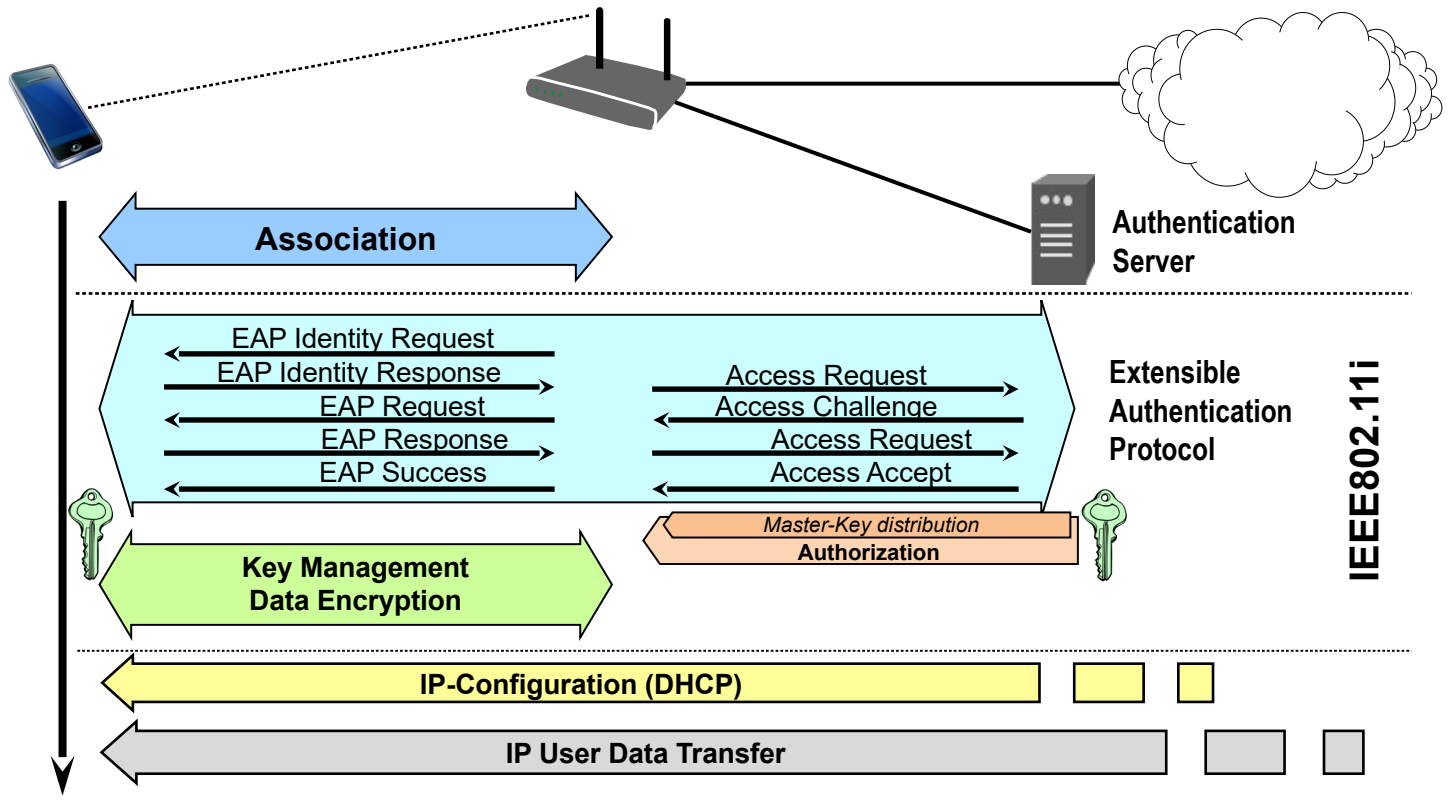
- SAE is based on a Dragonfly handshake as defined in RFC 7664
  - Mutually authenticates two peers using only a password.
  - Creates a shared secret between the two peers that is stronger than the passwords.
- The SAE handshake negotiates a fresh Pairwise Master Key (PMK) per client
  - PMK used in 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)

