NETMANIAS
www.netmanias.com

NMC
CONSULTING GROUP
www.nmcgroups.com

LTE Security II

- NAS and AS Security -

October 14, 2014

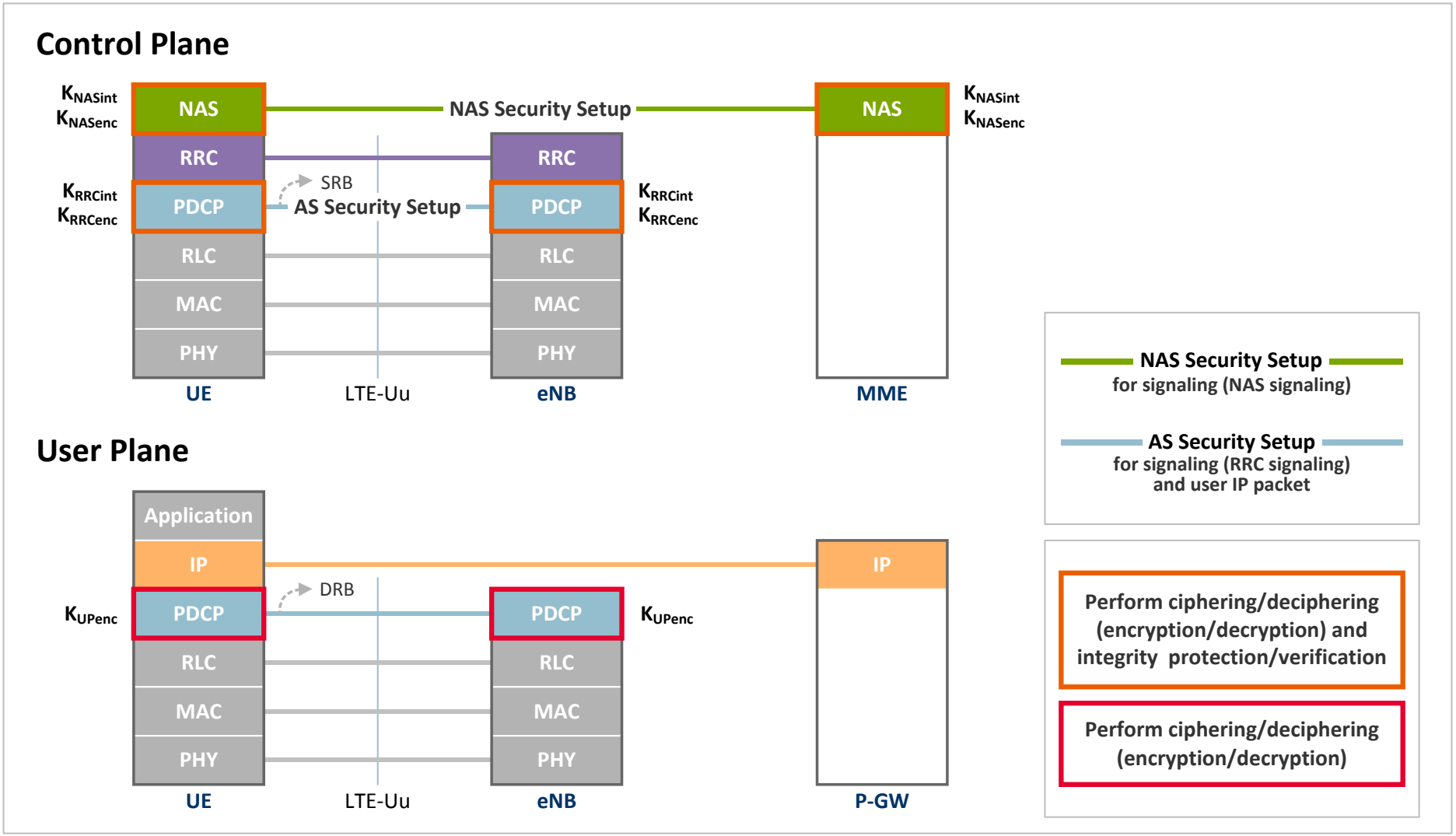
(Initial Release: August 21, 2012)

NMC Consulting Group (tech@netmanias.com)

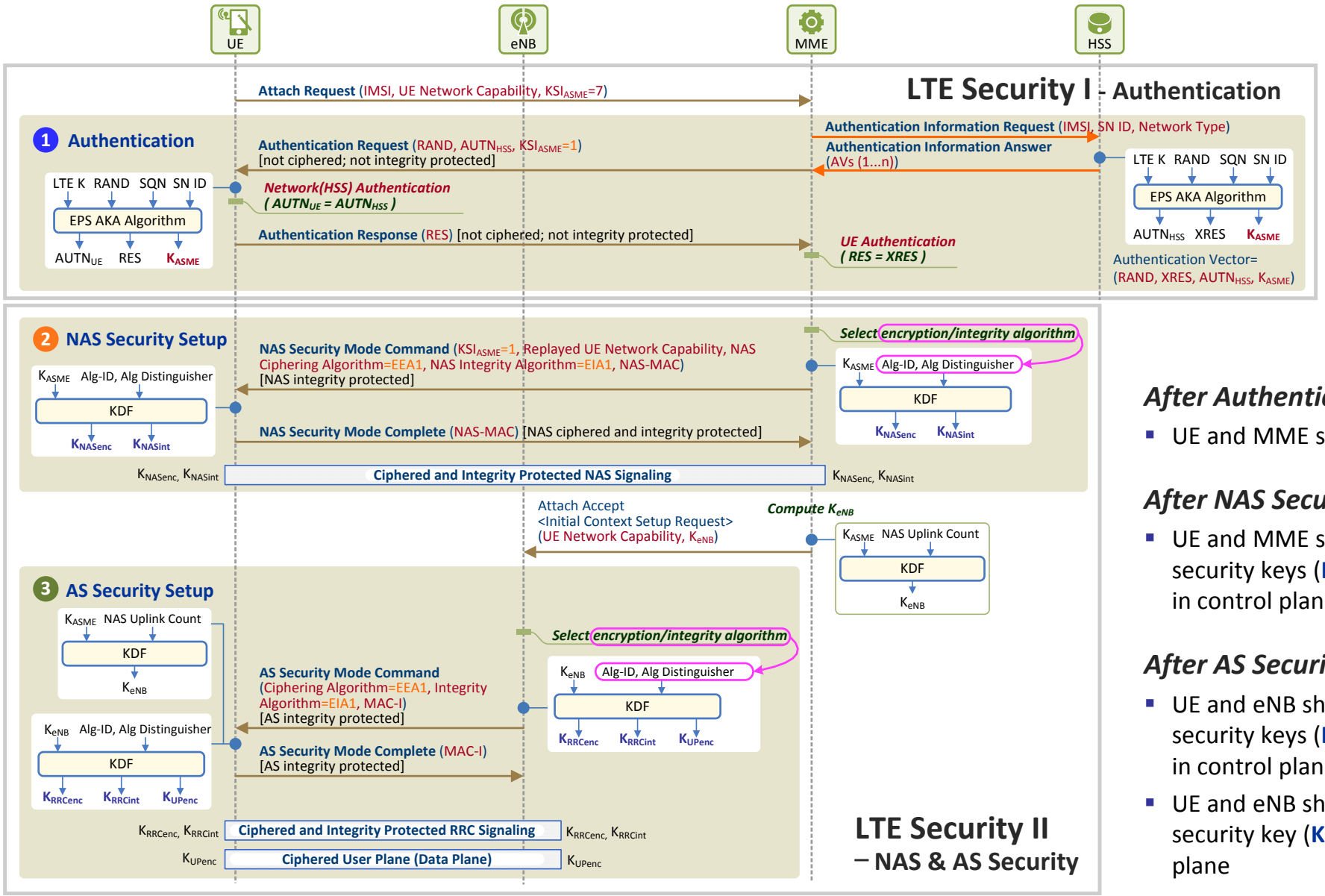
www.netmanias.com
www.nmcgroups.com

About NMC Consulting Group
NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.

