**3GPP TSG-SA3 Meeting #105-e *draft\_S3-213881-r1***

e-meeting, 8 - 19 November 2021

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Living document for BEST\_5G: draftCR to TS 33.163 |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | BEST has been specified for EPS networks only. There is a need for updating BEST for 5GS networks. |
|  |  |
| ***Summary of change:*** | The following changes have been made:* A 5G architecture incorporating the BEST functional entities HSE and EAS has been included.
* The EPS architecture incorporting the BEST functional entities HSE, EMKS, and EAS has been updated to reflect that it is applicable to EPS only.
* The architecture option for using GBA, 5G GBA, AKMA or proprietary key agreement has been included.
* The Overview of BEST procedures has been updated to be applicable to both EPS and 5GS networks.
* The BEST Session Initiation and Key Agreement procedure has been updated so that the supported and selected BEST key agreement (3G, 4G, ,5G, GBA, AKMA, or proprietary) can be included in the BEST UE capabilities and the BEST service parameters, respectively.
* The key setup messaging between HSE and UE has been enhanced with messaging applicable to 5GS networks. Support for both 3G, 4G, 5G AKA and EAP-AKA’ have been included.
* The key setup messaging between HSE and UE has been enhanced so that also key agreement based on GBA, 5G GBA, AKMA or proprietary key agreement is supported.
* The BEST key hierachy has been enhanced with a key hierarchy applicable to 5GS networks. Key hierarchies for 3G, 4G and 5G key hierarchies have been included.
* The BEST key hierarchy has been enhanced with a key hierarchy based on an agreed key derived from GBA, 5G GBA, AKMA and proprietary key agreement.
* Derivation of the new KHSE as root for 5G based key agreement has been added. The derivation is based on the derivation of KAUSF.
* Derivation of UE-to-HSE keys and Intermediate Key has been updated for 3G, 4G, and 5G keys based derivations. Also derivation based on an agreed key derived from GBA, 5G GBA, AKMA and proprietary key agreement has been included.
* Support of 5G algorithms for EMSDP Integrity protection has been provided.
* Support of 5G algorithms for EMSDP Encryption has been provided.
* Updates have been provided for the EMSDP protocol, in particular for the EMSDP Session Request, EMSDP Session Start, EMPSDP Session Confirmation, EMSDP Message Reject. The update now allows 4G, 5G, GBA, 5G GBA, AKMA and proprietary key agreement to be signalled by UE and by HSE, including the signalling of support for 5G algorithms for integrity protection and encryption. The update also allows for indication of request for BEST confidential service by the UE (for 5G), and indication to the UE (for 5G) of the selected authentication method selected by the UDM.
 |
|  |  |
| ***Consequences if not approved:*** | Without this change, BEST cannot be applied to 5GS networks. |
|  |  |
| ***Clauses affected:*** | 2, 4.2.1, new 4.2.2, new 4.2.3, 4.3.1, 4.3.2, 4.6.1.1, 4.6.2.2, new 5.1.0a, 5.1.1, 6.2.2, 6.2.4, 6.2.5, 6.2.6.1.1, 6.2.6.1.2, 6.2.6.1.3, 6.2.6.1.7 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

START OF CHANGE 1

# 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".

[xx] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[yy] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)"

[zz] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"

END OF CHANGE 1

START OF CHANGE 2

## 4.2 BEST Framework Service Description

### 4.2.1 EPS architecture

Figure 4.2.1-1 shows the EPS 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)

In an EPS network, 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.

### 4.2.2 5GS architecture

Figure 4.2.2-1 shows the 5GS architecture of the extended user plane protection service.



Figure 4.2.2-1: The architecture of the extended user plane protection service

In a 5GS network, 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 N3 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 N3 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.

The BEST service uses the following interfaces:

- SBA between the UDM 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.

### 4.2.3 Architecture when using GBA, 5G GBA, AKMA or proprietary key agreement

When using GBA, according to TS 33.220 [13], 5G GBA, according to TS 33.220 [13], Annex X, AKMA, according to TS 33.535 [yy], or proprietary key agreement, the architecture may be either as for EPS architecture or 5GS architecture as required. In this case, the HSE shall be connected to the EPS or 5GS architecture according to the GBA, 5G GBA, AKMA or proprietary service instead. For GBA and 5G GBA, the HSE shall act as NAF. For AKMA, the HSE shall act as AF.

END OF CHANGE 2

START OF CHANGE 3

### 4.3.1 Overview of BEST procedures

To use the BEST service, the UE shall setup a PDN connection (EPS) or PDU Session (5GS) to connect to the HSE. The UE may either use a locally stored IP address to locate the HSE or use a "BEST APN" (EPS) or "BEST DNN" (5GS) where the traffic is directed by the PDN Gateway (EPS) or UPF (5GS) 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 PDN connection (EPS) or PDU session (5GS) 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.

