LTE and the Evolution to 4G Wireless

Design and Measurement Challenges

Bonus Material:

Security in the LTE-SAE Network

www.agilent.com/find/lte

Security in the LTE-SAE Network

Introduction

This overview of the security aspects of 3GPP LTE and SAE is based on standardization as of December 2008. At this time the Release 8 specifications are not yet fully defined. The reader is encouraged to study the most recent versions of the 3GPP specifications to gain the most complete, up-to-date understanding of network security issues. Further modifications of the specifications are expected, including harmonization of Stage 2 and Stage 3 of the standards development process.

Security architecture and aspects of 3GPP accesses to the EPS, the topic of this overview, are covered in 33.401 [1]. Non-3GPP accesses are detailed in 3GPP Technical Specification 33.402 [2] and are not discussed here.

Service access in the Packet-Switched (PS) domain requires the establishment of a security association between the User Equipment (UE) and the Public Land Mobile Network (PLMN). A separate security association also must be established between the UE and the IMS Core Network Subsystem (IMS CN SS) before access can be granted to any multimedia services being hosted.

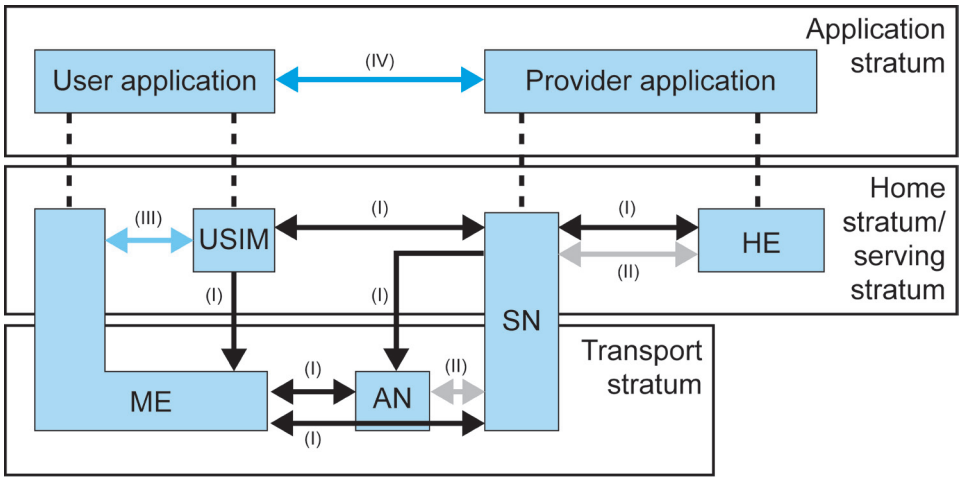

Figure 1. Security features in the network (from 33.401 [2] Fig.4-1)

As shown in Figure 1, five security feature groups are defined in 33.401 [1]:

(I) Network access provides users with secure access to services and protects against attacks on the access interfaces.

(II) Network domain enables nodes to securely exchange signalling data and user data, and protects against attacks on the wire line network.

(III) User domain provides secure access to mobile stations.

(IV) Application domain security enables applications in the user and provider domains to securely exchange messages.

(V) Visibility and configurability of security allow the user to learn whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

The security features in (I) and (II) are the subject of this overview. Details on (III), (IV) and (V) are available in 33.102 [3].

User Identity Confidentiality

During network access, the serving Mobility Management Entity (MME) is required to allocate a Globally Unique Temporary Identity (GUTI) to the UE, which is used in the EPS to avoid frequent exchange of the UE's permanent identity (IMSI) over the radio access link.

The GUTI consists of two components: a Globally Unique MME Identity (GUMMEI), which is the identity of the MME that has allocated the GUTI, and the M-TMSI, which is the identity of the UE within that MME.

The GUMMEI in turn consists of the following:

- PLMN Id: MCC, MNC
- MME Identifier (MMEI): MME Group Id (MMEGI) and MME Code (MMEC)

The MMEC provides a unique identity to an MME within the MME pool, while the MMEGI is used to distinguish between different MME pools.

The SAE TMSI (S-TMSI) is a shortened form of the GUTI that is used to identify the UE over the radio path and is included in the RRC connection request and paging messages. The S-TMSI contains the MMEC and M-TMSI components of the MMEI. Note, however, that the S-TMSI does not include the MMEGI—that is, the MME pool component. Thus, because MME pool areas can overlap, care must be taken to ensure that MMEs serving the overlapping areas are not allocated the same MMECs. More details about these identifiers can be found in 23.003 [4].

GUTI reallocation procedures can be used to "refresh" the UE's temporary identification and should be performed after Non-Access Stratum (NAS) ciphering procedures have been initiated. GUTI reallocation is further described in 23.401 [5] and 24.301 [6].

User Device Confidentiality

The International Mobile Equipment Identity (IMEI) is sent upon request from the network using NAS procedures. Typically confidentiality is protected.

Entity Authentication

An EPS Authentication and Key Agreement (AKA) procedure is used to provide mutual authentication between the user and the network, and agreement on the Key Access Security Management Entity (K_{ASME}). The K_{ASME} forms the basis for generation of Access Stratum (AS) and NAS ciphering and integrity keys to be used for AS Radio Resource Control (RRC) and user plane protection and NAS signalling protection, respectively.

ASME is defined in 33.401[1] as the entity in an access network that receives the top level keys from the Home Subscriber Server (HSS). For E-UTRAN access, MME the assumes the role of Access Security Management Entity (ASME).

EPS Security Context

An EPS security context is created as the result of the EPS AKA and is uniquely identified by the evolved Key Set Identifier (eKSI) of Type KSI_{ASME}, allocated by the MME as part of the EPS AKA procedure. An EPS security context consists of AS and NAS components.

The UE and MME each maintain up to two EPS security contexts simultaneously. For example, during a re-authentication procedure, both the current and new EPS security context exist during the period of transition.

An EPS security context can be stored for future system accesses, termed a "cached security context." A UE transitioning from the EMM-DEREGISTERED to EMM-REGISTERED state without an EPS security context typically requires the Extended Pedestrian A (EPA) AKA procedure to be run; however, the process is optional if cached security context is used.

Similarly, a UE transitioning from EMM-IDLE to EMM-CONNECTED state in EMM-REGISTERED state will always have EPS cached security context available; therefore, in this case EPS AKA is optional as well.

The EPS mapped security context is created by converting security contexts forwarded from the Serving GPRS Support Node (SGSN) over the S3 interface during the 3GPP Inter-RAT handover from the UTRAN/GERAN into the E-UTRAN.

Authentication Data Retrieval

Authentication information is retrieved from the HSS over the S6a interface upon request by the MME. An authentication data request includes the IMSI, the serving network identity (mobile country code and mobile network code), the network type (E-UTRAN), and the number of requested Authentication Vectors (AV) that the MME is prepared to receive.

Upon receipt of the authentication data request from the MME, the HSS requests that the Authentication Center (AuC) generate the corresponding AVs if they are not already available in the HSS database. The K_{ASME} is derived in the HSS as specified in 33.401 [1] and are returned to the MME as part of the EPS AV in the authentication data response. The EPS AVs returned can be less than or equal to the number of AVs requested by the MME. They consist of the random number (RAND),expected user response (XRES), authentication (AUTN), and K_{ASME}.

Message level details can be found in 29.272 [7]. Definitions of AV components can be found in TS 33.102 [3] and 33.401 [1].

UE Authentication

Authentication of the UE is initiated by the serving MME through EPS NAS procedures. An EMM authentication request is sent to the UE with authentication parameters (RAND, AUTN) and the NAS Key Set Identifier (eKSI) or KSI_{ASME}. See Figure 2.

The KSI_{ASME} is allocated by the MME and uniquely identifies the K_{ASME}. It is stored in the UE and serving MME together with the GUTI, if one is available, allowing the K_{ASME} to be cached and re-used during subsequent connections without re-authentication. A new authentication procedure must include a different KSI_{ASME}.