WPA 2/3-Enterprise Wi-Fi access control

IEEE 802.1X access authentication was introduced as part of RSN

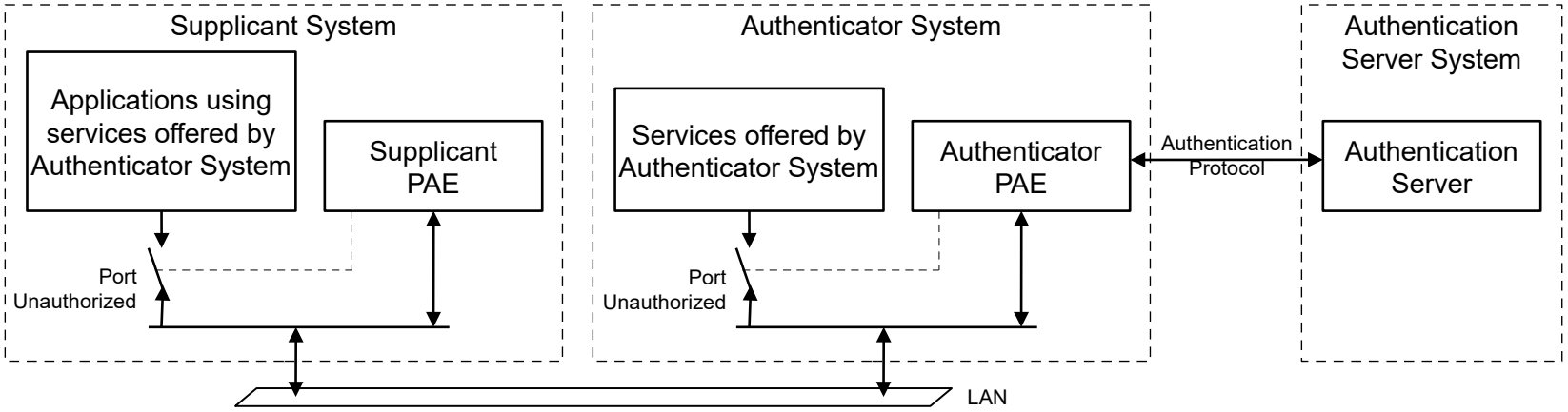


IEEE 802.1X (EAP over LAN) authentication

- 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

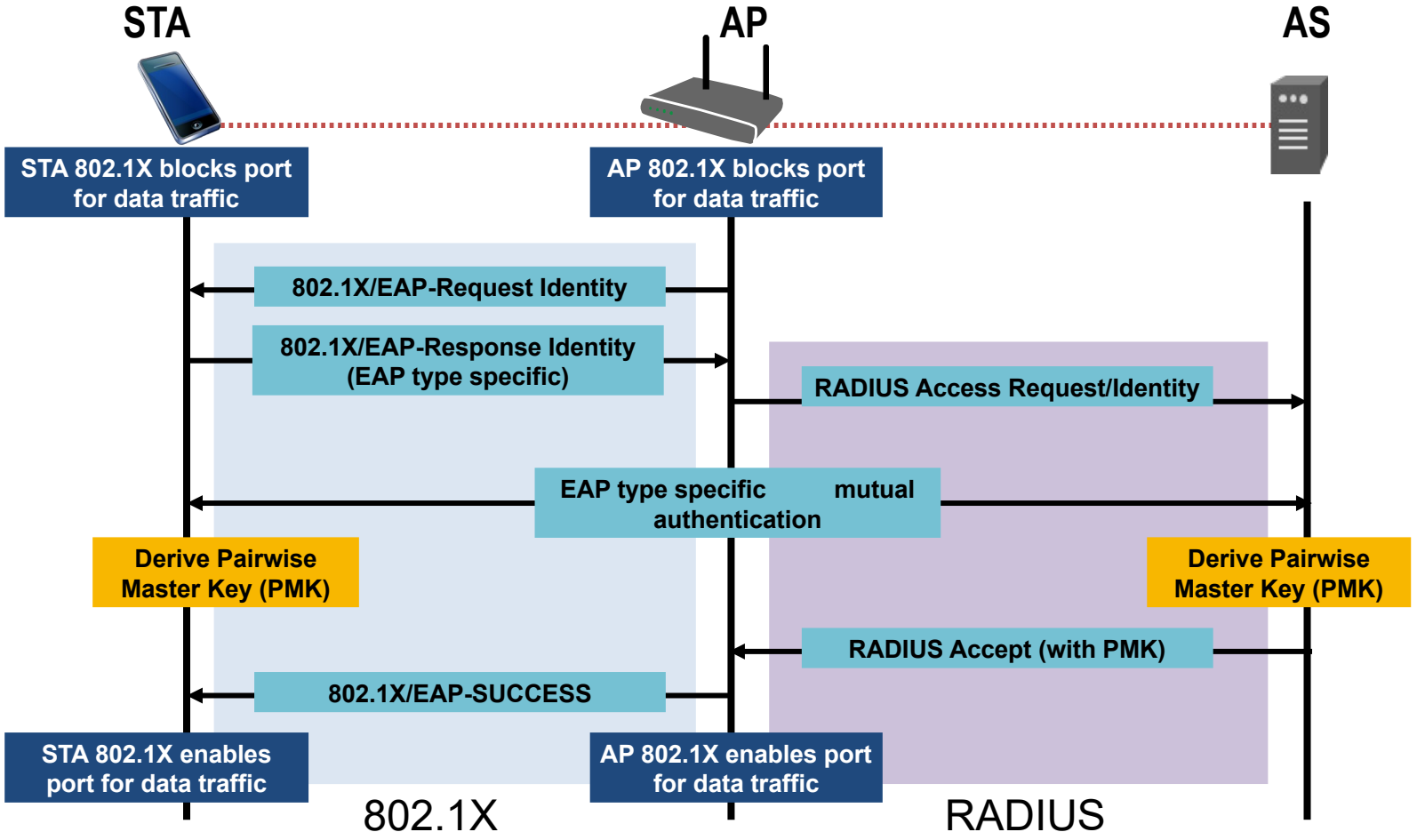
IEEE 802.1X aka EAPoL (EAP over LAN)

