ETSI TS 133 163 V16.2.0 (2020-11)

TECHNICAL SPECIFICATION

LTE;
5G;
Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST)
(3GPP TS 33.163 version 16.2.0 Release 16)

Reference

RTS/TSGS-0333163vg20

Keywords

5G,LTE,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This document describes communication security and key agreement processes that are optimised for battery constrained, very low throughput Machine Type Communication (MTC) devices.

Specifically:

- N-PDU data tampering and eavesdropping
- Efficient user data protection challenges
- VPLMN Specific Needs
- End-to-end security

1 Scope

The present document defines communication security processes designed for very low throughput Machine Type Communication (MTC) devices that are battery constrained.

These processes consist of:

- A Key agreement service for End to Middle and End to End security use
- An End to Middle secure transport service that includes the ability to verify and confidentiality protect low throughput data.
- An End to End secure transport service that includes the ability to verify and confidentiality protect low throughput data.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.863: "Study on battery efficient security for very low throughput Machine Type Communication (MTC) devices".

[3] 3GPP TS 33.102: "3G security; Security architecture".

[4] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[5] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[6] 3GPP TS 55.241: "Specification of the GIA4 integrity algorithm for GPRS; GIA4 specification"

[7] 3GPP TS 55.251: "Specification of the GEA5 encryption and GIA5 integrity algorithms for GPRS; GEA5 and GIA5 algorithm specification"

[8] 3GPP TS 35.201: " Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification".

[9] 3GPP TS 35.215: "Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications"

[10] 3GPP TS 35.221: "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[11] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[12] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[13] 3GPP TS 33.220: " Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[14] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[15] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

BEST: Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices

BEST Capable UE: A UE that is enabled for the BEST service

Enterprise Key: A secret key shared by the Enterprise Application Server and the UE for application in the BEST service

EAS PSK: An Enterprise Application Service specific key derived by the HSE and the UE from the Intermediate key and meant to be forwarded to a specific EAS by the HSE.

Intermediate Key: A key derived by the HSE and the UE from CK and IK to be used to derive the EAS PSK

Intermediate Key Identifier: A key identifier that identifies an Intermediate Key

UE-to-HSE keys: Keys derived by the HSE and the UE from CK and IK to be used on control and/or user plane between the UE and HSE.

UE-to-EAS keys: Keys derived by the EAS and the UE from EAS PSK and an Enterprise Key to be used for user plane between UE and EAS.

UE-to-HSE: UE to Home PLMN Security Endpoint

UE-to-EAS: UE to Enterprise Application Server

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

EAS	Enterprise Application Server
HSE	HPLMN Security Endpoint

4 Security Procedures for Battery Efficient Security for Very Low Throughput MTC Devices (BEST)

4.1 Introduction

This specification defines elements, protocols and procedures that enable battery efficient security for low throughput devices such as MTC devices. The BEST service is a secure channel between a UE and a HSE, optimised for low throughput and high latency devices that are battery constrained. The security is between the UE and either an element in the service provider home network (the HSE) or an element in the enterprise domain (the EAS). The design is modular and extensible so that it can be used to satisfy a wide range of use cases.

The following services are defined:

- BEST key agreement only service – This service is a battery efficient service for key agreement between a BEST compliant UE and the HSE or the EAS. The user plane for this service is provided by the application layer between the UE and the EAS and is out of scope of this specification.
- BEST user plane integrity protected service – This service is a battery efficient integrity protected user plane service for low throughput devices. This service includes the key agreement and includes integrity protected security over small data over NAS User Plane. The user plane for this service can be either terminated in the HSE (so called UE-to-HSE mode) or in the EAS (so called UE-to-EAS mode). Control messages are always terminated in the HSE.
- BEST user plane confidential service – This service is a battery efficient integrity and confidentiality protected user plane service for low throughput devices. The user plane for this service can be either terminated in the HSE (so called UE-to-HSE mode) or in the EAS (so called UE-to-EAS mode). Control messages are always terminated in the HSE.

It may be possible for the UE to have concurrent BEST sessions.

4.2 BEST Framework Service Description

4.2.1 Architecture

Figure 4.2.1-1 shows the architecture of the extended user plane protection service for the case where the UE's PDN connection terminates at the P-GW. Figure 4.2.1-2 shows the architecture of the extended user plane protection service for the case where the UE's PDN connection terminates at the SCEF.

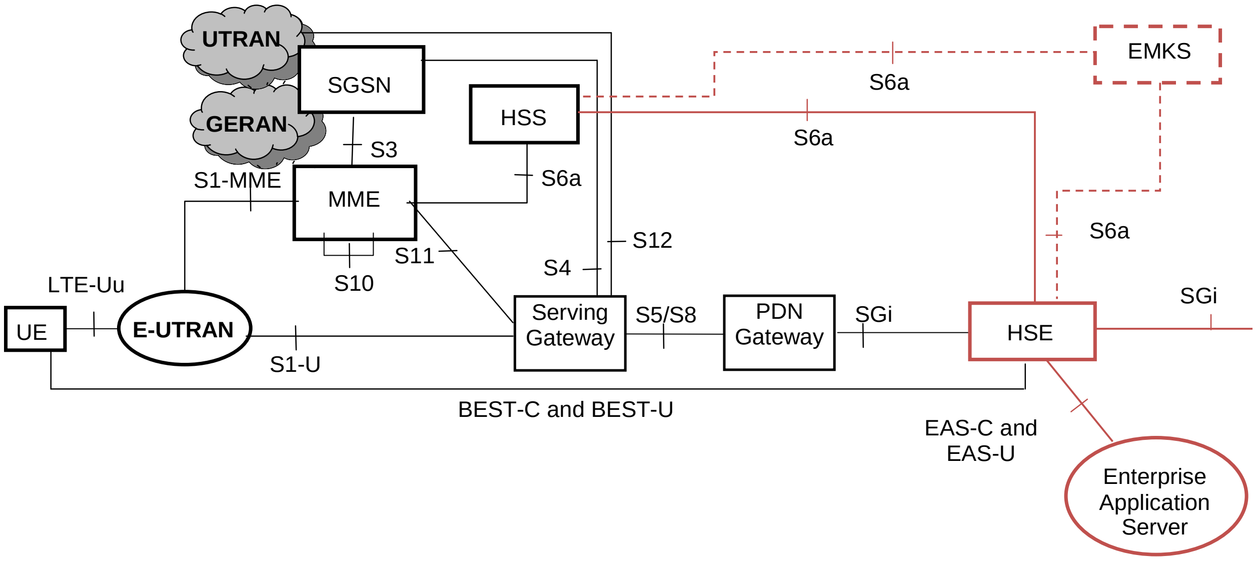

Figure 4.2.1-1: The architecture of the extended user plane protection service (P-GW Terminated PDN Connection Option)

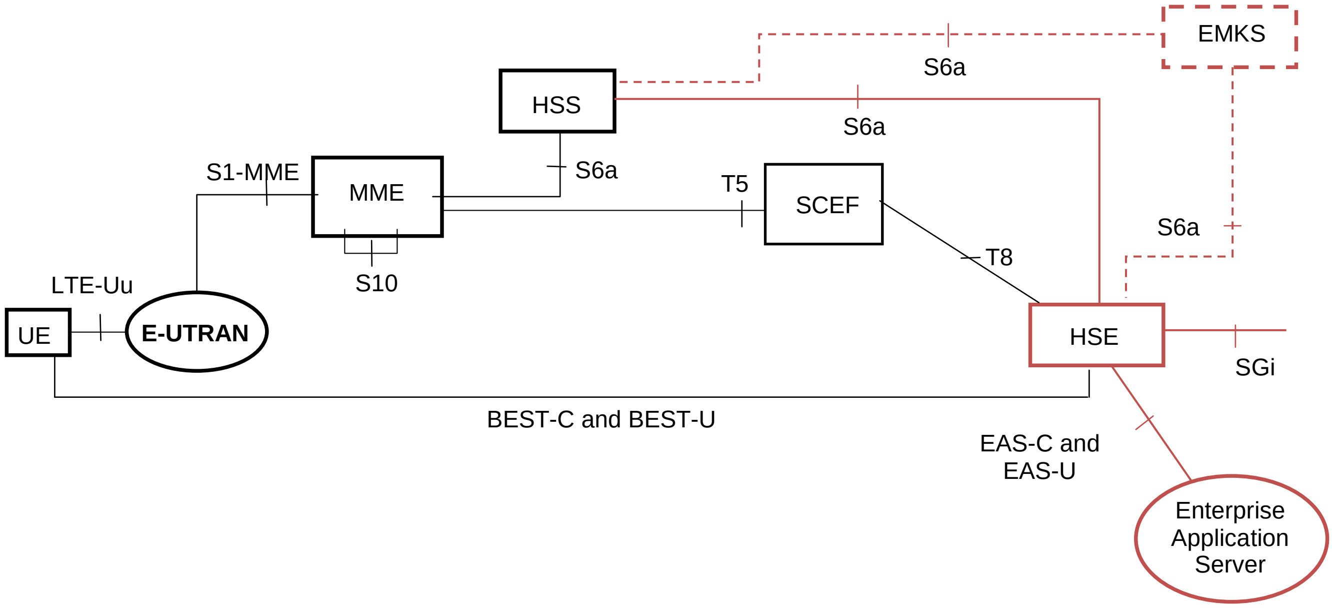

Figure 4.2.1-2: The architecture of the extended user plane protection service (SCEF Terminated PDN Connection Option)

The BEST service requires the following components:

- Home Security Endpoint (HSE) – This is the termination point in the home network that performs the following functions:
    - Terminating the control plane for BEST between the UE and the HSE
    - Terminating the secure communication for BEST between the UE and the HSE and forwarding to and from the Data Network via the SGi if UE-to-HSE security is selected.
    - Routing the user plane traffic for BEST between the UE and the Enterprise Application Server (EAS) via the SGi if UE-to-EAS security is selected.
    - Anchor for BEST Key agreement only service. Exposes an interface for EAS to obtain MNO provided pre-shared key.
- End to Middle Key Server (EMKS) – This is an optional key server element that manages the key communication with the HSS (for quintets) and stores keys to reduce loading on the HSE and HSS. The EMKS has interfaces to the HSS (S6a) and the HSE (S6a).

The BEST service uses the following interfaces:

- S6a between the HSS and the HSE
- S6a between the HSS and EMKS
- S6a between the EMKS and the HSE
- BEST-C and BEST-U between the UE and the HSE
- EAS-C and EAS-U between the HSE and the EAS. Definition of this interface is out of scope. Annex B describes a candidate interface based on Restful HTTP for the communication between the HSE and the EAS.

When the UE's PDN connection terminates at the SCEF as shown in Figure 4.2.1-2:

- The HSE may be implemented as part of the SCEF.

- The EAS may be an SCS/AS and use a T8 interface to access exposed network capabilities as described in TS 23.682 [14].
- EMSDP via the SCEF only supports non-IP PDU Type communication.

4.3 Procedures between the UE and the HSE

4.3.1 Overview of BEST procedures

To use the BEST service, the UE shall setup a PDN connection to connect to the HSE. The UE may either use a locally stored IP address to locate the HSE or use a "BEST APN" where the traffic is directed by the PDN Gateway to the correct HSE for that UE. Once a connection to the HSE exists, the UE may initiate the BEST service. It is up to the UE as to when it establishes the PDU session that is used for BEST control plane and user plane messages.

The BEST service consists of 5 general processes between the UE and the HSE: session initiation and key agreement, key management, data transfer, session termination, and message rejection. The details of the End to Middle Secure Data Protocol (EMSDP) used for the BEST control plane service and optionally for user plane security service, is detailed in clause 6.

When BEST user plane (UP) security services are used, UP data plane messages are between the UE and the HSE in UE to HSE security mode, and between the UE and the EAS in UE to EAS security mode.