The UE responds to the MME with an authentication response, including the user response (RES) upon successful processing of the authentication challenge data. The MME then must validate the correctness of RES, and the intermediate K_{ASME} is determined after successful completion of the current EPS AKA, as agreed upon by the UE and MME. The EPS AKA mechanism is further described in 33.401 [1], and the EPS NAS procedures used in the EPS AKA are described in 24.301 [6].

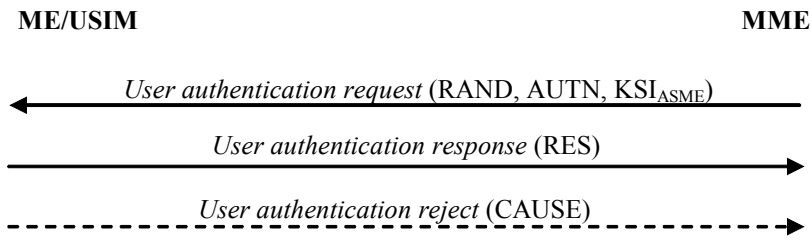

Figure 2. EPS user authentication (EPS AKS) (33.401 [1] Figure 6.1.1-1)

UE Identification

The UE identification request is initiated by the serving MME using EPS NAS procedures. An EPS Mobility Management (EMM) identity request is sent to the UE requesting that the permanent identity—that is, the IMSI—be sent to the MME. See Figure 3. This request is normally made when a GUTI is not available to provide a unique UE identification.

The EMM identity request can also be used to retrieve the International Mobile Equipment Identity (IMEI) as part of the Mobile Equipment (ME) identity check procedure, wherein the returned IMEI is passed on to the Equipment Identity Register (EIR) via the S13 interface for validation. The ME identity check procedure is covered in 29.272 [7].

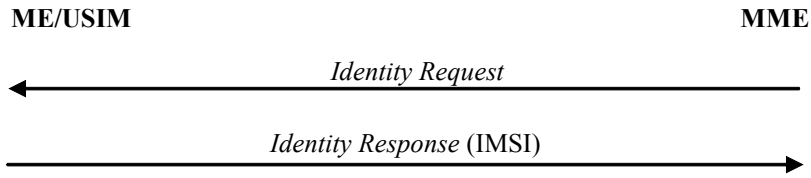

Figure 3. User identity query(33.401 [1] Figure 6.1.3-1)

Confidentiality and Integrity for Signalling and User Data

As we have seen, to ensure confidentiality and integrity protection for signalling and user data in the EPS, two levels of security associations exist: the Access Stratum (AS) and the Non Access Stratum (NAS).

Ciphering mechanisms can be used to provide signalling and user data confidentiality between the UE and the EPS, while integrity and replay mechanisms can be used to provide signalling and user data integrity. Table 1 summarizes the AS and NAS security associations and their relationships with the UE and EPS network elements, specifically the MME and eNB.

Table 1. AS and NAS security associations

Security Association	Access Stratum	Non-Access Stratum
Termination points	UE and eNB (E-UTRAN)	UE and MME
Ciphering (optional)	RRC signalling (signalling radio bearer) User plane (data radio bearer)	NAS signalling
Integrity and replay protection (mandatory)	RRC signalling (signalling radio bearer)	NAS signalling
Security protocol layers	PDCP (36.323 [8])	NAS (24.301 [6])
Security command procedures	RRC (36.331[9])	NAS (24.301 [6])

Note that there is no requirement for data protection for a user plane tunneled between the eNB and S-GW above network transport layer. Network Domain Security (NDS) can be used for transport layer protection. Also, note that integrity and replay protection is not required for user plane transfers between the UE and eNB.

The EPS Encryption Algorithms (EEA) below are specified in 33.401 [1]. Each is each assigned a 4-bit identifier with a 128-bit input key listed. (Other values are reserved for future use.)

"0000_2"	128-EEA0	Null ciphering algorithm
"0001_2"	128-EEA1	SNOW 3G
"0010_2"	128-EEA2	AES

The EPS Integrity Algorithms (EIA) below are also specified in 33.401[1]. Each is each assigned a 4-bit identifier with a 128-bit input key listed. (Other values are reserved for future use.)

"0001_2"	128-EIA1	SNOW 3G
"0010_2"	128-EIA2	AES

Please note the following:

- EEA0 specifies the null ciphering algorithm, which implies that ciphering is not activated, hence no confidentiality protection is offered.

- No EIA0 is specified, since integrity protection is mandatory for RRC (AS) and NAS signalling messages, with exceptions specified in 36.331 [9] and 24.301 [6] for the AS and NAS, respectively.

- EEA1/EIA1 is based on SNOW3G and is identical to the UMTS Encryption Algorithm, UEA2, introduced as part of 3GPP Release 7 for UMTS confidentiality protection.

- EEA2/EIA2 is based on the Advanced Encryption Standard (AES).

- AS and NAS EEA/EIA selected may not be the same. Selection of EIA and EEA are independent. RRC and User Plane in AS shall use the same EEA selected for Ciphering.

- RRC signalling, user plane, and NAS signalling use different keys generated from the base key (K_{ASME}) through the EPS AKA procedure. Key hierarchy and relationships are discussed in a later section.

AS Security

An EPS AS security context is initialized in the eNB by the MME when the UE enters the ECM-CONNECTED state and during the preparation for an intra-LTE handover. At this time the UE's security capabilities and context, including the transitional security key material, is transferred from the source to the target eNB. The EPS AS security context is deleted in the eNB when the UE enters the ECM-IDLE state or when the intra-LTE handover is completed.

An RRC security command procedure is used during initial establishment of the AS security context and is initiated by the eNB towards the UE. The SRB1 is established at this time; that is, prior to the establishment of the Signalling Radio Bearer 2 (SRB2) and Data Radio Bearers (DRBs) for user plane transfer.

An integrity-protected AS security mode command message is sent with the EIA and key belonging to the security context to be activated while non-ciphered. The EEA, EIA and eKSI selected for the new security context are sent in the same message. The EEA and EIA selections are based on the security capabilities of the UE. They indicate the supported EEA and EIA and the locally configured, prioritized support lists in the eNB. The system chooses the highest priority EEA and EIA supported by both the eNB and the UE.

The UE security capabilities list is provided by the MME in the S1-AP procedures during the initial UE context setup request or during the handover resource preparation phase for the S1-initiated intra-LTE handover. Such a list is also made available from the source eNB during preparation for an X2-initiated handover. Depending on the system, the EEA and EIA for the AS may be updated as part of the intra-LTE handover, as eNBs can have varying levels of support for security algorithms.

Ciphering and deciphering at the AS in the downlink is started after the security mode command has been sent by the eNB and received at the UE; it is not necessary to wait for the security mode complete message. In the uplink, however, the security mode complete message must be sent by the UE and received at the eNB before ciphering and deciphering at the AS can start. The AS security mode complete message is sent ciphered and integrity-protected with that of the security context to be activated.

An explicit start time for user plane ciphering is not required, since DRBs are always established after security mode procedures, and these DRBs share a common EEA with the SRBs. Keys may be updated through handovers and RRC connection re-establishments. Key refreshes are performed via intra-cell handover procedures. The RRC security procedures are further described in 36.331 [9].

For DRB Packet Data Units (PDUs), ciphering at the Packet Data Control Plane (PDCP) is performed using post header compression, and deciphering is performed using pre header decompression. Note that compression is not used for SRBs. Ciphering and deciphering is performed on the data part of the SRB or DRB, and Message Authentication Code (MAC-I) for the SRB. PDCP control PDUs are not ciphered.

Integrity protection and validation for the SRB is performed on the PDCP PDU header before ciphering on the data parts. Figure 4 shows the PDCP Data PDU format for SRBs, note MAC-I is included for Integrity protection purposes. PDCP Security procedures are further described in TS 36.323 [8].

