



FIT3031 INFORMATION & NETWORK SECURITY

COMMONWEALTH OF AUSTRALIA

Copyright Regulations 1969

WARNING

This material has been reproduced and communicated to you by or on behalf of Monash University pursuant to Part VB of the *Copyright Act 1968* (the Act).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.



MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

Lecture 6

Wireless Network Security

Unit Objectives

- ✓ OSI security architecture
 - **common security standards and protocols for network security applications**
 - **common information risks and requirements**
- ✓ operation of private key encryption techniques
- ✓ operation of public encryption techniques
- ✓ concepts and techniques for digital signatures, authentication and non-repudiation
- ✓ security threats of web servers, and their possible countermeasures
- ✓ **Wireless Network Security Issues**
 - security threats of email systems and their possible countermeasures
 - IP security
 - intrusion detection techniques for security purpose
 - risk of malicious software, virus and worm threats, and countermeasures
 - firewall deployment and configuration to enhance protection of information assets
 - network management protocol for security purpose

Lecture 6: Objectives

- **Appreciate the IEEE 802.11 Wireless Protocol**
 - Understand the wireless security mechanisms
- **4G (LTE) Security**
 - A brief introduction only!
 - Not expect to go through the details in this unit

IEEE 802.11

- **IEEE 802 committee for LAN standards**
- **IEEE 802.11 formed in 1990's**
 - charter to develop a protocol & transmission specifications for wireless LANs (WLANs)
- **since then demand for WLANs, at different frequencies and data rates, has exploded**
- **hence seen ever-expanding list of standards issued**

Table 1: IEEE 802.11 Standards

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s



IEEE 802 Terminology

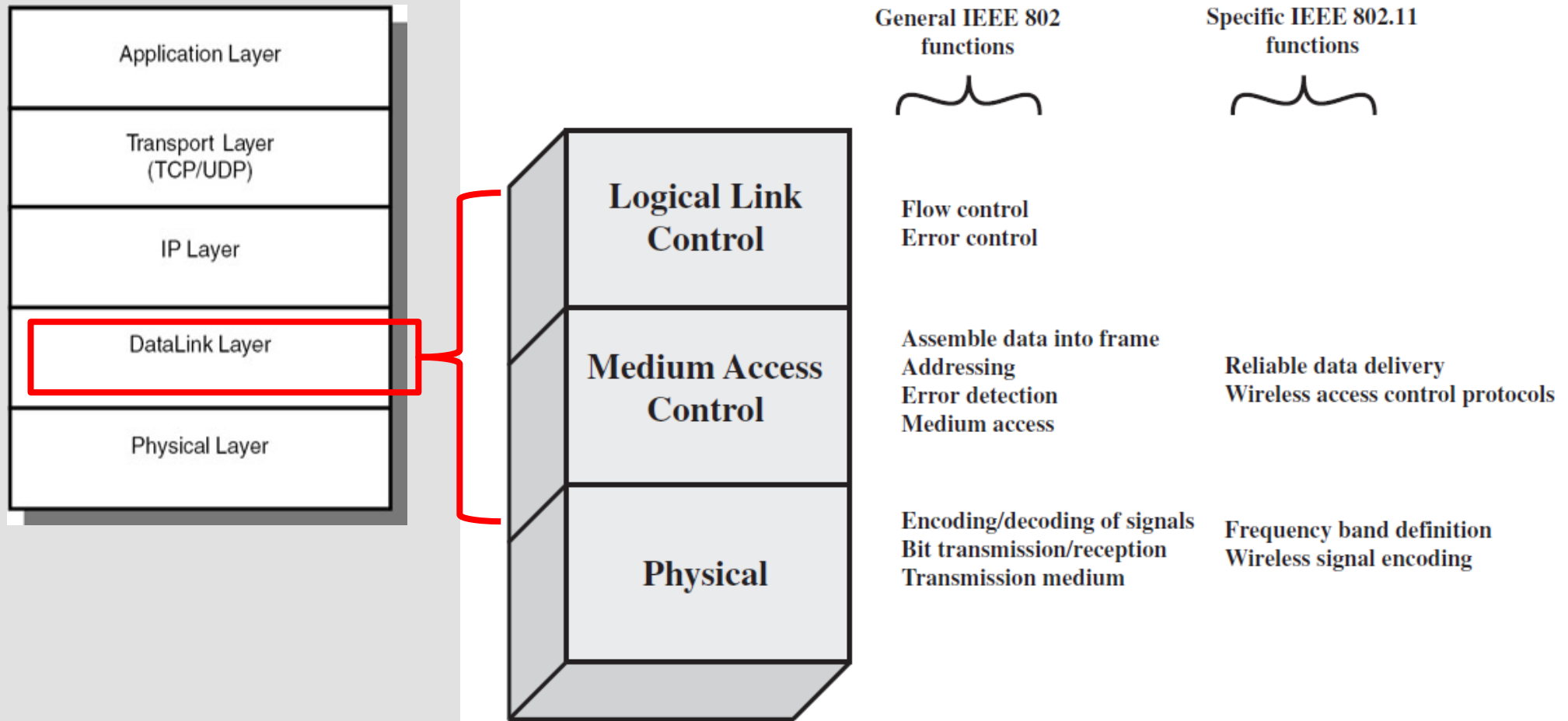
Table 6.1 IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

Wi-Fi Alliance

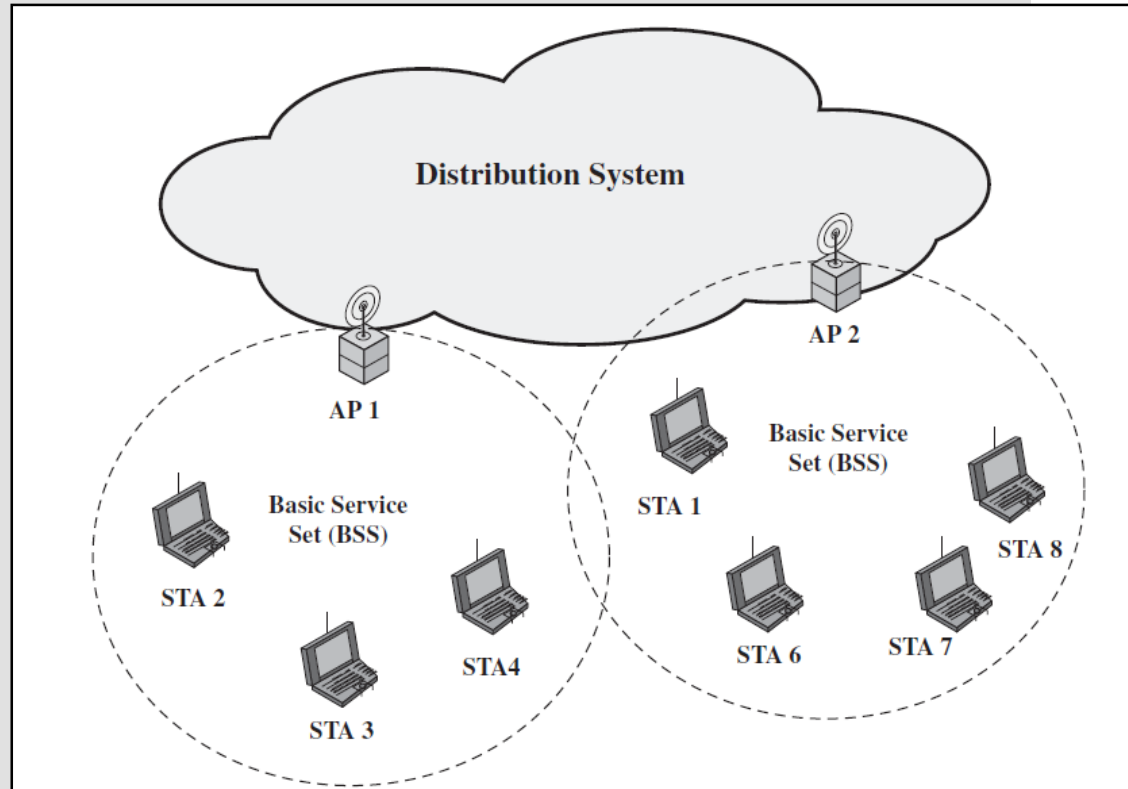
- **802.11b first broadly accepted standard**
- **Wireless Ethernet Compatibility Alliance (WECA) industry consortium formed 1999**
 - to assist interoperability of products
 - renamed Wi-Fi (Wireless Fidelity) Alliance
 - created a test suite to certify interoperability
 - initially for 802.11b, later extended to 802.11g
 - concerned with a range of WLANs markets, including enterprise, home, and hot spots

IEEE 802.11 Protocol Architecture (stack)



Network Components & Architecture

- **Basic Service Set (BSS)**
 - Smallest WLAN block
- **Distribution System (DS)**
 - Connects BSS blocks
- **Access Points (AP)**
 - Functions as a bridge or relay point
- **Extended Service Set (ESS)**
 - Two or more BSS interconnected by a DS