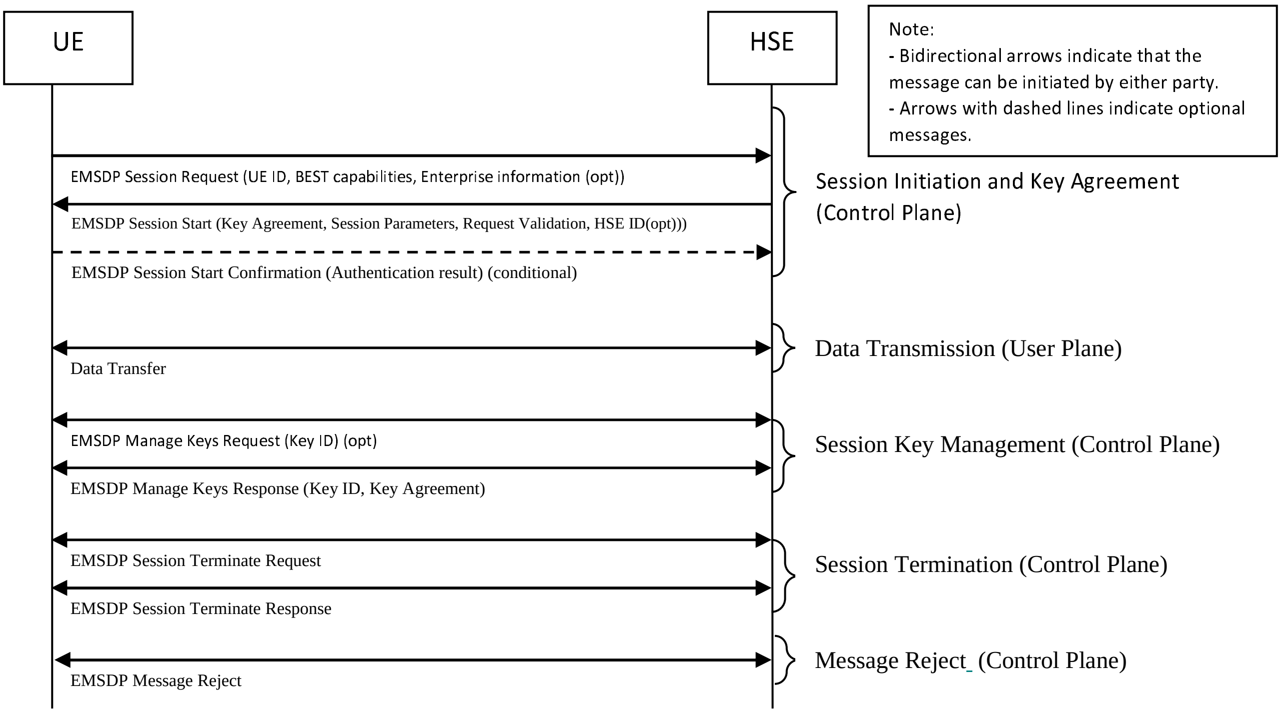
UE
HSE
Note:
- Bidirectional arrows indicate that the message can be initiated by either party.
- Arrows with dashed lines indicate optional messages.
EMSDP Session Request (UE ID, BEST capabilities, Enterprise information (opt))
EMSDP Session Start (Key Agreement, Session Parameters, Request Validation, HSE ID(opt)))
EMSDP Session Start Confirmation (Authentication result) (conditional)
Session Initiation and Key Agreement (Control Plane)
Data Transfer
Data Transmission (User Plane)
EMSDP Manage Keys Request (Key ID) (opt)
EMSDP Manage Keys Response (Key ID, Key Agreement)
Session Key Management (Control Plane)
EMSDP Session Terminate Request
EMSDP Session Terminate Response
Session Termination (Control Plane)
EMSDP Message Reject
Message Reject (Control Plane)

Figure 4.3.1-1: Generalised BEST service flow

4.3.2 BEST Session Initiation and Key Agreement

The UE shall initiate a BEST session using the EMSDP Session Request message following the establishment of the PDN connection To optimise the message flow for battery constrained devices, the EMSDP Session Response is combined with Session Key Agreement.

The EMSDP Session Request message shall include the UE Identity, BEST capabilities of the UE, the UE serving network (conditionally, cf. clause 6.2.6.1.5) and details of the enterprise service including the Enterprise server Id (EAS Id) that the BEST service is being used for.

The EMSDP Session Start message shall include the RAND and AUTN needed for a key agreement of the BEST keys, the BEST service parameters and a checksum validating the previous EMSDP Session Request message.

The HSE shall determine the parameters for the BEST service. The HSE may use the location information provided by the UE to determine whether aspects of the BEST service, such as cyphering, can be used in that location.

As a result of the key agreement exchange the UE and HSE shall derive the UE-to-HSE keys. In case of UE-to-EAS security mode and in case of Key agreement only service, the UE and HSE shall also derive the intermediate key and the EAS PSK.

To optimise the BEST service for battery constrained devices, confirmation of the BEST session start is not required. The UE sending a UP message to the HSE or EAS is by itself is an implied confirmation. However, if the BEST service is being used for key agreement only, the HSE shall require the UE to send EMSDP Session Start Confirmation by setting the indicator in the EMSDP Session Start message.

4.3.3 BEST Session Key Management

At any time during the BEST session, either the UE or the HSE may trigger a re-negotiation of the keys being used for the BEST service using the EMSDP Manage Keys Request and Response exchange. To avoid overloading of the HSE and the HSS, the HSE may throttle or not support UE triggered key renegotiation.

The newly generated keys take effect immediately for EMSDP based BEST UP services. For procedures when BEST Key management service is used to provide a pre-shared key to the application layer protocol, refer clause 4.4.4 for additional details.

4.3.4 BEST Session Termination

At any time, either the UE or the HSE may terminate the current BEST session using the EMSDP Session Termination Request and Response message exchange. Once terminated, all relevant keys and IDs shall be discarded and both the UE and HSE shall ignore further messages using that session ID, unless a session with that ID is re-established using the session initiation process.

4.3.5 BEST Message Reject

Either the UE or the HSE may at any time respond with a EMSDP Message Reject message, upon which the recipient shall discard all relevant keys and IDs of the session, and both the UE and HSE shall ignore further messages using that session ID.

The EMSDP Message Reject is also used when the HSE needs to prompt a UE to initiate a new session using the Session Start message. For example, if it receives a UP packet from the UE on a BEST session for which it aged out the context.

4.4 Procedures between the HSE and the EAS

4.4.1 Message Exchange Overview

The message exchanges between the HSE and the EAS are essentially a mirror of the ones between the UE and the HSE. All BEST control plane messages are terminated or initiated by the HSE. When BEST user plane security services are used in UE-to-EAS mode, the user plane security is end-to-end between the UE and the EAS.

NOTE: The actual details and standardization of the HSE to EAS interfaces is out of scope of this document.

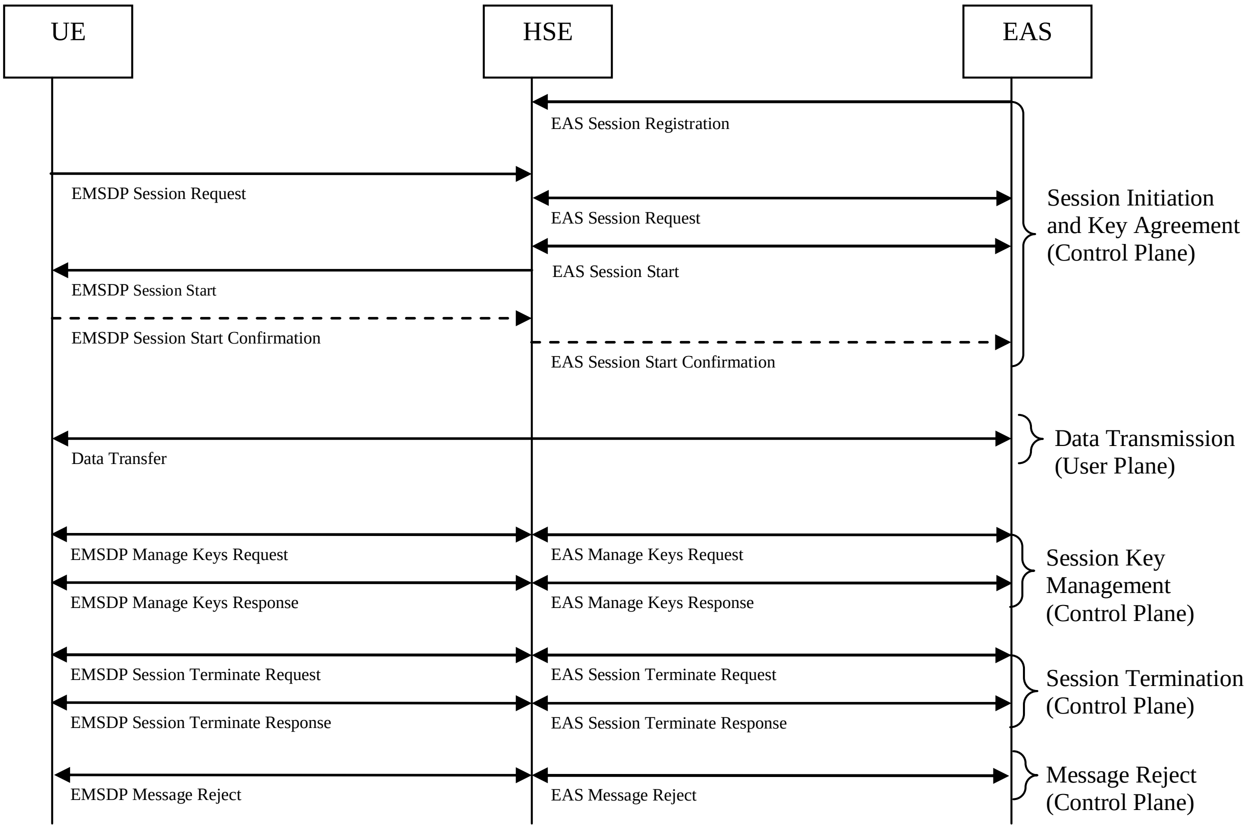
UE
HSE
EAS
EAS Session Registration
EMSDP Session Request
EAS Session Request
EAS Session Start
EMSDP Session Start
EMSDP Session Start Confirmation
EAS Session Start Confirmation
Session Initiation and Key Agreement (Control Plane)
Data Transfer
Data Transmission (User Plane)
EMSDP Manage Keys Request
EAS Manage Keys Request
EMSDP Manage Keys Response
EAS Manage Keys Response
Session Key Management (Control Plane)
EMSDP Session Terminate Request
EAS Session Terminate Request
EMSDP Session Terminate Response
EAS Session Terminate Response
Session Termination (Control Plane)
EMSDP Message Reject
EAS Message Reject
Message Reject (Control Plane)

Figure 4.4.1-1: Generalised BEST EAS service flow

4.4.2 EAS Registration for BEST Service

As a prerequisite to using BEST service, the EAS shall register with the HSE over a secure connection by providing its identity (Enterprise server Id). This results in a session context to be established in the HSE for the registered EAS.

A secure connection is established between the HSE and the EAS as part of the management of the BEST service between the Enterprise and the HSE, cf clause 7.1.

NOTE: The procedures for establishing up a secure connection and EAS registration with the HSE are out of scope of this TS.

4.4.3 Key Request

During the Key agreement procedure, described in clause 4.3.2, HSE may forward the derived key to the EAS in the EAS Session Request message.

When BEST is used for Key agreement only or when BEST UP service is used in UE-to-EAS mode, the HSE shall forward the pre-shared key (K_{EAS_PSK}) that is specifically derived for the enterprise as defined by key definition rules in clause 5.1.2. It also includes the Intermediate Key Id in this message. The EAS shall respond with the EAS Session Start message.

When BEST is used for Key agreement only, the EAS may initiate a Key Request by sending the EAS Session Request message. The UE includes Intermediate Key Id needed to identify the UE-specific Intermediate key and the associated EAS specific pre-shared key in the HSE. The EAS obtains the key identifier from the UE during application layer session establishment. The HSE shall respond with the pre-shared key (KEAS_PSK)..

4.4.4 Key Refresh

At any time during the BEST session, either the UE or the HSE or the EAS may trigger a re-negotiation of the keys being used for the BEST service. It is optional for the HSE to support UE initiated key refresh, which it signals to the UE in the Session Start message. If not supporting it, an HSE will ignore UE triggered key refresh messages.The UE and the HSE triggered re-negotiation is described in clause 4.3.3. For UE-to-EAS mode BEST UP service and BEST Key agreement only service, the newly derived pre-shared key (EAS PSK) may be sent by the HSE to the EAS. This is further described in clause 6.2.7.2.

The EAS-triggered re-negotiation of keys applies to BEST UP Service in UE-to-EAS mode. The trigger for generating new keys is appropriately propagated to the UE using EMSDP Manage Keys Request. The EAS is provided with newly derived EAS PSK from the HSE.

For BEST key-agreement only service, there is no provision for the application layer to trigger generation of the new EAS PSK. The application layer continues to use the existing pre-shared key to generate fresh session keys for consecutive instances of the protocol. When a new EAS PSK is generated in the HSE, the application layer obtains it either via an update from the HSE or when the EAS contacts the HSE again when a new application layer session is set up.

4.4.5 Session Termination

At any time, any of the BEST functions, the UE or the EAS or the HSE may terminate the current BEST session using the BEST or EAS Session Termination Request and Response message exchange. The session terminate request shall be applied to all the involved functions for a given session. Once terminated, all relevant keys and IDs shall be discarded and the UE, the EAS and HSE shall ignore further messages using that session ID, unless a session with that ID is re-established using the session initiation process.

4.4.6 Message Reject

The UE or the EAS or the HSE may at any time trigger a EAS Message Reject message, upon which the recipient shall discard all relevant keys and IDs of the session, and the UE, the EAS and HSE shall ignore further messages using that session ID.

4.5 BEST Data Service

Once the BEST session is successfully initiated, the UE or the HSE or EAS may send UP data using the negotiated keys.

If the BEST UP session is set up between the UE and the HSE, then the UP packets are initiated or terminated by the HSE. In this case, the low power optimized EMSDP protocol, as detailed in clause 6, is used.

If the BEST UP session is setup between the UE and the EAS, then the HSE passes the UP messages to the EAS after checking the message is formatted correctly and that it is a UP message. The key used by the UE and EAS to encrypt and decrypt data messages (when required) is $KE2E_{enc}$ and to integrity protect the message is $KE2E_{int}$. Verification of any Key ID, counter, message integrity and deciphering is the responsibility of the EAS.

If the BEST key agreement service is used to set up a data session between the UE and EAS, the UE and EAS need to use a security protocol with the EAS PSK other than EMSDP, e.g., IKE/IPsec or (D)TLS for user plane data transmission. In this case, the HSE does not handle the UP.