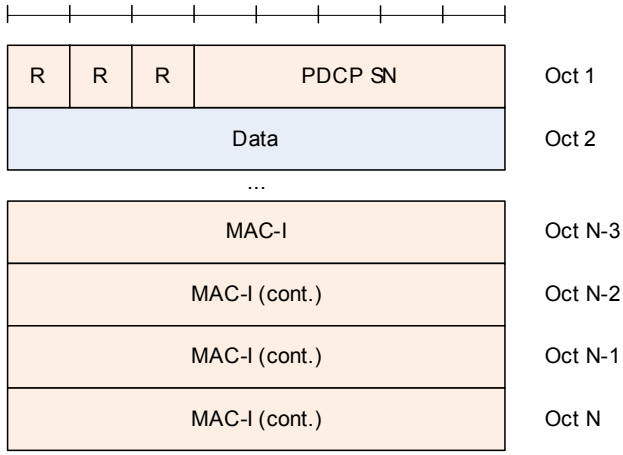

Figure 4. PDCP data PDU format for SRBs (TS 36.323 [8] Figure 6.2.2.1)

NAS Security

The NAS security context in the EPS can be either set or re-established. The NAS security context is set using the NAS security mode control procedure, which is initiated by the MME towards the UE. This procedure can be used during the initial establishment of security context, subsequent re-authentications, or context modification (such as an algorithm change).

To initiate the procedure, an integrity-protected NAS security mode command message is sent with the EIA and key belonging to the security context to be activated while non-ciphered. The EEA, EIA and eKSI selected for the new security context are sent in the same message. The EEA and EIA selections are based on the UE's security capabilities. They indicate the supported EEA and EIA and the locally configured, prioritized support lists in the MME. The system chooses the highest priority EEA and EIA supported by both the MME and the UE.

During MME relocation, the NAS EEA and EIA may be updated, as source and target MMEs can have varying levels of support for security algorithms.

The NAS security mode complete message is sent using ciphering and integrity protection with that of the security context to be activated. After the security procedures are exchanged, ciphering is applied on all NAS messages except the EMM attach request, tracking area update request, and security mode command until the NAS signalling connection is released and the MME is in the ECM-IDLE state.

In transiting from the ECM-IDLE state to the ECM-CONNECTED state, the system always sends the NAS initial messages without ciphering but with integrity protection with the EPS cached security context, if one exists. If an EPS cached security context is not available, the system sends the EPS AKA, NAS and AS Security Mode Control procedures to set the new EPS security context for the NAS and AS.

When an EPS cached security context is available, the UE sends the eKSI corresponding to the cached context, and the EPS AKA is optional. If the cached security context is to be activated, a new KeNB (eNB Key) is derived for this NAS signalling connection at the MME and forwarded to the eNB over the S1-AP interface. AS security mode control procedures are used to inform the UE of the eKSI, indicating the current K_{ASME} in use. Security keys for the AS are derived accordingly at both the eNB and the UE. NAS security mode control procedures are not required in this case. The NAS security context loop is closed when the MME responds to the UE initiating message by sending the corresponding NAS procedure. This response is ciphered and integrity protected with that of the cached security context to be activated. Examples are Tracking Area Update (TAU) accept and attach accept.

An exception applies in the case of a TAU procedure in which the active flag is not set; that is, a signalling-only NAS connection is made that does not require establishment of DRBs and that releases resources as soon as the TAU procedure is completed.

An NAS message is ciphered and transferred in the NAS message portion of a security protected NAS message. After ciphering, integrity protection is performed on the NAS

message and sequence number, after which the Message Authentication Code (MAC) is computed and filled in. Integrity validation is performed prior to deciphering of the embedded NAS message. Figure 5 shows the organization of a security protected NAS message.

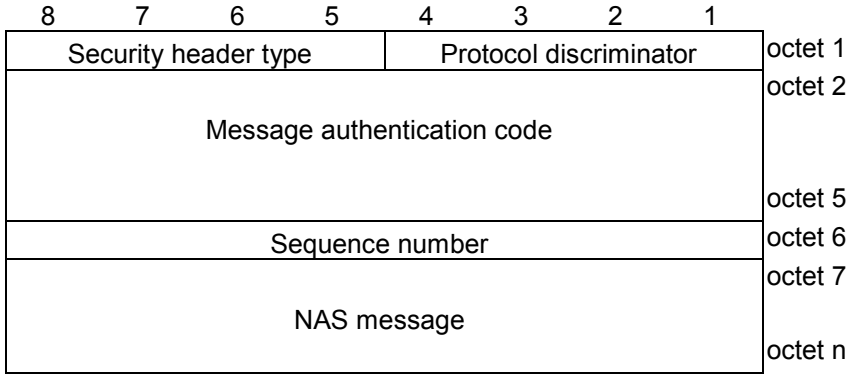

Figure 5. General message organization for a security protected NAS message (24.301 [6] Figure 9.1.2)

A security header, which is included in every EMM message, contains security information for the NAS PDU. Security header types are shown in Table 2. NAS security procedures are further described in 24.301 [6].

Table 2. Security header type (24.301 [6] Table 9.3.1)

Security header type (octet 1)				
8	**7**	**6**	**5**	
0	0	0	0	Plain NAS message, not security protected
				Security protected NAS message:
0	0	0	1	Integrity protected
0	0	1	0	Integrity protected and ciphered
0	0	1	1	Integrity protected with new EPS security context (NOTE 1)
0	1	0	0	Integrity protected and ciphered with new EPS security context (NOTE 2)
				Non-standard L3 message:
1	1	0	0	Security header for the SERVICE REQUEST message
1	1	0	1	These values are not used in this version of the protocol.
to				If received they shall be interpreted as ‘1100’. (NOTE 3)
1	1	1	1	
All other values are reserved.				

NOTE 1:	This codepoint may be used only for a SECURITY MODE COMMAND message.
NOTE 2:	This codepoint may be used only for a SECURITY MODE COMPLETE message.
NOTE 3:	When bits 7 and 8 are set to '11', bits 5 and 6 can be used for future extensions of the SERVICE REQUEST message.

EPS Key Hierarchy

Figure 6 depicts the hierarchy of security keys used in the EPS. Table 3 further summarizes the relationships among these security keys.

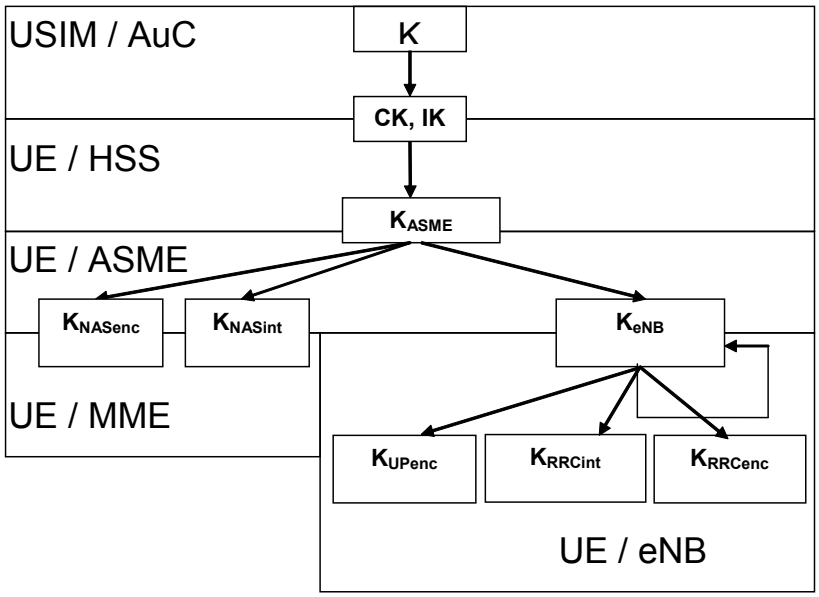

Figure 6. Key hierarchy (33.401 [1] Figure 6.2-1)