IEEE 802.11 Services

- **WLAN needs to provide 9 services to achieve functional wired equivalence**
 - Provider
 - > Either a DS or Station
 - Used to Support
 - > Security or Delivery


Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

802.11 Wireless LAN Security

- **Wireless traffic can be monitored by any radio in range, not physically connected**
- **Original 802.11 spec had security features**
 - Wired Equivalent Privacy (WEP) algorithm
 - but found this contained major weaknesses
- **802.11i task group developed capabilities to address WLAN security issues**
 - Wi-Fi Alliance Wi-Fi Protected Access (WPA)
 - final 802.11i Robust Security Network (RSN)

WEP Problems

- **No centralized key management**
 - Manual key distribution → Difficult to change keys
- **Single set of Keys shared by all → Frequent changes necessary**
- **No mutual authentication**
- **IV value is too short. Not protected from reuse.**
- **Weak integrity check.**
- **Directly uses master key**
- **No protection against replay**

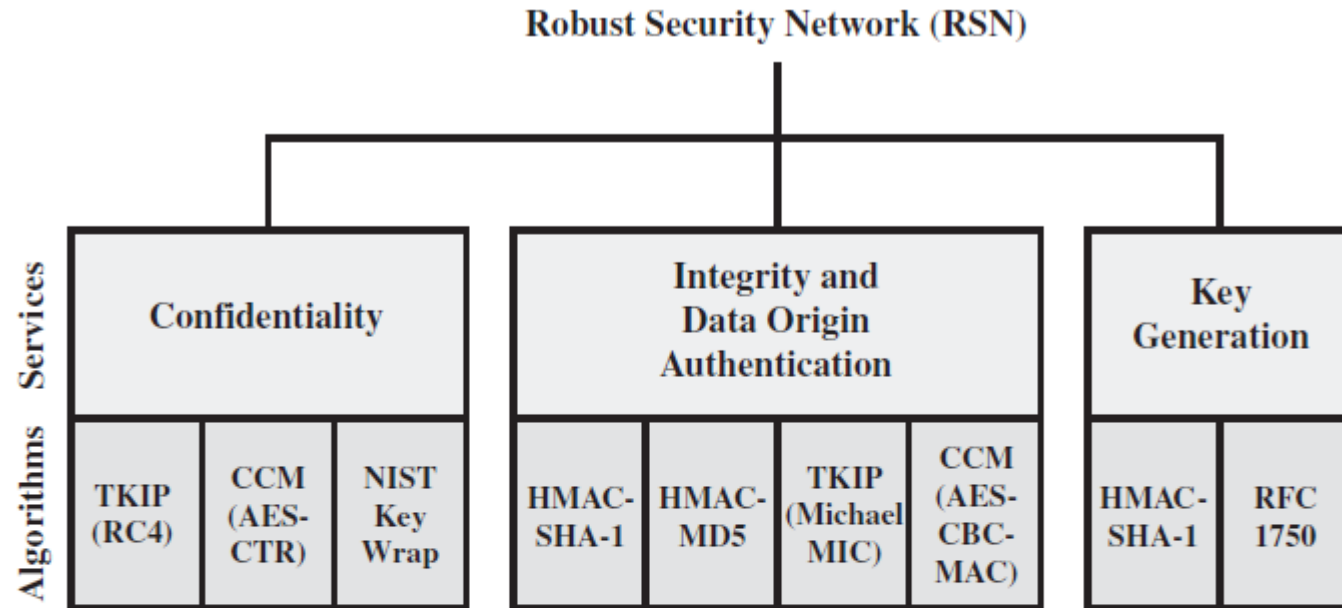


**Bottom line:
Weakness: Key
Management
and Key Size**

802.11i RSN Services and Protocols

- **Authentication**
 - used to define an exchange between a user and an AS that provides mutual authentication and generates **temporary keys** to be used between the client and the AP over the wireless link.
- **Access Control**
 - enforces the use of the authentication function, routes the messages properly, and **facilitates key exchange**.
- **Privacy with message integrity**
 - MAC-level encryption, message integrity code

802.11i RSN Cryptographic Algorithms



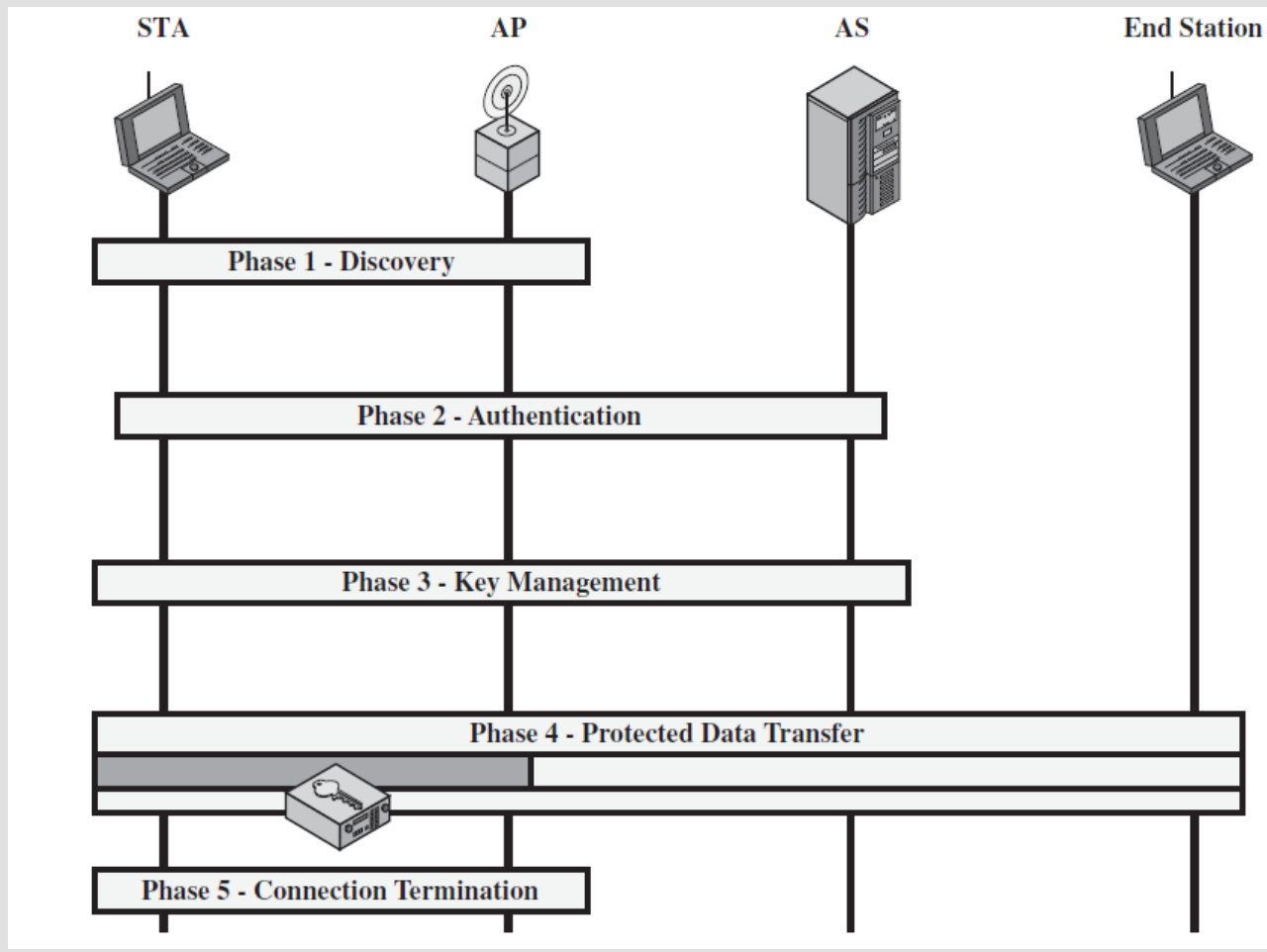
(b) Cryptographic algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure 6.4 Elements of IEEE 802.11i