- 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

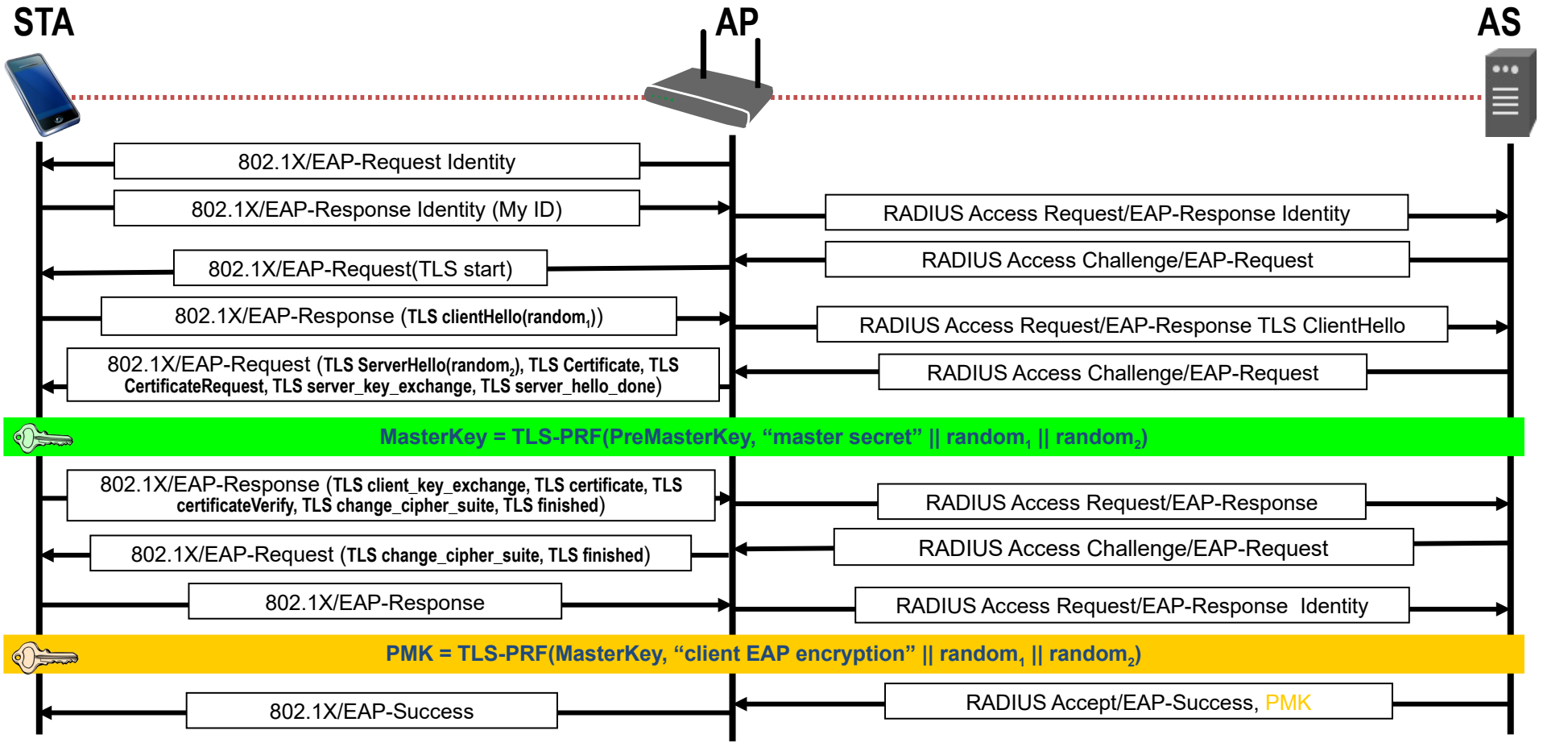
IEEE 802.1X message flow



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



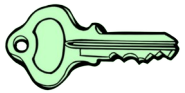
Wi-Fi Security

KEY MANAGEMENT

Key Management

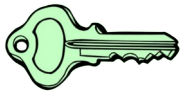
- Redesigned through IEEE 802.11i to fix original 802.1X key management
  - Based on availability of a Pairwise Master Key (PMK)
  - AP and STA use PMK to derive Pairwise Transient Key (PTK)
  - PTK used to protect the data link
- Limitations:
  - No explicit binding to preceding association, authentication
  - 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

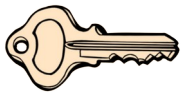


Master Key (MK)

Pairwise Key Hierarchy

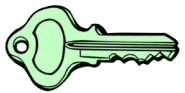


Master Key (MK)

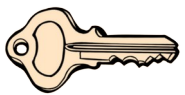


Pairwise Master Key (PMK) = TLS-PRF(MasterKey, “client EAP encryption” | clientHello.random | serverHello.random)

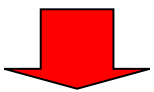
Pairwise Key Hierarchy

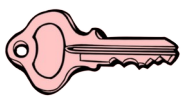


Master Key (MK)



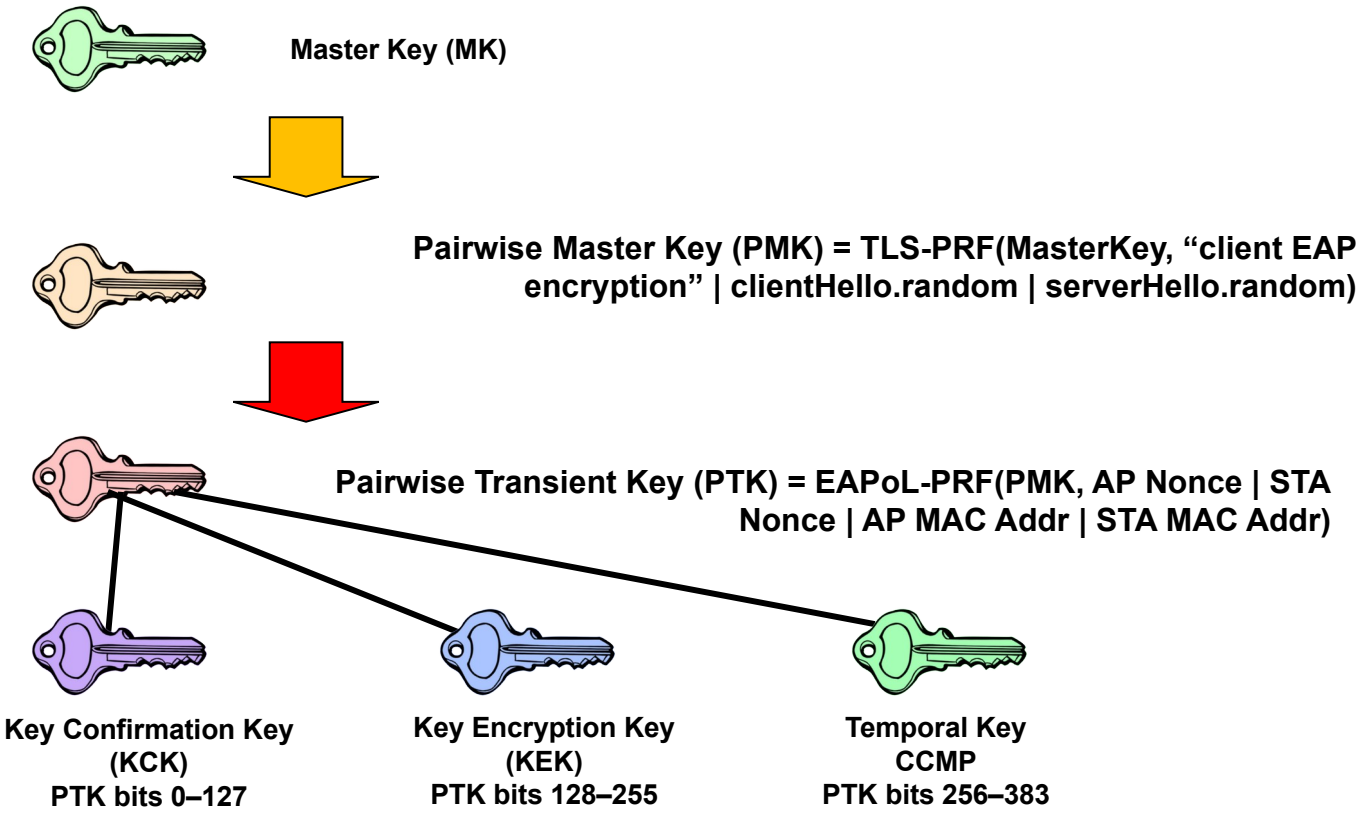
Pairwise Master Key (PMK) = TLS-PRF(MasterKey, “client EAP encryption” | clientHello.random | serverHello.random)