Table 3. Summary description of EPS security keys

Key	Purpose	Length	Derived from	Description
K	Master Base Key for GSM, UMTS, EPS	128	-	Secret Key stored permanently in USIM and AuC
CK, IK	Cipher and Integrity Keys	128	K	Pair of Keys derived in AuC and USIM during a AKA run. CK and IK should be handled differently for EPS as compared to Legacy context
K_{ASME}	MME (ASME) Base/Intermediate Key	256	CK, IK	Intermediate Key derived in HSS and UE from CK, IK during AKA. This is sent as part of the EPS AVs from HSS which include RAND, XRES, AUTN, and uniquely identified with eKSI allocated by the MME during AKA process. MME assumes the role of ASME in EPS
K_{eNB}	eNB Base Key	256	K_{ASME} K_{eNB}*	Intermediate Key derived in MME and UE from K_{ASME} when UE transits to ECM-CONNECTED State or by UE and Target eNB from K_{eNB}* during Handover
K_{eNB}*	eNB Handover Transition Key	256	K_{eNB} (H) NH (V)	Intermediate Key derived in Source eNB and UE during Handover when performing Horizontal (K_{eNB}) or Vertical Key (NH) Derivation. Used at Target eNB to derive K_{eNB}
NH	Next Hop	256	K_{eNB}	Intermediate Key derived in MME and UE used to provide forward security, and forwarded to eNB via the S1-MME interface
K_{NASint}	Integrity Key for NAS Signaling	256 (128 LSB)	K_{ASME}	Integrity Key for protection of NAS data derived in MME and UE
K_{NASenc}	Encryption Key for NAS Signaling	256 (128 LSB)	K_{ASME}	Encryption Key for protection of NAS data derived in MME and UE
K_{UPenc}	Encryption Key for User Plane (DRB)	256 (128 LSB)	K_{eNB}	Encryption Key for protection of user plane data derived in eNB and UE
K_{RRCint}	Integrity Key for RRC Signaling (SRB)	256(128 LSB)	K_{eNB}	Integrity Key for protection of RRC data derived in eNB and UE
K_{RRCenc}	Encryption Key for RRC Signaling (SRB)	256 (128 LSB)	K_{eNB}	Encryption Key for protection of RRC data derived in eNB and UE

All EPS security keys are 256 bits in length; however, ciphering and integrity keys for AS and NAS algorithms use only the 128 Least Significant Bits (LSB) of the derived keys. Note that the ciphering and integrity keys are dependent on the algorithms in use. This, if the security algorithms change for any reason, the associated keys must be re-derived.

The eKSI key is used to uniquely identify the K_{ASME} and all of the associated keys derived from the K_{ASME}. The K_{eNB}* and Next Hop (NH) keys are transitional, intermediate keys generated during Intra-LTE handovers and are used to derive an updated K_{eNB}. These particular keys are discussed in more detail below. Additional information about key hierarchy and derivation can be found in 33.401 [1].

Key Handling in Handovers

Figure 7 shows the handover key chaining model for intra-LTE handovers. This model is used to determine the K_{eNB} in the serving eNB. The principles are described here to illustrate the work flow of this model in the EPS. Please see 33.401 [7] for more details.

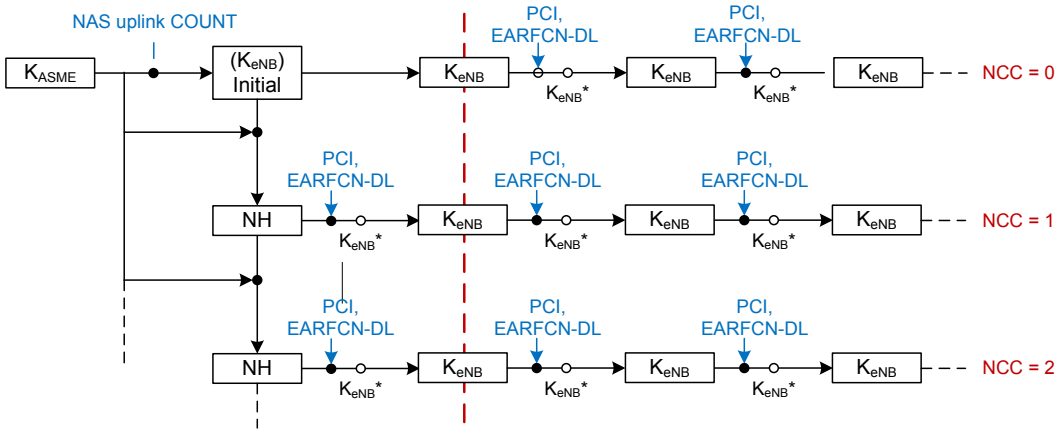

Figure 7. Model for the handover key chaining (33.401 [1] Figure 7.2.8.1-1)

The K_{eNB} (initial) is derived by the MME and sent to the serving eNB as the UE transits from the ECM-IDLE state to the ECM-CONNECTED state. The EPS security context can be new (EPS AKA) or existing (cached). The K_{eNB} (initial) has a Next Hop Chaining Counter (NCC) of "0" at this time. NCC and NH (described previously) have a one-to-one relationship. NH generation is possible only in the MME and UE, hence fresh updates of the {NCC, NH} pair are always sent from the MME to the serving eNB during the inter-eNB handover procedures.

During an intra- or inter-eNB (S1 or X2-intiated) handover, the source eNB always derives the K_{eNB}*, which is sent to the target eNB and used to derive K_{eNB} that becomes the base E-UTRAN key for subsequent AS ciphering and integrity key derivations. The K_{eNB}* is always derived using the Physical Cell Id (PCI) of the target cell and the current K_{eNB} or NH parameter.

Horizontal key derivation is defined as using the K_{eNB}, moving across the key chaining model. Vertical key derivation is defined as using the NH parameter, moving down the chain. For inter-eNB handovers, vertical key derivation is used when the source eNB holds a {NCC, NH} pair, with the NCC larger than that of the currently active K_{eNB}. Otherwise horizontal key derivation is used. For intra-eNB handovers, the source eNB has the choice of using either.

Key Change

Dynamic key changing can be the result of explicit re-keying or implicit key-refresh procedures. Note that this discussion excludes key changing for handovers, discussed earlier.

Re-keying for the access stratum occurs when the AS EPS security context to be activated differs from the currently active security context. During AS re-keying, the MME sends the updated K_{eNB} to the serving eNB, which is used to derive the security keys for SRBs and DRBs. AS intra-cell handover procedures are used to activate the new AS EPS security context.

Similarly, re-keying for the non-access stratum occurs when the NAS EPS security context to be activated differs from the currently active security context. During NAS re-keying, the MME derives the security keys for the NAS, and the NAS security mode control is used to set the new NAS EPS security context. If the K_{ASME} is changed, the NAS re-key procedure will be followed by an AS re-key.

Key refresh for the AS occurs when the eNB detects that the PDCP COUNT values are about to wrap around. This process is triggered by the eNB through the AS intra-cell handover procedures. Similarly, key refresh for the NAS occurs when the MME detects that the NAS COUNT values are about to wrap around. A new EPS AKA procedure is initiated by the MME, and the entire key hierarchy is re-keyed.

Network Domain Security (NDS)

Protection of IP-based interfaces in EPS is implemented in accordance with recommendations outlined in 33.210 [10], which defines the security architecture for Network Domain IP-based (NDS/IP) interfaces. Security protection is provided at the network layer using IPSec security protocols as defined by the IETF in RFC 2401 [11].

Table 4 lists the security services provided by the NDS/IP through the IPSec security framework:

Table 4. Security services provided by the NDS/IP interfaces

Data integrity	Mandatory
Data origin authentication	Mandatory
Anti-replay protection	Mandatory
Confidentiality (encryption)	Optional
Limited protection against traffic flow analysis with confidentiality applied	Offered as ESP is used in tunnel mode

The features listed in Table 5 are defined as minimum IPSec features that must be supported in NDS/IP usage and are discussed in this section. Refer to RFC 2401 [11] and RFC 4303 [12] for a more complete discussion of IPSec security services and Encapsulating Security Payload (ESP) protocols.

Table 5. IPSec features supported in NDS/IP

Security protocol	Encapsulating security payload ESP (RFC 4303/2406) with support for RFC 4303 as priority
Security mode	Tunnel (mandatory) Transport (optional)
Encryption algorithms	Null (RFC 2410) 3DES-CBC (RFC 2405/2451) with 3x64-bit key, 64-bit block size AES-CBC (RFC 3602) with 128-bit key, 128-bit block size
Authentication algorithm	HMAC-SHA-1-96 (RFC 2404) with 160-bit key, 512-bit block size Null is not to be supported
Security association	Single (mandatory) Bundle (optional)

Internet key exchange protocols IKEv1 and IKEv2 are used in NDS/IP networks to negotiate, establish and maintain security associations between SEGs. IKEv1 and IKEv2 are not interoperable. It is recommended that both IKE versions—IKEv1 and IKEv2—be supported in the Security Gateway (SEG). IKEv2 is used if it is common across Security Association (SA) peers; otherwise IKEv1 is used. Encryption and authentication algorithms required by IPSec for confidentiality and integrity protection forms parts of the key requirements for IKE. Further details for IKEv1 are available in RFC 2407 [13], RFC 2408 [14] RFC 2409 [15], and IKEv2 RFC-4306 [16].