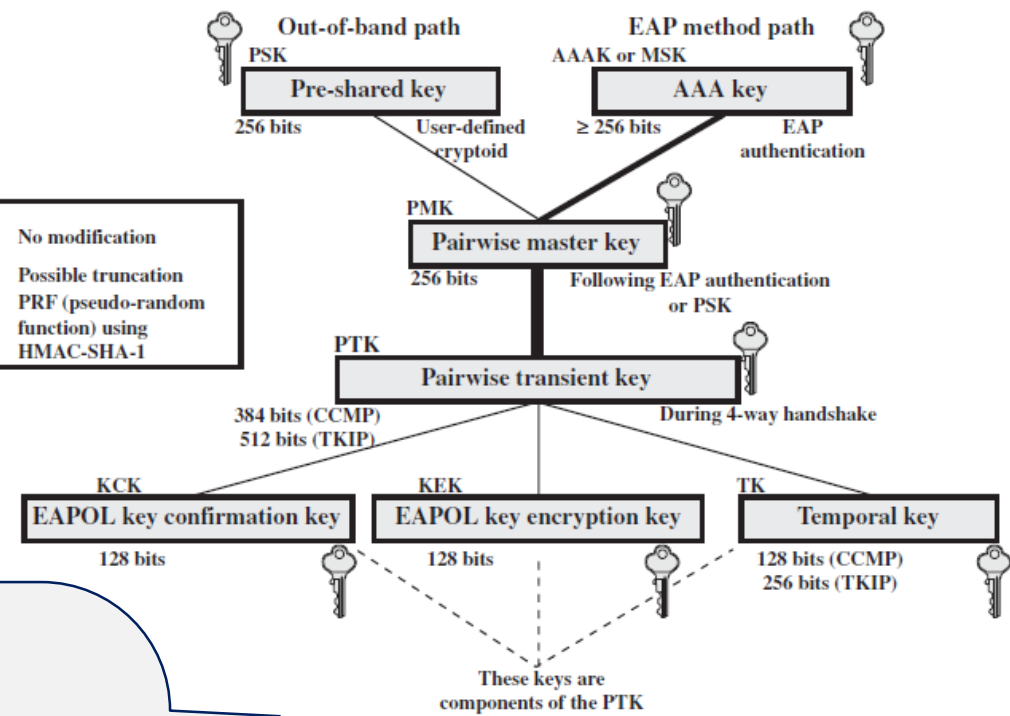
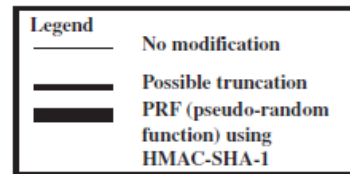


802.11i Phases of Operation

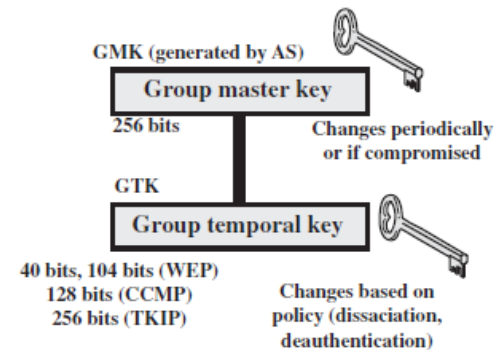


802.11i Key Management Phase

There are two types of keys: **pairwise keys**, used for communication between an STA and an AP; and **group keys**, for multicast communication. Figure shows the two key hierarchies.



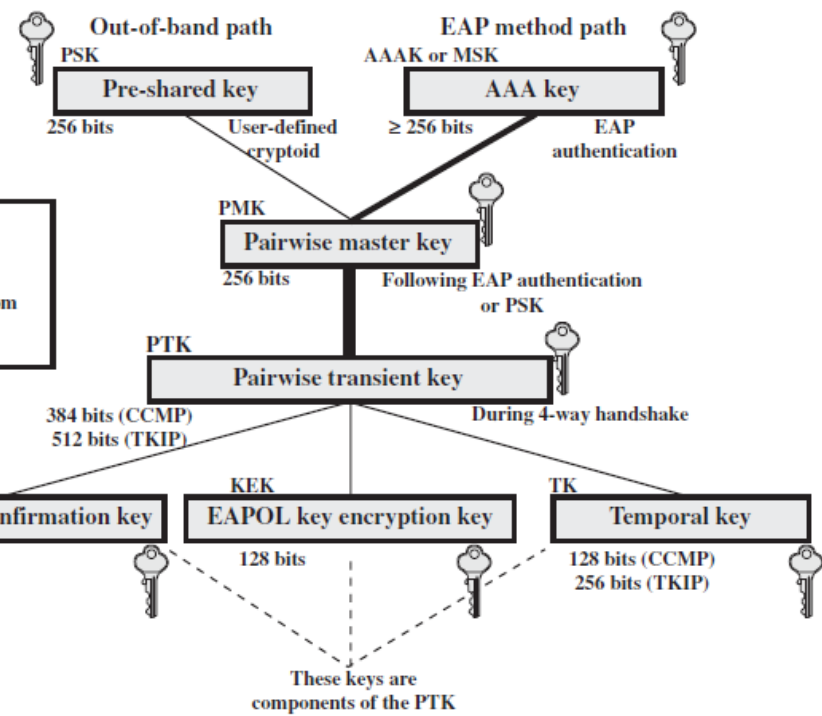
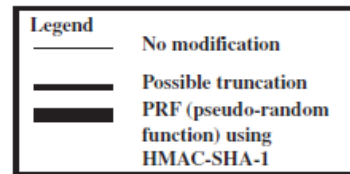
(a) Pairwise key hierarchy



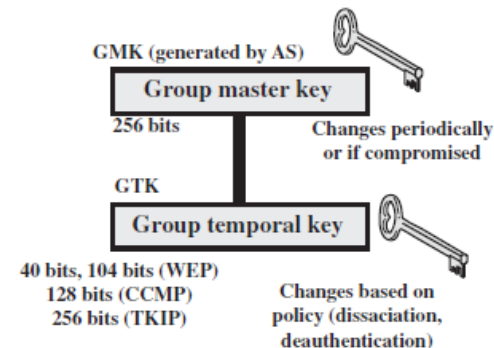
(b) Group key hierarchy

802.11i Key Management Phase

Pairwise keys are used for communication between a pair of devices, typically between an STA and an AP. **These keys form a hierarchy, beginning with a master key** from which other keys are derived dynamically and used for a limited period of time.