Protocol Stack for NAS and AS Security Setup



Overview of LTE Security



After Authentication

- UE and MME share K_{ASME}

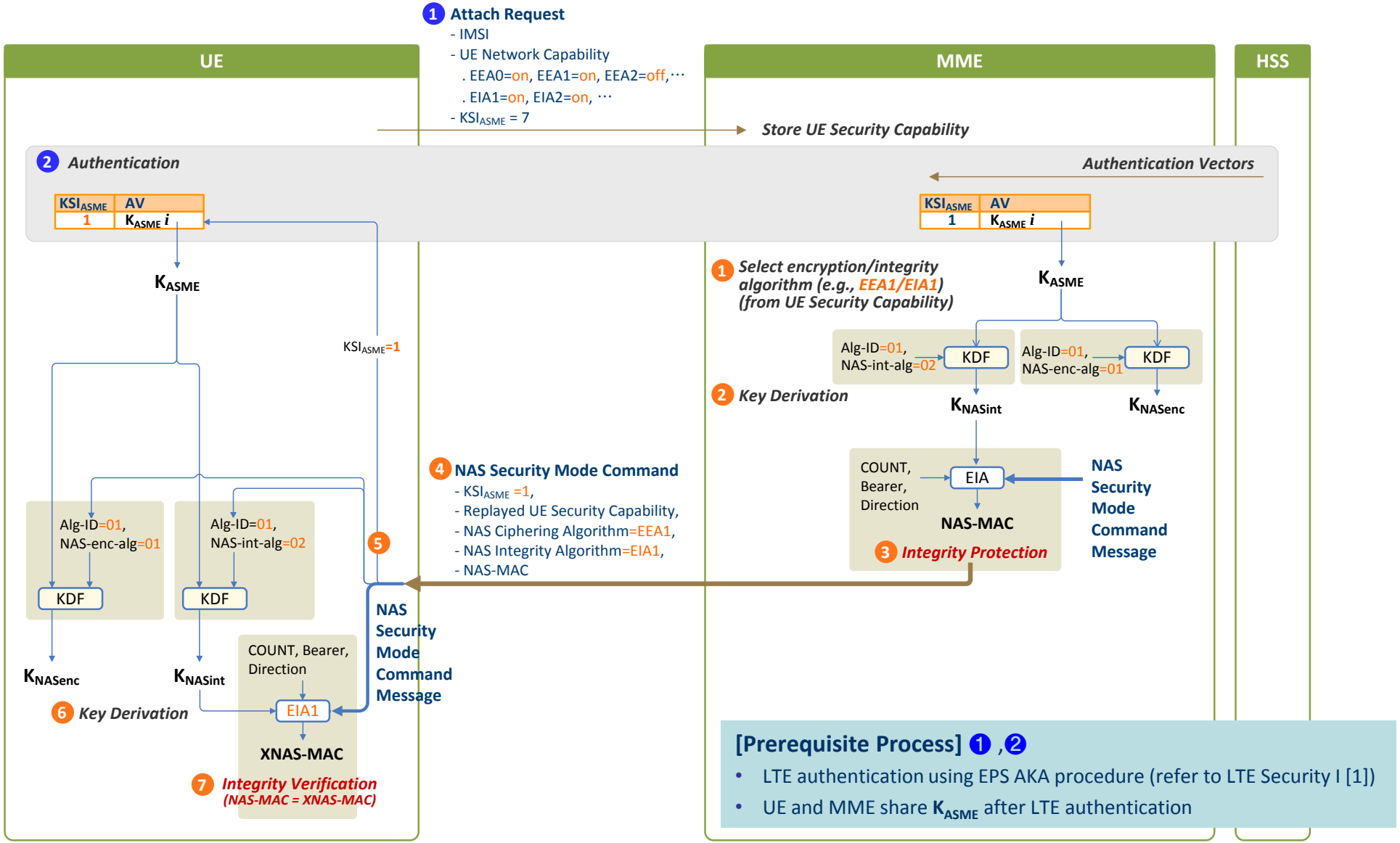
After NAS Security Setup

- UE and MME share NAS security keys (K_{NASenc}, K_{NASint}) in control plane

After AS Security Setup

- UE and eNB share AS security keys (K_{RRCenc}, K_{RRCint}) in control plane
- UE and eNB share a AS security key (K_{UPenc}) in user plane

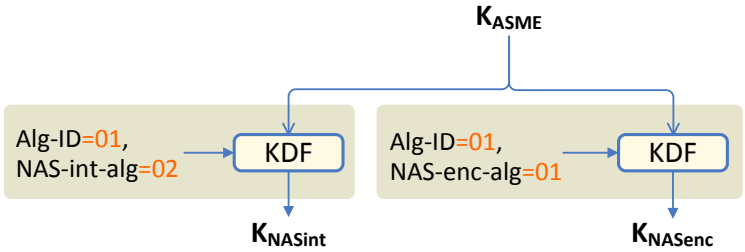
[NAS Security Setup] Security Mode Command (1)



[NAS Security Setup] Security Mode Command (2)

❶ [MME] Selection of security algorithms

- Selects encryption and integrity protection algorithms applied to NAS messages based on UE Security Capability information (e.g. EEA1 and EIA1)



❷ [MME] Derivation of NAS security keys, K_{NASint} and K_{NASenc}

- Derives K_{NASint} and K_{NASenc} with the following input parameters:
  - K_{ASME} derived in ❷ (authentication process)
  - Security algorithm ID selected in ❶
  - Security algorithm distinguisher

K_{NASint} = KDF (K_{ASME}, NAS-int-alg, Alg-ID)
K_{NASenc} = KDF (K_{ASME}, NAS-enc-alg, Alg-ID)

Security Algorithm ID

Algorithm ID	Description	Value
128-EEA0	Null ciphering algorithm	0000
128-EEA1	SNOW 3G	0001
128-EEA2	AES	0010
128-EEA3	ZUC (optional)	0011
128-EIA1	SNOW 3G	0001
128-EIA2	AES	0010
128-EIA3	ZUC (optional)	0011

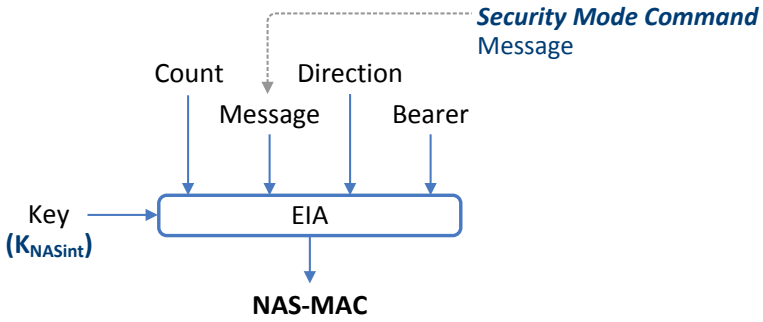
Algorithm Distinguisher

Algorithm Distinguisher	Value
NAS-enc-alg	0x01
NAS-int-alg	0x02
RRC-enc-alg	0x03
RRC-int-alg	0x04
UP-enc-alg	0x05
UP-int-alg*	0x06

* for relay nodes only, not discussed herein

❸ [MME] Calculation of NAS-MAC for integrity protection

- Generates ***Security Mode Command*** message and calculates **NAS-MAC** for the message using K_{NASint}



Calculation of NAS-MAC

Input Parameters for EIA Algorithm

Input Parameter	Description
Count	32-bit downlink NAS count
Message	NAS Message, ***Security Mode Command*** message herein
Direction	1-bit direction of message transmission, set to 1 for downlink
Bearer	5-bit bearer ID, constant value (set to 0)
K_{NASint}	128-bit Integrity protection key for NAS messages

[NAS Security Setup] Security Mode Command (3)

❹ [UE ← MME] Transmitting the *Security Mode Command* message

- ***Security Mode Command***: Integrity protected but not ciphered
- MME sends the ***Security Mode Command*** *(KSI_{ASME}, Replayed UE Security Capability, NAS Ciphering Algorithm, NAS Integrity Protection Algorithm)* message with NAS-MAC to UE

Information Element	Description
KSI_{ASME}	3-bit value associated with a K_{ASME}, allocated by MME and used to identify the K_{ASME}, (KSI_{ASME} = 1 herein)
Replayed UE Security Capability	UE Security Capability included in the ***Attach Request*** message sent by UE (parts of UE Network Capability)
NAS Ciphering Algorithm	NAS ciphering algorithm selected by MME, EEA1 herein
NAS Integrity Protection Algorithm	NAS integrity protection algorithm selected by MME, EIA1 herein

