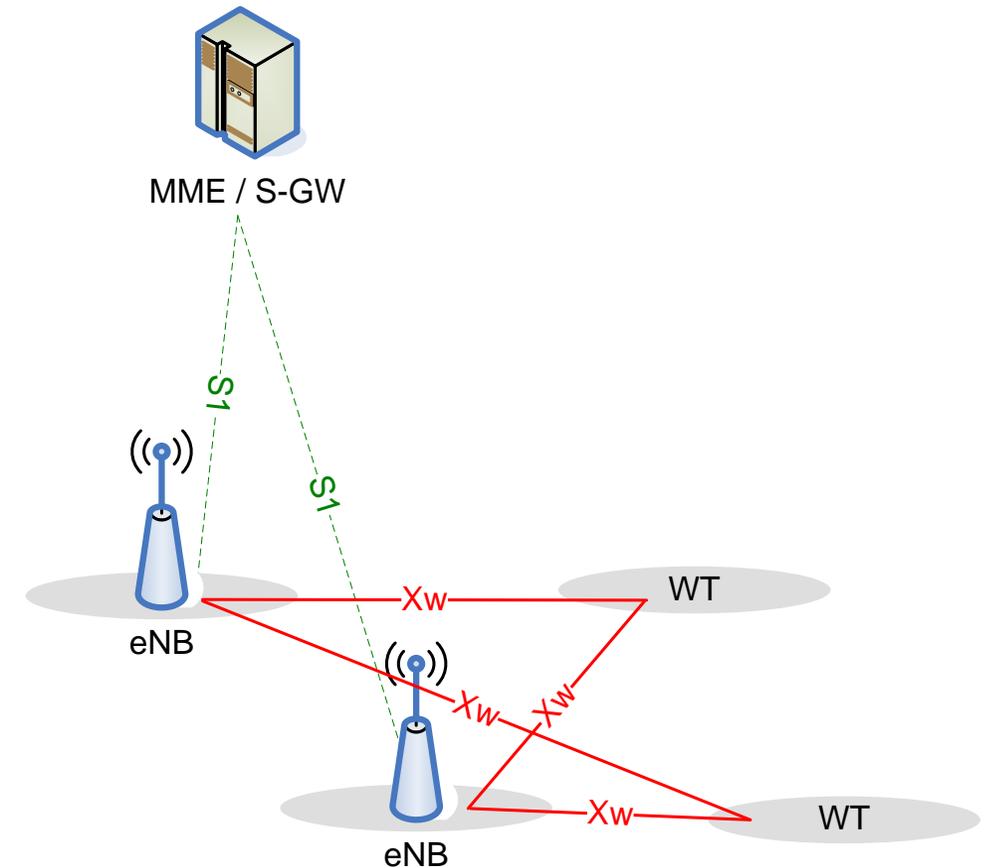

LWA PMK handling

QUALCOMM®



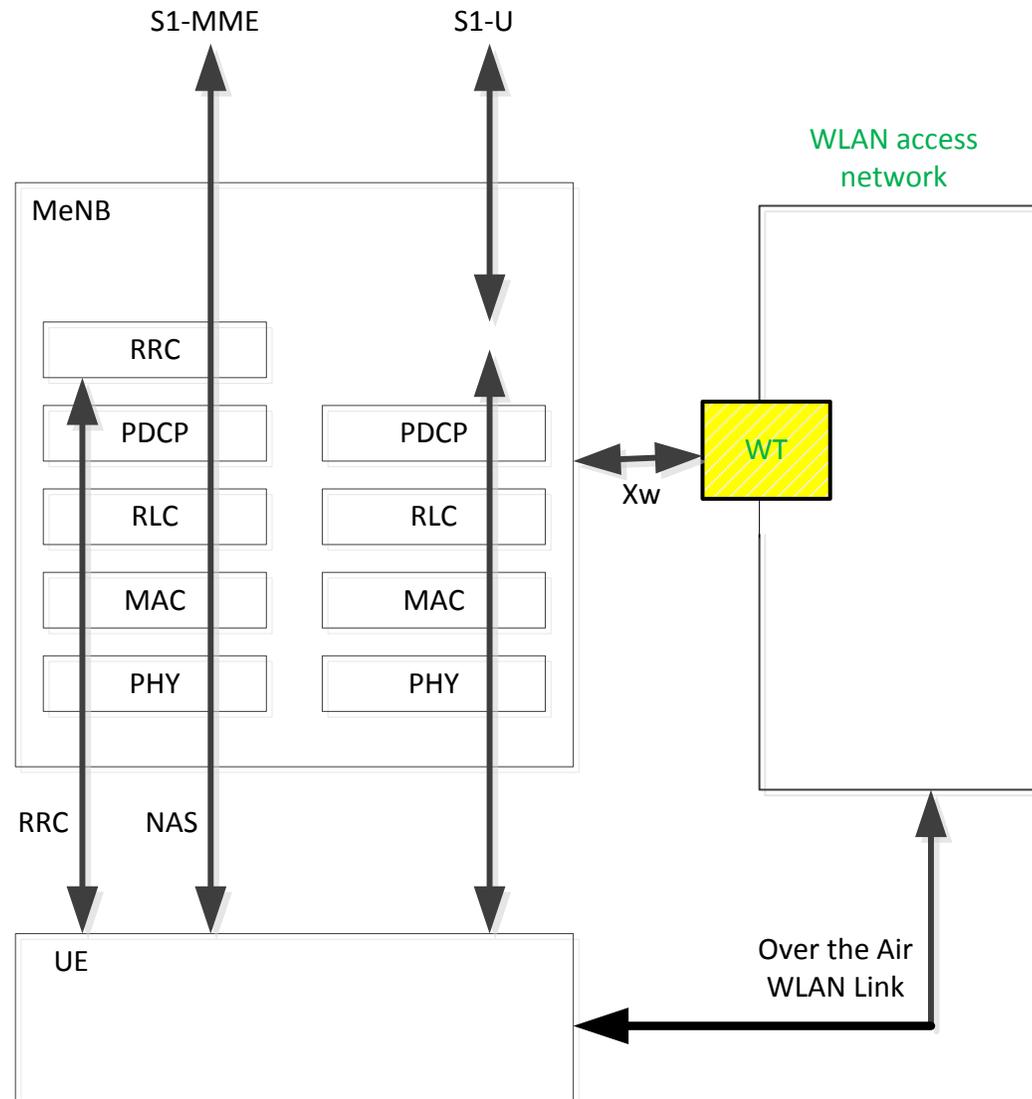
LTE-WLAN Aggregation (LWA)

- LWA enables an UE in RRC_CONNECTED to utilize radio resources of both LTE and WLAN
 - Based on the WLAN measurements from the UE, eNB controls the LTE bearers that are offloaded to WLAN
- WLAN Termination (WT) for Non-Collocated case
 - May contain one or more WLAN AP/ AC (herein onwards AP for simplicity); Two options:
 - Terminated at the AP
 - WT terminated at entity other than AP, e.g., central WT gateway
 - WT may be connected to multiple APs
 - These existing AP may not be LWA aware
- Issue: How does LWA security specified in TS 33.401 used with 802.1x AP/ACs?



LWA Reference Model (non-collocated case)