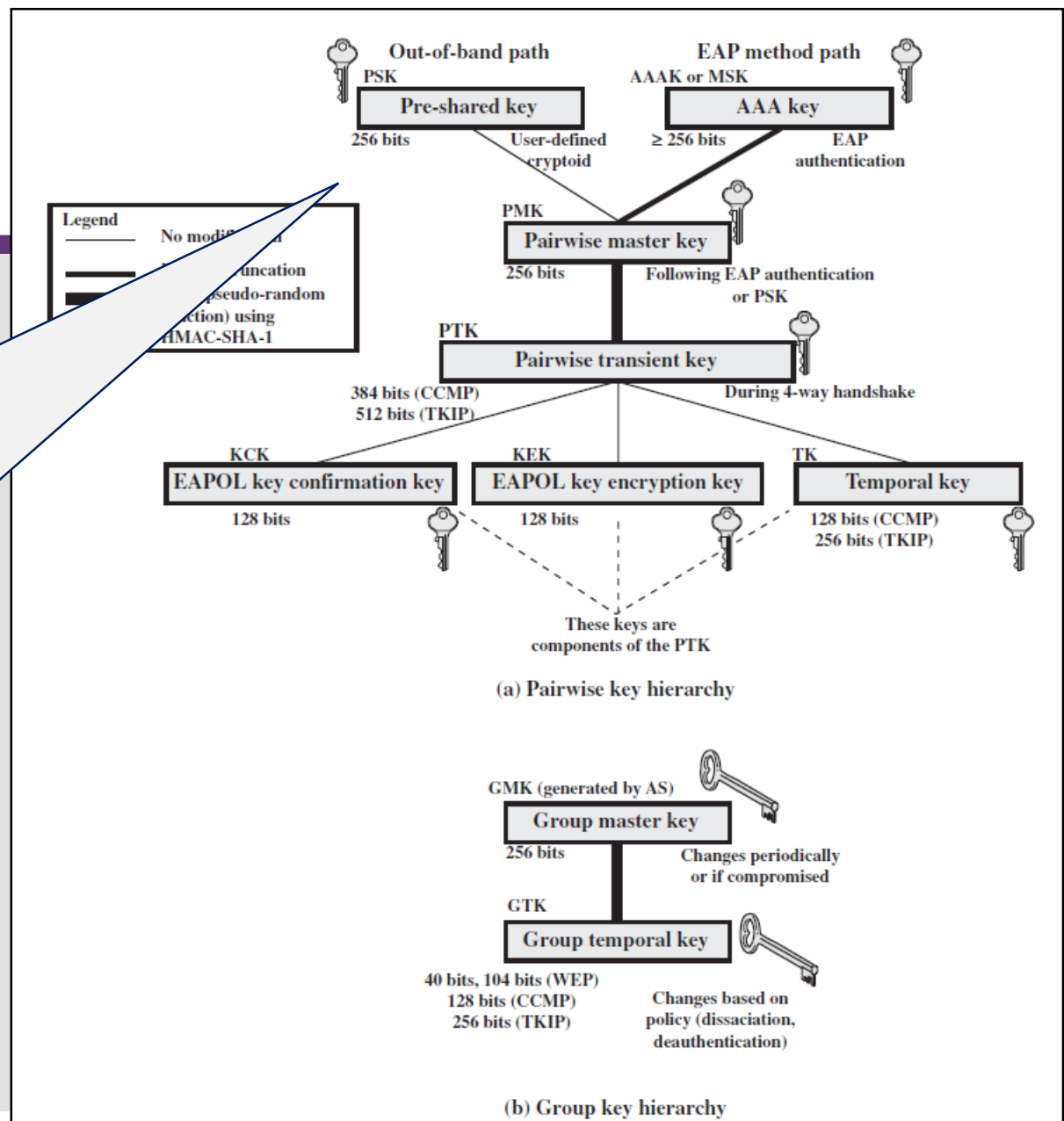
(a) Pairwise key hierarchy



(b) Group key hierarchy

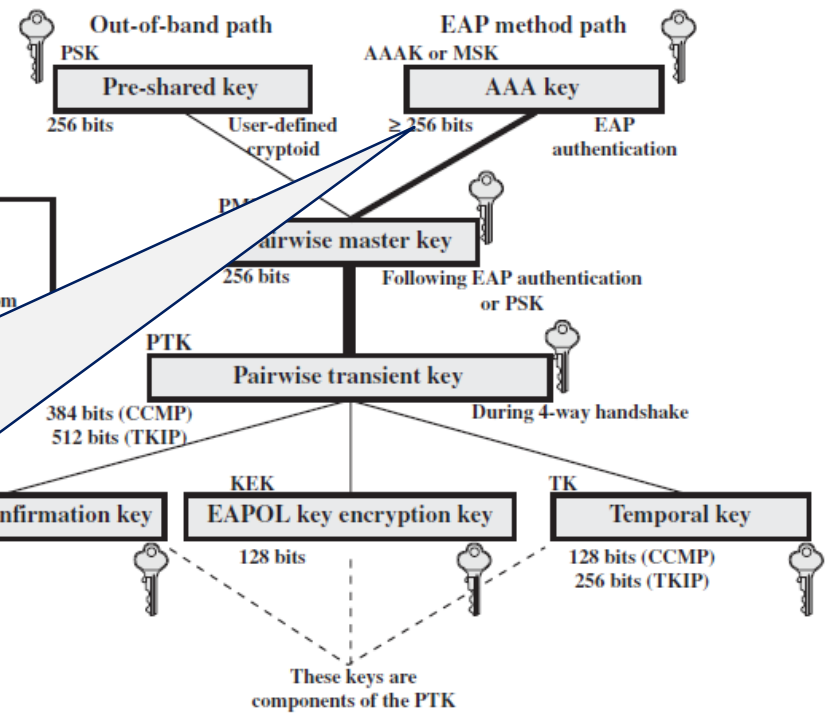
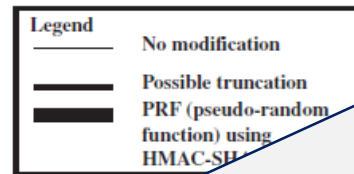
802.11i Key Management Phase

A pre-shared key (PSK) is a secret key shared by the AP and a STA, and installed **in some fashion outside the scope of IEEE 802.11i.**

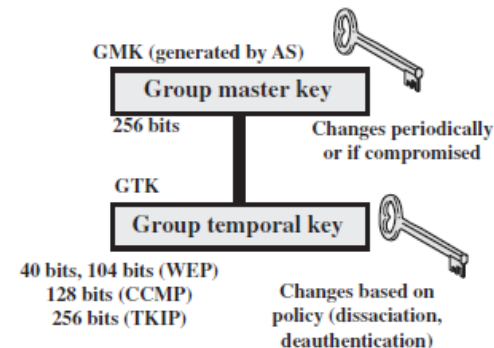


802.11i Key Management Phase

The other alternative is the master session key (MSK), also known as the AAAK, which is generated using the IEEE 802.1X protocol during the authentication phase.