❺ [UE] Setting of KSI_{ASME}

- Sets KSI_{ASME} to the same value of KSI_{ASME} in the ***Security Mode Command*** message
  (KSI_{ASME} : Identifier of K_{ASME}. Used on behalf of K_{ASME} between UE and MME)

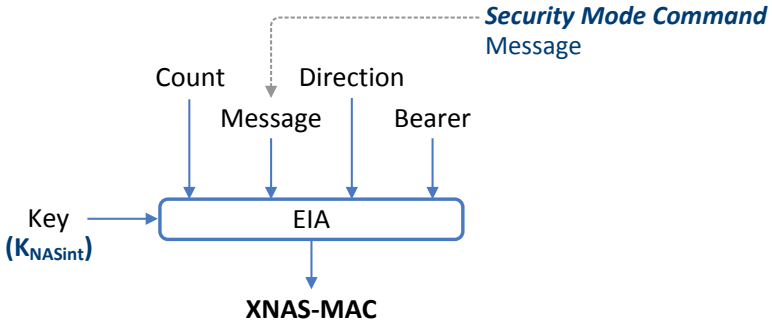
❻ [UE] Derivation of NAS security keys, K_{NASint} and K_{NASenc}

- Derives K_{NASint} and K_{NASenc} with the following the following input parameters:
  - K_{ASME} derived in ❷ (authentication process)
  - Security algorithm ID delivered in ❹
  - Security algorithm distinguisher

K_{NASint} = KDF (K_{ASME}, NAS-int-alg, Alg-ID)
K_{NASenc} = KDF (K_{ASME}, NAS-enc-alg, Alg-ID)

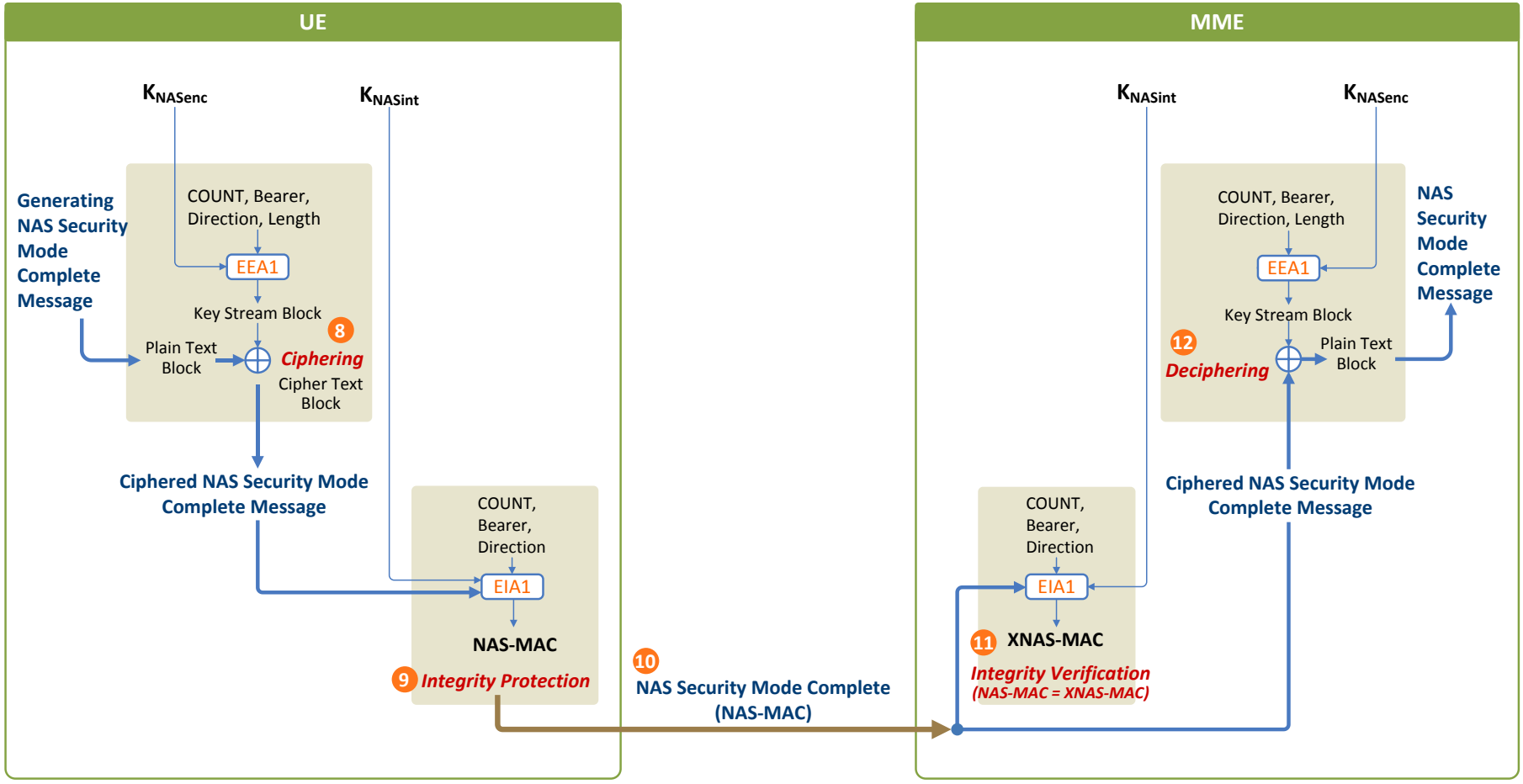
❼ [UE] Integrity verification for the *Security Mode Command* message

- Calculates XNAS-MAC, and performs integrity verification using K_{NASint} by comparing NAS-MAC with the calculated XNAS-MAC



Calculation of XNAS-MAC

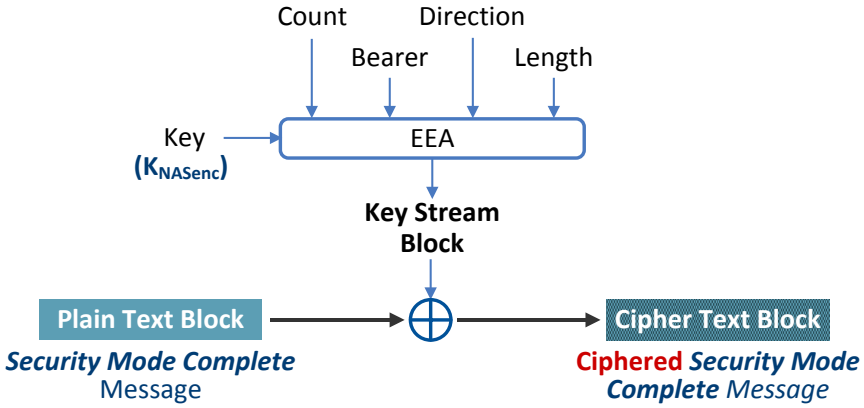
[NAS Security Setup] Security Mode Complete (1)



[NAS Security Setup] Security Mode Complete (2)

❽ [UE] Ciphering message using the selected ciphering algorithm

- Generates ***Security Mode Complete*** message, then encrypts the message using K_{NASenc}



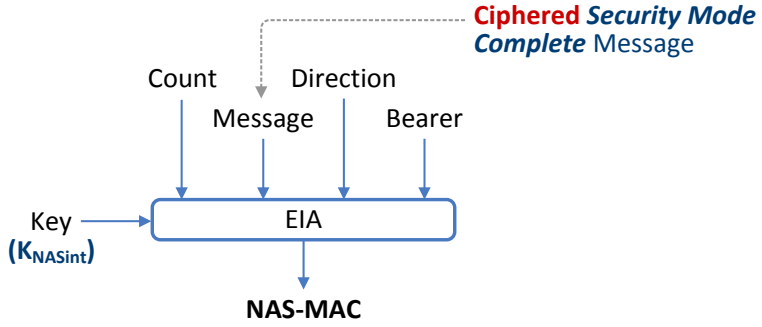
Ciphering of Security Mode Complete Message

Input Parameters for EEA Algorithm

Input Parameter	Description
Count	32-bit uplink NAS count
Bearer	5-bit bearer ID, constant value (set to 0)
Direction	1-bit direction of message transmission, set to 0 for uplink
Length	length of key stream block
K_{NASenc}	128-bit ciphering key for NAS messages

❾ [UE] Calculation of NAS-MAC for integrity protection

- Calculates NAS-MAC for the ciphered ***Security Mode Complete*** message using K_{NASint}