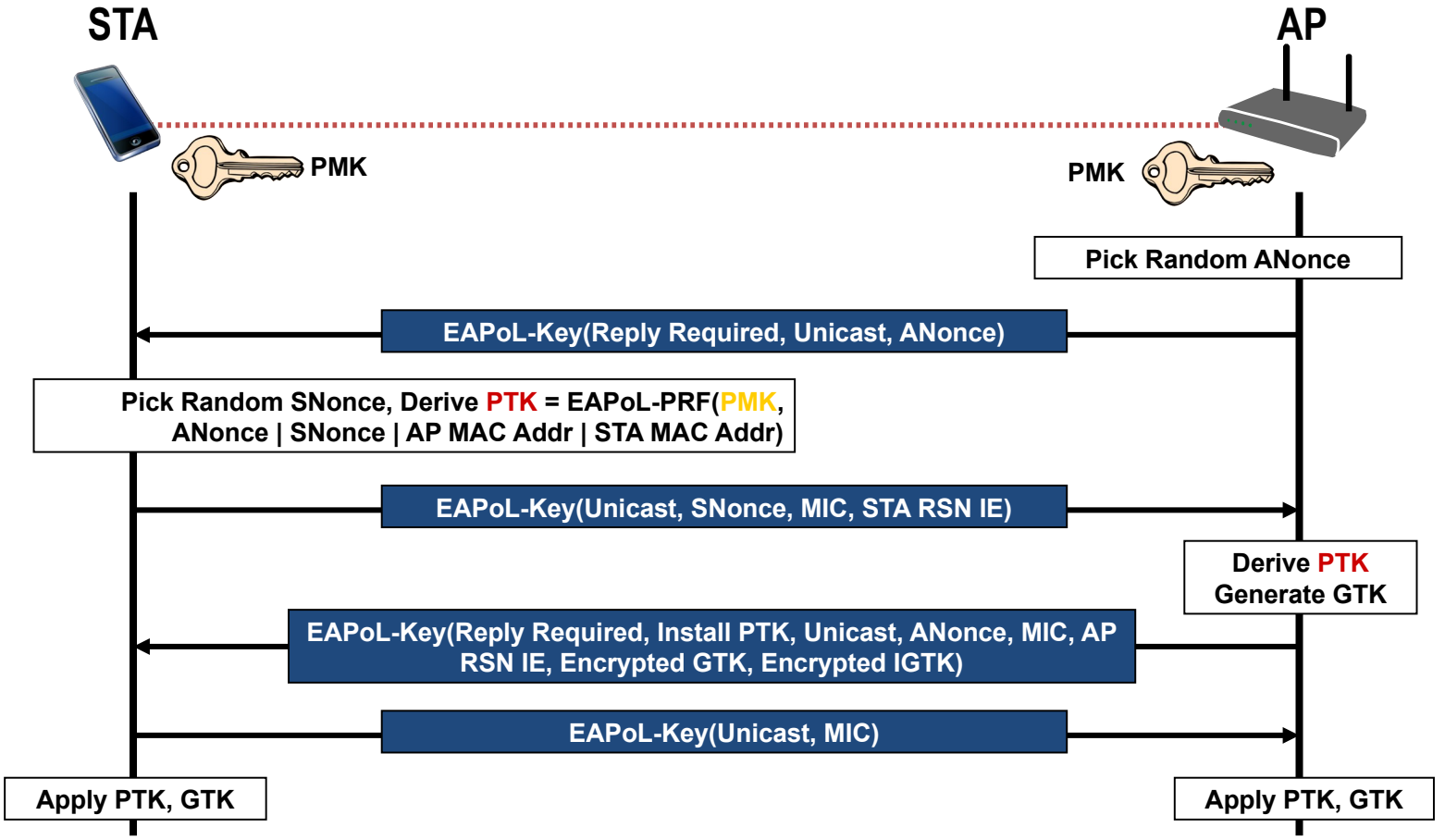


Pairwise Transient Key (PTK) = EAPoL-PRF(PMK, AP Nonce | STA Nonce | AP MAC Addr | STA MAC Addr)