ESP tunnel mode processing for IPv4 packets is shown in Figure 8 (RFC 4303 [12]).

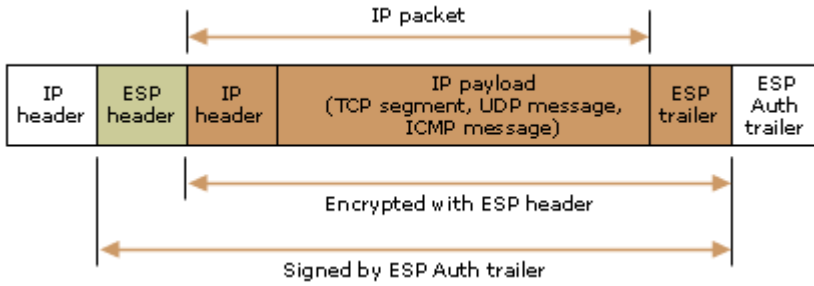

Figure 8. ESP tunnel mode processing(RFC 4303 [12])

Figure 9 shows the substructure of the IP payload data including the ESP header (RFC 4303 [12]).

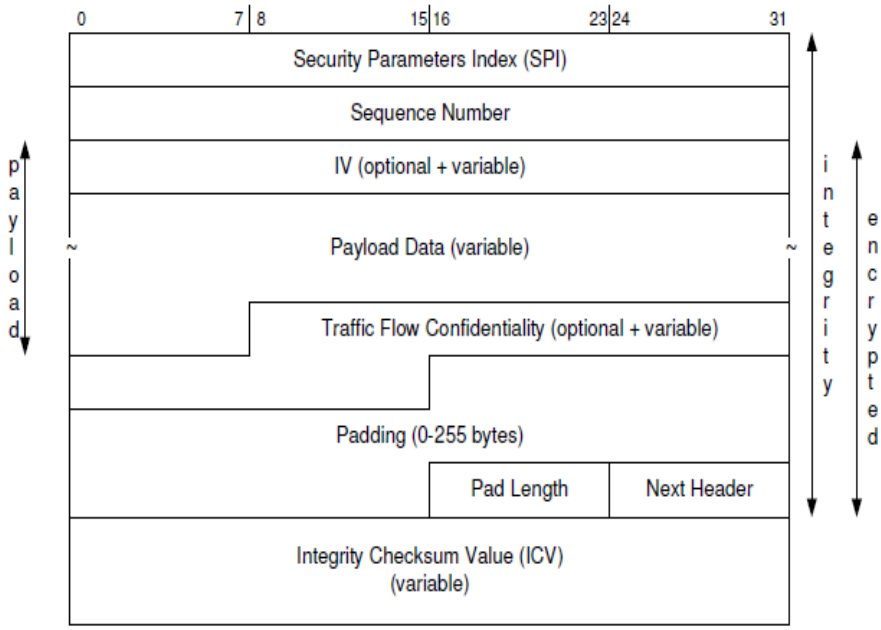

Figure 9. Substructure of payload data with ESP header(RFC 4303 [12])

Figure 10 shows the separate encryption and integrity algorithms used to process the payload data (RFC 4303 [12]).

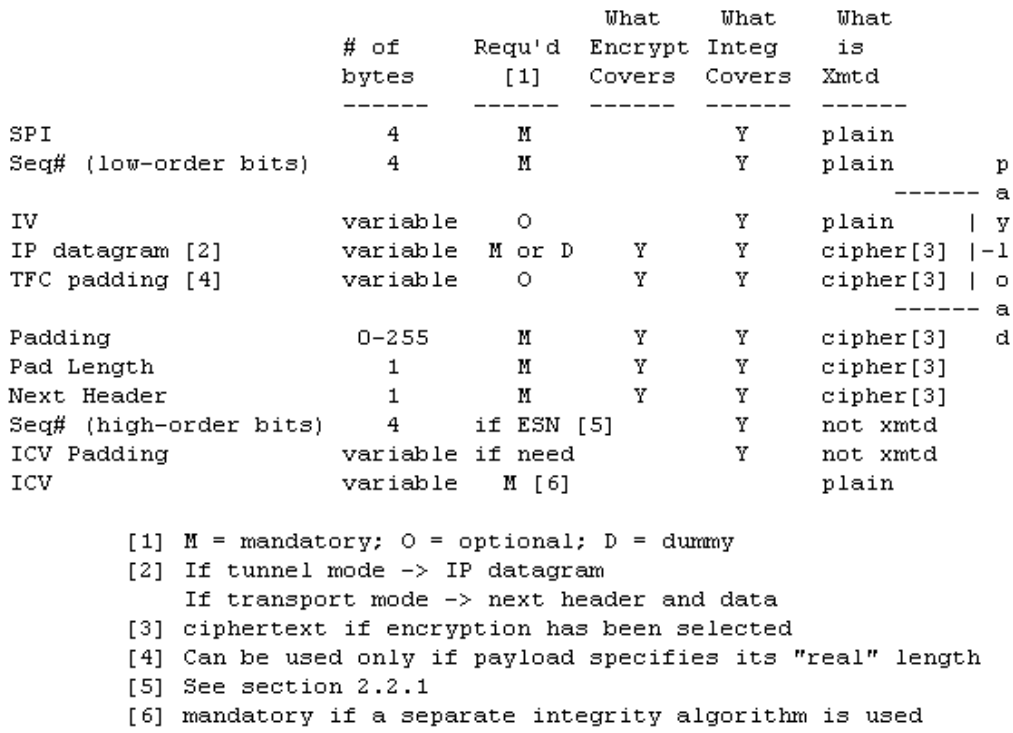

Figure 10. Separate encryption and integrity algorithms used for network domain security (RFC 4303 [12])

In tunnel mode, the ESP protects the entire inner IP packet, including the inner IP header. A new IP header will be created containing the IP addresses of the IPSec security association peers (that is, the security gateways), with the Protocol Id set to an ESP value of 59.

The ESP can be operated with or without enabling the confidentiality protection. If confidentiality protection is not enabled, null encryption is used. In this case, in tunnel mode, the original IP frame inclusive of header and payload is still encapsulated in the tunneled ESP frame, but the payload will not be encrypted.

When both confidentiality (encryption) and integrity protection are enabled, encryption is performed before integrity protection; in other words, integrity protection is provided on the encrypted payload.

An ESP header is inserted after the new IP header. This ESP header consists of a 32-bit Security Parameter Index (SPI) and a 32-bit Sequence Number (SN).

An ESP trailer is appended after the tunneled IP datagram. This ESP trailer consists of the following:

- Traffic Flow Confidentiality (TFC) padding
- Padding
- Pad length
- Next header
- Extended Sequence Numbering (higher order, 32-bit)

Security associations are uniquely identified by the following parameters at the receiver:

- Security Parameter Index (SPI)
- Destination IP address (SA end point)
- Security protocol (ESP in NDS/IP)

The Security Parameter Index is a 32-bit arbitrary value and is allocated when the SA is created.

The 32-bit Sequence Number (SN) is a per-SA packet sequence number and must be incremented by 1 for each of the sender's outbound packets. The SN is initialized with a value of 0 when the SA is established, and the first packet sent takes a value of 1. If anti-replay is enabled, the transmission SN is not allowed to be recycled. Hence a new SA must be established to replace the current SA before sender transmits the final outbound packet.