4.6 Key Management

4.6.1 Key Agreement and Refresh

4.6.1.1 Key setup messaging between HSE and UE

New keys are agreed either at the start of a BEST session or as required due to key aging or counter thresholds being met. Key agreement is based on the 3GPP AKA mechanism detailed in TS 33.102 [3] and the AKA challenge is transported between the HSE and the UE as part of the BEST service detailed in clause X.3.2. The key hierarchy is shown in clause 4.6.2.2.

The EMDSP protocol has 7 Key IDs for each session ID. Each Key ID has a separate keyset consisting of an integrity Key (K_{E2Mint}), an encryption key (K_{E2Menc}), optionally an Intermediate Key ($K_{Intermediate}$) and optionally an EAS PSK (K_{EAS_PSK}). The Key IDs shall be set during the derivations of the keys as specified in clause 5.1.

The Intermediate Key ($K_{Intermediate}$) is used together with a separate enterprise server identifier (EAS Id) to calculate the EAS PSK (K_{EAS_PSK}). There can be many KEAS_PSK derived from one $K_{Intermediate}$.

The EAS PSK ($K_{EAS\_PSK)}$ is used together with the Enterprise Key to calculate K_{E2Eint} and K_{E2Eenc} when BEST User plane security services are used in UE-to-EAS mode.

Figure 4.6.1.1-1 shows the generic key agreement process:

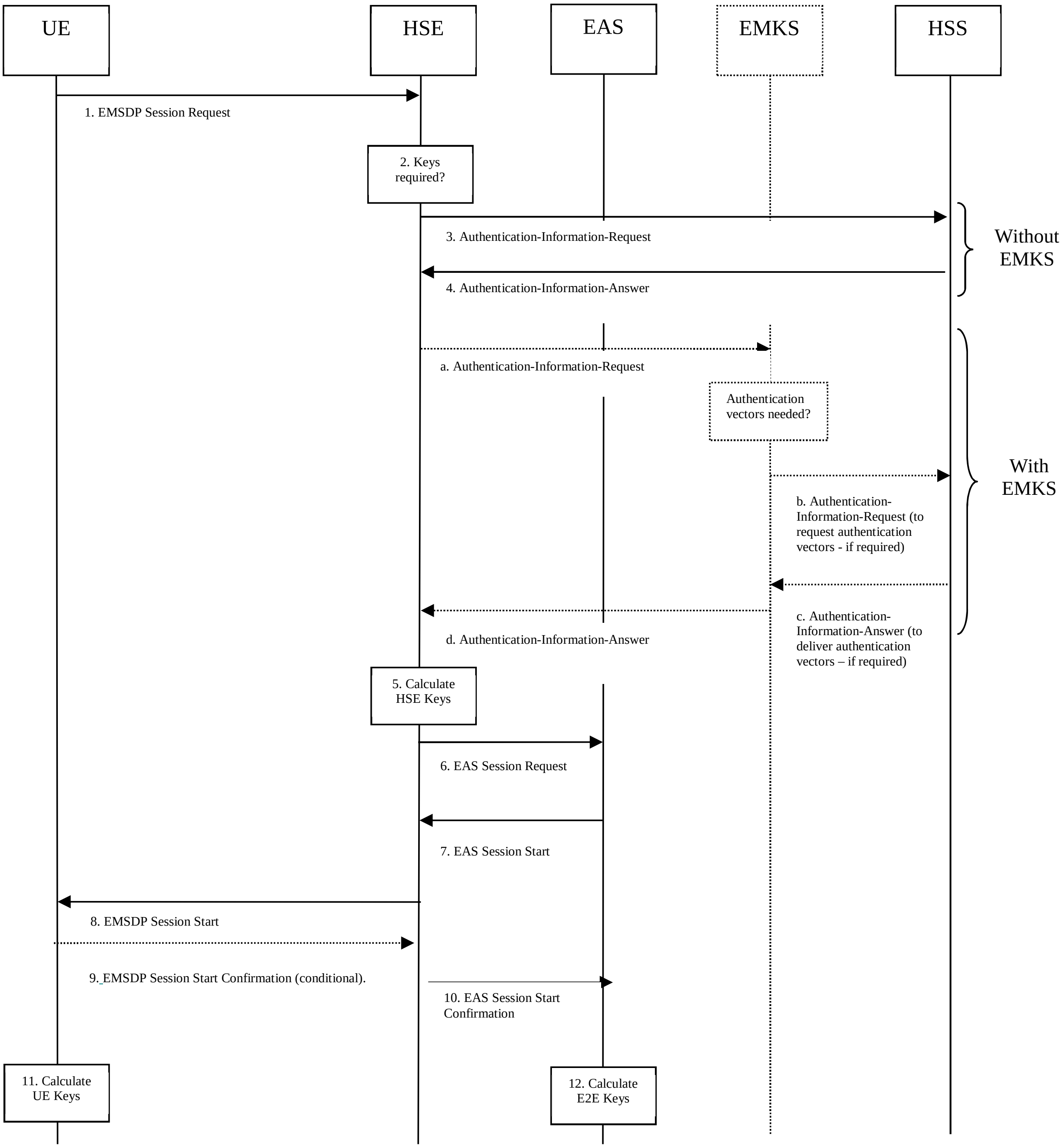
UE
HSE
EAS
EMKS
HSS
1. EMSDP Session Request
2. Keys required?
3. Authentication-Information-Request
4. Authentication-Information-Answer
Without EMKS
a. Authentication-Information-Request
Authentication vectors needed?
b. Authentication-Information-Request (to request authentication vectors - if required)
With EMKS
c. Authentication-Information-Answer (to deliver authentication vectors – if required)
d. Authentication-Information-Answer
5. Calculate HSE Keys
6. EAS Session Request
7. EAS Session Start
8. EMSDP Session Start
9. EMSDP Session Start Confirmation (conditional).
10. EAS Session Start Confirmation
11. Calculate UE Keys
12. Calculate E2E Keys

Figure 4.6.1.1-1 Generic BEST key agreement process

The Key agreement steps are:

1. **EMSDP Session Request (UE ID, BEST capabilities, Enterprise information (opt), location ID).** The UE shall send the EMSDP Session Request (UE ID, BEST capabilities, Enterprise information (opt) to set up a new BEST session.

2. **Keys required?** - the HSE shall check to see if there are valid keys with valid counter values available in the HSE for that UE then the following is checked:

   - If the HSE has a valid set of keys for the indicated session and the UE ID is valid for that session then the HSE may start the BEST session without re-negotiating the keys (step 8).

- If the UE ID is valid for that HSE and the HSE does not have a valid set of keys for the indicated session or the HSE wishes to update the keys, then it shall first renegotiate the keys (steps 2 to 7) and then start the BEST session (step 8).

- If the UE ID is not valid for that session ID or the UE does not support the level of service required by the HSE or the enterprise information is not valid for the HSE, then the HSE may reject the command.

3**. Authentication-Information-Request over S6a interface** – The HSE shall use the S6a interface to the HSS to request one or more authentication vectors using the UE IMSI.

4. Authentication-Information-Answer over S6a interface – The HSS uses the S6a interface to the HSE to return the requested authentication vectors.

a. Authentication-Information-Request over the S6a interface between HSE and EMKS – Where an EMKS is used, the HSE shall use the S6a interface to the EMKS to request an authentication vector using the UE IMSI.

b. Authentication-Information-Request over the S6a interface between EMKS and HSE – The EMKS shall use the S6a interface to the HSS to request one or more authentication vectors using the UE IMSI.

c. Authentication-Information-Answer over the S6a interface between EMKS and HSE – The HSS shall use the S6a interface to the EMKS to return the requested authentication vectors. These vectors may be stored on the EMKS for later use.

d. Authentication-Information-Answer over the S6a interface between HSE and EMKS – The EMKS uses the S6a interface to the HSE to return the requested authentication vector.

5. Calculate UE-to-HSE Keys - See key derivation details in clause 5.

6. The HSE may optionally send "EAS Session Request" to the EAS– In case BEST UP service is used in UE-to-EAS mode, the HSE shall use the HSE interface to the EAS to inform the EAS of the new UE-to-EAS session request and shall forward the EAS PSK (K_{EAS_PSK}) to the EAS. In case the BEST key agreement service is used, the HSE shall forward to the EAS, the EAS PSK (K_{EAS_PSK}) and the key identifier for the Intermediate Pre Shared Key ($K_{Intermediate}$).

7. The Enterprise Server sends a "EAS Session Start" to the HSE – The Enterprise Server shall respond by sending the "UE-to-EAS Session Start" message. In case BEST UP service is used, this message may contain an EAS container that includes an identifier for the Enterprise Key.

8. EMSDP Session Start message - The HSE shall send a EMSDP Session Start (Key Agreement, Session Parameters, Request Validation, HSE ID(opt) , EAS container (opt)).

9. **EMSDP Session Start Confirmation** - UE optionally, if requested in the Session Start Confirmation, responds with an EMSDP Session Start Confirmation message.

10. EAS Session Start Confirmation - The HSE may optionally send EAS Session Start Confirmation.

11. Calculate UE Keys – See key derivation details in clause 5.

12. Calculate UE-to-EAS Keys – In case of the UE-to-EAS BEST UP service, the Enterprise server generates UE-to-EAS keys as per the key derivation details in clause 5.

4.6.1.2 Usage of Keys

For UE-to-HSE BEST UP sessions, the following keys shall be used:

- The K_{E2Menc} shall be used by the UE and the HSE for the encryption of the user plane and the control plane, according to the agreed encryption algorithm.

- The K_{E2Mint} shall be used by the UE and the HSE for the integrity protection of the user plane and the control plane according to the agreed integrity protection algorithm.

For UE-to-EAS BEST UP sessions, the following keys shall be used:

- The K_{E2Menc} shall be used by the UE and the HSE for the encryption of the control plane, according to the agreed encryption algorithm.

- The K_{E2Mint} shall be used by the UE and the HSE for the integrity protection of the control plane according to the agreed integrity protection algorithm.

- The K_{E2Eenc} shall be used by the UE and the EAS for the encryption of the user plane, according to the agreed encryption algorithm.

- The K_{E2Eint} shall be used by the UE and the EAS for the integrity protection of the user plane according to the agreed integrity protection algorithm.

For key-agreement only BEST service, the following key shall be used:

- The EAS PSK (K_{EAS_PSK}) shall be used by the EAS and UE for protection of the user plane between the EAS and UE. The protocol to be used between the UE and EAS is out of scope of this specification. Optionally, further keys may be derived from the EAS PSK.

NOTE: As the K_{EAS_PSK} is known to the HSE, the EAS and the UE will have to transform the key further to achieve end to end security. This transformation is out of scope of this specification.

- The K_{E2Menc} shall be used by the UE and the HSE for the encryption of the control plane, according to the agreed encryption algorithm.

- The K_{E2Mint} shall be used by the UE and the HSE for the integrity protection of the control plane according to the agreed integrity protection algorithm.

4.6.1.3 Key Setup for BEST session end point modification

The modification of a BEST UE-to-EAS UP session to a BEST UE-to-HSE UP session does not require any new calculations of keys.

The modification of a BEST UE-to-HSE UP session to a BEST UE-to-EAS UP session requires new keys to be calculated when no UE-to-EAS keys are available in the EAS. Before sending the EMSDP Modification command the HSE does the following:

- Checks with the EAS whether it has UE-to-EAS keys in storage

- If not, obtains a EAS container that may contain a key identifier for the Enterprise Key from the EAS and forwards this to the UE in the EMSDP Modification command.

4.6.1.4 BEST Key Handling

The aging of keys and any counter window used are out of scope of this specification.

4.6.2 BEST Key Hierarchy

4.6.2.1 Introduction

This clause describes the key hierarchy for BEST for both the BEST user plane services and the key agreement service:

4.6.2.2 BEST Key Hierarchy for Separate BEST Domain

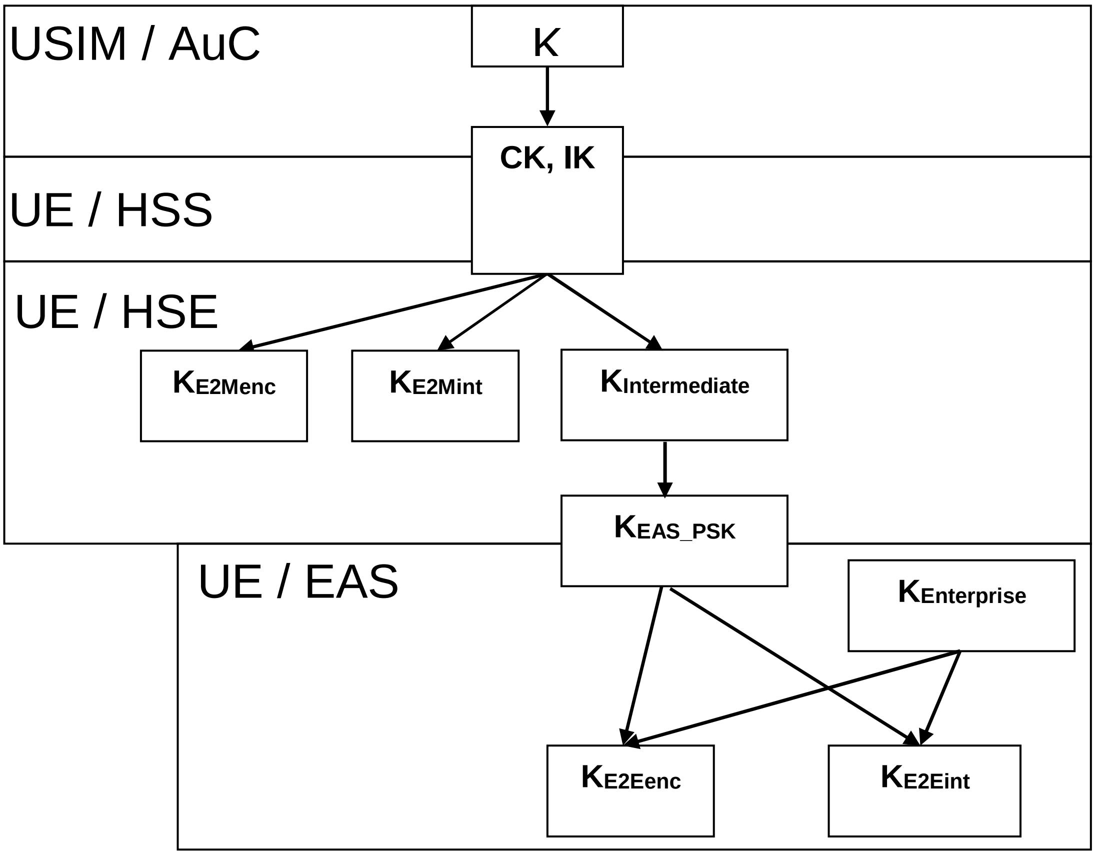

Figure 4.6.2.2-1: Key Hierarchy

The $K_{Intermediate}$, K_{EAS_PSK} and all of the keys derived from them are generated when indicated to do so in the BEST CP messaging.