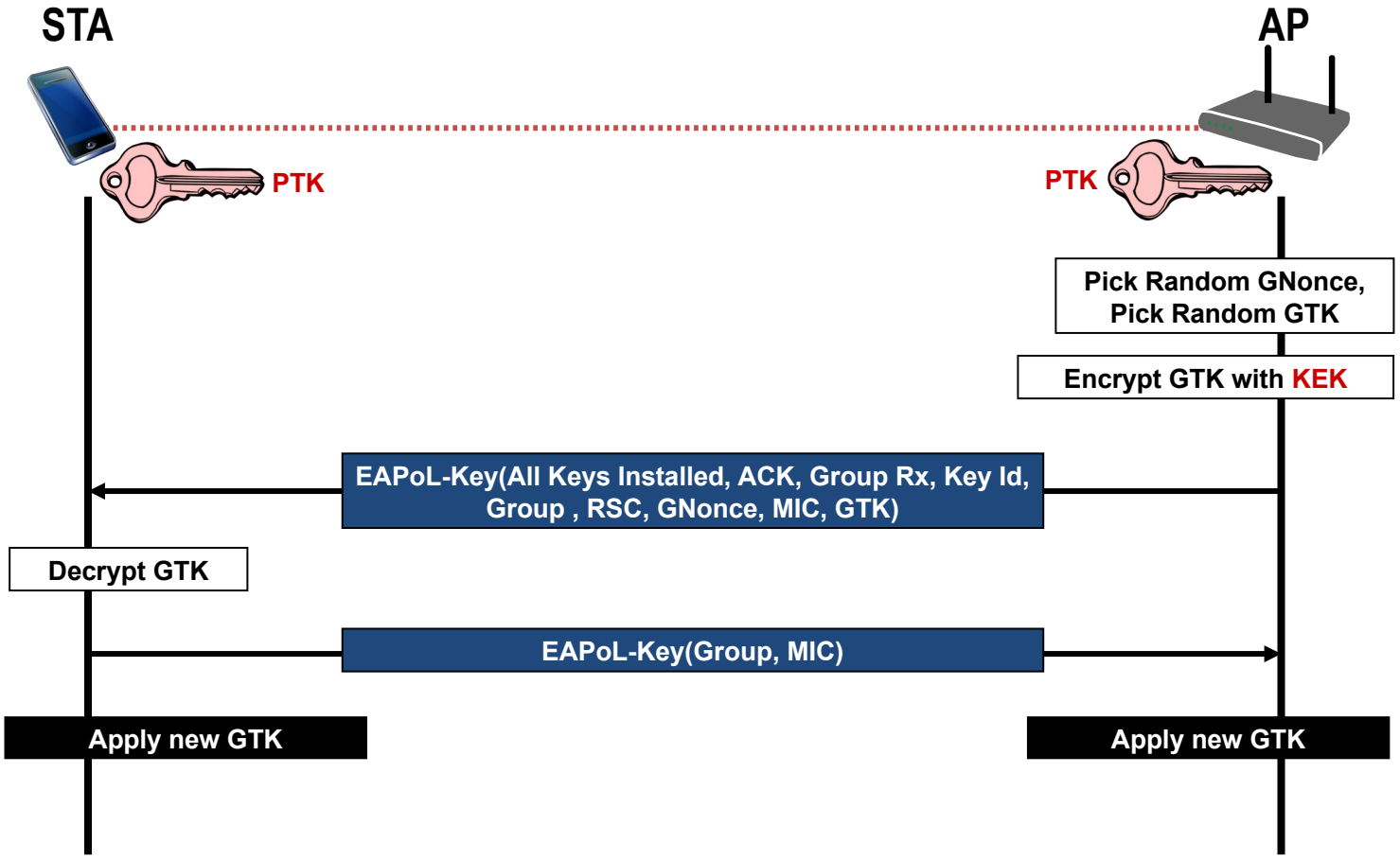
Pairwise Key Hierarchy



4-Way Handshake to establish Temporal Keys



Optional Group Key handshake to refresh GTK



Wi-Fi Security

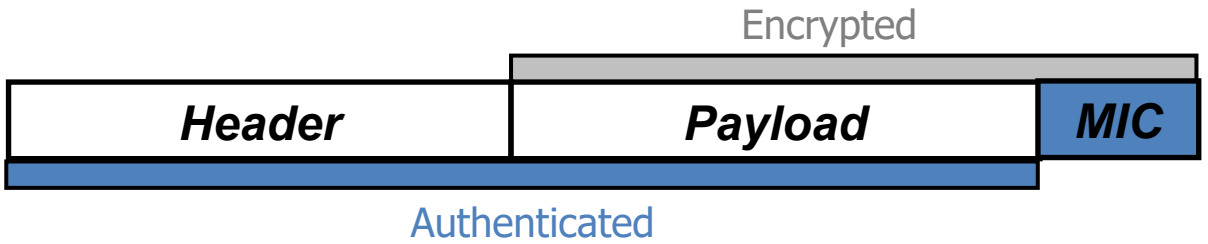
DATA PROTECTION

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)

- Especially designed for IEEE 802.11i
- CCMP makes use of CCM to
  - 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
- Same 128-bit temporal key for encryption and message authentication at both AP and STA
  - Generated and established through 4-way handshake

CCM provides strong cryptography

Counter mode with **C**ipher-block chaining **M**essage authentication code (CCM) is specified in IETF RFC 3610

- A symmetric key block cipher mode providing
  - **confidentiality** using counter mode (CTR) and
  - **data origin authenticity** using Cipher-Block Chaining Message Authentication Code (CBC-MAC)
  - Assumes 128 bit block cipher – IEEE 802.11i uses AES
- CCM Properties
  - CCM provides authenticity and privacy
  - CCM is packet oriented
  - CCM can leave a number of initial plaintext blocks unencrypted

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

WPA3 Operational Enhancements

- EAP Server Certificate Validation (SCV)
  - Mandatory for Wi-Fi CERTIFIED WPA3-Enterprise
- SAE Hash-to-Element
  - 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

Mandatory WPA3 enhancements briefly explained...