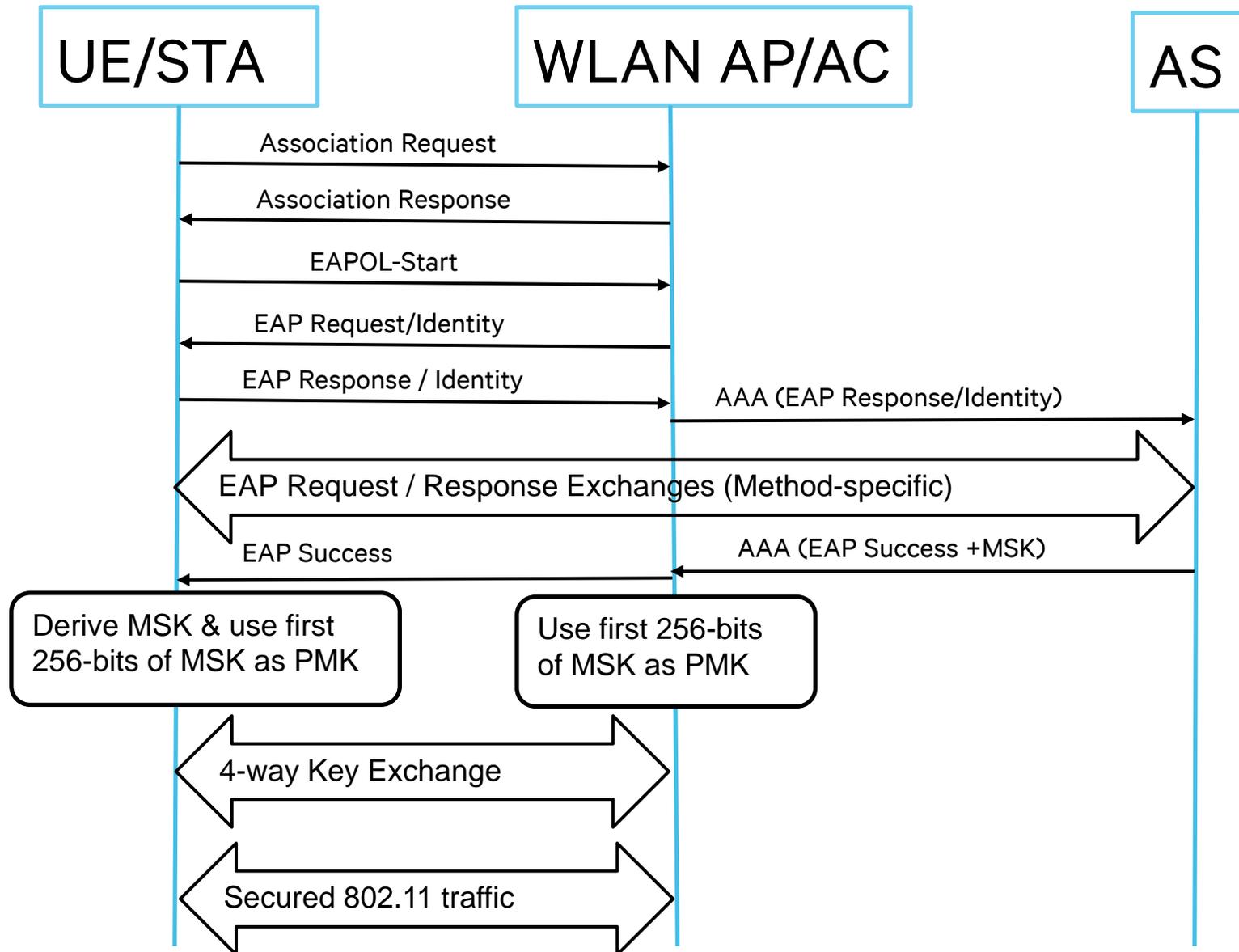
LWA Architecture



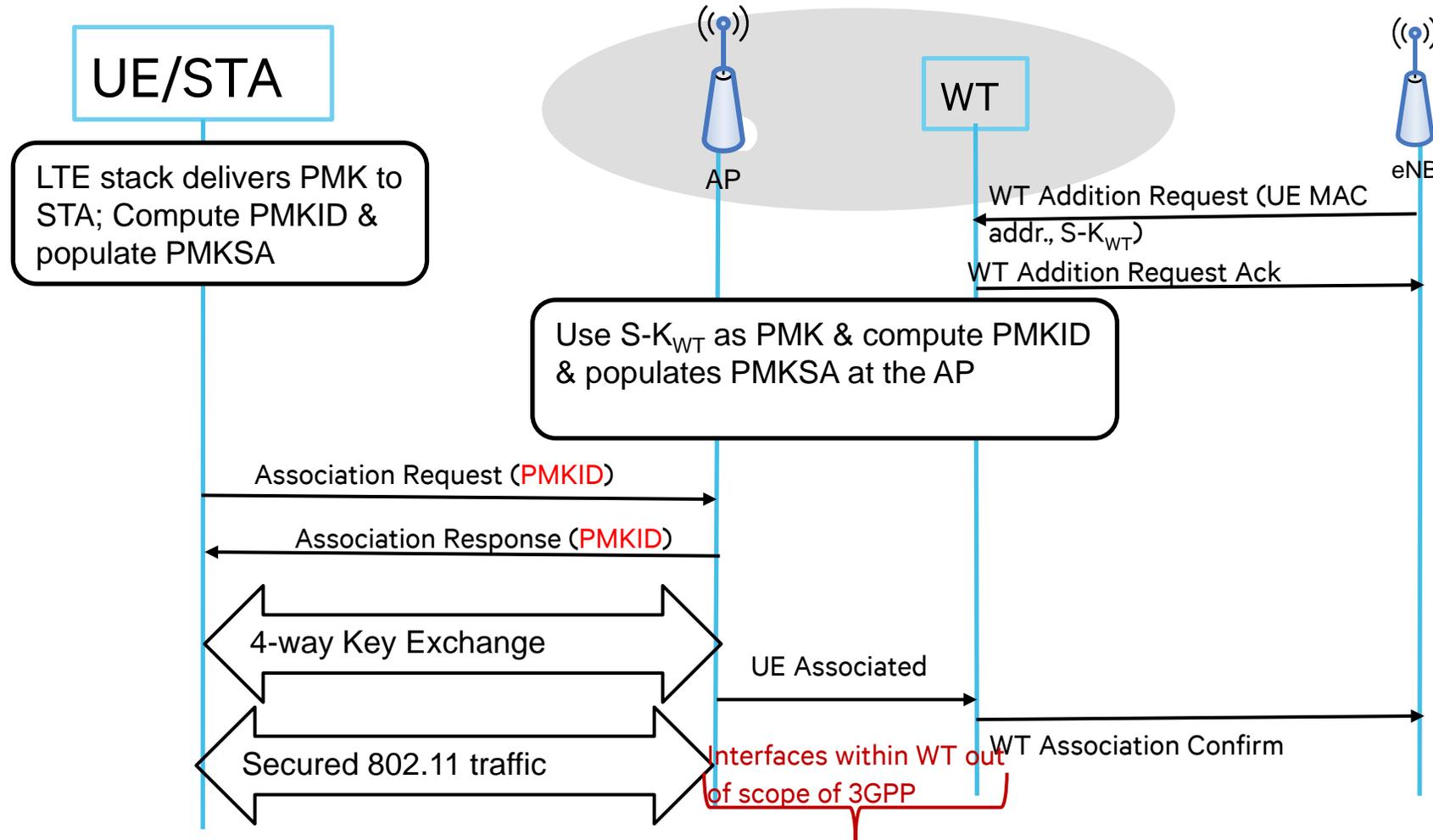
LWA Security (Annex G of TS 33.401v13.2.0) – Background / Issues

- Derive 256-bit shared key called $S-K_{WT}$ from current LTE security context (KeNB) both at the eNB and UE
 - LTE stack of the UE provides this key to the STA (of the UE)
 - eNB provides this key to the WT
- 3GPP spec only requires that $S-K_{WT}$ is used as the equivalent to PMK (pair-wise master key) to start 4-way key exchange
- How this is achieved both at the UE and WT is lacking some details in couple of areas
 - **Issue #1:** PMKID derivation (IEEE 802.11 spec allows two methods for PMKID derivation)
 - **Issue #2:** How to install PMK at an 802.11 compliant AP / AC that is not collocated with WT
- Correcting these two issues is required in order to enable interoperability between LWA UEs and 802.1x APs

802.1x Authentication - Overview



AP supports OOB install of PMK by WT (e.g., AP & WT collocated)



- Requires WT to support installation of PMK received from out-of-band (OOB) channel and creation of PMKSA at the AP
 - Issue #2: Existing APs/ACs (that are not collocated with WT) may not support this; need a way to install PMK at the existing 802.1x APs/ACs in this case