Input Parameters for EIA Algorithm

Input Parameter	Description
Count	32-bit uplink NAS count
Message	NAS Message, ***Security Mode Complete*** message herein
Direction	1-bit direction of message transmission, set to 0 for uplink
Bearer	5-bit bearer ID, constant value (set to 0)
K_{NASint}	128-bit integrity protection key for NAS messages

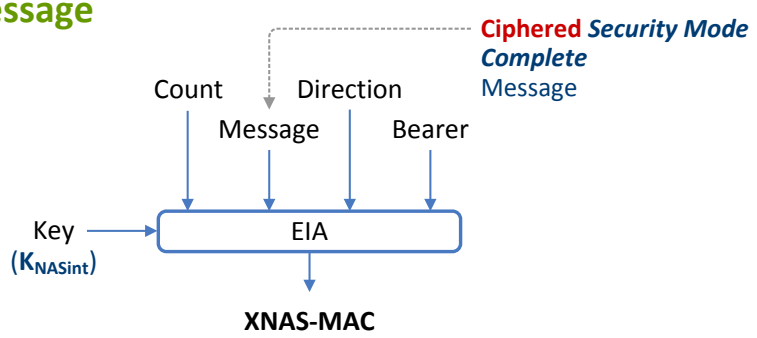
[NAS Security Setup] Security Mode Complete (3)

⑩ [UE → MME] Transmitting the *Security Mode Complete* message

- ***Security Mode Complete***: Ciphered and integrity protected
- UE sends the ***Security Mode Complete*** message with NAS-MAC to MME

⑪ [MME] Integrity verification for the *Security Mode Complete* message

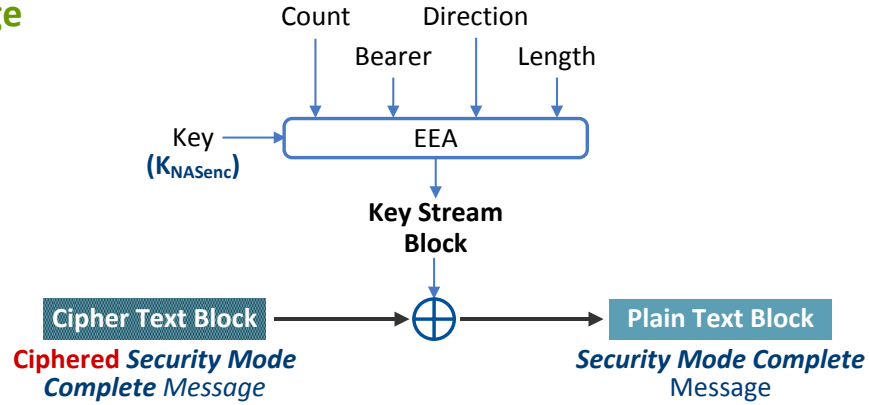
- Calculates XNAS-MAC
- Performs integrity verification using K_{NASint} by comparing NAS-MAC with the calculated XNAS-MAC



Calculation of XNAS-MAC

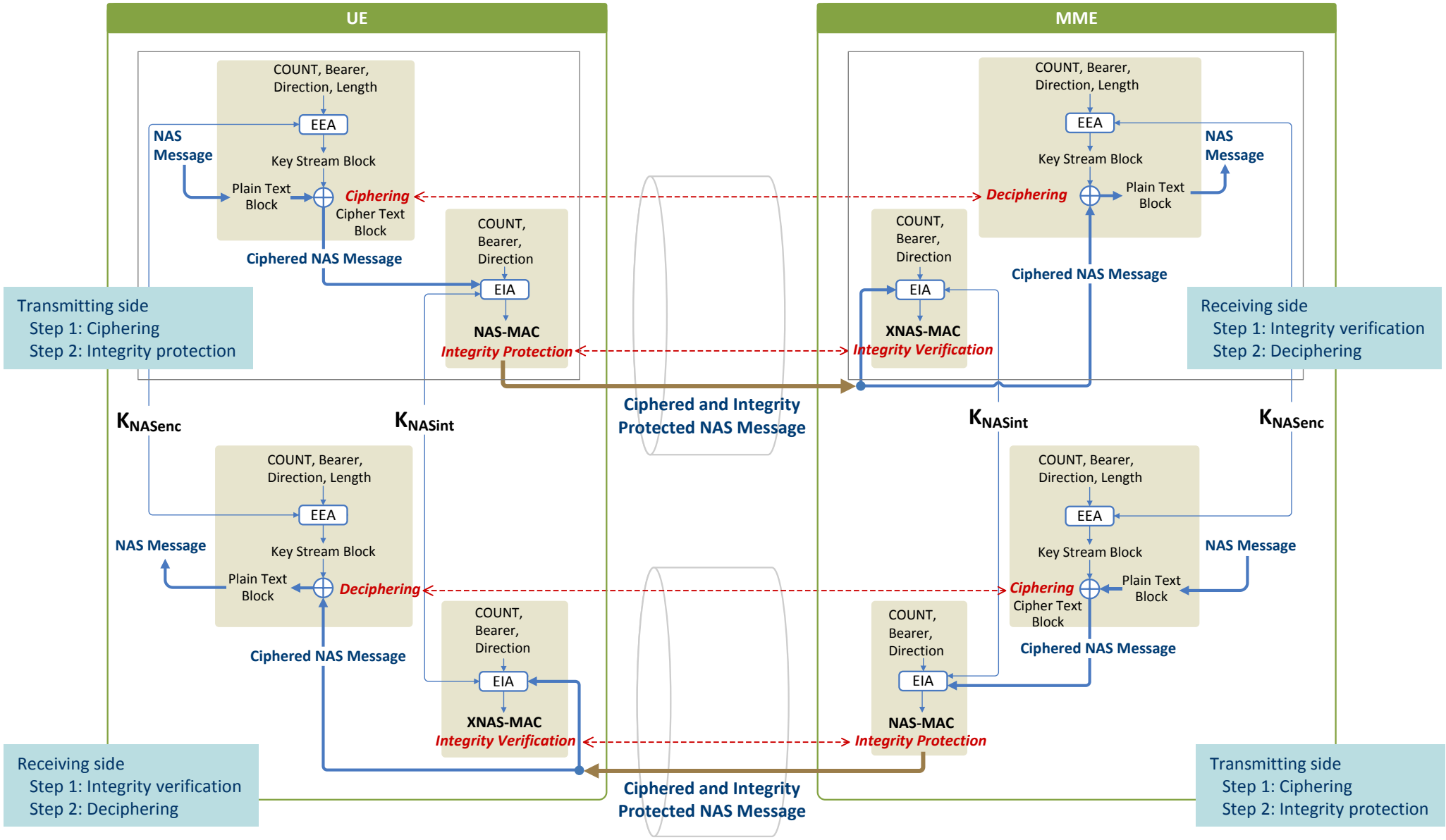
⑫ [MME] Deciphering the *Security Mode Complete* message