A 64-bit Extended Sequence Numbering (ESN) is introduced in RFC 4303 [12] to support high speed environments. Use of the ESN mechanism is negotiated through the SA management protocol, though in IKEv2, the default is assumed to be 64-bit ESN. In this case use of the 32-bit SN has to be explicitly negotiated. If ESN is in use, an SN transmitted in the SN field within the ESP header contains only the lower-order 32 bits. If separate encryption and integrity algorithms are used, the higher-order 32 bits are not transmitted as part of the

IPSec ESP packet, although they are still be included in the Integrity Check Value (ICV) computation.

An **Initiation Vector** (IV) is explicitly required for encryption algorithms operating in Cipher Block Chaining (CBC) mode—for example, 3DES-CBC or AES-CBC. This IV is prefixed before the payload data (or, in the case of tunnel mode, before the entire original IP header and payload) for 3DES-CBC and AES-CBC, and the IV is not encrypted. The IV field is the same size as the encryption algorithm in use. The 3DES-CBC and AES-CBCI are 64-bits and 128-bits, respectively. Note that SAs in which ESP null encryption is enabled do not have the IV preceding the payload data.

Payload data in the case of tunnel mode consists of the entire IP datagram, including the IP header and payload information.

Traffic Flow Confidentiality (TFC) padding is used to hide traffic characteristics relative to the traffic flow confidentiality requirements and is optional. It can be added only if the payload data contains the original length of the IP datagram, which is always true in tunnel mode.

Padding for the data to be encrypted must align to either (a) block size of the CBC encryption algorithm or (b) a 4 byte boundary. Since 3DES-CBC and AES-CBC both have block sizes divisible by 4 bytes, satisfying (a) will automatically meet the requirements for (b). Data to be encrypted includes payload data, Transport Format Combination (TFC) padding, padding, pad length and next header field. It does not include the IV, which is non-encrypted, as described earlier.

Pad length indicates the number of padding bytes, excluding any TFC padding bytes.

Next header is used to indicate the type of data contained in the payload data field—for example, an IPv4 or IPv6 datagram or the next layer header and data. Value of the next header field is chosen from the IP protocol numbers defined by IANA (http://www.iana.org/assignments/protocol-numbers/). Thus IPv4 uses a value of 4, IPv6 uses 41, and so on.

The **Integrity Check Value** (ICV) is computed over the ESP header, payload (inclusive of IV), ESP trailer and, if available, the integrity padding and higher-order ESN (32-bit) fields. Note that although used for ICV computation, integrity padding and higher-order ESN are not transmitted as part of the ESP packet with separate encryption and integrity algorithms implemented. HMAC-SHA-1-96 produces a 160-bit authenticator value of which the first 96 bits are stored in the ICV. The receiver computes the 160-bit authenticator value and uses only the first 96 bits, which are compared to the value stored in the ICV. As mentioned previously, the ICV is computed over an encrypted payload.

ICV padding is used for ICV computation, although it is not transmitted. HMAC-SHA-1-96 operates on a 64-byte block of data; thus ICV padding is used to pad up to a 64-byte boundary.

Fragmentation may be performed before and after ESP processing. In tunnel mode, ESP can be applied on an IP fragment, but this is not usually so in transport mode. In this case ESP is applied to the whole IP datagram. When applied on an IP fragment, ESP packets may also be fragmented either through the IPSec implementation or via en-route routers. IP reassembly must be performed prior to ESP processing or, in tunnel mode, after ESP processing. Such processing complicates the SA bundle application.

SA bundle refers to a sequence of SAs through which data is processed to satisfy the requirements of a set of security policies. SAs in the bundle may terminate at different end points. For example, it is possible to have ESP tunneling within another ESP tunnel. This feature is not mandatory for NDS/IP purposes, as a single ESP SA is expected to sufficiently secure the link between the end nodes.

Anti-replay, often referred to as a partial sequence integrity protection service offered in IPSec, is used to detect the arrival of duplicate IP datagrams by maintaining an anti-replay window at the receiver that validates the IPSec packet sequence number marked by the transmitter. Packets classified as duplicates are not processed further by the receiver. Anti-replay is enabled only if integrity protection is activated. See RFC 4303 [12] for more details.

Network Domain Security Architecture

Figure 11 shows the NDS architecture for IP based protocols. The network domain of the NDS/IP network is logically and physically partitioned into security domains. Security domains are separated by security gateways (SEGs). These gateways are border entities of the security domains, providing secure access for inter-domain security on the Za interface, over which all inter-domain data passes. More than one SEG may be used for each security domain. SEGs implement IKEv1 and IKEv2 and offer capabilities for long term key storage. The Zb interface is defined to provide secure access for intra-domain security.

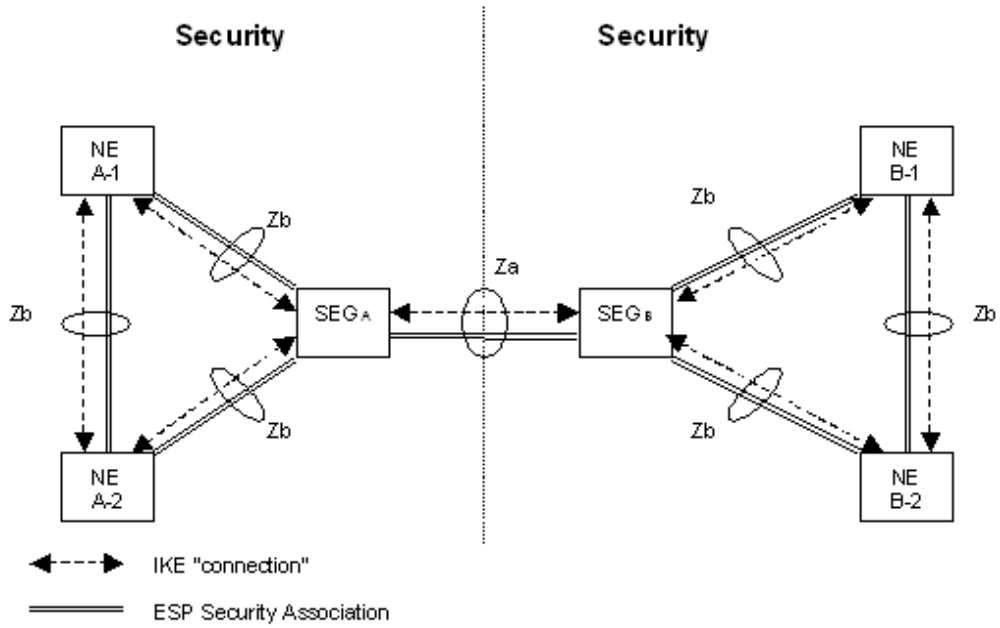

Figure 11. NDS architecture for IP-based protocols (33.210 [10] Figure 1)

Table 7 summarizes some of the key aspects of the NDS Za and Zb interfaces outlined in 33.210 [10].

Table 7. Requirements for NDS interfaces

NDS interfaces	Za	Zb
Implementation	Mandatory	Optional
Authentication/integrity	Mandatory	Mandatory
Encryption	Optional	Optional
Security protocol	ESP	ESP
Security mode	Tunnel	Tunnel Transport (optional)
Security scope	Inter-domain	Intra-domain
Termination points	SEG-SEG	SEG-NE or NE-NE
IKE support	IKEv1 and IKEv2	IKEv1 and/or IKEv2

EPS Applicability

Technical specification 33.401 [1] recommends protection for the control, user and management planes at the transport network layer of the EPS. This protection is provided through the NDS/IP security framework outlined in 33.210 [10]. Recommended security services include integrity, confidentiality and anti-replay.

The following are requirements are also to be implemented in the eNB:

- Security protocol: ESP (RFC 4303 [12])
- Security mode: tunnel (mandatory) with transport (optional)
- IKE version: IKEv2

A SEG for SA termination may be optional at the EPC-end. Further, if the physical interfaces are protected (trusted environments), NDS/IP security framework protection may not be necessary.

Security Architecture in IMS

The IP Multimedia Subsystem (IMS) is expected to be a key component of the LTE-SAE architecture. Five security associations for protection of the IMS are defined in 33.203 [17] and shown in Figure 12. This security architecture is implemented in the IMS Core Network Subsystem (IM CN SS).