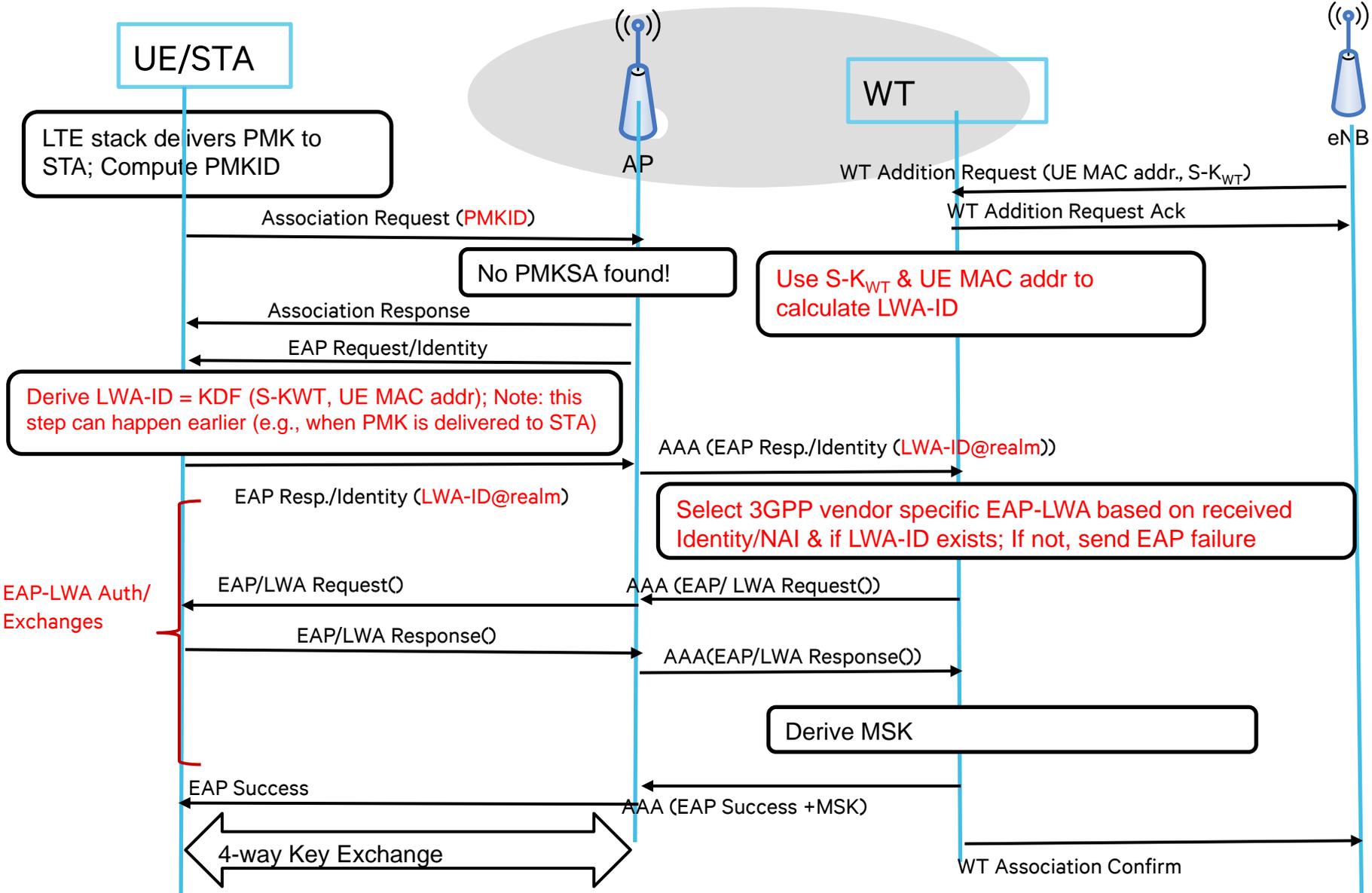
PMKID Derivation

- Before starting 4-way key exchange, UE needs to create PMKSA
- PMKSA consists of the following (see 11.5.1.1.2 of IEEE 802.11-2012)
 - PMKID (802.11-2012 defines multiple methods for PMKID derivation!)
 - A method for PMKID derivation needs to be mandated in TS 33.401
 - We propose the following method defined in 802.11-2012
 - $\text{PMKID} = \text{Truncate-128}(\text{HMAC-SHA-256}(\text{PMK}, \text{"PMK Name"} \parallel \text{AA} \parallel \text{SPA}))$, where AA = Authenticator's MAC address; SPA = Supplicant's MAC address
 - Authenticator (AP) or Peer (STA) MAC address
 - PMK
 - Lifetime (defined in 11.6.1.3) - PMK validity time; No need to specify as this is controlled by AP
 - AKMP - No need to specify as this is controlled by AP
 - Authorization info & other info (e.g., SSID) - Only AP needs these and would be based on local policy/policies delivered by AAA (e.g., WT)
- Conclusion: PMKID derivation method needs to be mandated