- EAP Server Certificate Validation (SCV)
  - STA must perform SCV whenever EAP-TLS, EAP-TTLS or EAP-PEAP is used
  - Allowed trust anchors are server certificate, or CA root cert, pinned to network profile, or CA in trust root store plus explicit domain name (partial or FQDN)
- SAE Hash-to-Element
  - Computationally efficient technique to mitigate side-channel attacks, based on crypto best practice (see IETF draft-irtf-cfrg-hash-to-curve)
  - Defined in IEEE 802.11-2020; AKMs remain the same (SAE and FT-SAE)
- Transition Disable
  - Provides protection against Transition mode downgrade attacks on STAs
  - When configured, AP sends Transition Disable indication to STAs at association
  - The STA disables the indicated Transition modes in its network profile for subsequent connections to that network (SSID)

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 (same AKM) through password is specially 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)

Optional WPA3 enhancements briefly explained...

- Beacon Protection
  - Provides integrity protection of Beacon frames to protect against malicious manipulation of Beacon frame content, e.g. denial-of-service “quiet” attack and WMM parameter set attack, Transmit Power Control limit attack
- 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 to protect against channel-based man-in-the-middle attacks
- Privacy Extension Mechanisms
  - Consistent implementation guidelines and use cases for MAC address randomization
    - 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

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

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

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

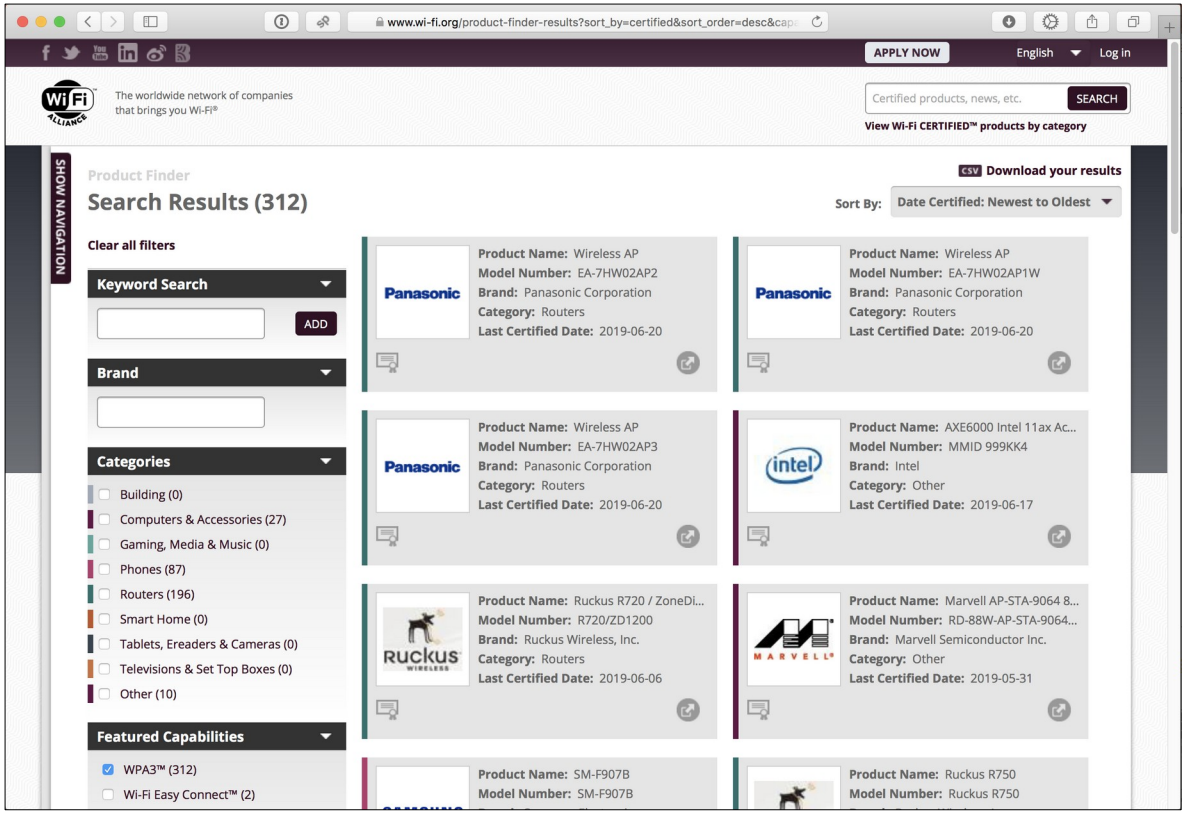
Steps of Wi-Fi security establishment

- **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

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)

WPA3 product support



- https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc provides overview of WPA3 certified products.