5 Derivation of BEST Keys

5.1 BEST key derivation

5.1.0 Key derivation function

BEST key derivation shall use the key derivation function (KDF) defined in 3GPP TS 33.220 [13], with input parameters as defined in clause 5 of the present document.

5.1.1 Derivation of UE-to-HSE keys and Intermediate Key

The HSE and UE shall derive the BEST UE-to-HSE keys and the Intermediate key which are derived from CK and IK. The following input string shall be used when the UE and the HSE derive the BEST UE-to-HSE user plane service keys K_{E2Menc} and/or K_{E2Mint} or the Intermediate BEST key for usage in further key derivations for the UE-to-EAS user plane services or the key agreement services:

- FC = 0x60,
- P0 = HSE id if supplied else NULL,
- L0 = length of HSE id (i.e. 0x00 0x03 if HSE id supplied or 0x00 0x00 if not),
- P1 = SQN ⊕ AK

- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06)
- P2 = algorithm type distinguisher
- L2 = length of algorithm type distinguisher (i.e. 0x00 0x01)

Table 5.1.1-1: Algorithm type distinguishers

Algorithm type distinguisher	Value
BEST encryption key (K_{E2Menc})	0x01
BEST integrity Key (K_{E2Mint})	0x02
BEST Intermediate Key ($K_{Intermediate}$)	0x03

The input key shall be equal to the concatenation CK || IK of CK and IK.

The Intermediate Key ID shall be set equal to SQN ⊕ AK.

5.1.2 Derivation of EAS specific pre-shared key (K_{EAS_PSK})

The following input string shall be used when the UE and the HSE derive the enterprise specific pre-shared key K_{EAS_PSK} from $K_{Intermerdiate}$

- FC = 0x61,
- P0 = Enterprise Application Server id,
- L0 = length of Enterprise Application Server id (i.e. 0x00 0x03)

The input key shall be $K_{Intermerdiate}$, as derived in clause 5.1.1.

5.1.3 Derivation of UE-to-EAS keys

The following input string shall be used when the UE and the EAS derive the BEST User plane keys K_{E2Eenc} or K_{E2Eint} from $K_{EAS\_PSK.:}$

- FC = 0x62,
- P0 = algorithm type distinguisher
- L0 = length of algorithm type distinguisher (i.e. 0x00 0x01)

Table 5.1.3-1: Algorithm type distinguishers

Algorithm type distinguisher	Value
BEST e2e encryption key (KE2Eenc)	0x01
BEST e2e integrity Key (KE2Eint)	0x02

The input key shall be equal to the concatenation K_{EAS_E2E} || $K_{Enterprise}$ of K_{EAS_PSK} and $K_{Enterprise}$.

NOTE: The Enterprise_Key provisioning is outside the scope of 3GPP.

6 End to Middle Secured Data Protocol (EMSDP)

6.1 Introduction

The EMSDP protocol is used for the BEST service. This protocol runs between the UE and the HSE and has been optimised for efficient, secure transfer of both BEST user plane and control plane data.

6.2 EMSDP Protocol Description

6.2.1 Data Stack

Figures 6.2.1-1, 6.2.1-2, 6.2.1-3, and 6.2.1-4 show examples with the LTE network of the data stacks for the EMSDP transfers (based on 3GPP TS 23.401 [4]) between the HSE and the UE.

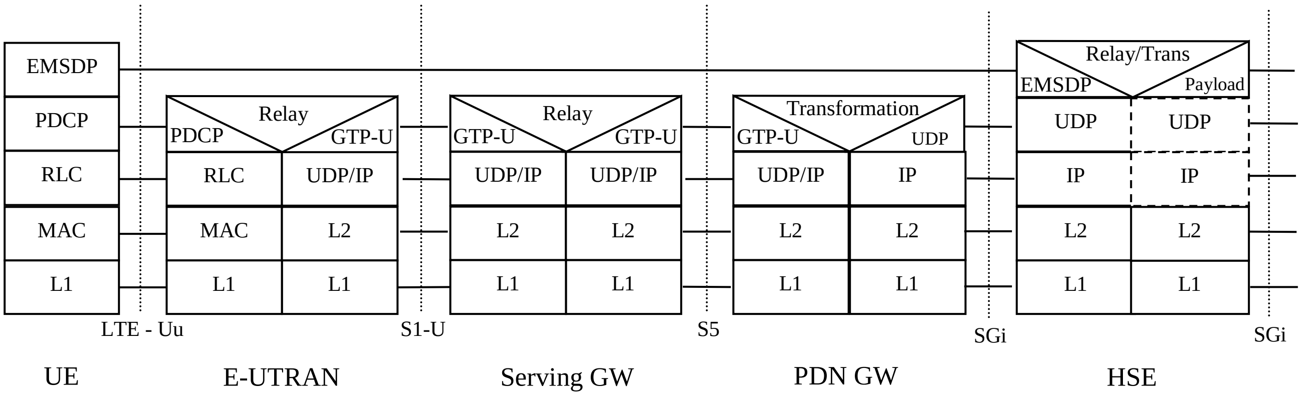

Figure 6.2.1-1: Non-IP PDU Type data stack for the EMSDP transfers over UP

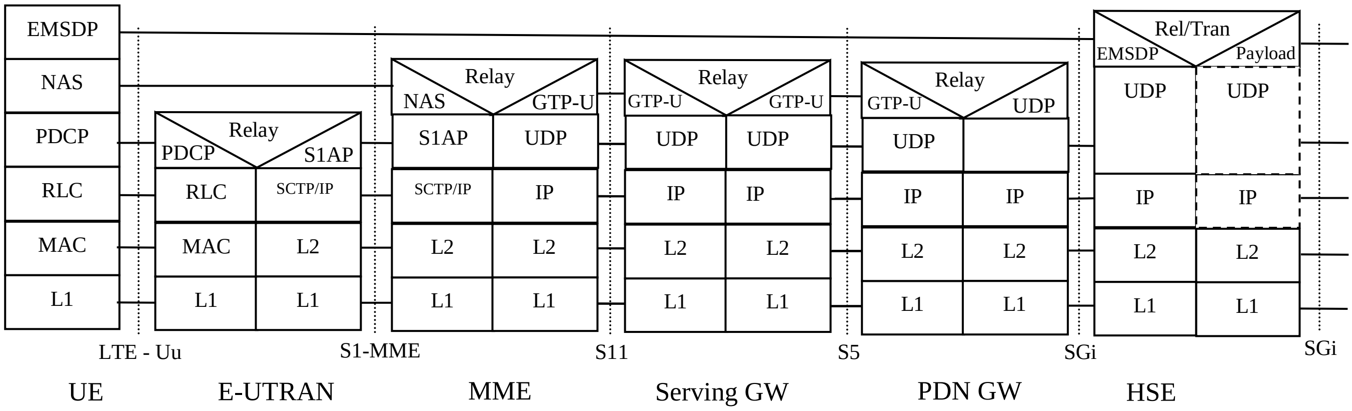

Figure 6.2.1-2: Non-IP PDU Type data stack for the EMSDP transfers over NAS via the PDN GW

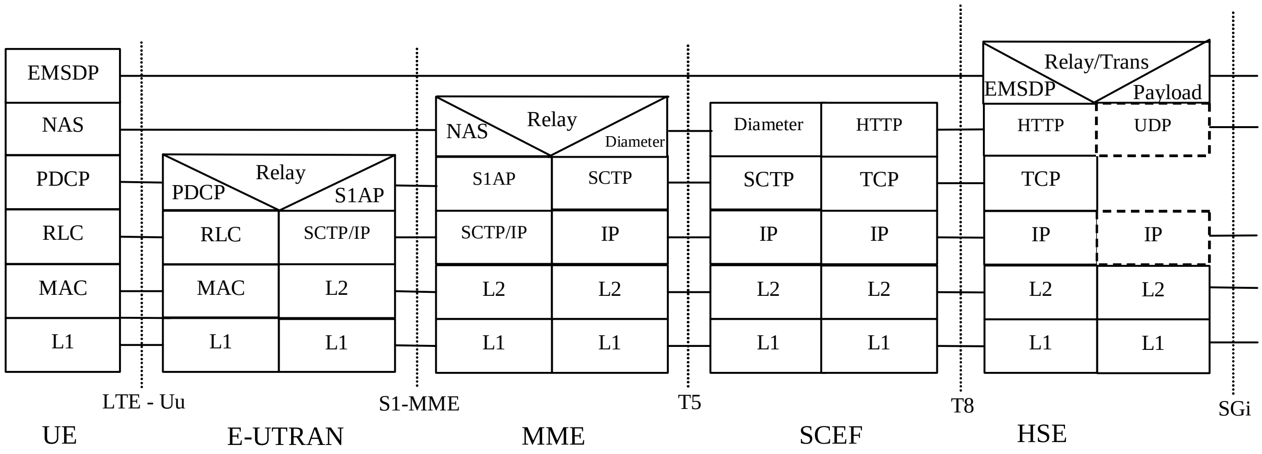

Figure 6.2.1-3: Non-IP PDU Type data stack for the EMSDP transfers over NAS via the SCEF

If the UE selects the non-IP PDU data type as defined in clause 4.3.17.8 of 3GPP TS 23.401[2], the PDN GW encapsulates the non-IP EMSDP payload in PtP (IP and UDP as detailed in clause 4.3.17.8.3.3.2 of 3GPP TS 23.401[4]) for the communication with the HSE. In case of the EMSDP is in IP PDU Type, the PtP encapsulation is unnecessary, and the UE's IP packet is directly forwarded to the HSE. This is shown on Figure 6.2.1-2.

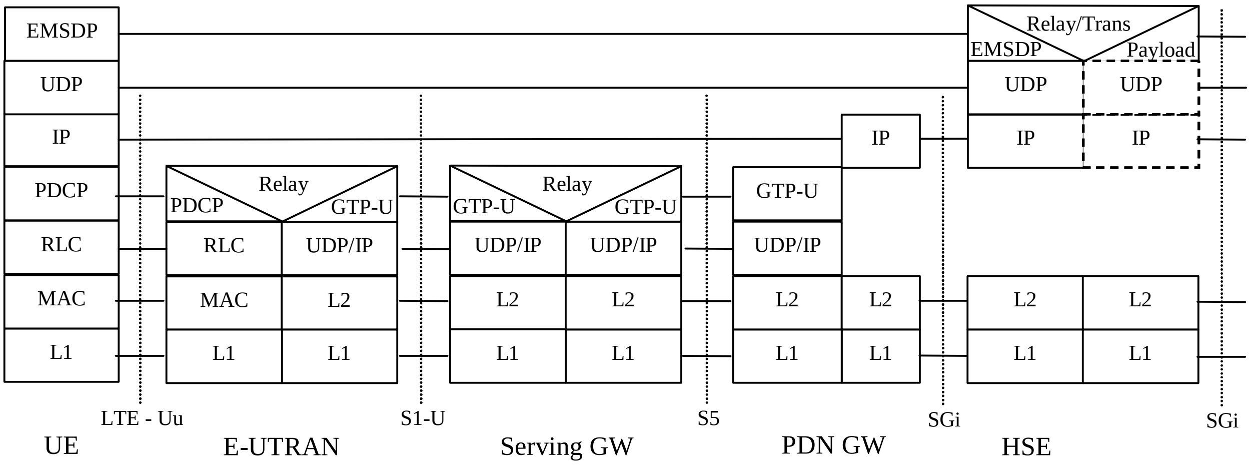

Figure 6.2.1-4: IP PDU Type data stack for the EMSDP transfers

In all four scenarios for UE-to-EAS BEST sessions, the HSE may forward the EMSDP user plane unmodified to the EAS. When the session uses a non-IP PDU Type connection that terminates at the SCEF, SCEF API's are used to forward the EMSDP user plane unmodified to the HSE. The signalling plane always terminates in the HSE.

Note 1: It is up to the operator to decide the protocol between the HSE and the EAS. For example, an operator may agree to use the optional Annex B protocol. In that case, the HSE will have to encapsulate the user data in an agreed message format.

Note 2: The method by which the UE discovers the IP address of the HSE is an operational matter, out of scope.