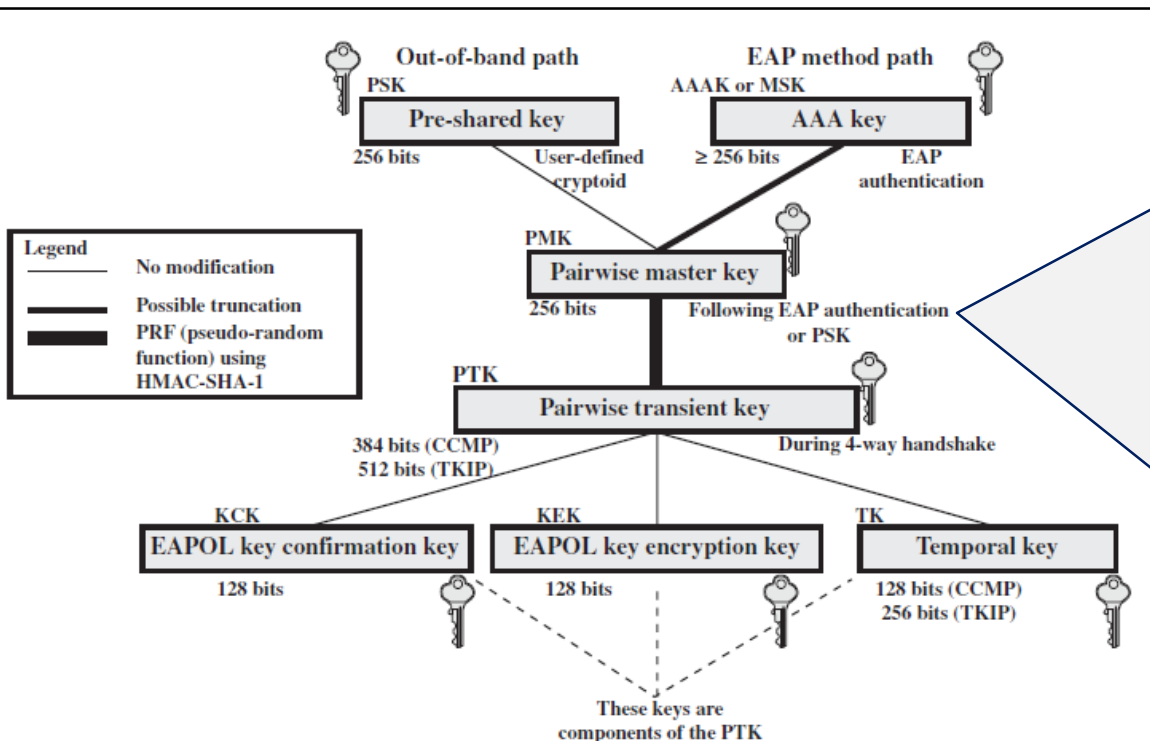


(a) Pairwise key hierarchy

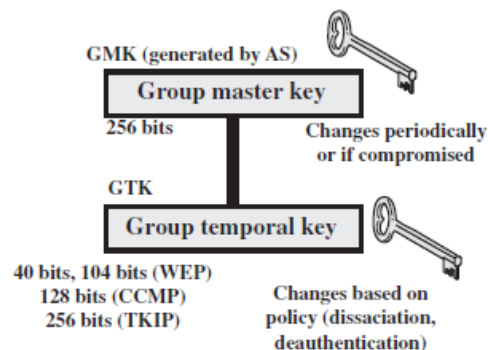


(b) Group key hierarchy





(a) Pairwise key hierarchy

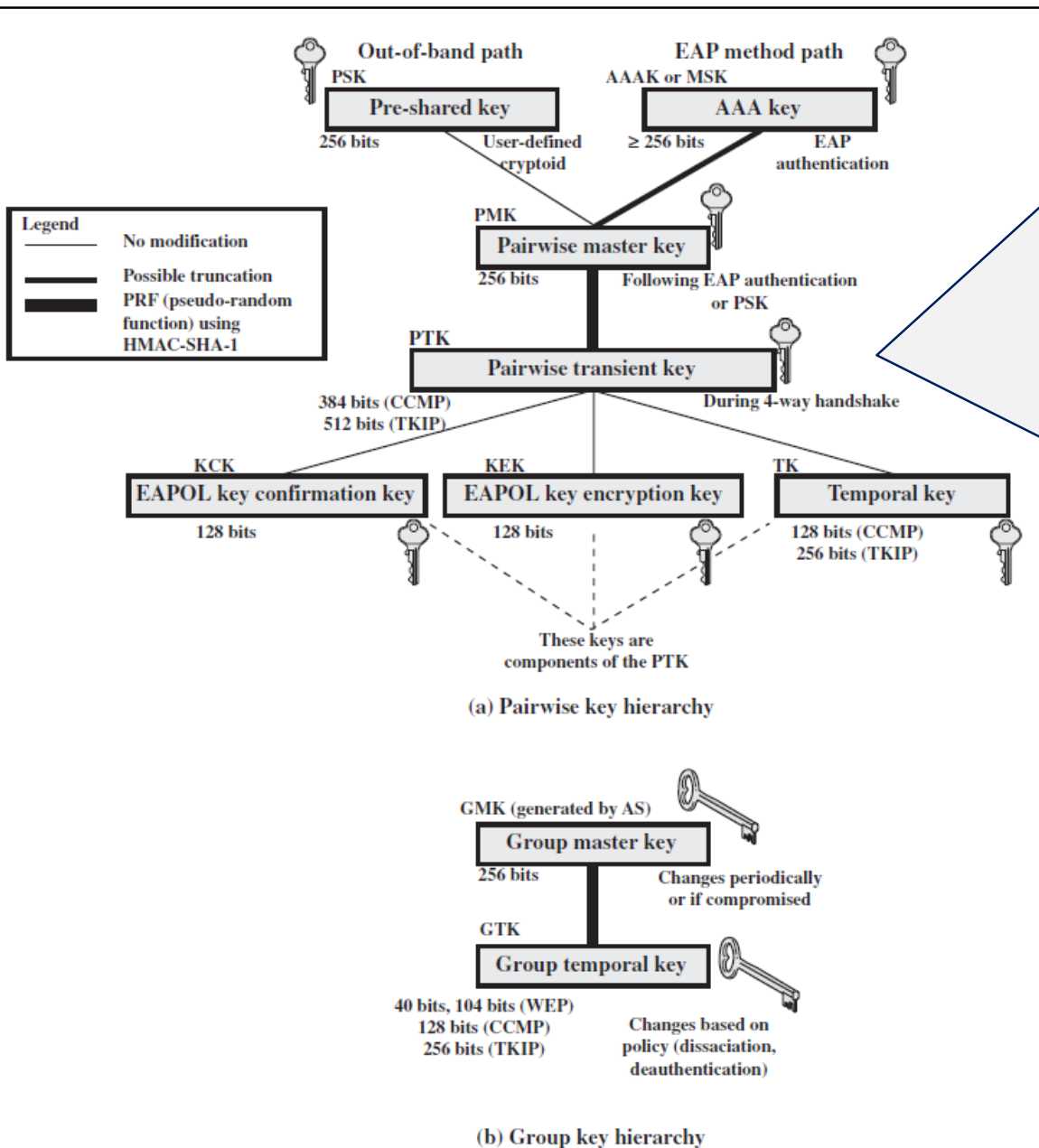


(b) Group key hierarchy

The pairwise master key (PMK) is derived from the master key .

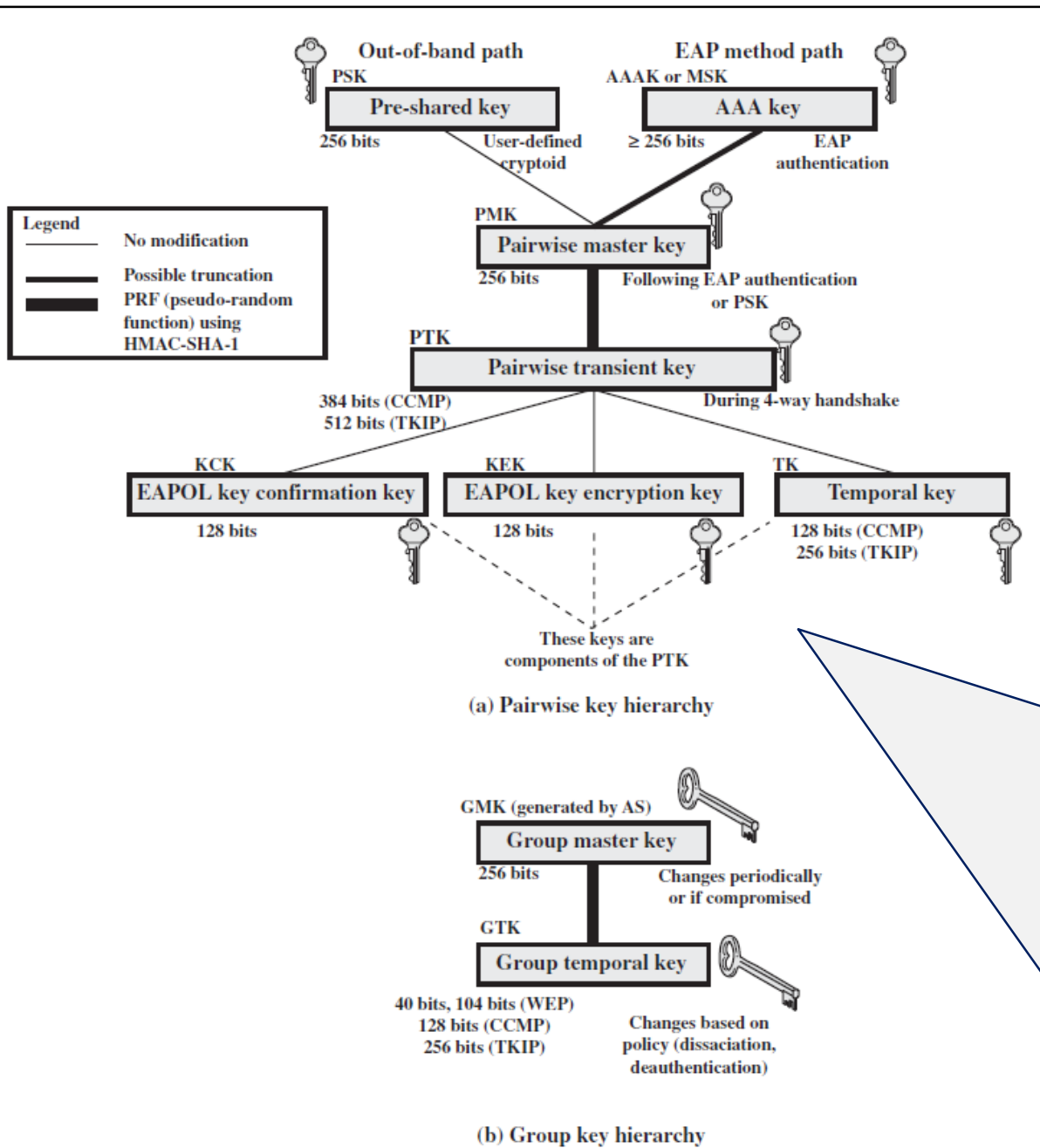
As follows:

- 1. If a PSK is used, then the PSK is used as the PMK;**
- 2. if a MSK is used, then the PMK is derived from the MSK by truncation (if necessary).**



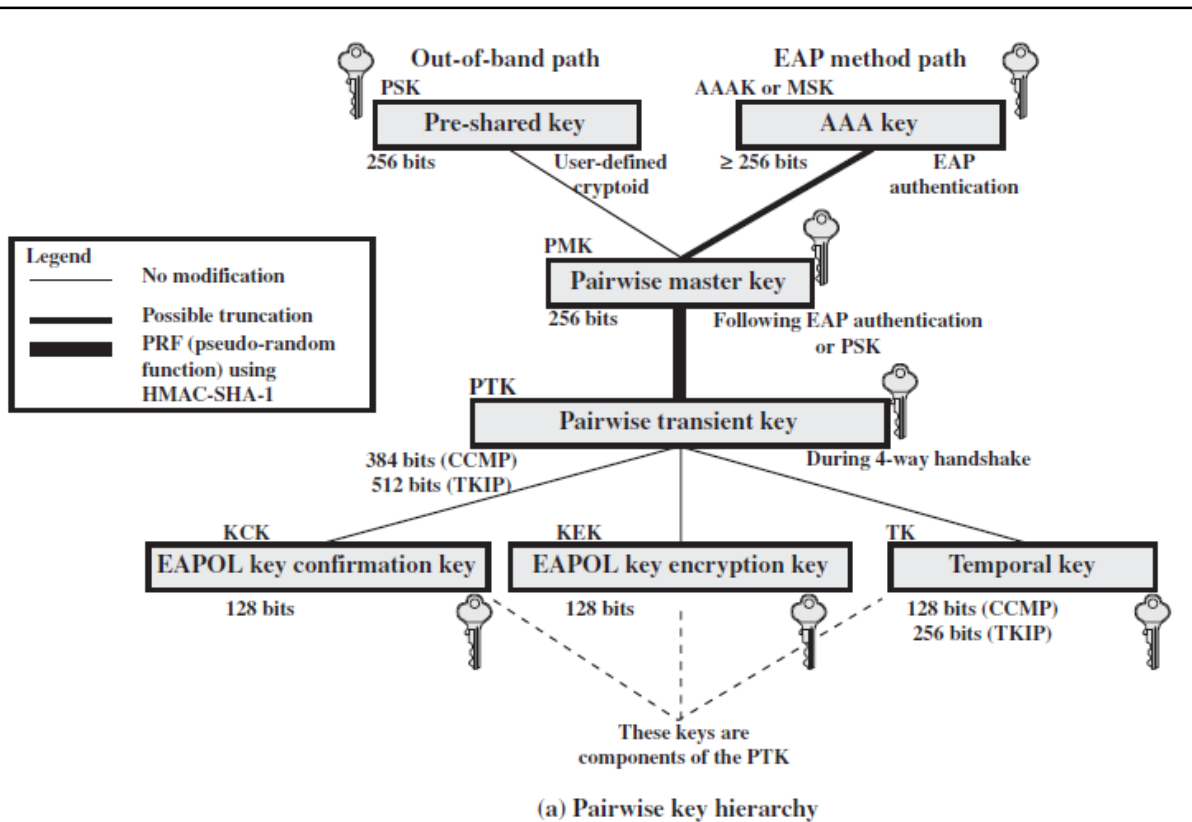
The PMK is used to generate the pairwise transient key (PTK), which in fact consists of three keys to be used for communication between an STA and AP after they have mutually authenticated.