Figure 4.3.1-1: Generalised BEST service flow

END OF CHANGE 3

START OF CHANGE 4

### 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 (EPS) or PDU Session (5GS). 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 (i.e. BEST UE configuration), 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 BEST capabilities of the UE includes the BEST release supported by the UE and, for a UE supporting the Rel.17 release of BEST, it also includes the BEST key agreement(s) that are supported (e.g. 3G, 4G, 5G, etc.).

The EMSDP Session Start message shall include the information needed for a key agreement of the BEST keys, the BEST service parameters (i.e. BEST Service configuration), and a checksum validating the previous EMSDP Session Request message. The BEST service parameters include an indication of the BEST key agreement selected by the HSE.

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. The UE may request that the BEST user plane is confidentiality protected in the EMSDP Session Request message, in this case the HSE should take this information into account to decide whether to activate the user plane confidential service for the UE.

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.

END OF CHANGE 4

START OF CHANGE 5

#### 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 can be based on the 3GPP AKA mechanism detailed in TS 33.102 [3], TS 33.401 [12], or TS 33.501 [xx], respectively, or based on one of the following external key agreement methods: GBA [13], 5G GBA [13], Annex X, AKMA [yy], or proprietary key agreement. For 3GPP AKA based key agreement, the AKA challenge is then transported between the HSE and the UE as part of the BEST service detailed in clause 4.3.2. 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 (KE2Mint), an encryption key (KE2Menc), optionally an Intermediate Key (KIntermediate) and optionally an EAS PSK (KEAS\_PSK). The Key IDs shall be set during the derivations of the keys as specified in clause 5.1.

The Intermediate Key (KIntermediate) is used together with a separate enterprise server identifier (EAS Id) to calculate the EAS PSK (KEAS\_PSK). There can be many KEAS\_PSK derived from one KIntermediate.

The EAS PSK (KEAS\_PSK) is used together with the Enterprise Key to calculate KE2Eint and KE2Eenc 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 for EPS networks:

With EMKS

Without EMKS

UE

HSE

1. EMSDP Session Request

EMKS

HSS

2. Keys required?

3. Authentication-Information-Request

4. Authentication-Information-Answer

d. Authentication-Information-Answer

c. Authentication-Information-Answer (to deliver authentication vectors – if required)

a. Authentication-Information-Request

b. Authentication-Information-Request (to request authentication vectors - if required)

Authentication vectors needed?

8. EMSDP Session Start

5. Calculate HSE Keys

EAS

6. EAS Session Request

7. EAS Session Start

12. Calculate E2E Keys

9. EMSDP Session Start Confirmation (conditional).

11. Calculate UE Keys

10. EAS Session Start Confirmation

Figure 4.6.1.1-1: Generic BEST key agreement process for EPS networks

The Key agreement steps are:

**1. EMSDP Session Request (UE ID, BEST capabilities, Enterprise information, serving network (cond)).** The UE shall send the EMSDP Session Request (UE ID, BEST capabilities, Enterprise information, serving network (cond)) to set up a new BEST session. For UEs supporting the Rel.17 release of BEST, the BEST capabilities shall indicate that 4G key agreement is supported.

**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. For UEs supporting the Rel.14 release of BEST, the request shall indicate that UMTS authentication vectors are requested. For UEs supporting the Rel.17 release of BEST, the request shall indicate that EPS authentication vectors are requested.

**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 (KEAS\_PSK) to the EAS. In case the BEST key agreement service is used, the HSE shall forward to the EAS, the EAS PSK (KEAS\_PSK) and the key identifier for the Intermediate Pre Shared Key (KIntermediate).

**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)). The Session Parameters shall contain RAND and AUTN from the received authentication vectors. As described in TS 33.401 [12], clause 6.1.2, the "separation bit" in the AMF field of AUTN shall be set to 0 if UMTS authentication vectors have been received, and the "separation bit" in the AMF field of AUTN shall be set to 1 if EPS authentication vectors have been received. For UEs supporting the Rel.17 release of BEST, the Session Parameters shall indicate the selected key agreement (i.e. 4G key agreement).

**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.

Figure 4.6.1.1-2 shows the generic key agreement process for 5GS networks:



Figure 4.6.1.1-2: Generic BEST key agreement process for 5GS networks

The Key agreement steps are:

**1. EMSDP Session Request (UE ID, BEST capabilities, Enterprise information, serving network).** The UE shall send the EMSDP Session Request (UE ID, BEST capabilities, Enterprise information, serving network) to set up a new BEST session. The BEST capabilities shall indicate that 5G key agreement is supported.