- Decrypts the ***Security Mode Complete*** message using K_{NASenc}

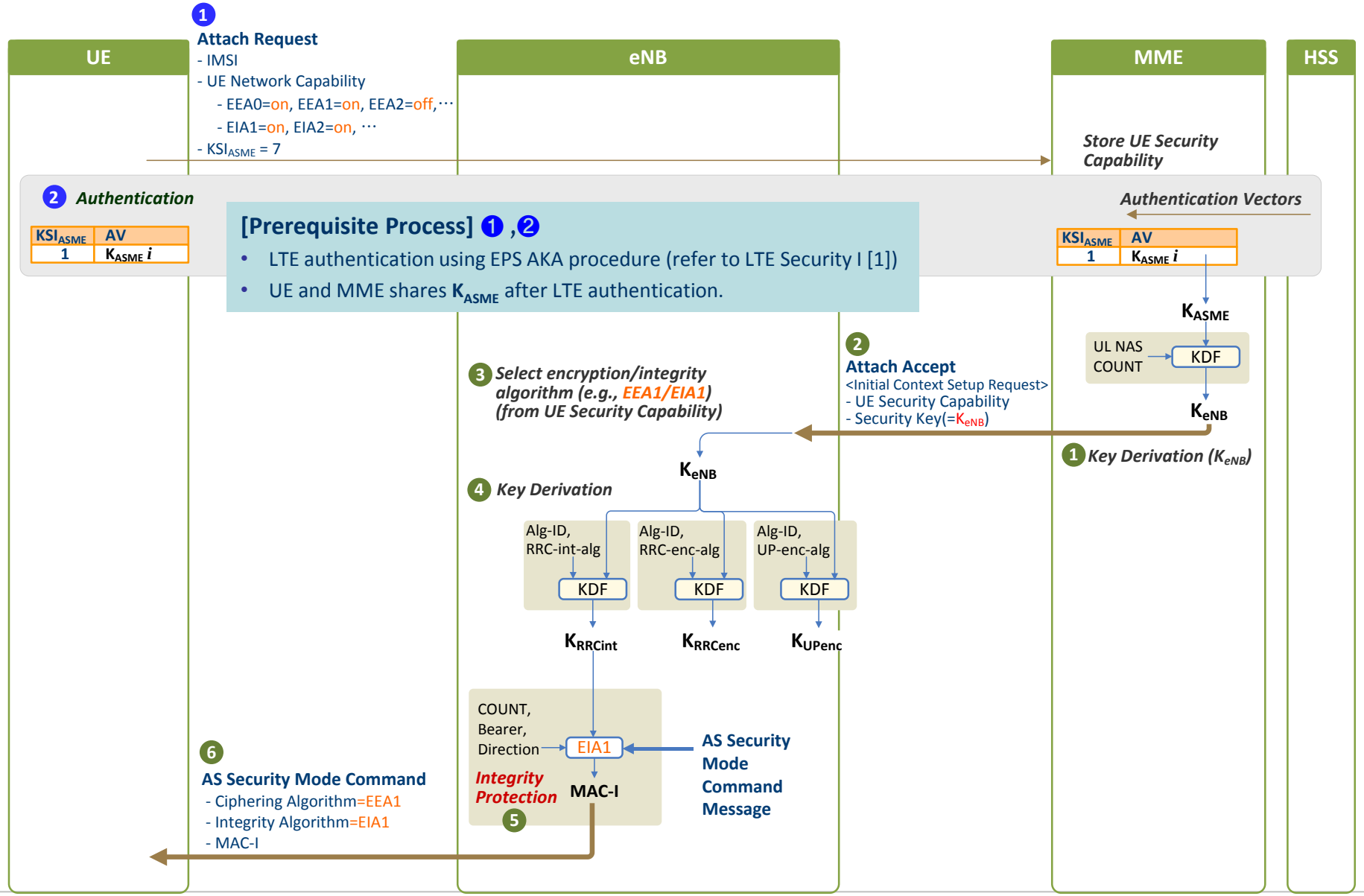


Deciphering of Security Mode Complete Message

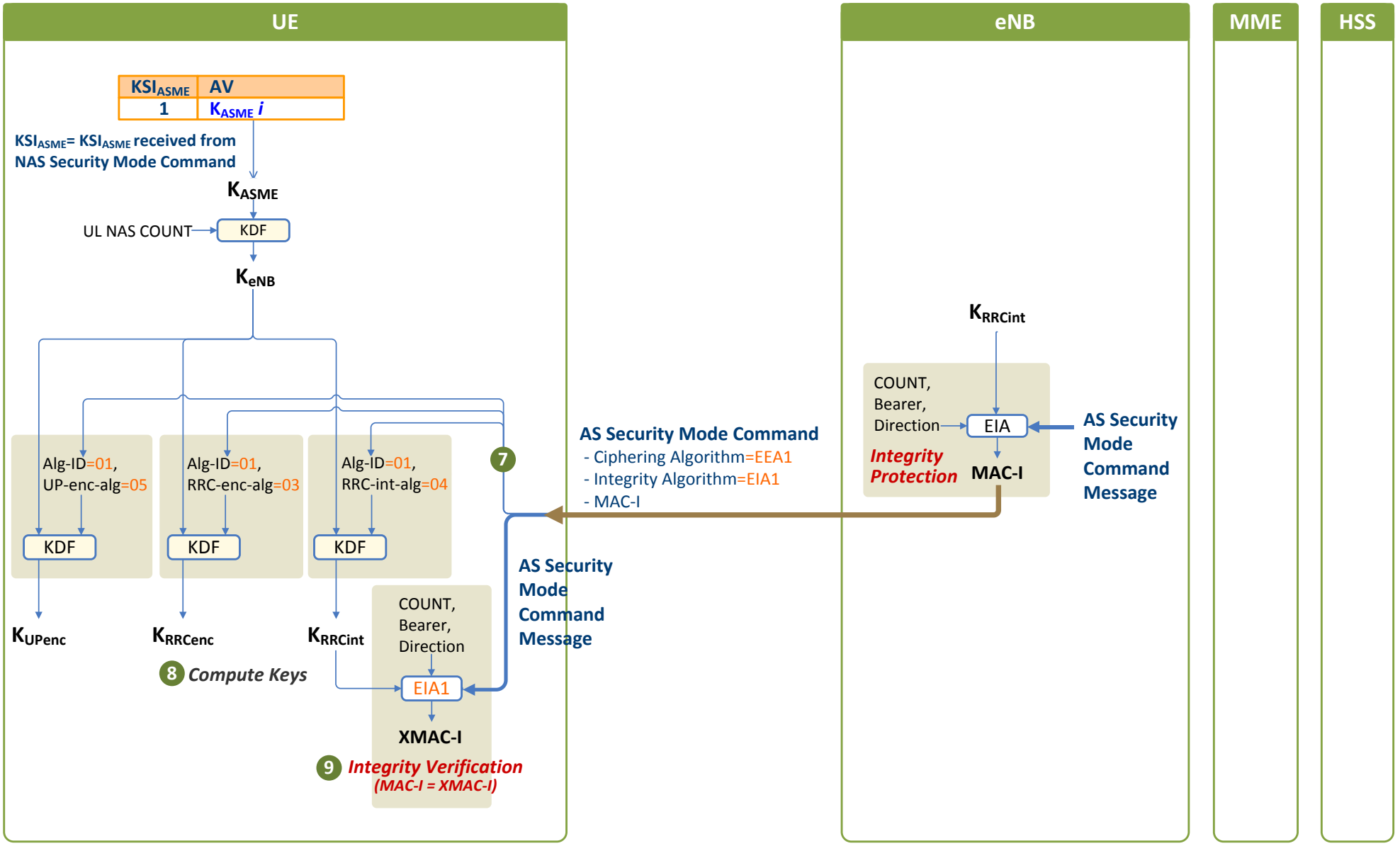
After NAS Security Setup



[AS Security Setup] Security Mode Command (1)



[AS Security Setup] Security Mode Command (2)



[AS Security Setup] Security Mode Command (3)

❶ [MME] Derivation of K_{eNB}

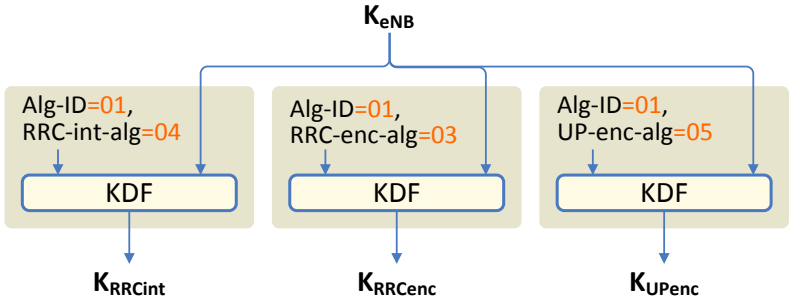
- Derives eNB base key, K_{eNB} using KDF with inputs, K_{ASME} and UL count

❷ [eNB ← MME] Transfer of K_{eNB}

- MME sends ***Attach Accept*** message to UE as the response of the ***Attach Request*** message
- The ***Attach Accept*** message is delivered through S1 signaling, ***Initial Context Setup Request*** message which includes
  - UE Security Capability: UE security information included in the ***Attach Request*** message sent by UE
  - Security Key: eNB base key, K_{eNB} (256-bit)

❸ [eNB] Selection of security algorithms

- Selects ciphering and integrity protection algorithms applied to RRC messages and user IP packets based on UE Security Capability information (e.g. EEA1 and EIA1)
  - Integrity protection algorithm for RRC messages (SRBs)
  - Ciphering algorithms for RRC messages and user IP packets (SRBs and DRBs)