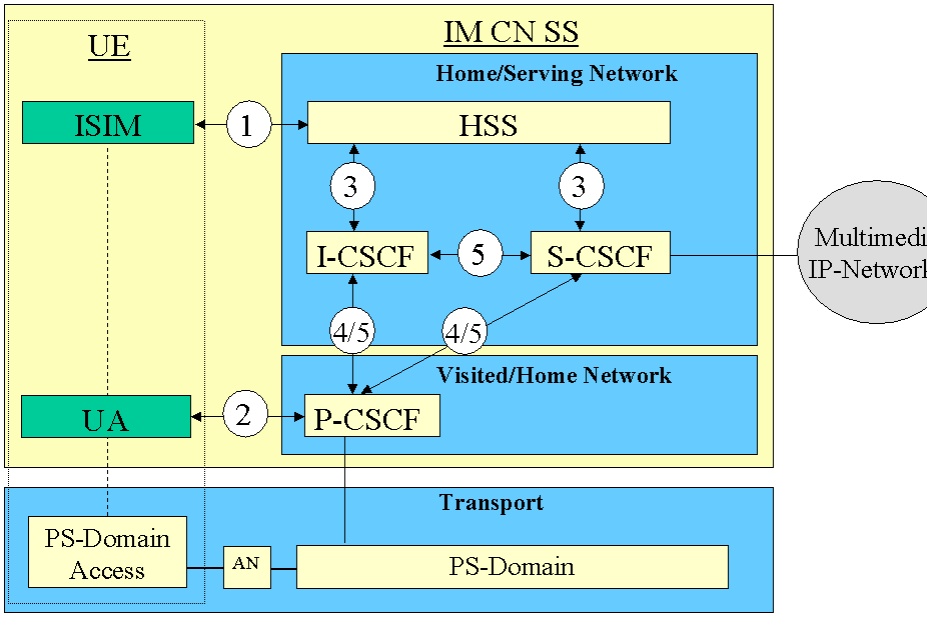

Figure 12. IMS security architecture (33.203 [17] Figure 1)

Five different security associations address different needs for IMS security protection as follows:

1. Mutual authentication provides authentication of subscriber IM Services Identity Module (ISIM) with the Home Subscriber Server (HSS) through the Serving Call Session Control Function (S-CSCF).

2. Network access (Gm) establishes a secure link and a security association between the UE and a Proxy Call Session Control Function (P-CSCF) for protection of the Gm reference point. Data origin authentication is provided.

3. Network domain (Cx) provides security within the network domain—between HSS and Interrogating Call Session Control Function (I-CSCF) and between HSS and S-CSCF—for protection of the Cx-interface.

4. Network domain (Mw) provides security between different networks for Session Internet Protocol (SIP) capable nodes. This security association is only applicable when the P-CSCF resides in the Visited Network (VN)

5. Network domain (Mw) provides security within the network internally between SIP capable nodes. This security association also applies when the P-CSCF resides in the Home Network (HN)

With the exception of the Gm interface, all interfaces and reference points in the IMS inclusive of (3), (4) and (5), whether they are in the same or different security domains, are protected as specified in 33.210 [10] for the NDS/IP framework.

Secure Access to the IMS

The IMS Authentication and Key Agreement (AKA) procedure is used to provide mutual authentication between the user and the home network. The IMS AKA uses the same concept and principles as the UMTS/EPS AKA procedure. Usually it is performed when the UE registers with the IMS CN, before access is granted. The IMS AKA procedure creates an IMS security context.

Figure 13 shows a successful IMS AKA procedure for an unregistered IMS user. The UE attempts to register with the IMS CN, sending a SIP register message towards the IMS CN, which is routed onwards to the S-CSCF.

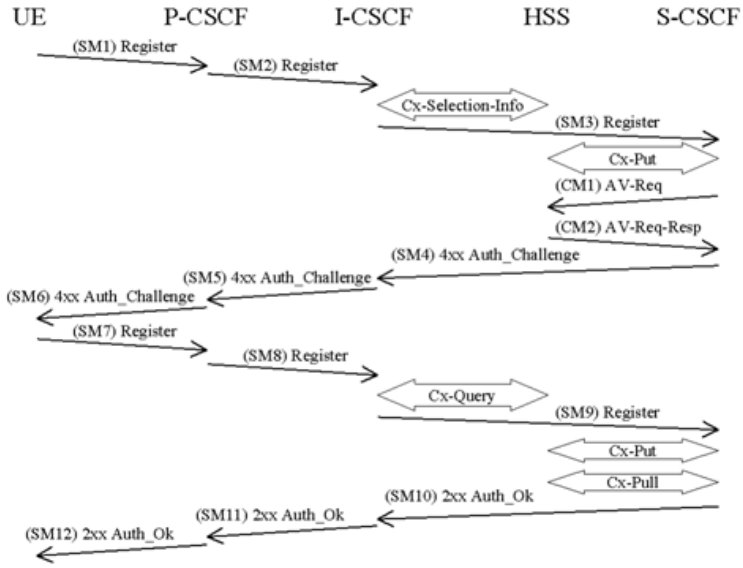

Figure 13. Successful IMS AKA procedure (33.203 [17] Figure 4)

Authentication Data Retrieval

Authentication information is retrieved from the HSS in the home network upon request by the S-CSCF in the IMS CN. This request is sent over the Cx interface. The authentication request (CM1: Cx-AV-Req) includes the IP Multimedia Private Identity (IMPI), IP Multimedia Public Identity (IMPU), S-CSCF Id, and number of requested Authentication Vectors (AV) that the S-CSCF is prepared to receive.

Upon receipt of the authentication request from the S-CSCF, the HSS returns one or more IMS AVs to the S-CSCF via an authentication request response (CM2: Cx-AV-Req-Resp) consisting of the RAND, XRES, AUTN, CK and IK in an ordered array. Each AV is valid for one IMS AKA transaction between the S-CSCF and UE. Message level details can be found in 29.228 [18] and 29.229 [19].

UE Authentication

Authentication of the UE is initiated by the S-CSCF. If the S-CSCF does not have any valid IMS AV available, a request is made to the HSS prior to authenticating the UE. The S-CSCF then

selects an AV from the ordered list retrieved from the HSS, and sends an authentication challenge to the P-CSCF with the following authentication parameters: RAND, AUTN, IK, and CK. The P-CSCF stores the AV sent from the S-CSCF and forwards the authentication challenge to the UE with the IK and CK parameters removed.

The UE must respond with an authentication response (including XRES) upon successful processing of the authentication challenge data. The CK and IK session keys are computed in the UE at this time. The authentication response is received by the P-CSCF and forwarded to the S-CSCF. Once the S-CSCF has validated the correctness of the XRES received, the IMS AKA is successfully completed. The UE is now registered with the IMS CN.

Confidentiality and Integrity

A ciphering mechanism can be used to provide SIP signalling confidentiality between the UE and the P-CSCF at the Gm reference point. Similarly, an integrity and replay protection mechanism can be used to provide SIP signalling integrity between the UE and the P-CSCF at the Gm reference point.

IPSec is used to provide confidentiality and integrity for all SIP messages exchanged over the Gm interface. Table 8 lists the IPSec features that are used.

Table 8. IPSec features for confidentiality and integrity of SIP messages

Security protocol	Encapsulating security payload (RFC 2406)
Security mode	Transport UDP encapsulated tunnel (with NAT-T Enabled) (RFC 3948)
Encryption algorithms (confidentiality)	Null (RFC 2410) 3DES-CBC (RFC 2405/2451) with 3x64-bit key, 64-bit block size AES-CBC (RFC 3602) with 128-bit key, 128-bit block size
Authentication algorithm (integrity)	HMAC-SHA-1-96 (RFC 2404) with 160-bits key, 512-bit block size HMAC-MD5-1-96 (RFC 2403) with 128-bits Key, 512-bits Block Size
Security associations	2 pairs of unidirectional SAs shared by TCP/UDP a. UE [client port] and P-CSCF [server port] b. UE [server port] and P-CSCF [client port]

The ESP SAs are set up during the SIP registration process as part of the authenticated registration procedure. Two pairs of unidirectional SAs are established between the UE and P-CSCF as a result of successful registration. Agreement is made concerning the encryption and integrity algorithms that will be used as part of the SA parameters.