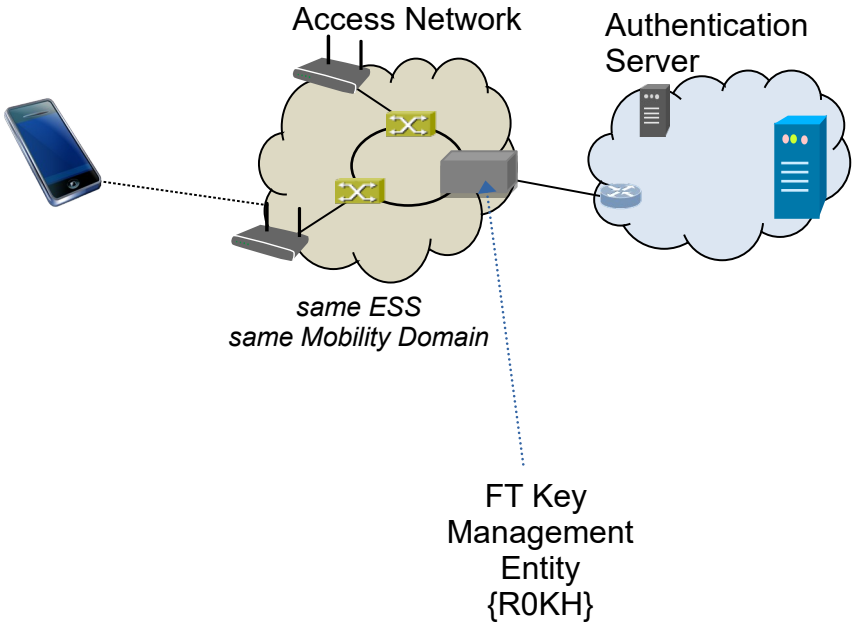
Wi-Fi

WI-FI MOBILITY

The need for Fast BSS Transition (FT)

- Without FT, a BSS transition/handover requires the following four stages:
  - 1. Scanning for target APs.
  - 2. Open 802.11 authentication.
    - Required for backward compatibility reasons
  - 3. Reassociation.
  - 4. PTK derivation and installation.
    - The complexity of this step depends on whether a new complete 802.1X authentication is involved in providing the PMK at the new AP.
    - At minimum, at least a four-way handshake is required to derive the PTK.
- PTK derivation and installation causes the vast majority of handover latency.
- FT completely removes need for re-authentication and succeeding 4-way handshake
  - Defining a new key hierarchy allowing for local derivation of PMK for APs of the same mobility domain.
  - Collapsing the four-way handshake into the 802.11 authentication/association exchange (2, 3)

FT Keying Architecture



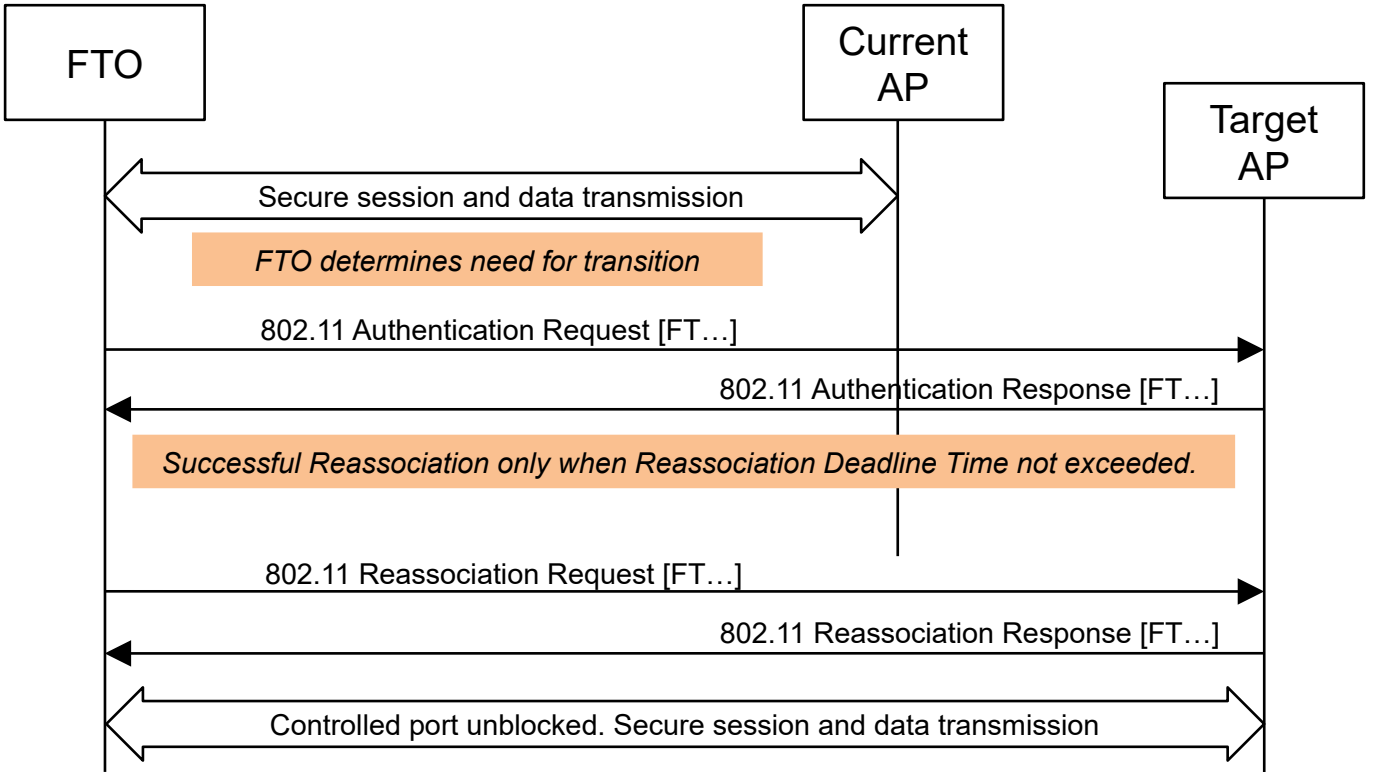
- FT introduces extended key management with two layer key management.
  - R0KH/S0KH: ‘master’ key for whole mobility domain
  - R1KH/S1KH: AP specific ‘working’ keys
- Authentication is proxied by a central R0KH entity, which computes and stores the ‘master key’ (PMK-R0) for hole mobility domain for each STA
- R0KH key management entity computes the ‘working keys’ (PMK-R1) for each of the APs when needed for transition.