Note 3: The SCEF does not support IP routing towards the EAS.

Note 4: The EMSDP Payload may carry a non-IP or an IP message. If the message in the EMSDP Payload is already IP, after decapsulating the payload the HSE just forwards it onto the SGi. If the message in EMSDP Payload is non-IP, then the HSE needs to encapsulate it, for example in IP/UDP, which shown on the above diagrams with dashed boxes. Handling of the EMSDP Payload is controlled by operator policy and is out of scope.

6.2.2 EMSDP general structure

This clause details a type 01 control plane EMSDP message and a type 01 user plane EMSDP message.

Figure 6.2.2-1 shows the general structure of the EMSDP type 01 message:

Control Plane type 01 message:

UP / CP Flag	RFU	Key ID	CP COUNTER	Session ID	EMSDP Command	Cmd Options	MAC
1 bit	1 bit	3 bits	Note 4	Note 1 Note 2	Note 1 Note 2 Note 3	Note 2 Note 3	Note 1 Note 3

User Plane type 01 message:

UP / CP Flag	RFU	Key ID	UP COUNTER	Session ID	Data Length	Data	MAC
1 bit	1 bit	3 bits	Note 4	*Note 1* *Note 2*	Note 1 Note 2 Note 3	Note 2 Note 3	Note 1 Note 3

Note 1: The length of these fields is indicated in the BEST HSE configuration TLV from the HSE.
Note 2: These fields are included in the integrity protection calculation.
Note 3: These fields are encrypted when encryption is used. When encrypted these fields are replaced by the encrypted output.
Note 4: The length of this field is as defined in the BEST Counter Scheme being used.

Figure 6.2.2-1: data stack for the EMSDP transfers

UP / CP Flag: This is a 1 bit field that when set to '1' means that the data packet is a User Plane message and when set to '0' means that the message is a control plane message.

RFU: This is a 1 bit field that is reserved for future use. Set to '0'.

Key ID: This is a 3 bit field that indicates the key being used for encryption and Integrity protection. If no keys have been agreed between the HSE and the UE then this shall be '000'. The Key ID is associated to a specific Session ID.

CP COUNTER: This is a counter, used for control plane data messages, that is incremented every control plane message. It is used to protect control plane data messages against replay attacks and its length is set based on the counter scheme indicated in the BEST HSE configuration TLV (minimum length is 3 bits). There are separate counter values for UE to HSE and HSE to UE. This counter value is associated to a specific Session ID. There are two independent CP counter values, one for messages from the UE and one for messages to the UE. The HSE shall not check the CP counter value if the incoming message is "EMSDP Session Request " and the Session ID is 0.

UP COUNTER: This is a counter, used for user plain data messages, that is incremented every user plain data message. It is used to protect user plain data message against replay and its length is set based on the counter scheme indicated in the BEST HSE configuration TLV (minimum length is 3 bits). There are separate counter values for UE to HSE and HSE to UE. This counter value is associated to a specific Session ID. There are two independent UP counter values, one for messages from the UE and one for messages to the UE.

Session ID: This indicates the identifier for the current session. The value is assigned by the HSE. Its length is determined according to the Session ID scheme that is agreed. For signalling messages sent from the UE, outside of a BEST session, the Session ID length shall be 1 octet and the Session ID value shall be all 0's.

EMSDP Command: This is a 1 byte field that contains the signalling command. The defined commands are detailed below.

Cmd Options: This is a TLV container that contains TLV elements that detail the options for the EMSDP command. The defined options TLVs are detailed below.

MAC: This contains the truncated integrity result for this data packet calculated using the agreed integrity algorithm. Its length is set in the BEST HSE configuration TLV. For an EMSDP session request command the MAC shall not be present.

Data length: This holds the length of the following data in this data packet. Its length is set in the EMSDP Session Request message. This is not present if the data length is set to 0 in the BEST HSE configuration TLV.

Data: This is the data being transferred.

Note: The content and processing of the BEST UP EMSDP data payload is out of scope.

6.2.3 EMSDP Counter and Session ID Schemes

6.2.3.1 Optimised EMSDP counter scheme

The optimised EMSDP counter scheme has a 3 bit counter length followed by the counter value. This allows the counter length to be changed on a per message basis. The 3 bits are used to indicate the number of octets the counter is on, the value "000" is reserved for future use. So for instance:

Counter value "1" is represented as "001 00000001"

Counter value "257" is represented as "010 00000001 00000001"

Counter values are rejected if the counter value is less than or equal to a valid counter value already received. The HSE and the UE may also reject a message with a counter higher than a specific offset from the last valid counter value received. The HSE shall not check the counter value if the message is EMSDP Session Request and the Session ID is 0.

The optimised EMSDP counter scheme is defined as scheme 01.

6.2.3.2 Optimised EMSDP Session ID scheme

The Optimised EMSDP session ID scheme enables the EMSDP session ID to have a known length that can be as long as the application requires it.

In this scheme the highest bit of every session ID byte is an indication that the following byte is also part of the session ID.

For example the following session IDs are valid under this scheme: '01', 'F469', '82A57F'

This is the default session ID scheme for EMSDP messages and is defined as scheme 01.

6.2.4 EMSDP Integrity protection

The integrity protection algorithm to be used and the length of the MAC is selected by the HSE with the EMSDP Session Start message.

Integrity protection is mandatory for all control plane and user plane messages except for the following control plane commands when no valid keyset is agreed between the UE and HSE:

- an EMSDP session request command originating from the UE or the HSE. For this command the MAC shall not be present.

For an EMSDP start session command, originating from the HSE, if the Key Id for the message is the same as the Key Id indicated in the Key agreement TLV then the MAC shall be calculated using the new keys resulting from the authentication vectors in the Key agreement TLV.

For all other signalling plane and user plane data packets the MAC shall be computed as follows:

First the following fields are calculated (where needed for the chosen algorithm):

INPUT-I set to the message Counter Value expanded and right padded with 0's to a fixed size of 4 bytes.

COUNT-C set to the message Counter Value expanded and right padded with 0's to a fixed size of 4 bytes

M (GSM) set to the length of message in bytes. It is coded on 2 bytes.

LENGTH set to the length of message in bytes. It is coded on 2 bytes.

MESSAGE the fields marked for integrity protection in figure 6.8.2.4.3.1: "data stack for the EMSDP transfers" concatenated in the order they appear in the data packet.

M (LTE) the fields marked for integrity protection in figure 6.8.2.4.3.1: "data stack for the EMSDP transfers" concatenated in the order they appear in the data packet.

DIRECTION The DIRECTION bit shall be "0" for UE to HSE data packets and set to "1" for HSE to UE data packets.

BEARER For control plane messages this shall be set to "00000" and for user plane messages this shall be set to "10101"

FRAMETYPE For control plane messages this shall be set to "00" and for user plane messages this shall be set to "AA".

KI128 This is the agreed integrity key value truncated to the lowest 128 bits.

IK This is the agreed integrity key value truncated to the lowest 128 bits.

If GIA4 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 55.241 [6] shall be used to generate the MAC value. If the MAC length selected by the HSE with the EMSDP Session Start message is less than the length of the MAC produced by the GIA4 function, then the MAC shall be truncated to the correct size from the right.

If GIA5 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 55.251 [7] shall be used to generate the MAC value. If the MAC length selected by the HSE with the EMSDP Session Start message is less than the length of the MAC produced by the GIA5 function, then the MAC shall be truncated to the correct size from the right.

If UIA1 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 35.201 [8] shall be used to generate the MAC-I value. The MAC shall be set to the MAC-I truncated to the correct size from the right.

If UIA2 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 35.215 [9] shall be used to generate the MAC-I value. The MAC shall be set to the MAC-I truncated to the correct size from the right.

If 128-EIA1 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 33.401[12] Annex B.2.2 shall be used to generate the MAC-I value. The MAC shall be set to the MAC-I truncated to the correct size from the right.

If 128-EIA2 is indicated in the HSE BEST protocol ID element, then the algorithm specified in A3GPP TS 33.401[12] annex B.2.3 shall be used to generate the MAC-I value. The MAC shall be set to the MAC-I truncated to the correct size from the right.

If 128-EIA3 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 35.221 [10] shall be used to generate the MAC-I value. The MAC shall be set to the calculated MAC-I value truncated to the correct size from the right.

6.2.5 EMSDP Encryption

The encryption protection algorithm to be used is selected by the HSE with the EMSDP Session Start message. If EEA0 is indicated then the message shall not be encrypted.

Encryption is mandatory for all control plane and user plane messages when an encryption algorithm other than EEA0 is selected by the HSE with the EMSDP Session Start message, except for the following control plane commands when no valid keyset is agreed between the UE and HSE:

- an EMSDP session request command originating from the UE or the HSE
- an EMSDP start session command originating from the HSE

For all other messages the following encryption shall be applied the fields indicated in figure 6.2.1-1: "data stack for the EMSDP transfers" to be encrypted.

First the following are computed (where relevant for the algorithm being used):

INPUT-I set to the message Counter Value expanded and right padded with 0's to a fixed size of 4 bytes.

COUNT-C set to the message Counter Value expanded and right padded with 0's to a fixed size of 4 bytes

M (GSM) set to the length of message in bytes. It is coded on 2 bytes.

LENGTH set to the length of message in bytes. It is coded on 2 bytes.

MESSAGE the fields marked for encryption protection in figure 6.8.2.4.3.1: "data stack for the EMSDP transfers" concatenated in the order they appear in the data packet.

M (LTE) the fields marked for encryption protection in figure 6.8.2.4.3.1: "data stack for the EMSDP transfers" concatenated in the order they appear in the data packet.

DIRECTION The DIRECTION bit shall be "0" for UE to HSE data packets and set to "1" for HSE to UE data packets.

BEARER For signalling data packets this shall be set to "00000" and for user plane data packets this shall be set to "10101"

FRAMETYPE For control plane messages this shall be set to "00" and for user plane messages this shall be set to "AA".

KI128 This is the agreed encryption key value truncated to the lowest 128 bits.

CKThis is the agreed encryption key value truncated to the lowest 128 bits.

If GEA4 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 55.241 [6] shall be used to generate the OUTPUT value. The OUTPUT value replaces the fields that are encrypted in the data packet.

If GEA5 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 55.251 [7] shall be used to generate the OUTPUT value. The OUTPUT value replaces the fields that are encrypted in the data packet.

If UEA1 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 35.201 [8] shall be used to generate the OBS value. The OBS value replaces the fields that are encrypted in the data packet.

If UEA2 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 35.215 [9] shall be used to generate the OBS value. The OBS value replaces the fields that are encrypted in the data packet.

If 128-EEA0 is indicated in the HSE BEST protocol ID element, then the NULL algorithm as specified in 3GPP TS 33.401 [12] Annex B.0 shall be used to generate the OBS value. The OBS value replaces the fields that are encrypted in the data packet.

If 128-EEA1 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 33.401 [12] Annex B.1.2 shall be used to generate the OBS value. The OBS value replaces the fields that are encrypted in the data packet.

If 128-EEA2 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 33.401 [12] Annex B.1.3 shall be used to generate the OBS value. The OBS value replaces the fields that are encrypted in the data packet.

If 128-EEA3 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP TS 35.221 [10] shall be used to generate the OBS value. The OBS value replaces the fields that are encrypted in the data packet.

6.2.6 EMSDP Control Plane Commands

6.2.6.1 Overview

The following EMSDP commands are proposed Table 6.2.6.1-1:

Table 6.2.6.1-1: EMSDP commands

Code (Hex)	Command
10	EMSDP Session Request
11	EMSDP Session Start
12	EMSDP Session Start Confirmation
20	EMSDP Session Terminate Request
21	EMSDP Session Terminate Response
30	EMSDP Manage Keys Request
31	EMSDP Manage Keys Response
80	EMSDP Message Reject

In defining the EMSDP commands the following convention is used for categorising parameters:

M the inclusion of the parameter is mandatory.

O the inclusion of the parameter is optional.

C the inclusion of the parameter is conditional.

6.2.6.1.1 EMSDP Session Request

The EMSDP Session Request command shall be used by the UE to trigger a new BEST session from the HSE. This message shall include an identification of the UE, an indication of its BEST support Optionally, the EMSDP Session Request command may include information on the end enterprise service that this data is a part of. If the UE is requesting a 'BEST user plane confidential service' then the Serving network information shall be present, else this information is optional.

This message may be sent after a PDP context has been setup.

Note: the content of this message is used in the following EMSDP start session.

The cmd options for the EMSDP session request command are as follows:

Table 6.2.6.1.1-1: EMSDP session request command options

Name	M / C / O
IMSI TLV	M
BEST UE configuration TLV	M
Enterprise Setup Information Element TLV	M
Serving Network TLV	C

IMSI TLV: This is a TLV that contains the IMSI as follows:

Table 6.2.6.1.1-2: IMSI TLV

Name	Size	M / C / O	Value
IMSI TLV Tag	1 byte	M	01
Length	1 byte	M	Length of IMSI value (X)
IMSI value	X bytes	M	according to TS 31.102 [15] clause 4.2.2 bytes 2 to 9..