❹ [eNB] Derivation of AS security keys, K_{RRCint}, K_{RRCenc} and K_{UPenc}

- Derives K_{RRCint}, K_{RRCenc} and K_{UPenc} with the following input parameters:
  - K_{eNB} received in ❷ (***Initial Context Setup Request*** message)
  - Security algorithm ID selected in ❸
  - Security algorithm distinguisher

K_{RRCint} = KDF (K_{eNB}, RRC-int-alg, Alg-ID)
K_{RRCenc} = KDF (K_{eNB}, RRC-enc-alg, Alg-ID)
K_{UPenc} = KDF (K_{eNB}, UP-enc-alg, Alg-ID)

Security Algorithm ID

Algorithm ID	Description	Value
128-EEA0	Null ciphering algorithm	0000
128-EEA1	SNOW 3G	0001
128-EEA2	AES	0010
128-EEA3	ZUA (optional)	0011
128-EIA1	SNOW 3G	0001
128-EIA2	AES	0010
128-EIA3	ZUA (optional)	0011

Algorithm Distinguisher

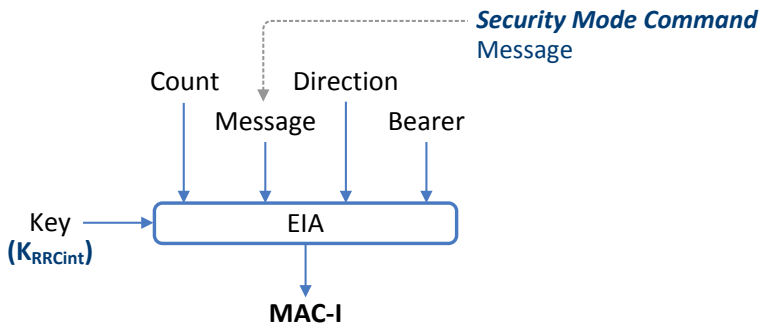
Algorithm Distinguisher	Value
NAS-enc-alg	0x01
NAS-int-alg	0x02
RRC-enc-alg	0x03
RRC-int-alg	0x04
UP-enc-alg	0x05
UP-int-alg*	0x06

* for relay nodes only, not discussed herein

[AS Security Setup] Security Mode Command (4)

❺ [eNB] Calculation of MAC-I for integrity protection

- Generates ***Security Mode Command*** message and calculates MAC-I using K_{RRCint}



Calculation of MAC-I

Input parameters for EIA algorithm

Input Parameter	Description
Count	32-bit downlink PDCP count
Message	RRC Message, ***Security Mode Command*** message herein
Direction	1-bit direction of message transmission, set to 1 for downlink
Bearer	5-bit radio bearer ID
K_{RRCint}	128-bit integrity protection key for RRC messages

❻ [UE ← eNB] Transmission of the *Security Mode Command* message

- ***Security Mode Command***: Integrity protected but not ciphered
- eNB sends the ***Security Mode Command*** *(AS Ciphering Algorithm, AS Integrity Protection Algorithm)* message with MAC-I to UE

Information Element	Description
AS Ciphering Algorithm	AS ciphering algorithm selected by eNB (here EEA1)
AS Integrity protection Algorithm	AS integrity protection algorithm selected by eNB (here EIA1)

❼ [UE] Checking of selected AS security algorithms

- Checks which ciphering and integrity protection algorithms are selected by eNB (e.g. EEA1, EIA1)

[AS Security Setup] Security Mode Command (5)

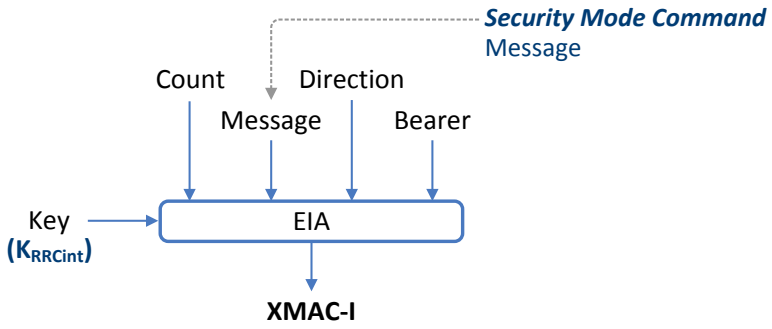
❽ [UE] Derivation of AS security keys, K_{RRCint}, K_{RRCenc} and K_{UPenc}

- Derives K_{RRCint}, K_{RRCenc} and K_{UPenc} with the following input parameters:
  - K_{eNB} derived in from K_{ASME} in ❷ (authentication process)
  - Security algorithm ID delivered in ❻
  - Security algorithm distinguisher

K_{RRCint} = KDF (K_{eNB}, RRC-int-alg, Alg-ID)
K_{RRCenc} = KDF (K_{eNB}, RRC-enc-alg, Alg-ID)
K_{UPenc} = KDF (K_{eNB}, UP-enc-alg, Alg-ID)

❾ [UE] Integrity verification for the *Security Mode Command* message

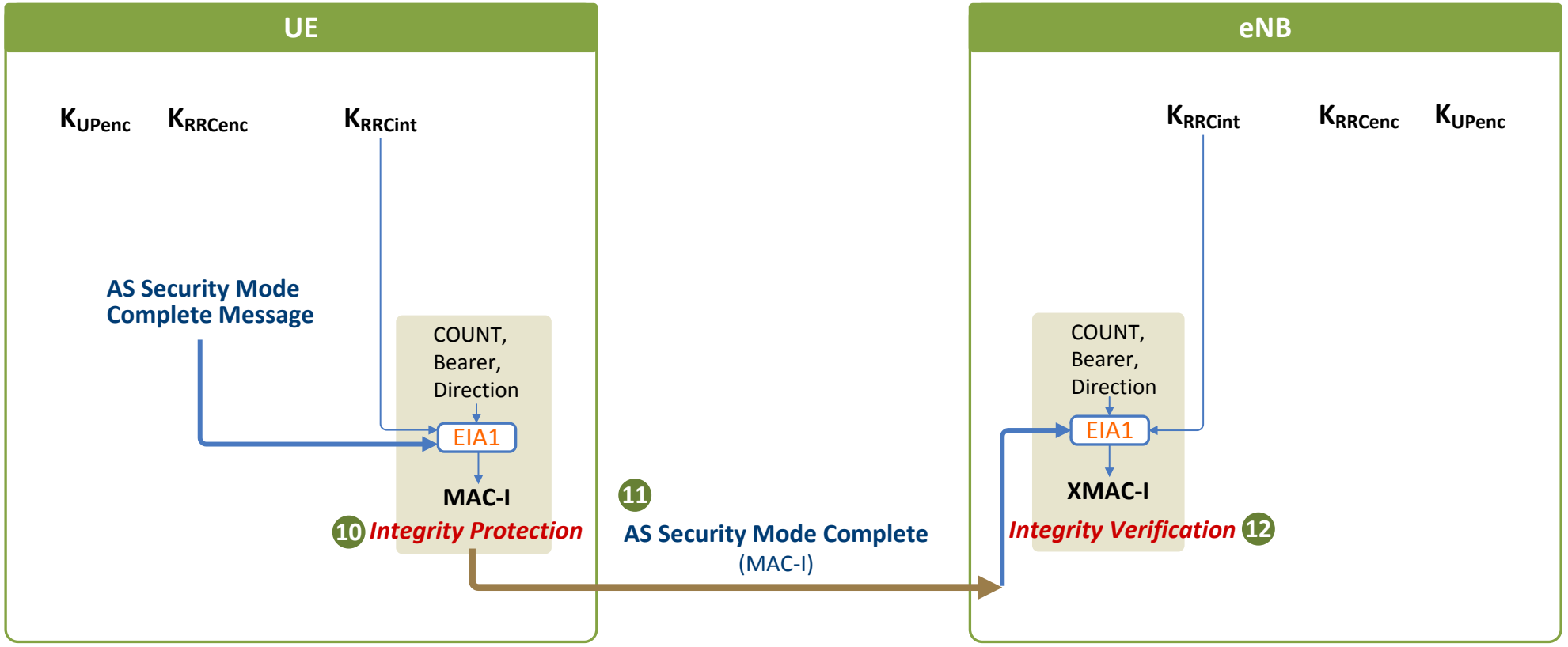
- Calculates XMAC-I
- Performs integrity verification using K_{RRCint} by comparing MAC-I with the calculated XMAC-I