FT protocol overview

- FT protocol was specified through IEEE 802.11r-2008
- Protocol initiated in initial association of FT Originator (FTO, i.e. Station) and AP.
  - FT protocol is an extension to the re-association messaging
    - Only apply for transitions between APs within the same mobility domain within the same ESS.
  - Initial exchange: FT initial mobility domain association
    - Establishes ‘central’ PMK which is used for all subsequent associations within mobility domain
  - Subsequent re-associations to APs within the same mobility domain may make use of the FT protocols and keying architecture
- Two FT protocols are defined:
  - FT Protocol when no resource request prior to its transition.
  - FT Resource Request Protocol when a FTO has to request a resource prior to transition.
- Two FT methods:
  - Over-the-Air
  - Over-the-DS
- APs advertise both, capabilities and policies for the support of the FT protocols and methods through FTIE.

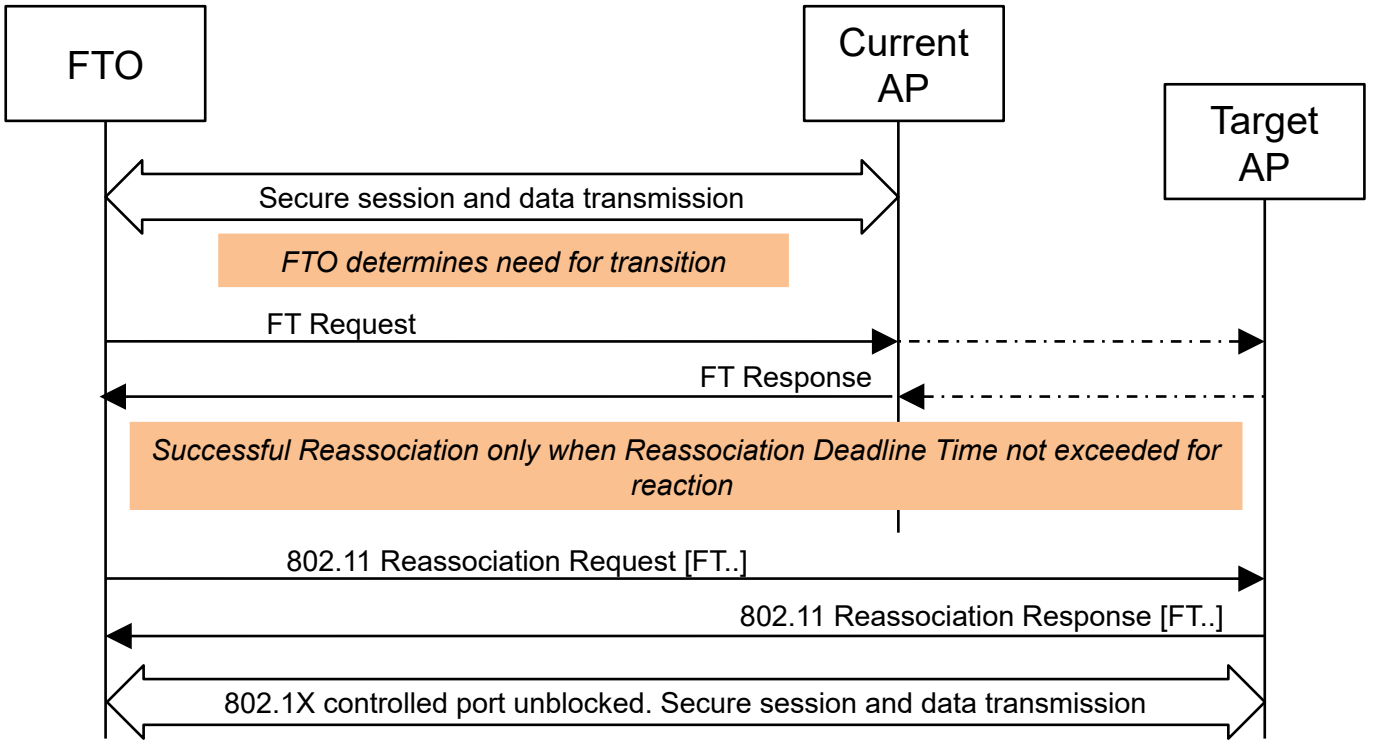
Over-the-air Fast BSS Transition

- The FTO communicates directly with the target AP
  - Use of IEEE 802.11 authentication frame with the FT authentication algorithm.

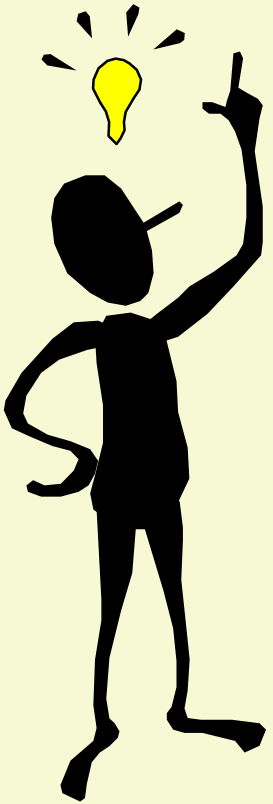


Over-the-DS Fast BSS Transition

- The FTO communicates with the target AP via the current AP.
  - The communication between the FTO and the target AP is carried in FT Action frames between the FTO and the current AP.



Questions and answers



Security questions…

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

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?
20) What is the purpose of Fast BSS Transition?
21) Which entity stores the R0-PMK?
22) How can the Fast Transition Originator communicate with the Target AP?

THE END

Questions and remarks