BEST configuration TLV: This is a TLV that contains the BEST configuration details for the UE as follows:

Table 6.2.6.1.1-3: BEST UE configuration TLV

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
BEST UE configuration TLV Tag = '02'							
Length of Best protocol ID contents = x bytes							
BEST release supported by the UE				BEST counter schemes supported by the UE	Reserved for future use (set to 000)		
BEST protocols supported for control plane messages	Reserved for future use (set to 000)			BEST protocols supported for user plane messages	Reserved for future use (set to 000)		
User data push to UE Supported	BEST encryption algorithm GEA4 supported	BEST encryption algorithm GEA5 supported	BEST encryption algorithm UEA1 supported	BEST encryption algorithm UEA2 supported	BEST encryption algorithm EEA0 supported	BEST encryption algorithm 128-EEA1 supported	BEST encryption algorithm 128-EEA2 supported
BEST encryption algorithm 128-EEA3 supported	BEST integrity algorithm GIA4 supported	BEST integrity algorithm GIA5 supported	BEST integrity algorithm UIA1 supported	BEST integrity algorithm UIA2 supported	BEST integrity algorithm 128-EIA1 supported	BEST integrity algorithm 128-EIA2 supported	BEST integrity algorithm 128-EIA3 supported

Where:

- BEST release supported by the UE – an indicator the release of the BEST solution that the UE has been designed to. If no release is indicated this means that the BEST service is not supported.
  - Value: This shall be a 4 bit field where "0000" = Rel.14 and "0001" to "1111" are RFU,
- BEST counter schemes supported by the UE – a flag for each supported scheme. At least one scheme must be supported and indicated.

  - Value: '1' – Optimised EMSDP counter scheme.

- BEST protocols supported for control plane messages – a flag for each BEST control plane protocol that is supported by the UE. At least one scheme must be supported and indicated.

  - Value: '1' – EMSDP.

- BEST protocols supported for user plane messages – a flag for each BEST control plane protocol that is supported by the UE. At least one scheme must be supported and indicated.

  - Value: '1' – EMSDP.

  - This flag is set to 0 if BEST Key agreement service is used

- User data push to UE Supported – a flag to indicate whether the UE supports user data pushed to the UE without a request for user data from the UE.

  - Values:

    '1' = User data push to UE supported,

    '0' = User data push to UE not supported.

- BEST encryption algorithms supported by the UE – a flag for each supported algorithm: GEA4, GEA5, UEA1, UEA2, EEA0, 128-EEA1, 128-EEA2 and 128-EEA3. EEA0 shall always be supported and means no encryption.

  - Values:

    '1' = Algorithm supported,

    '0' = Algorithm not supported.

- BEST integrity algorithms supported by the UE – a flag for each supported algorithm: GIA4, GIA5, UIA1, UIA2, 128-EIA1, 128-EIA2 and 128-EIA3.

  - Values:

    '1' = Algorithm supported,

    '0' = Algorithm not supported.

Enterprise Setup Information Element TLV: This is a TLV element that contains information from the UE that is used by the HSE to setup the HSE to enterprise connection as follows:

Table 6.2.6.1.1-4: Enterprise Setup Information Element TLV

Name	Size	M / C / O	Value
Enterprise Setup Information Element TLV Tag	1 byte	M	03
Length	1 byte	M	Length of Enterprise URL (X+1)
UE-to-EAS flag	1 byte	M	
Enterprise Id	X bytes	O	

UE-to-EAS flag: If set to 0 it indicates that the UE requests a UE-to-HSE BEST secure session. If set to 1, it means that the UE requests a UE-to-EAS BEST secure session. This flag is not used if BEST User plane security services are not used.

Enterprise Id: The enterprise Id is used by the HSE to identify the enterprise and the service that the data belongs to. These services are out of scope of this specification. As an example, a URL may be used to identify the enterprise.

Serving network TLV: This is a TLV that contains information on the serving network.

Table 6.2.6.1.1-5: Serving Network TLV

Name	Size	M / C / O	Value
Serving Network Element TLV Tag	1 byte	M	0B
Length	1 byte	M	Length of MCC/MNC value (3)
MCC/MNC	3 bytes	M	MCC/MNC as defined in 3GPP TS 24.008 [5]

Response:

If the HSE agrees to setup the session, it shall respond with an EMSDP Session Start command.

If the HSE does not agree to setup a BEST session, it may respond with a EMSDP Message Reject command. This command may include the reason that the request has been rejected.

6.2.6.1.2 EMSDP Session Start

The EMSDP Session Start command is used by the HSE to setup a new BEST session. This message shall contain information on the BEST service setup, key agreement details, a hash of the information sent by the UE in the prior EMSDP Session Request command and optionally, the HSE identity.

On receipt of this command the UE shall:

- Perform a 3G security context authentication with the USIM using the RAND and AUTN combination from the Key Agreement TLV. If the USIM returns IK and CK values, the UE uses these keys and the HSE identity supplied (if the HSE Identity TLV is present) to generate the session keys for the EMSDP messages as detailed in clause 5. If the USIM determines re-synchronisation is required and returns an AUTS then the UE sends a EMSDP Message Reject command containing the AUTS to the HSE.

- Verify that the UE supports the BEST service indicated in the BEST Service configuration TLV.

- Verify the received message format, the CP COUNTER value and the message MAC value.

- Verify that the MAC supplied in the MAC TLV matches the MAC that would be produced for the previous EMSDP Session Request message if the BEST configuration in the BEST Service configuration TLV had been applied using the integrity key calculated from the Key agreement TLV.

The EMSDP Session Start command has the following cmd options:

Table 6.2.6.1.2-1: EMSDP Session Start command options

Name	M / C / O
BEST Service configuration TLV	M
Key agreement TLV	M
EMSDP session request MAC TLV	C
HSE Identity TLV	O
EAS Container	O

BEST Service configuration TLV: The BEST Service configuration TLV sets the BEST service parameters to be used in this session as follows:

Table 6.2.6.1.2-2: BEST Service configuration TLV

<table>
<tr><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td colspan="8">BEST HSE configuration TLV Tag = '04'</td></tr>
<tr><td colspan="8">Length of Best protocol ID contents = x bytes</td></tr>
<tr><td>BEST Service Activated</td><td>BEST encryption algorithm GEA4 to be used</td><td>BEST encryption algorithm GEA5 to be used</td><td>BEST encryption algorithm UEA1 to be used</td><td>BEST encryption algorithm UEA2 to be used</td><td>BEST encryption algorithm EEA0 to be used</td><td>BEST encryption algorithm 128-EEA1 to be used</td><td>BEST encryption algorithm 128-EEA2 to be used</td></tr>
<tr><td colspan="8">BEST signalling plane protocol identifier</td></tr>
<tr><td colspan="8">BEST user plane protocol identifier</td></tr>
<tr><td>BEST encryption algorithm 128-EEA3 to be used</td><td>BEST integrity algorithm GIA4 to be used</td><td>BEST integrity algorithm GIA5 to be used</td><td>BEST integrity algorithm UIA1 to be used</td><td>BEST integrity algorithm UIA2 to be used</td><td>BEST integrity algorithm 128-EIA1 to be used</td><td>BEST integrity algorithm 128-EIA2 to be used</td><td>BEST integrity algorithm 128-EIA3 to be used</td></tr>
<tr><td colspan="2">Reserved for future use (set to 00)</td><td>UE triggered key refresh supported</td><td>Local BEST configuration management allowed</td><td colspan="4">Reserved for future use (set to 0000)</td></tr>
<tr><td>New Session Required</td><td>Use EAS UP Keys</td><td colspan="2">EMSDP MAC length</td><td colspan="4">Size of EMSDP Data Length</td></tr>
</table>

- BEST Service Activated – a bit flag that when set instructs the UE to use the BEST service and when clear instructs the UE not to use the BEST service,

- BEST signalling plane protocol identifier – 1 octet that is used to determine the BEST signalling protocol to be used from the following list (only one shall be indicated): 01 = type 01 signalling plane EMSDP message. All other values are reserved for future use.

- BEST user plane protocol identifier – 1 octet that is used to determine the BEST signalling protocol to be used from the following list (only one shall be indicated): 01 = type 01 user plane EMSDP message. All other values are reserved for future use.

- BEST encryption algorithm to be used – 1 octet that is used to define which of the following algorithms to use for encryption: GEA0, GEA4, GEA5, UEA0, UEA1, UEA2, EEA0, 128-EEA1, 128-EEA2 and 128-EEA3. Only one algorithm from this list shall be indicated. If the Visited network indicated that BEST encryption is restricted, then the HSE shall indicate EEA0.

- BEST integrity algorithm to be used – 1 octet that is used to define which one of the following algorithms to use for integrity:GIA4, GIA5, UIA1, UIA2, 128-EIA1, 128-EIA2 and 128-EIA3). Only one algorithm from this list shall be indicated.

- Local BEST configuration management allowed – a flag to indicate that the software connected to the UE is allowed to manage the BEST service.

- UE triggered key refresh supported – The HSE indicating to the UE whether key refresh requests will be ignored or responded.

- New Session Required – 1 bit that indicates if a new session is required. If this bit is set to 0 then the details agreed for the last session can be used and a new session is not required to be setup.

- Use EAS UP keys – If set to 0 it indicates that the UE should not derive the UE-to-EAS keys. If set to 1 it means that the UE shall derive UE-to-EAS keys to be used in a UE-to-EAS BEST secure session.

- EMSDP MAC length – 2 bits that indicates how many octets in the EMSDP data packet the integrity checksum (MAC) will be on, as follows: "00"=4 octets, "01"=8 octets, "10"=12 octets and "11"= 16 octets. This value shall not be set to a size that is greater than MAC size produced by the chosen algorithm.
- Size of EMSDP Data Length – 4 bits that indicate how many octets are used for the EMSDP Data Length. "0000" is reserved for future use.

Any remaining bits are reserved for future use and are set to "0..0".

Key agreement TLV: this contains the RAND IE and AUTN IE specified in 3GPP TS 24.008 [5] as follows:

Table 6.2.6.1.2-3: Key Agreement TLV

Name	Size	M / C / O	Value
Key Agreement TLV	1 byte	M	05
Length	1 byte	M	1 or 36
Additional Information	1 Byte	M	Additional Keys to be generated
RAND IE	17 bytes	C	See 10.5.3.1 in 3GPP TS 24.008 [5]
AUTN IE	18 bytes	C	See 10.5.3.1.1 in 3GPP TS 24.008 [5]

If the 'Length of the Key agreement' is set to 1 then this means use current keyset agreed for this KEY ID. In this case the RAND IE and AUTN IE shall not be present.

The Additional information are as follows:

Table 6.2.6.1.2-4: Additional information

b8	b7	b6	b5	b4	b3	b2	b1
Confirm Authentication flag	RFU	RFU	RFU	RFU	Key ID		

b8: Confirm Authentication flag:

1 = Confirmation message required.

0 = Confirmation message not required.

b7 to b4: RFU (set to 0)

b3 to b1: Key ID

Key ID to be used for this keyset.

EMSDP Session Request MAC TLV: The EMSDP session request MAC TLV shall be present if the previous command was an EMSDP session request message. Its contents are as follows:

Table 6.2.6.1.2-5: EMSDP session request MAC TLV

Name	Size	M / C / O	Value
EMSDP session request MAC Tag	1 byte	M	06
Length	1 byte	M	Length of MAC (X)
EMSDP session request MAC	X bytes	M	Result of MAC calculation on previous EMSDP session request message using current keys and BEST configuration in this message.

HSE Identity TLV: this contains a 4 octet numeric identifier for the HSE. This should be unique to the HSE being used within the home network. It is formatted as follows:

Table 6.2.6.1.2-6: HSE Identity TLV

Name	Size	M / C / O	Value
HSE Identity Tag	1 byte	M	07
Length	1 byte	M	Length of HSE Identity (04)
HSE Identity	4 bytes	M	4 octet numeric identifier for the HSE

The EAS Container TLV: this contains a 4 octet numeric identifier for the Enterprise Key ID.

Table X.2.6.1.2-7: EAS Container TLV

Name	Size	M / C / O	Value
EAS Container Tag	1 byte	M	08
Length	1 byte	M	Length of Enterprise Key ID
Enterprise Key ID	4 bytes	M	numeric identifier for the Enterprise Key

Response:

If the Confirmation message required flag in the Key agreement TLV is set and the message verifies, then the UE shall send an EMSDP start session confirmation message.

If the Confirmation message required flag in the Key agreement TLV is set and the message verifies, then the UE may send an EMSDP start session confirmation message.

If the message does not verify, then the UE shall respond with a Request Rejected command. This command may include the reason that the request has been rejected.

If the USIM returns a AUTS as a result of the authentication, the UE shall respond with a Request Rejected command with the reason "Authentication ReSync required" and including the AUTS.

6.2.6.1.3 EMSDP Session Start Confirmation message

The EMSDP Session Start conformation message is sent by the UE to confirm a previous EMSDP Session Start command.

This message is optional for the UE to send unless the "Confirmation message required" flag is set in the EMSDP start Session Start command in which case this message shall be sent.

This command has the following cmd options:

Table 6.2.6.1.3-1: EMSDP start session confirmation command options

Name	M / C / O
AUTHENICATION RESPONSE TLV	M

AUTHENICATION RESPONSE TLV: This TLV contains the authentication response for a successful authentication as follows:

Table 6.2.6.1.3-2: AUTHENICATION RESPONSE TLV

Name	Size	M / C / O	Value
AUTHENICATION RESPONSE Tag	1 byte	M	0C
Length	1 byte	M	Length of HSE Identity (X+1)

Key Information	1 byte	M	Key identifier
RES	X bytes	M	As returned by the USIM.