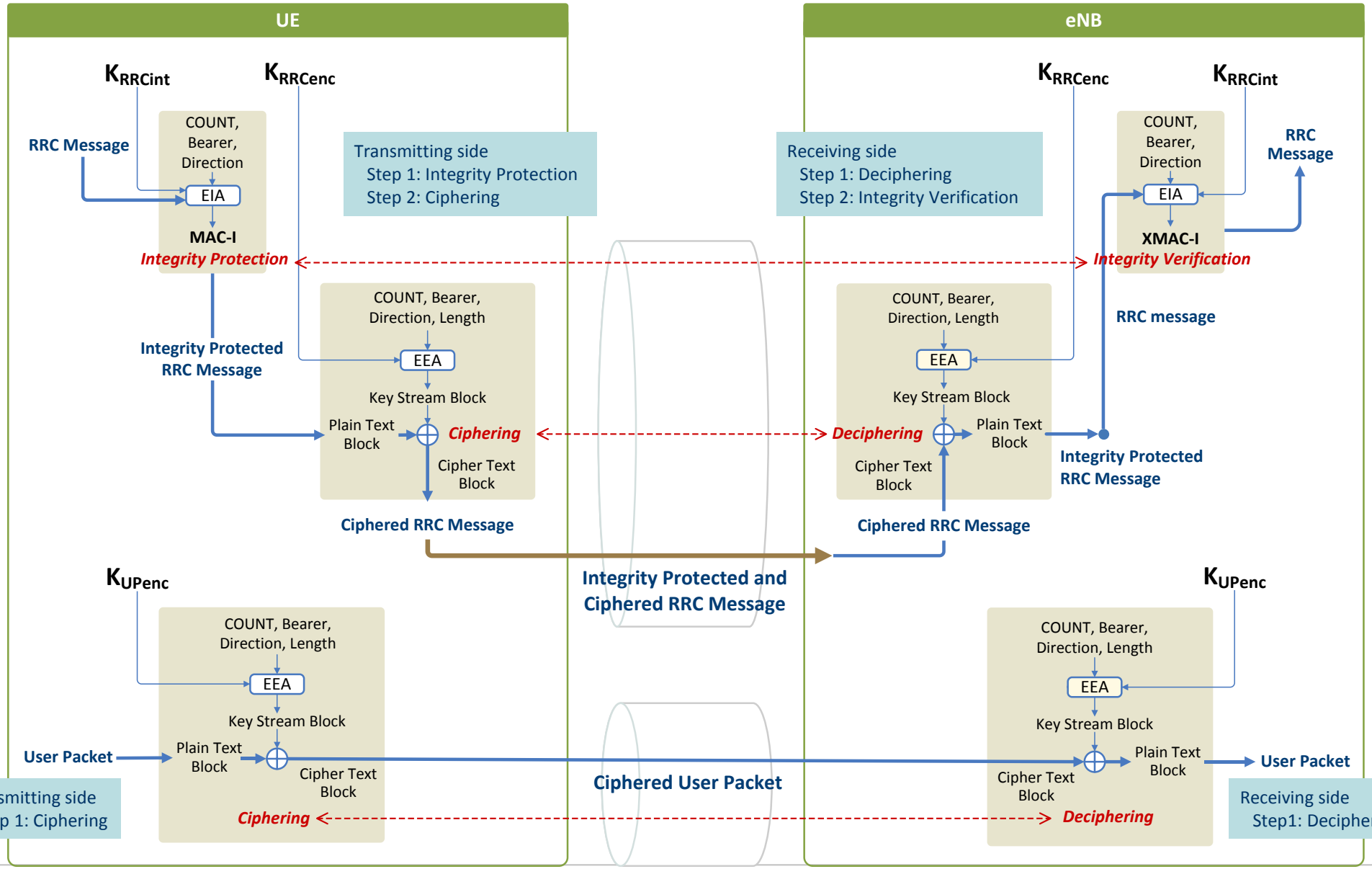
Calculation of XMAC-I

[AS Security Setup] Security Mode Complete

Only Integrity Protection and Integrity Verification are performed for AS *Security Mode Complete* message



After AS Security Setup

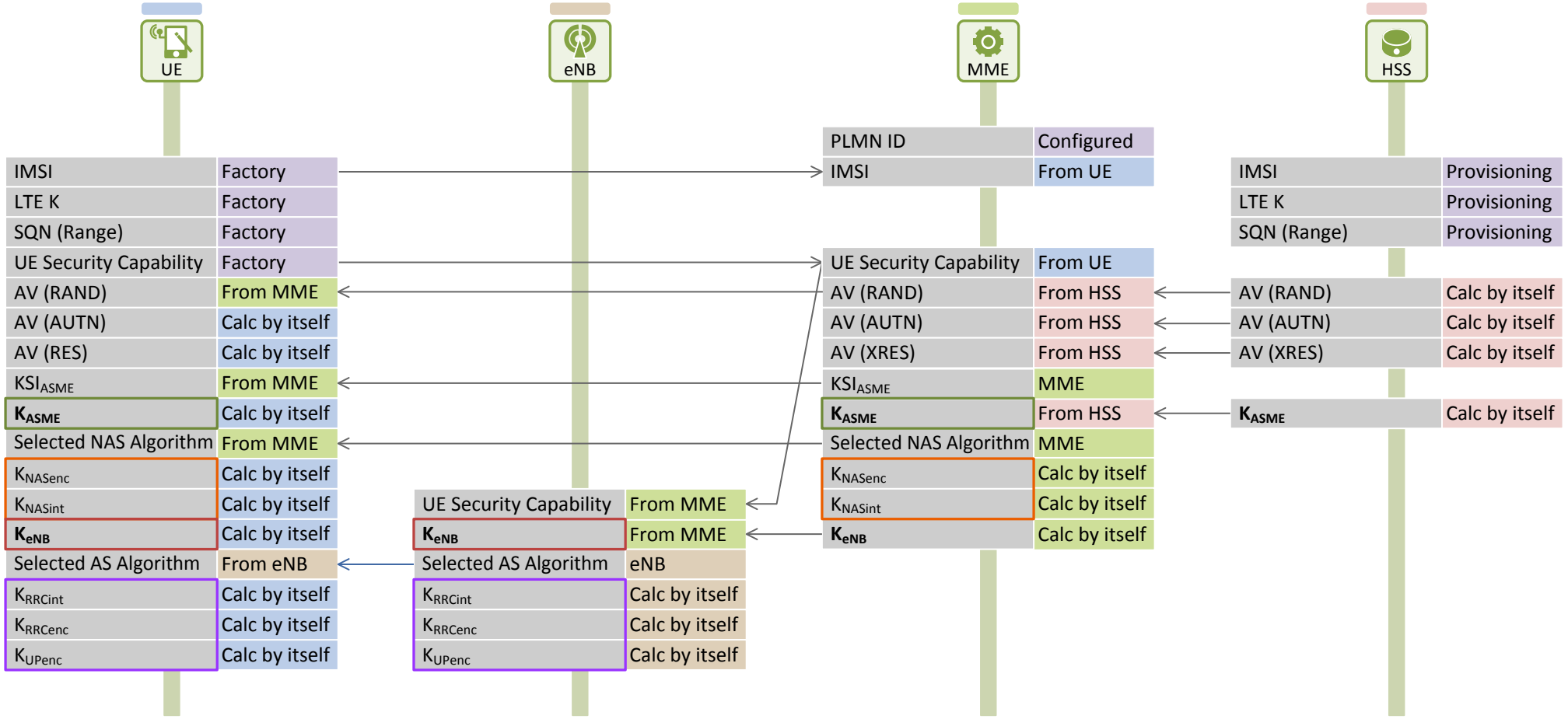


LTE Security Contexts

LTE Security Contexts

Partial Native EPS NAS Security Context	Full Native EPS NAS Security Context	EPS AS Security Context
UE Security Capability	UE Security Capability	UE Security Capability
K_{ASME}	K_{ASME}	K_{eNB}
KSI_{ASME}	KSI_{ASME}	-
UL Count	UL Count	UL Count
DL Count	DL Count	DL Count
-	EIA ID	EIA ID
-	EEA ID	EEA ID
-	K_{NASint}	K_{RRCint}
-	K_{NASenc}	K_{RRCenc}
-	-	K_{UPenc}