To derive the PTK, the **PMK, the MAC addresses of the STA and AP, and nonce's generated** when needed are all input to the HMAC-SHA-1 function.

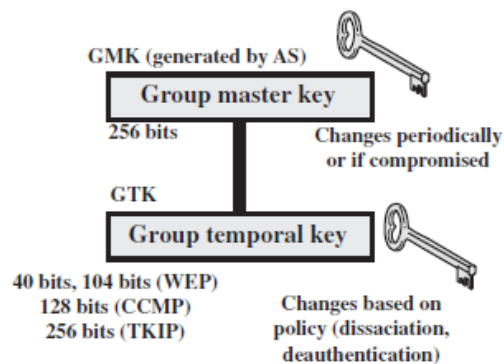


The three parts of the PTK are as follows.

- EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK):** Supports the integrity and data origin authenticity of STA-to-AP control frames . It also performs an access control function.
- EAPOL Key Encryption Key (EAPOL-KEK):** Protects the confidentiality of keys and other control frames.
- Temporal Key (TK):** Provides the **actual protection for user traffic**.



(a) Pairwise key hierarchy



(b) Group key hierarchy

GROUP KEYS Group keys are used for **multicast** communication in which one STA sends MPDU's to multiple STAs.

Group Master Key (GMK)

The GMK is a key-generating key used with other inputs to derive the Group Temporal Key (GTK). The GTK is distributed securely using the pairwise keys that are already established. The GTK is changed every time a device leaves the network.

802.11i Protected Data Transfer Phase

- have **two schemes** for protecting data
- **Temporal Key Integrity Protocol (TKIP)**
 - software changes only to older WEP
 - adds 64-bit message integrity code (MIC)
 - encrypts MPDU plus MIC value using RC4
- **Counter Mode-CBC MAC Protocol (CCMP)**
 - uses the cipher block chaining (CBC) message authentication code (CBC-MAC) for integrity
 - uses the CTR block cipher mode of operation with AES for encryption

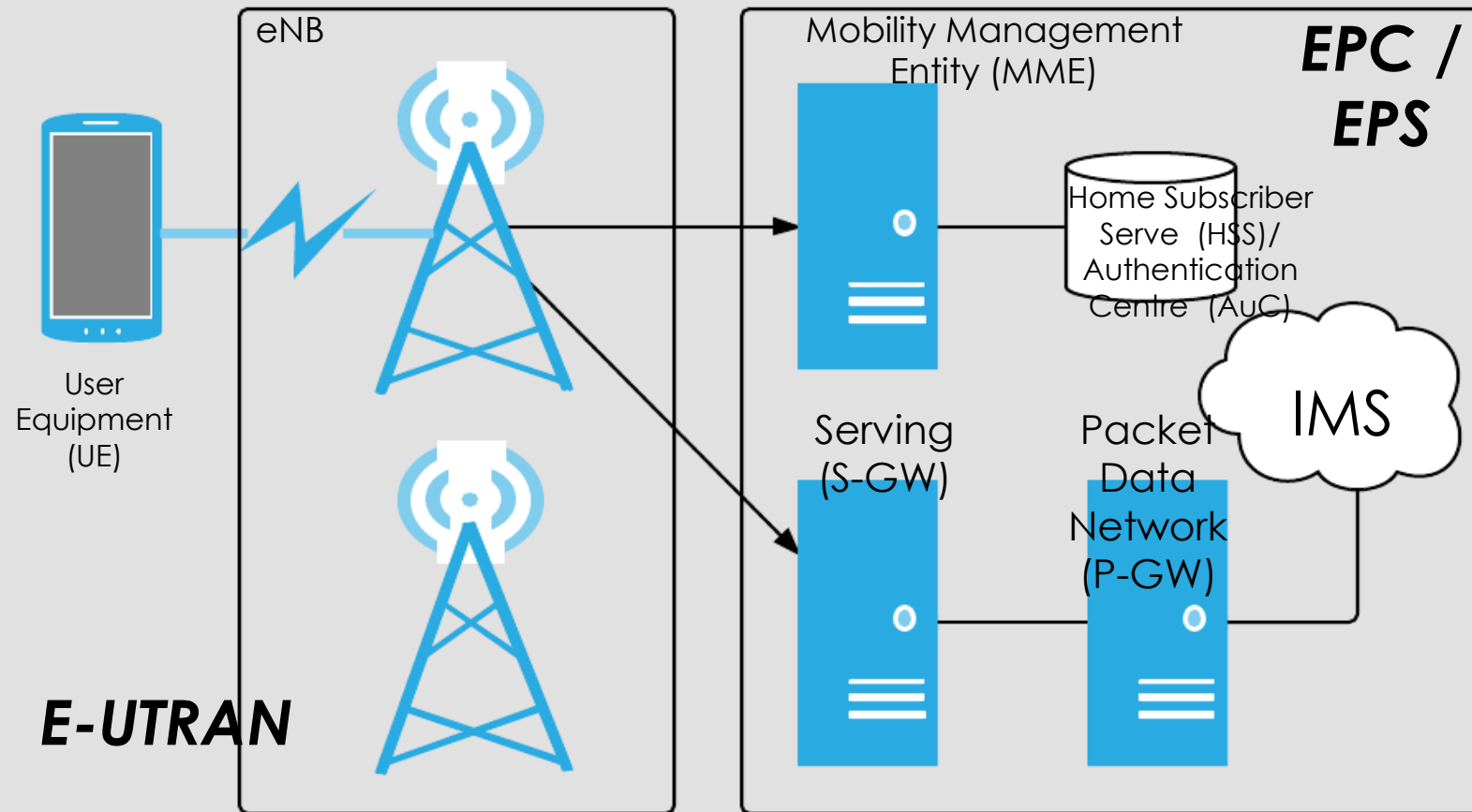
LTE

- **LTE (Long Term Evolution)**
- **The most common type of 4G cellular standard**
- **A completely packet-switched technology for both data and voice (VoLTE - voice over LTE)**
- **3 main components:**
 - Evolved Universal Terrestrial Radio Access Network (E-UTRAN) - Radio Network
 - Evolved Packet Core (EPC) / Evolved Packet System (EPS) - Backhaul
 - IP Multimedia Subsystem (IMS) - Extended backhaul functionality

LTE Other Components

- **User equipment (UE)**
 - your mobile phone
- **Evolved Node B (eNodeB)**
 - a complex base station that handles radio communications with multiple devices in the cell and carries out radio resource management and handover decisions
- **Mobility Management Entity (MME)**
- **Serving Gateway (S-GW)**
- **Packet Data Network Gateway (P-GW)**
- **Home Subscriber Server (HSS)**
- **Authentication Centre (AuC)**

LTE



LTE Security Requirements

- EPS shall provide a **high level of security**
- EPS should provide **protection against threats and attacks**
- Appropriate **traffic protection measures** should be provided
- EPS shall ensure that **unauthorized users cannot establish communications** through the system
- EPS shall allow a network to **hide its internal structure** from the terminal
- **Security policies shall be under home operator control** (in case for roaming)

LTE Security Requirements

- EPS shall provide several **appropriate levels of user privacy** for communication, location and identity
- Communication contents, origin and destination shall be **protected against disclosure to unauthorized parties**
- EPS shall be able to **hide user location from unauthorized parties**, including another party with which the user is communicating
- Etc.....

High-Level Threats to LTE

- **Tracking identity, privacy or devices**
- **Jamming handsets or network equipment or other attacks on availability**
- **Physical attacks on base stations or network equipment**
- **Threats related to interaction between base stations, or dropping to older standards or other networks**
- **Cloning of SIM card**
- **Etc.....**

LTE Security Mechanisms

- **Continue to use the USIM hardware module**
- **Subscriber and network authentication via Authenticated Key Agreement (AKA)**
- **Cryptography**
 - Algorithms
 - Key hierarchy
 - Protected Interfaces
 - Protected Planes
- **Independent Domains**
 - Access Stratum (AS)
 - Non-access Stratum (NAS)

LTE Hardware Token

- **The LTE USIM is identical to UMTS (3G)**
- **Contains a new hardware protected 128-bit key: K**
 - Keys are derived from K as needed
 - AuC stores an IMSI and K
(International Mobile Subscriber Identity (IMSI): an unique SIM card identity number)