Where:

Key Information is coded:

Table 6.2.6.1.3-3: Key Information

b8	b7	b6	b5	b4	b3	b2	b1
RFU	RFU	RFU	RFU	RFU	Key ID		

b8 to b4: RFU (set to 0)

b3 to b1: Key ID

Key ID to be used for this keyset.

6.2.6.1.4 EMSDP Session Terminate Request and Response

The EMSDP Session Terminate Request may be sent by either the UE or the HSE to terminate an existing EMSDP session.

The sending party shall close their session on sending this command and the receiving party shall close the session upon reception of this command. All future BEST User Plane messages and BEST control plane messages for the session indicated in the session ID shall be either refused or ignored.

This command has no cmd options.

6.2.6.1.5 EMSDP Manage Keys Request

The EMSDP Manage Keys request command shall be sent by the UE to request the HSE to negotiate new key material.

If the BEST session requested includes cyphering then the UE shall send a Serving Network TLV (as defined in clause 6.2.6.1.1).

6.2.6.1.6 EMSDP Manage Keys Response

The EMSDP Manage Keys command is used by the HSE to agree new keys,replace a key and delete existing keys.

When the HSE indicates "Add new key" and the key ID indicated in the Key Agreement TLV is not currently used in the UE, then the UE shall use the information in the Key Agreement TLV to create a new key that can be used in this EMSDP session. If the Key ID is already in use then the UE shall send a EMSDP Message Reject command.

When the HSE indicates "Update key" and the Key ID in the Key Agreement TLV is the same as the Key ID in the in the Key Management TLV, then the UE shall delete the key indicated in the Key Management TLV and then create a new key use the information in the Key Agreement TLV that can be used in this EMSDP session. If the Key ID of the key to be deleted is no longer valid then the UE shall silently ignore this request.

When the HSE indicates " Update key" and the Key ID in the Key Agreement TLV is different to the Key ID in the in the Key Management TLV, then the UE shall create a new key using the information in the Key Agreement TLV that can be used in this EMSDP session. The key indicated in the Key Management TLV shall be deleted when the UE receives the first EMSDP message using the new key ID. If the Key ID of the key to be created is already in use then the UE shall send a EMSDP Message Reject command. If the Key ID of the key to be deleted is no longer valid then the UE shall silently ignore this request.

When the HSE indicates "delete key" then the UE shall delete the key indicated in the Key Management TLV. If the Key ID of the key to be deleted is no longer valid then the UE shall silently ignore this request.

The EMSDP Manage Keys command has the following cmd options:

Table 6.2.6.1.6-1: EMSDP Manage Keys command options

Name	M / C / O
Key Management TLV	M
Key agreement TLV	C

Key management TLV:

Table 6.2.6.1.6-2: Key Management TLV

Name	Size	M / C / O	Value
Key Management Tag	1 byte	M	0D
Length	1 byte	M	01
Key Management Information	1 byte	M	Key Management Information

Where:

Key Management Information is coded:

Table 6.2.6.1.6-3: Key Information

b8	b7	b6	b5	b4	b3	b2	b1
Key Action		RFU	RFU	RFU	Key ID		

b8 and b7: Action to be performed

'00' – RFU

'01' – add new key or update existing key (Key ID set in Key agreement TLV)

'11' – Update Key (Key to be added is Key ID set in Key agreement TLV, key to be deleted is indicated in b3 to b1).

'10' – Delete key (key to be deleted is indicated in b3 to b1).

B6 to b4: RFU (set to 0)

b3 to b1: Key ID

Key ID for this operation.

Key agreement TLV: As detailed in clause 6.2.6.1.2.

6.2.6.1.7 EMSDP Message Reject command

The EMSDP Message Reject command may be used by either the UE or the HSE to reject messages, data or control plane.

The EMSDP Message Reject command has the following cmd options:

Table 6.2.6.1.7-1: Request Rejected command options

Name	M / C / O
Rejection details TLV	C
AUTS TLV	C

Where:

Rejection details TLV: Contains the rejection reason. If the rejection reason is "Authentication ReSync required" then the Rejection details TLV and the AUTS TLV shall be present. For all other reasons the rejection details TLV may be present.

Table 6.2.6.1.7-2: Rejection details TLV

Name	Size	M / C / O	Value
Rejection details Tag	1 byte	M	09
Length	1 byte	M	Length of HSE Identity (X+1)
Rejection reason	1 byte	M	See below

Rejection reason:

'00' = "Best session refused by the HSE"

'01' = "HSE not compatible with configuration request"

'02' = "UE not compatible with configuration request"

'03' = "HSE temporary error – try again later"

'04' = "Command Message error"

'05' = "Command message counter error"

'06 = "Authentication ReSync required"

'07' = "EMSDP session request MAC incorrect"

'08' = "Sesion ID not valid"

'09' = "Command not allowed"

Table 6.2.6.1.7-3: AUTS TLV

Name	Size	M / C / O	Value
AUTS Tag	1 byte	M	0A
Length	1 byte	M	Length of HSE Identity (X)
AUTS	1 byte	M	AUTS as returned by the USIM

6.2.7 Procedures for BEST when using EMSDP

6.2.7.1 Introduction

This clause contains the procedures between the UE, HSE, HSS and EAS for the following BEST Services when using EMSDP:

- BEST key agreement only service in clause 6.2.7.2
- BEST user plane integrity protected service in clause 6.2.7.3
- BEST user plane confidential service in clause 6.2.7.4

6.2.7.2 Procedures for BEST Key Agreement Only Service using EMSDP

Figure 6.2.7.2-1 shows the messages exchanged between the UE, HSE, HSS/EMKS and EAS in order to setup a BEST Session when using EMSDP. In this figure, the EMKS and HSS are collapsed into one.

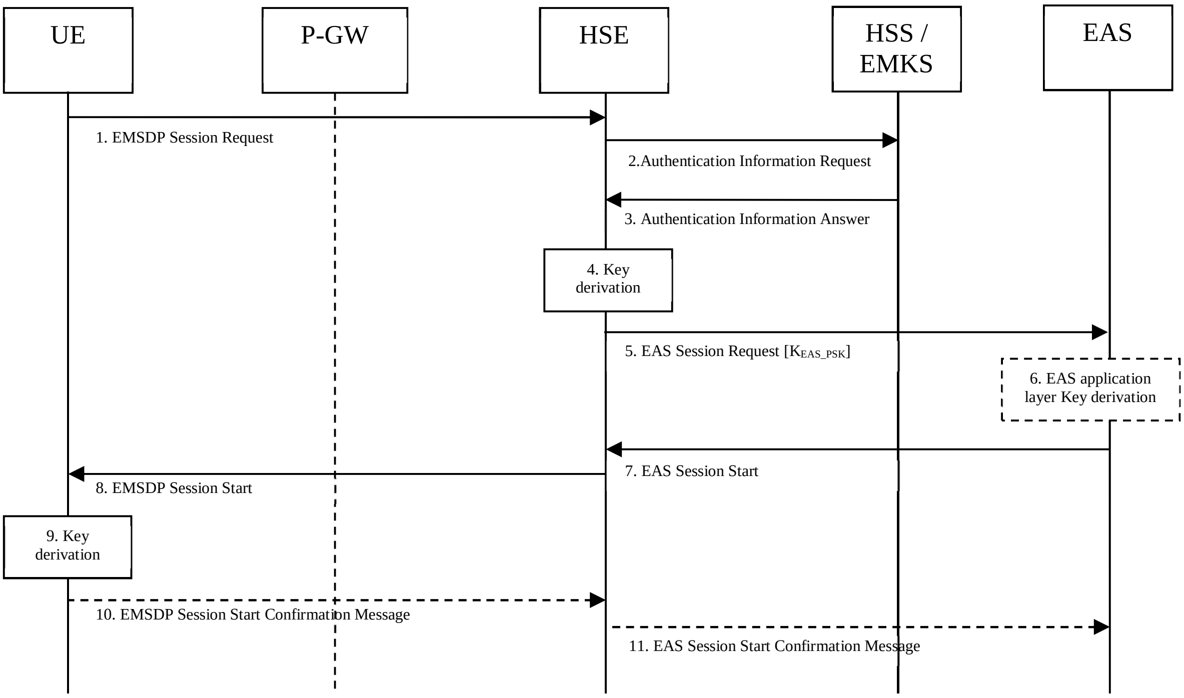
UE
P-GW
HSE
HSS / EMKS
EAS
1. EMSDP Session Request
2.Authentication Information Request
3. Authentication Information Answer
4. Key derivation
5. EAS Session Request [K_EAS_PSK]
6. EAS application layer Key derivation
7. EAS Session Start
8. EMSDP Session Start
9. Key derivation
10. EMSDP Session Start Confirmation Message
11. EAS Session Start Confirmation Message

Figure 6.2.7.2-1: BEST Session Setup Procedure for BEST Key Agreement Only Service using EMSDP

The above figure depicts BEST Session setup procedure for Key Agreement Only service. The EAS PSK is provided by the HSE to the EAS in step 5. The UE derives all the required keys in Step 9.

The EAS shall also be able to obtain the EAS PSK anytime after the BEST Session is setup by the UE. The EAS initiates a EAS Session Request message with the required Key Id (specific to the UE). The HSE derives EAS PSK and provides it in the EAS Session Start message.

NOTE1: The Key Id refers to the Intermediate Key Identifer that uniquely identifies the UE-specific Intermediate key. The mechanism by which UE provides Key Id to the EAS is out of scope of this specification.

NOTE 2: The EAS application layer key derivation in step 6 when using key agreement only service is out of scope of this specification.

Figure 6.2.7.2-2 shows the messages exchanged between the UE, HSE, HSS/EMKS and EAS in order to refresh the keys when using EMSDP. In this figure, the EMKS and HSS are collapsed into one.

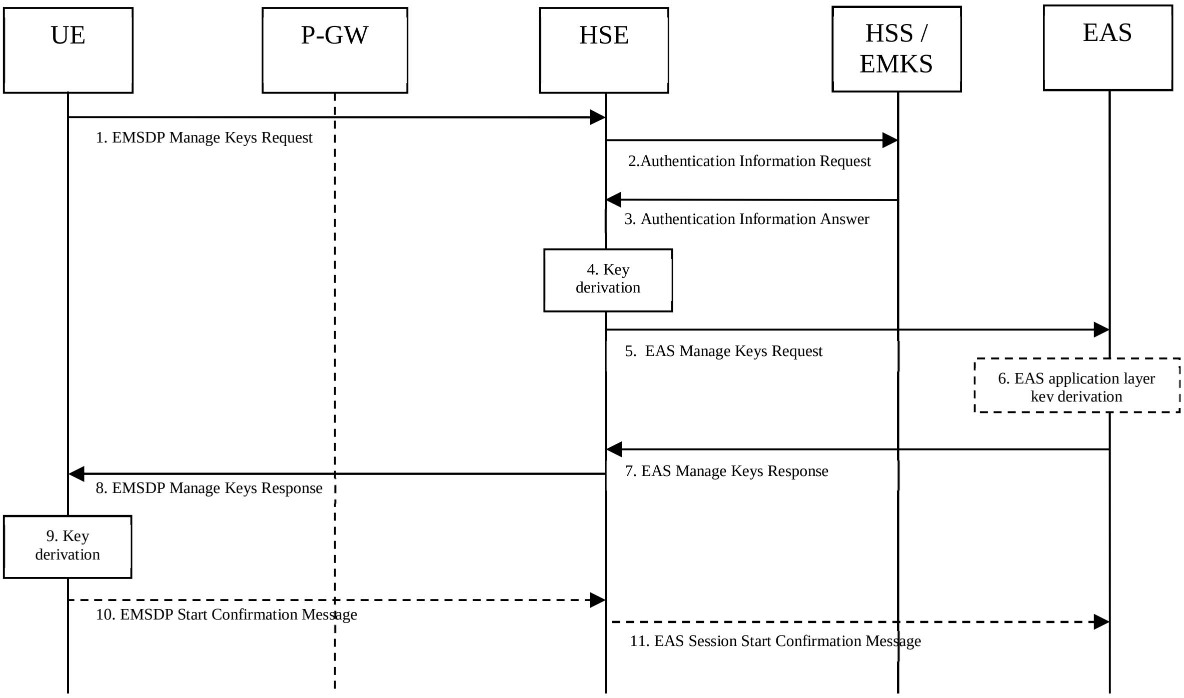
UE
P-GW
HSE
HSS / EMKS
EAS
1. EMSDP Manage Keys Request
2.Authentication Information Request
3. Authentication Information Answer
4. Key derivation
5. EAS Manage Keys Request
6. EAS application layer key derivation
7. EAS Manage Keys Response
8. EMSDP Manage Keys Response
9. Key derivation
10. EMSDP Start Confirmation Message
11. EAS Session Start Confirmation Message

Figure 6.2.7.2-2: BEST Procedure for Key Refresh using EMSDP

In the above figure, steps 1-5 and 7-9 are mandatory. Steps 10 and 11 are optional depending on whether the HSE has set the 'Confirm Authentication' flag in the 'EMSDP Session Response' message. The contents of the respective commands are given in the respective clauses that detail the commands. Step 6 is optional and out of scope.

6.2.7.3 Procedures for BEST User Plane Integrity Protected Service using EMSDP

Figure 6.2.7.3-1 shows the messages exchanged between the UE, HSE, HSS/EMKS and EAS in order to setup a BEST Session when using EMSDP. In this figure, the EMKS and HSS are collapsed into one.