AP does not support PMK installation

- Already deployed 802.1x APs (e.g., that are not collocated with WT) may not support out-of-band (OOB) installation of PMK without EAP authentication
 - In such cases, when the AP receives Association Request (with PMKID IE) from LWA UE, the AP/AC would initiate EAP authentication
- EAP authentication (in order to create PMK & the subsequent PMKSA) is started by AP sending EAP-Identity Request
 - Successful EAP authentication would result in PMK and the subsequent creation of PMKSA via 4-way handshake
- However, existing TS 33.401 does not have any specification text on how to handle this case
- Conclusion #2: TS 33.401 needs to specify how this case is handled
 - We propose that existing EAP authentication framework supported by legacy AP/AC is leveraged to install PMK; Such a method is described in the next few slides

Installing PMK at AP leveraging existing EAP procedures



Installing PMK at AP - Details

- AS & UE perform method (e.g., 3GPP LWA) specific EAP message exchange
 - Method specific EAP exchanges are required to ensure compliance with EAP RFC (3748)
- Option1: AS & EAP Peer exchange EAP/LWA Request () / Response () messages
 - Once the EAP/LWA Response () is received, AS sends EAP success +MSK
 - Set MSK = PMK | PMK, where “|” represents concatenation
 - Upon receiving EAP-success, the EAP authenticator sets PMK to S-Kwt (first 256-bits of MSK) and performs 4-way key exchange to initialize PMKSA
- Option2 :AS & EAP Peer exchange EAP Request/LWA-challenge (ASNonce) & EAP Response/LWA Challenge (AUTHRES, STANonce) messages
 - AUTHRES = KDF (S-Kwt, ANonce, STANonce, “LWA AUTHRES”);
 - Upon receipt of EAP-Response, AS calculates expected AUTHRES and compares with received AUTHRES; If equal, AS sends EAP success + MSK
 - MSK = KDF (S-Kwt, ANonce, STANonce, “LWA MSK Key Derivation”)
 - the first 256-bits of MSK used as the PMK for 4-way key exchange
- We recommend option 2
 - To avoid potential security issues with WLAN deployments that may utilize 256 LSBs of MSK for other purposes (e.g., 802.11r Fast BSS transitions)

EAP-Identity for LWA

- When PMKSA identified by PMKID is not found (e.g., AP not collocated with WT), AP starts EAP authentication process by sending EAP Request/Identity
- In EAP Identity Response, UE sets EAP-Identity to LWA-ID@realm
 - LWA-ID = SHA256 (S-K_{WT}, UE MAC addr, “LWA Identity”) – LWA-ID is needed for WT to uniquely identify the UE/ S-K_{WT} pair
 - realm = lwa.wtid<WTID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org
 - Where MCC & MNC obtained from serving network PLMN Identity (of the eNB)
 - Identity of the E-UTRAN Cell ID (ECI) may be included in the realm as WTID (used to route AAA messages to right WT)
 - LTE stack of the UE provides MCC/MNC & WTID to the STA
- WT (acting as the Auth Server) uses LWA-ID to index S-Kwt
- Use of realm with ECI and Serving Network PLMN ID enables WLAN access network to interwork with multiple serving networks (e.g., eNBs from different serving PLMN or different eNBs of the same PLMN)
 - Note that AAA routing can ignore lower order (i.e., left side) part of the realm if not required to identify the WT/Auth Server

PMKID Replay attack?

- An eavesdropping attacker may try to capture PMKID & replay it
- However, attacker will not be successful as the 4-way handshake will fail (as the attacker doesn't know PMK)
- Also, note that LTE bearers offloaded to WLAN are also encrypted at PDCP layer between the UE and eNB

Conclusion & Proposal

- TS 33.401 needs to mandate PMKID derivation at the UE
- In order to use LWA with existing WLAN deployments, it is useful to specify in TS 33.401 how EAP can be used to install PMK at existing WLAN AP/Acs
- S3-160xxx is the CR to TS 33.401 implements these two proposals

Thank you

Follow us on:  

For more information on Qualcomm, visit us at:
www.qualcomm.com & www.qualcomm.com/blog

© 2013 Qualcomm Incorporated. All rights reserved. Qualcomm, Snapdragon, and Gobi are trademarks of Qualcomm Incorporated, registered in the United States and other countries. Vuforia and Wireless Reach are trademarks of Qualcomm Incorporated. Atheros and Skifta are trademarks of Qualcomm Atheros, Inc., registered in the United States and other countries. Hy-Fi is a trademark of Qualcomm Atheros, Inc. Alljoyn is a trademark of Qualcomm Innovation Center, Inc., registered in the United States and other countries. Other products and brand names may be trademarks or registered trademarks of their respective owners.