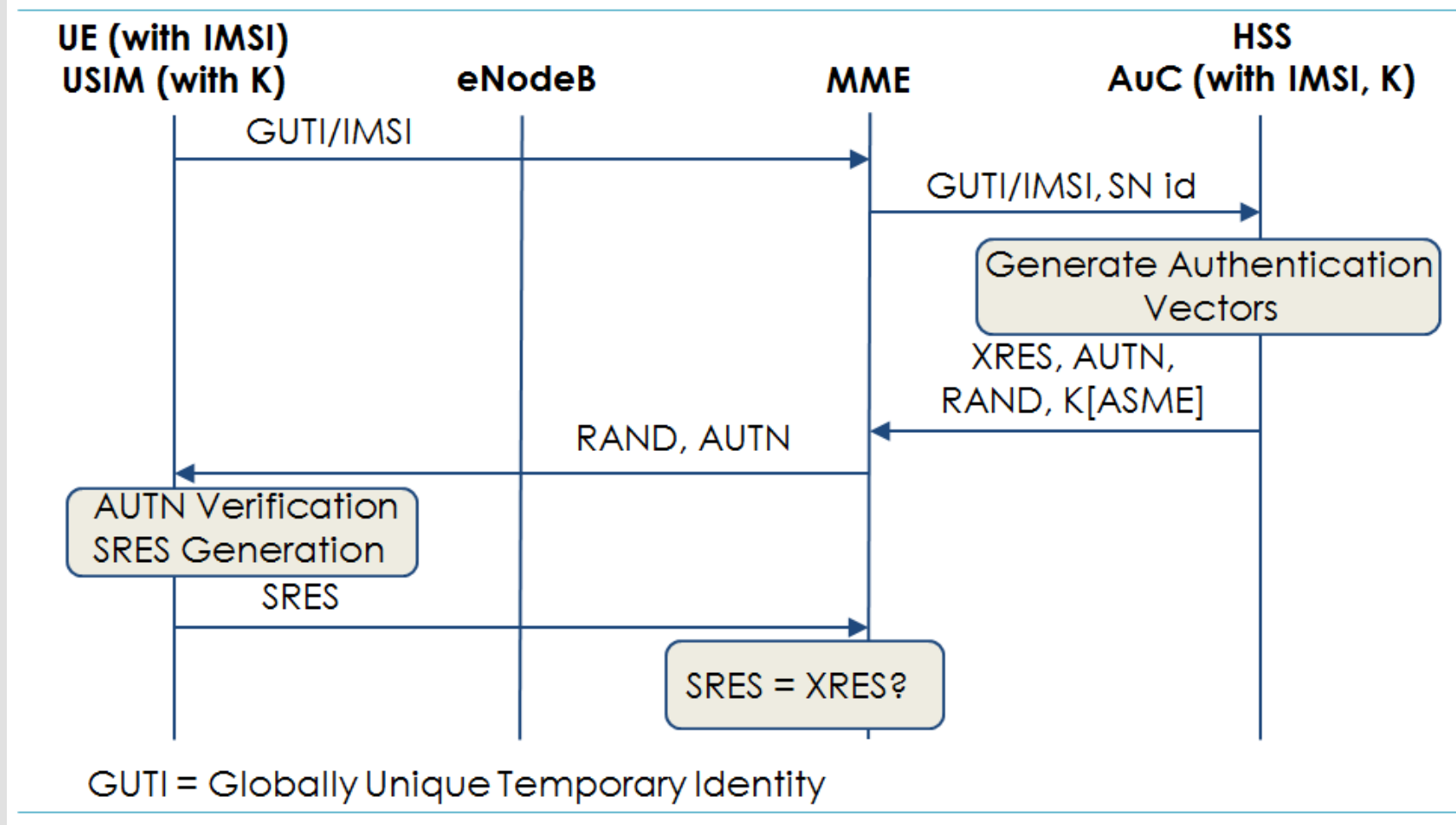
LTE AKA

- **Very similar to GSM and UMTS AKA**
 - Anchored in hardware token (UICC/USIM)
- **2G SIMs are deprecated**
 - They are unable to authenticate to LTE
 - UEs may drop down to UMTS or GSM
- **We will discuss LTE AKA in detail**
 - Overall ladder diagram
 - Generation of AKA security parameters
 - Verification within the USIM

LTE AKA

- **UMTS and LTE AKA are extremely similar**
 - Originally specified in [TS 33.102](#)
- **Largest update to AKA: network separation**
 - Prevents a breach on one telco's network to spill into another's
 - Network identity is bound to certain keys
 - AKA directly authenticates network identity
- **New key derivation function specified in LTE**

LTE AKA Ladder Diagram



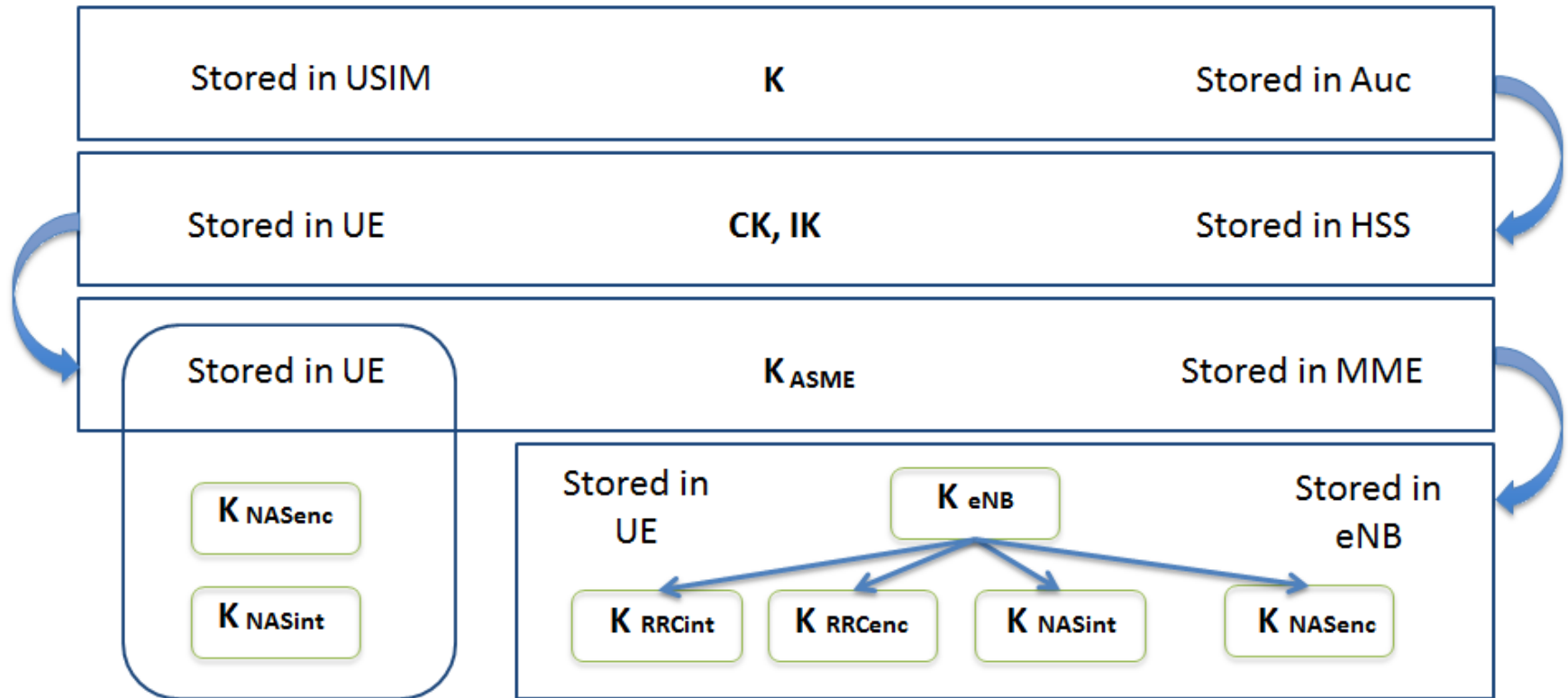
Authentication Vectors (AVs) Generation

- The authentication vectors (AVs) are necessary to perform AKA
- They are requested by the MME
 - Generated by the HSS/AuC
- **LTE Authentication Vector = (XRES || AUTN || RAND || K[ASME])**
- **AK = Anonymity key**
- **AUTN = (SQN xor AK || AMF || MAC)**
 - MAC = Message authenticate code in this instance
- **AMF = Authentication Management Field**
- **CK = Cipher key**
- **IK = Integrity key**
- **KDF = Key derivation function**
- **MAC = A message authentication function**
- **SQN = Sequence Number**
- **XRES = Expected response**
- **SRES = Signed response**

Cryptography in LTE

- **Large change to cryptographic key structure**
 - Introduced a new set of intermediate keys
 - Unique keys for each connection/bearer - large complicated hierarchy
- **Similar to UMTS, we have 2 sets of algorithms for confidentiality and integrity**
 - EEA1/EIA1 - based on SNOW 3G
 - EEA2/EIA2 - based on AES
 - EEA3/EIA3 - based on ZUC (China)
- **Control Plane (CP) and User Plane (UP) may use different algorithms**