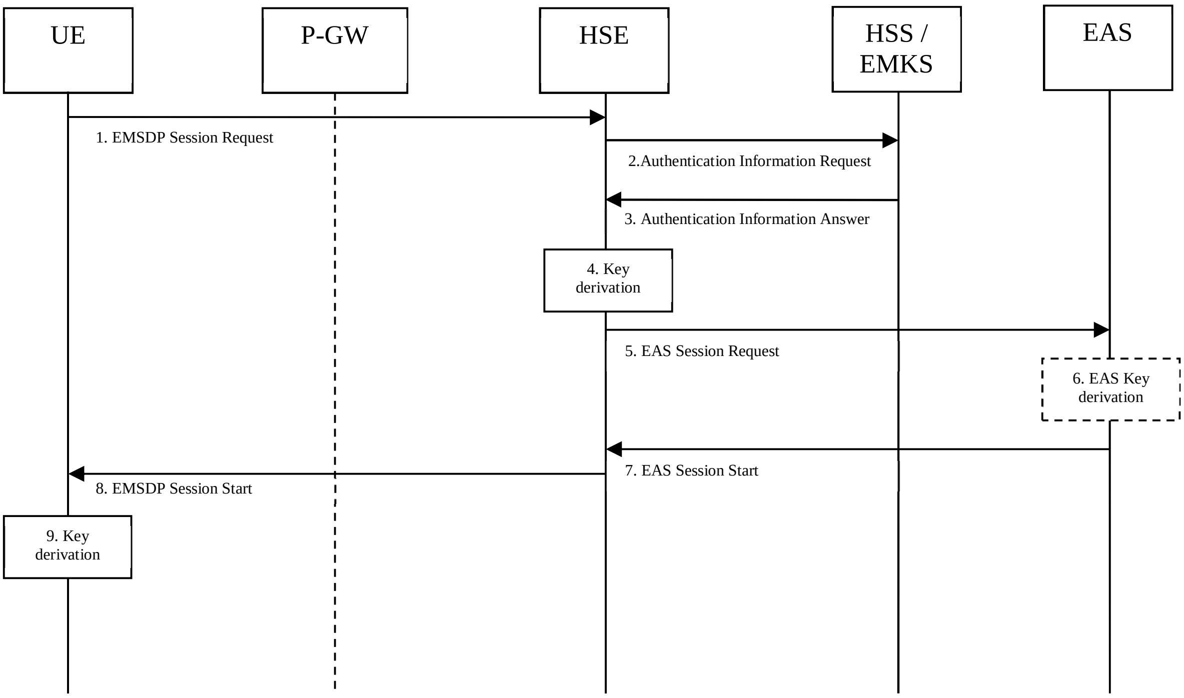

Figure 6.2.7.3-1: BEST Session Setup Procedure for BEST User Plane Integrity Only Service using EMSDP

In the above figure, steps 1-8 are mandatory. The contents of the respective commands are given in the respective clauses that detail the commands. Step 6 is only performed when a BEST UE-to-EAS UP session is setup.

Figure 6.2.7.3-2 shows the messages exchanged between the UE, HSE, HSS/EMKS and EAS in order to refresh the keys when using EMSDP. In this figure, the EMKS and HSS are collapsed into one.

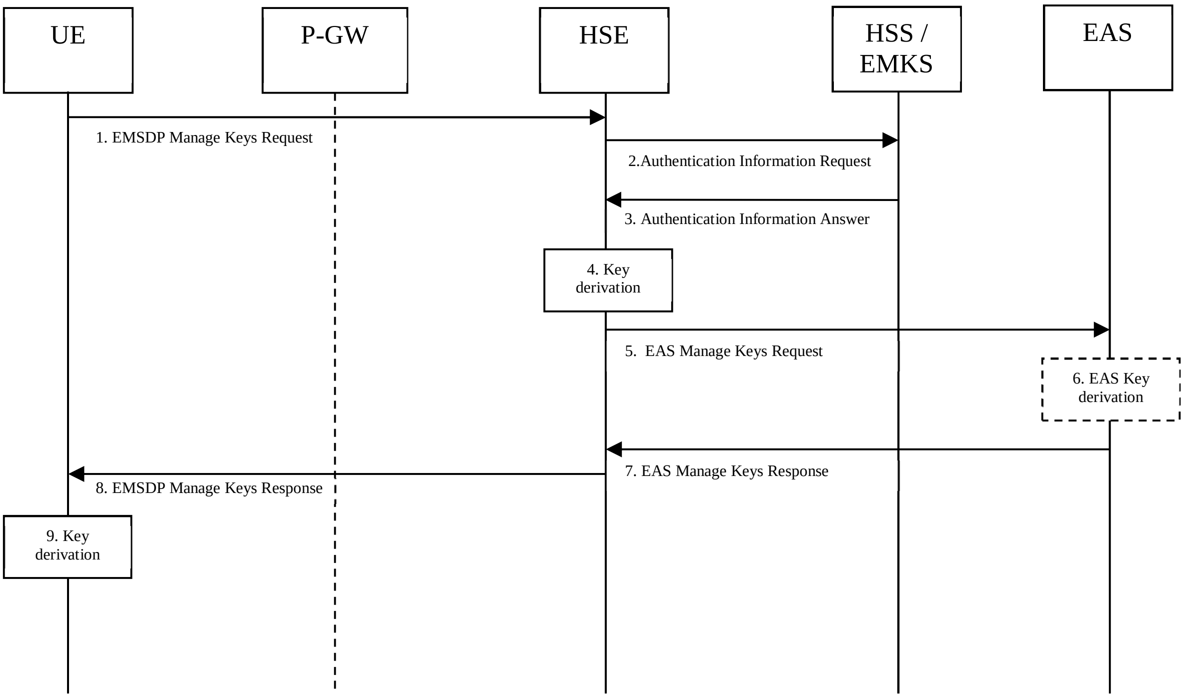
UE
P-GW
HSE
HSS / EMKS
EAS
1. EMSDP Manage Keys Request
2.Authentication Information Request
3. Authentication Information Answer
4. Key derivation
5. EAS Manage Keys Request
6. EAS Key derivation
7. EAS Manage Keys Response
8. EMSDP Manage Keys Response
9. Key derivation

Figure 6.2.7.3-2: Best Session for Key Refresh Procedure for BEST User Plane Integrity Only Service using EMSDP

In the above figure, steps 1-8 are mandatory. The contents of the respective commands are given in the respective clauses that detail the commands. Step 6 is only performed when a BEST UE-to-EAS UP session is setup.

6.2.7.4 Procedures for BEST User Plane Confidential Service using EMSDP

The procedures for the BEST User Plane Confidentiality Service are the same as the one detailed in clause 6.7.4.3.

7 BEST Service Management

7.1 Ability to enable and disable the BEST service

The HSE may allow the enterprise to manage the BEST service. The service shall allow enable / disable of the BEST service down to an individual UE level. The interface for the management of the BEST service between the enterprise and the HSE is out of scope of this document. However it is expected that such an interface would have the following abilities:

- a mechanism that allows the service to be removed for a specific subscriber at the network end (probably re-using a service provisioning service).

- the ability for the enterprise to enable / disable the E2M security service for one or many of their endpoints through communication with the operators CIoT interface. (This may be because other security mechanisms are being used).

- The ability for the home network to disable the BEST service due to non-payment or security concerns.

If the BEST service parameters in the HSE change as a result of the management of the BEST service for a specific UE and the BEST service is not currently active with that UE then the changes shall take effect the next BEST session.

If the BEST service parameters in the HSE change as a result of the management of the BEST service for a specific UE and the BEST service is currently active with that UE then the HSE shall end the current BEST session and where appropriate start a new BEST session using the new BEST service parameters.

The UE may allow the application connected to it to manage the BEST service if the Local BEST configuration management flag within the protocol configuration options of a ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST indicates this is allowed.

If the BEST service parameters in the UE change as a result of the management of the BEST service and the BEST service is not currently active then the changes shall take effect the next BEST session.

If the BEST service parameters in the UE change as a result of the management of the BEST service and the BEST service is currently active in that UE then the UE shall end the current BEST session and where appropriate start a new BEST session using the new BEST service parameters.

The UE may choose not to accept data that does not meet the defined security requirements.

When the BEST service is disabled the HSE and UE shall act as though the BEST service is not supported.

Annex A (informative): Structure of APN names for BEST

Due to regulatory requirements, operators may have to disable the best service for UEs roaming in their network. A simple, but effective method relies on the MME capability to filter specific APNs. For that reason, a BEST APN structure is proposed in this section. Operators may agree on a different method in bilateral requirements.

APNs that are used for the BEST service may reside in a specific subdomain of the operator. It is proposed to use the subdomain 'best' for this specific service.

Note: For example, if the operator uses operator.cc as a domain for APNs, the best servers should be in the domain 'best.operator.cc'. So 'apn.best.operator.cc' would be an APN that is best capable.

Annex B (informative): HSE to EAS interface based on Restful HTTP

B.1 Introduction

This annex contains example of a RESTful HTTP interface between the HSE and the EAS.

B.2 Restful HTTP interface

B.2.1 Overview

It is described as follows:

- TCP provides communication service at the transport layer
- TLS provides security to the communication
- HTTP based transport of XML data
- XML documents used to embed specific data structures, such as keys etc.

Figure B.2.1-1 illustrates the protocol stack of this reference point.

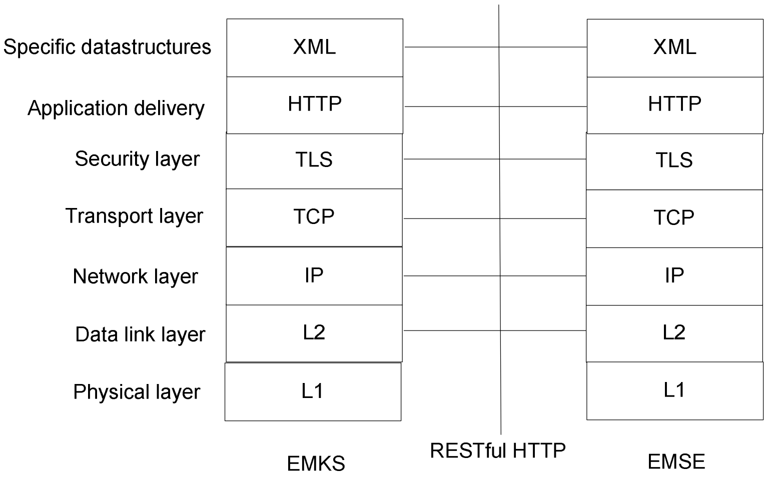

Figure: B.2.1-1 RESTful HTTPS between EMKS(HSE) and EMSE(EAS)

The HSE and the EAS act as both HTTP client and server. The underlying TCP connection permits bidirectional communication between the EAS and the HSE.

RESTful HTTP is used at the application delivery layer. The content type of the RESTful HTTP is XML.

The unsecured HTTP protocol shall be combined with TLS, as HTTPS, to provide confidentiality and integrity protection. Mutual authentication shall be enabled in TLS for authenticating and allowing only an authorized third party EAS to access the HSE. The profile for TLS implementation and usage shall follow the provisions given in 3GPP TS 33.310 [11], Annex E.

B.2.2 Procedures over the RESTful HTTP reference point

B.2.2.1 Overview of the procedures

Following procedures are supported over the RESTful HTTP reference point:

- Initial registration by the EAS
- Obtaining UE specific pre-shared key from the HSE
- Obtaining UE specific pre-shared key during BEST Session Setup
- Deregistration by EAS

B.2.2.2 Initial registration by EAS

The EAS registers with the HSE by sending an HTTP POST "EAS Session Register" message to the HSE including its identifier (EAS_Id). The HSE establishes a session context for this EAS and returns session id in HTTP 201 CREATED.

B.2.2.3 Obtaining UE specific pre-shared key from the EAS

The EAS obtains UE specific pre-shared key ($K_{Int\_EAS\_PSK}$) from the HSE by sending an EAS Session Request message including an identity of the UE and the key identifier received from the UE. The HSE derives EAS specific pre-shared key and provides it in the EAS Session Start message.

B.2.2.4 Obtaining UE specific pre-shared key during BEST Session Setup

During BEST Session setup, the HSE forwards the EAS specific pre-shared key ($K_{Int\_EAS\_PSK}$) in the EAS Session Request message. The EAS responds with a EAS Session Start message.

B.2.2.5 Deregistration by EAS

When the session needs to be terminated, EAS may send an HTTP DELETE message including the session ID to the HSE.

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-09	SA#77	SP-170644	0001	1	F	Collection of changes to BEST TS as a result of implementations	15.1.0
2018-01	SA#78	SP-170875	0002	1	F	Collection of editorial changes to BEST	15.2.0
2018-03	SA#79	SP-180045	0003	2	F	Collection of clarifications and editorial changes	15.3.0
2018-09	SA#81	SP-180700	0005	-	F	Correction of Tag Values and Names	15.4.0
2018-09	SA#81	SP-180700	0007	-	F	Clarification as to when the Serving Network TLV is required	15.4.0
2018-09	SA#81	SP-180700	0004	1	B	Adding BEST Support for non-IP PDN Connections that Terminate at the SCEF	16.0.0
2019-06	SA#84	SP-190353	0010	1	A	Interface and protocol stack clarifications and corrections to TS 33.163	16.1.0
2019-06	SA#84		0011	1	C	Making UE initiated key refresh optional in TS33.163	16.1.0
2019-09	SA#85	SP-190679	0013	1	A	Corrections to EAS and IMSI TLVs in 33163	16.2.0

History

Document history		
V16.2.0	November 2020	Publication