Security Data in EPS Entities



Summary of LTE Security Keys: Authentication and NAS/AS Security

LTE Security Keys: Total

Key	Length	Location	Derived from	Description
K	128 bits	USIM, HSS/AuC	-	EPS master key
CK	128 bits	USIM, HSS/AuC	K	Cipher key
IK	128 bits	USIM, HSS/AuC	K	Integrity key
K_{ASME}	256 bits	UE, MME, HSS	CK, IK	MME base key
K_{eNB}	256 bits	UE, eNB, MME	K_{ASME}	eNB base key
K_{NASint}	128/256 bits	UE, MME	K_{ASME}	Integrity key for NAS message between UE and MME
K_{NASenc}	128/256 bits	UE, MME	K_{ASME}	Encryption key for NAS messages between UE and MME
K_{RRCint}	128/256 bits	UE, eNB	K_{eNB}	Integrity key for RRC messages on SRB between UE and eNB
K_{RRCenc}	128/256 bits	UE, eNB	K_{eNB}	Encryption key for RRC messages on SRB between UE and eNB
K_{UPenc}	128/256 bits	UE, eNB	K_{eNB}	Encryption key for user IP packets on DRB between UE and eNB

References and Abbreviations

[1] Netmanias Technical Document, "LTE Security I: LTE Security Concept and LTE Authentication", August 2013, http://www.netmanias.com/en/?m=view&id=techdocs&no=5902

[2] 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture".

[3] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[4] NMC Consulting Group Confidential Internal Report, "E2E LTE Network Design", August 2010.

Abbreviations

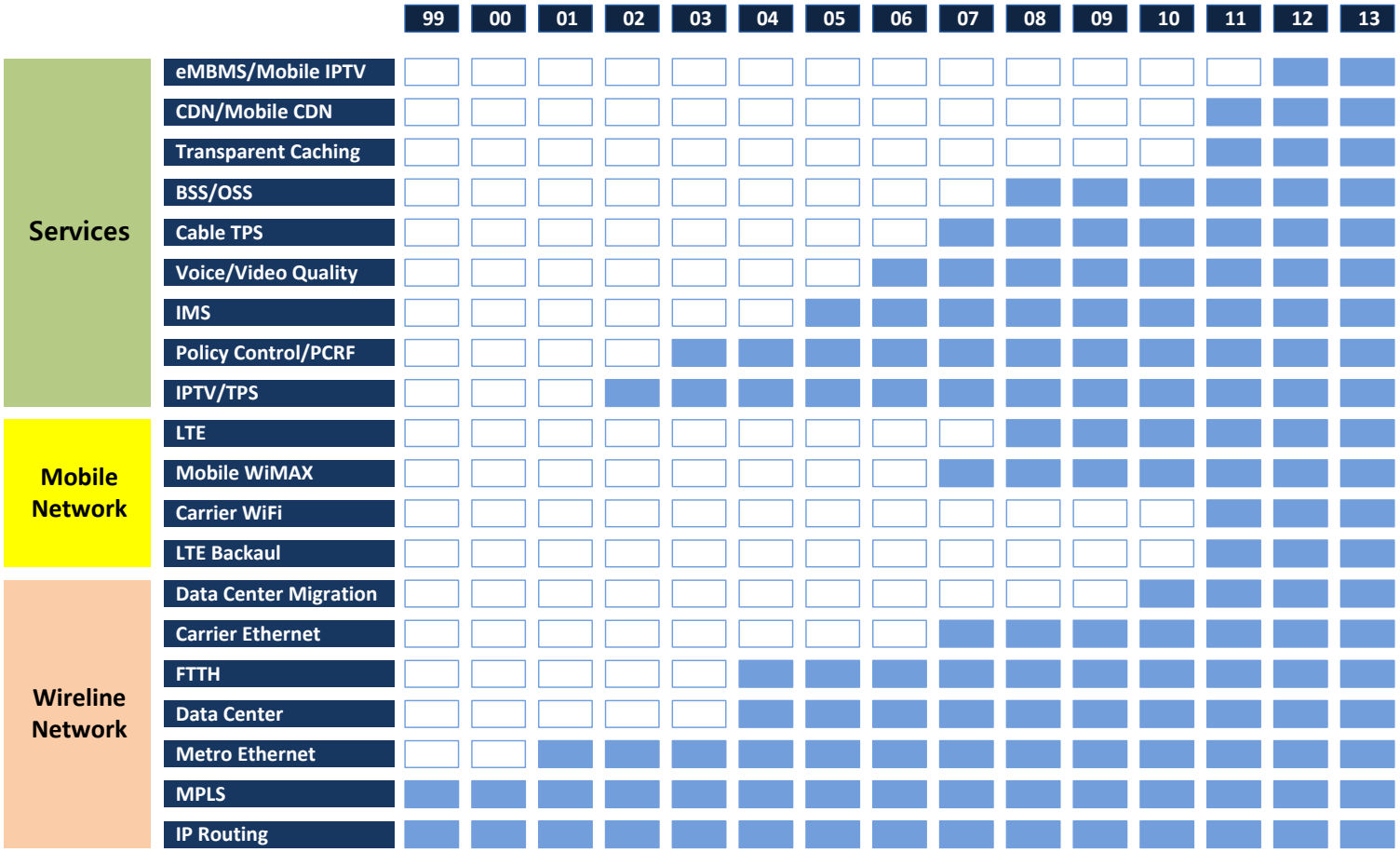
AES	:	Advanced Encryption Standard
AKA	:	Authentication and Key Agreement
AS	:	Access Stratum
ASME	:	Access Security Management Entity
AuC	:	Authentication Center
CK	:	Cipher Key
DRB	:	Data Radio Bearer
EEA	:	EPS Encryption Algorithm
EIA	:	EPS Integrity Algorithm
EPS	:	Evolved Packet System
HSS	:	Home Subscriber Server
IK	:	Integrity Key
IMSI	:	International Mobile Subscriber Identity
KDF	:	Key Derivation Function
KSI	:	Key Set Identifier
LTE	:	Long Term Evolution
MAC	:	Message Authentication Code
MAC-I	:	Message Authentication Code for Integrity
MME	:	Mobility Management Entity
NAS	:	Non Access Stratum
NAS-MAC	:	Message Authentication Code for NAS for Integrity
PDCP	:	Packet Data Convergence Protocol
RRC	:	Radio Resource Control
SRB	:	Signaling Radio Bearer
UE	:	User Equipment
UP	:	User Plane
USIM	:	Universal Subscriber Identity Module

Netmanias LTE Technical Documents

Visit http://www.netmanias.com to view and download more technical documents.

Index	Topic	Document title	Document presented here
1	Network Architecture	LTE Network Architecture: Basic	
2	Identification	LTE Identification I: UE and ME Identifiers	
3		LTE Identification II: NE and Location Identifiers	
4		LTE Identification III: EPS Session/Bearer Identifiers	
5	Security	LTE Security I: LTE Security Concept and LTE Authentication	
6		LTE Security II: NAS and AS Security	O
7	QoS	LTE QoS: SDF and EPS Bearer QoS	
8	EMM	LTE EMM and ECM States	
9		Eleven EMM Cases in an EMM Scenario	
10		LTE EMM Procedure 1. Initial Attach – Part 1. Case of Initial Attach	
11		LTE EMM Procedure 1. Initial Attach – Part 2. Call Flow of Initial Attach	
12		LTE EMM Procedure 2. Detach	
13		LTE EMM Procedure 3. S1 Release	
14		LTE EMM Procedure 4. Service Request	
15		LTE EMM Procedure 5. Periodic TAU	
16		LTE EMM Procedure 6. Handover without TAU – Part 1. Overview of LTE Handover	
17		LTE EMM Procedure 6. Handover without TAU – Part 2. X2 Handover	
18		LTE EMM Procedure 6. Handover without TAU – Part 3. S1 Handover	
19		LTE EMM Procedure 7. Cell Reselection without TAU	
20		LTE EMM Procedure 8 & 9. Handover and Cell Reselection with TAU	
21		LTE EMM Procedure 10 & 11. Move to Another City and Attach	
22	PCC	LTE Policy and Charging Control (PCC)	
23	Charging	LTE Charging I: Offline	
24		LTE Charging II: Online (TBD)	
25	IP Address Allocation	LTE: IP Address Allocation Schemes I: Basic	
26		LTE: IP Address Allocation Schemes II: A Case for Two Cities	

Netmanias Research and Consulting Scope



Visit http://www.netmanias.com to view and download more technical documents.