The encryption key CKESP and the integrity key IKESP apply for both pairs of simultaneously established SAs. These are derived from the CKIM and IKIM, respectively, using a key expansion function.

A security mode setup procedure is used to negotiate the SA parameters to be used for IMS confidentiality and integrity protection. These parameters are further described in Table 9.

Table 9. SA parameters used for IMS confidentiality and integrity protection

Parameter	Value	Negotiation Status
Security mode	Transport UDP encapsulated tunnel (with NAT-T enabled) (RFC 3948)	Yes (with NAT-T enabled)
Encryption algorithms (confidentiality)	NULL (RFC 2410) 3DES-CBC (RFC 2405/2451) AES-CBC (RFC 3602)	Yes
Encryption key length	In accordance with encryption algorithm selected	No
Authentication algorithm (integrity)	HMAC-SHA-1-96 (RFC 2404) HMAC-MD5-1-96 (RFC 2403)	Yes
Integrity key length	In accordance with integrity algorithm selected	No
Security parameter index	Allocated for inbound SAs; one for each SA	Yes
Life type	Seconds	No
Duration (lifetime)	232-1	No

SA selectors include the following:

- IP addresses for the two pairs of SAs
- Transport port for both the TCP and the UDP
- 2 ports each at the P-CSCF and UE, one for the client and one for the server

All SIP messages exchanged in the SAs need to be ESP protected. Non ESP protected messages should be exchanged over non-protected ports. See 33.203 [17] for a list of messages that may be exchanged unprotected after the IMS security context has been activated. Any messages other than those listed that are not received from a protected port will be rejected and discarded.

Figure 14 shows the SA setup sequence during a security setup procedure. The UE triggers this procedure by sending the following security setup parameters to the P-CSCF: SPI_U, Port_U, UE encryption and integrity algorithm list. The security setup parameters are sent using

a SIP register message. The SPI_U and Port_U parameters contain the SPIs and client ports allocated by the UE for the protected client and server ports.

The P-CSCF selects the SPIs (SPI_P) and port numbers (Port_P) to be used for the protected client and server ports of the SAs. The P-CSCF also selects an encryption and integrity algorithm by matching its internally supported list with those sent by the UE. It returns these selections to the UE: SPI_P, Port_P, and P-CSCF encryption and integrity algorithms list. The UE responds with the SPI_U, Port_U, SPI_P, Port_P, and P-CSCF encryption and integrity algorithms list. The message is now encrypted and integrity protected, and a response is sent to the UE indicating successful IMS security context activation.

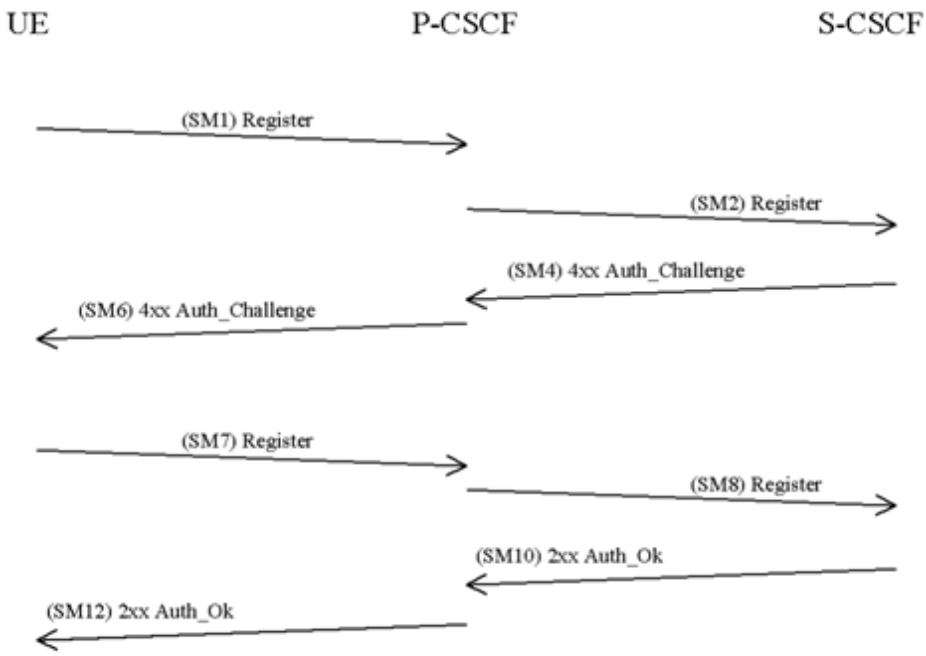

Figure 14. SA setup sequence (33.203 [17] Figure 8)

IMS Key Hierarchy

Table 10 summarizes the hierarchy and relationships between the various security keys used in IMS AKA over the Gm reference point. See 33.203 [17] for more details on IMS key derivation.

Table 10. Security keys for IMS AKA over Gm

Key	Purpose	Length	Derived from	Description
IK_{IM}	Base Integrity Key for IMS	128	-	Integrity Key IMS Derived as part of IMS AKA
IK_{ESP}	Integrity Key for Gm HMAC-MD5-96	128	IK_{IM}	$IK_{ESP} = IK_{IM}$
	Integrity Key for Gm HMAC-SHA-1-96	160	IK_{IM}	$IK_{ESP} = IK_{IM}$+32 Trailing '0's
Same IK_{ESP} Applies for Both Pairs of Simultaneously Established SAs				
CK_{IM}	Base Encryption Key for IMS	128	-	Encryption Key IMS Derived as part of IMS AKA $CK_{IM} = CK_{IM1} \mid\mid CK_{IM2}$, Each of Block 64-bits
CK_{ESP}	Encryption Key for Gm DES-EDE3-CBC	192	CK_{IM}	$CK_{ESP} = CK_{IM1} \mid\mid CK_{IM2} \mid\mid CK_{IM1}$
	Encryption Key for Gm AES-CBC	128	CK_{IM}	$CK_{ESP} = CK_{IM}$
Same CK_{ESP} Applies for Both Pairs of Simultaneously Established SAs				

IMS CN Applicability

Technical specification 33.203 [17] recommends protection for all IMS CN interfaces at the transport network layer. This protection is based on the NDS/IP security framework outlined in 33.210 [10]. Protection should include integrity, confidentiality, and anti-replay services.

The following requirements are to be implemented in the eNB:

- Security protocol: ESP (RFC 4303)
- Security mode: tunnel (mandatory) with transport (optional)
- IKE version: IKEv2

A SEG may be optional at the EPC-end for SA termination. If the physical interfaces are protected (trusted environments), the NDS/IP security framework protection may not be necessary.

References

[1] 3GPP TS 33.401 V8.2.1 (2008-12) 3GPP System Architecture Evolution (SAE); Security architecture

[2] 3GPP TS 33.402 V8.2.1 (2008-12) 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses

[3] 3GPP TS 33.102 V8.1.0 (2008-12) 3G security; Security architecture

[4] 3GPP TS 23.003 V8.3.0 (2008-12) Technical Specification Group Core Network and Terminals; Numbering, addressing and identification

[5] 3GPP TS 23.401 V8.4.0 (2008-12) General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

[6] 3GPP TS 24.301 V8.0.0 (2008-12) Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3

[7] 3GPP TS 29.272 V8.1.1 (2009-01) Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol

[8] 3GPP TS 33.323

[9] 3GPP TS 36.331 V8.4.0 (2008-12) Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification

[10] 3GPP TS 33.210 V8.2.0 (2008-12) 3G security; Network Domain Security (NDS); IP network layer security

[11] IETF RFC 2401

[12] IETF RFC 4303

[13] IETF RFC 2407

[14] IETF RFC 2408

[15] IETF RFC 2409

[16] IKEv2 RFC-4306

[17] 3GPP TS 33.203 V8.5.0 (2008-12) 3G security; Access security for IP-based services

[18] 3GPP TS 29.228 V8.4.0 (2008-12) IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents

[19] 3GPP TS 29.229 V8.4.0 (2008-12) Cx and Dx interfaces based on the Diameter protocol; Protocol details