Key Hierarchy



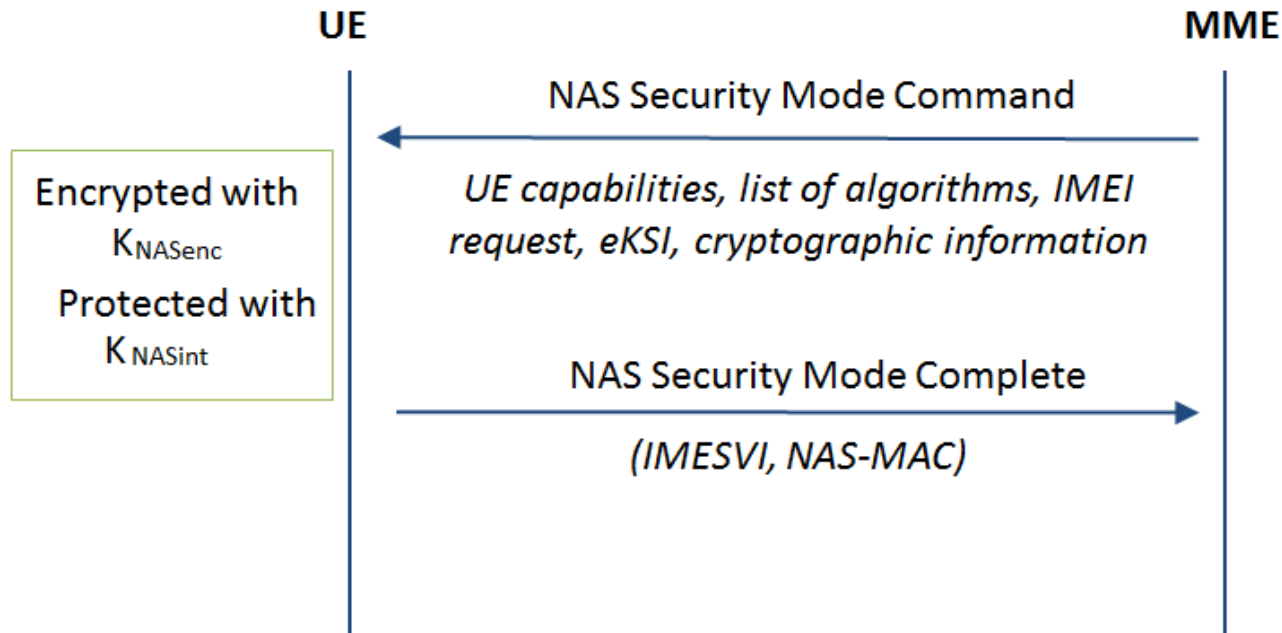
Key Discussion

- **K** – The master key. Permanent pre-shared key stored in hardware. Located on USIM and HSS/AuC
- **CK** and **IK** – Cipher key and Integrity key
- **K[ASME]** – Local master. The serving network ID (SNid) is used to derive this key in addition to CK and IK.
- **K[eNB]** – Used to derive additional keys used in handoff
- **K[NASent]** & **K[NASint]**- Protection of NAS traffic
- **K[RRCent]** & **K[RRCint]** - Protection of RRC traffic

LTE Non-Access Stratum (NAS)

- **A functional layer between the core network and UE**
- **Used to manage the establishment of communication sessions and for maintaining continuous communications with UE as it moves**
- **Security-related signaling between UE and the backhaul**
 - Algorithm selection occurs between the UE and the MME
 - MME contains a list of confidentiality and integrity algorithms in a priority order
- **NAS negotiation precedes AKA**
- **Negotiation begins when an MME sends an integrity protected Security Mode Command to UE**
 - Contains evolved key set identifier (eKSI), list of security capabilities and algorithms, IMSI request, and additional cryptographic information
- **The UE responds with an integrity protected encrypted message called the NAS Security Mode Complete containing its IMEI and a MAC of the message**

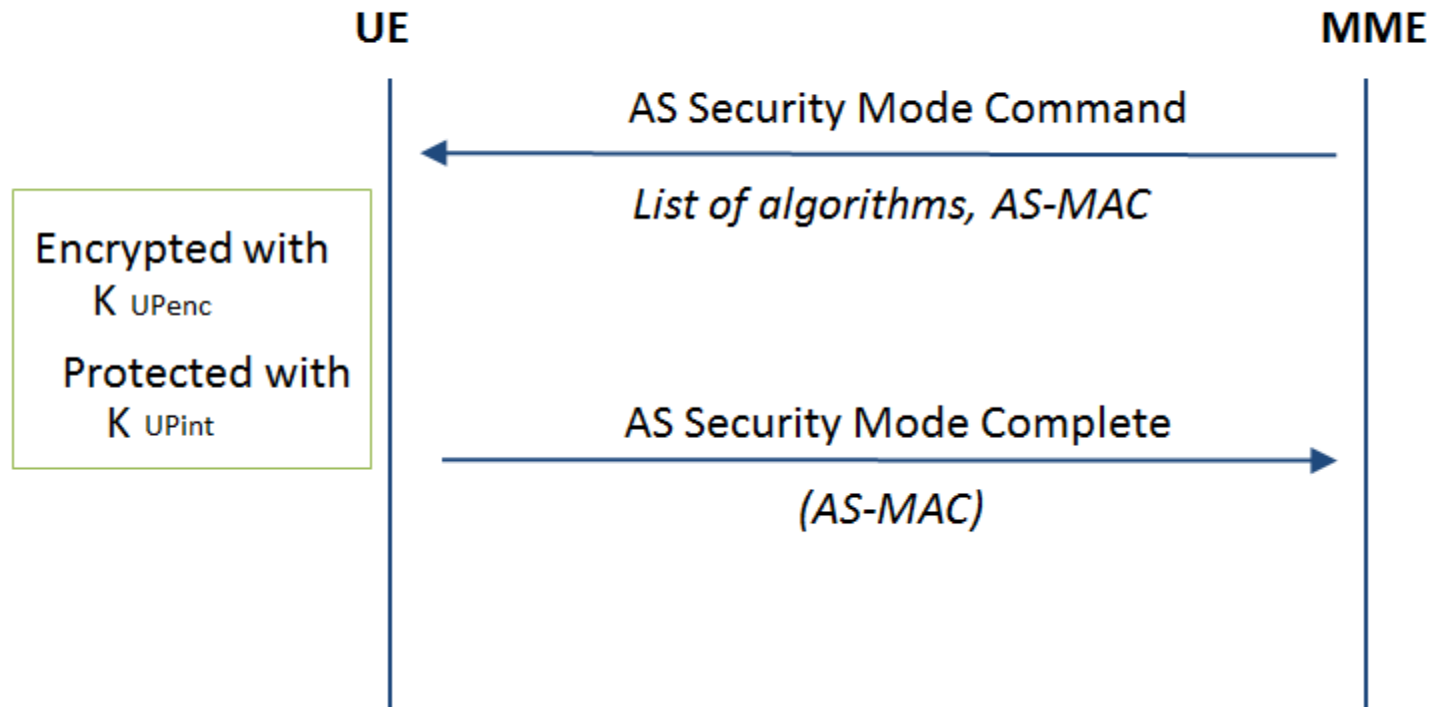
LTE NAS Negotiation



LTE Access Stratum

- **Signaling between UE and eNB**
 - Algorithm selection occurs between these components
 - eNB contains a list of confidentiality and integrity algorithms in a priority order
- **AS protection is optional**

LTE AS Negotiation



Signaling Protection

- **Network components create protected channels for each component that it is communicating with, for example:**
 - UE and eNB communicate with a unique key
 - UE and MME communicate with a unique key
 - eNB and S-GW communicate with a unique key
- **NAS security is *always* setup if a UE is registered to the network**
- **AS security is setup as an *option***
- **A common claim is that LTE is “fully encrypted”**
 - Initial radio access and signaling is not, but no data is being transmitted at that point
 - The standard states that ciphering may be provided to Radio Resource Control (RRC)-signaling
 - “RRC signaling confidentiality is an operator option.”



Handover

- **Unfortunately, UEs are constantly on the move**
- **This causes the need to be able to switch from eNB to eNB, and possibly from network to network**
- **The procedures for this are quite complex as keys and other protected information needs to be transferred or renegotiated**
 - Cryptographic keys and encryption/integrity algorithms may need to be changed
 - Refer to any LTE Security book for additional details and the relevant 3GPP standard for additional information

Security Contexts

- **Security contexts are a collection of security-related information**
 - Algorithms, keys, and other parameters
- **Many contexts are defined:**
 - NAS
 - AS
 - Etc.....
- **Depending on sensitivity they are stored in the USIM or the RAM of the UE**

Backwards Compatibility

- **At times LTE service may be lost and a 2G or 3G system may be available**
- **Security Contexts are mapped from one system to another**
- **A NAS security context is generated if moving to LTE**
- **K[ASME] is used to derive GSM/UMTS security contexts if needed**
- **Once mapping has occurred - a new native security context is re-established as soon as possible**
 - AKA can be run again as well

SIM Cloning

- **Clone of SIM card using Side-Channel Attack**
- **Can call and receive SMS as the original SIM**
- **Lead to many attacks to a lots of apps that require OTP (e.g. to reset password)**
- **Cloning 3G/4G SIM Cards With A PC And An Oscilloscope: Lessons Learned In Physical Security**
- **<https://www.youtube.com/watch?v=qKCQ1KL9GEc>**
(demo on 24:37)
- **<http://yuyu.hk/files/us-15-Yu-Cloning-3G-4G-Sim-Cards.pdf>**