**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 EMSDP Session Request is sent with a valid Session ID (i.e., not 0) and there is a valid key set for that session, then the HSE may start the BEST session without re-negotiating the keys (step 8). In this case the received UE ID may be ignored.

- If the EMSDP Session Request is sent without a valid Session ID or using a single byte Session ID set to 0 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 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.** **Nudm\_UEAuthentication\_GetBESTav Request over SBA interface** – The HSE shall use the SBA interface to the UDM/ARPF to request an authentication vector using the UE SUCI. The service operation Nudm\_UEAuthentication\_GetBESTav Request has the same inputs as the service operation Nudm\_UEAuthentication\_Get Request.

**4. Nudm\_UEAuthentication\_GetBESTav Response over SBA interface** – The UDM/ARPF uses the SBA interface to the HSE to return a BEST-adapted 5G HE authentication vector (if 5G AKA is the selected authentication method) or a transformed authentication vector (if EAP-AKA' is the selected authentication method).The service operation Nudm\_UEAuthentication\_GetBESTav Response has the same outputs as the service operation Nudm\_UEAuthentication\_Get Response, except that in the BEST-adapted 5G HE authentication vector the parameter KAUSF is replaced by KHSE (see clause 5.1.0a).

**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 (KEAS\_PSK) to the EAS. In case the BEST key agreement service is used, the HSE shall forward to the EAS, the EAS PSK (KEAS\_PSK) and the key identifier for the Intermediate Pre Shared Key (KIntermediate).

**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)). The Session Parameters shall contain RAND and AUTN from the received authentication vectors. The "separation bit" in the AMF field of AUTN shall be set to 1. The Session Parameters shall indicate that 5G key agreement has been selected.

**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.

END OF CHANGE 5

START OF CHANGE 6

#### 4.6.2.2 BEST Key Hierarchy for Separate BEST Domain

For EPS networks, and UEs supporting the Rel.14 release of BEST, the BEST key hierarchy is as depicted in Figure 4.6.2.2-1.



Figure 4.6.2.2-1: BEST Key Hierarchy for EPS networks and Rel.14 BEST UEs

For EPS networks, and UEs supporting the Rel.17 release of BEST, the BEST key hierarchy is as depicted in Figure 4.6.2.2-2.



Figure 4.6.2.2-2: BEST Key Hierarchy for EPS networks and Rel.17 BEST UEs

For 5GS networks the BEST key hierarchy is as depicted in Figure 4.6.2.2-3.



Figure 4.6.2.2-3: BEST Key Hierarchy for 5GS networks

The derivation of the key KHSE is described in clause 5.1.0a.

For GBA and 5G GBA based key agreement, the BEST key hierarchy is as depicted in Figure 4.6.2.2-4.



Figure 4.6.2.2-4: BEST Key Hierarchy for GBA and 5G GBA based key agreement

For AKMA based key agreement, the BEST key hierarchy is as depicted in Figure 4.6.2.2-5.



Figure 4.6.2.2-5: BEST Key Hierarchy for AKMA based key agreement

For proprietary key agreement, the BEST key hierarchy is as depicted in Figure 4.6.2.2-6.



Figure 4.6.2.2-6: BEST Key Hierarchy for proprietary key agreement

The KIntermediate, KEAS\_PSK and all of the keys derived from them are generated when indicated to do so in the BEST CP messaging.

END OF CHANGE 6

START OF CHANGE 7

### 5.1.0a Derivation of KHSE

When deriving a KHSE from CK, IK and the serving network name when producing authentication vectors, and when the UE computes KHSE according to 5G AKA, the following parameters shall be used to form the input S to the KDF:

- FC = 0x63;

- P0 = serving network name;

- L0 = length of the serving network name (variable length as specified in TS 24.501 [zz]);

- P1 = SQN ⊕ AK,

- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06).

The XOR of the Sequence Number (SQN) and the Anonymity Key (AK) is sent to the UE as a part of the Authentication Token (AUTN), see TS 33.102 [3]. If AK is not used, AK shall be treated in accordance with TS 33.102 [3], i.e. as 000…0.

The serving network name shall be constructed as specified in clause 6.1.1.4 of TS 33.501 [xx].

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

When deriving a KHSE from CK', IK' and the serving network name when producing authentication vectors, and when the UE computes KHSE according to EAP-AKA', the following parameters shall be used to form the input S to the KDF:

- FC = 0x64;

- P0 = serving network name;

- L0 = length of the serving network name (variable length as specified in TS 24.501 [zz]);

- P1 = SQN ⊕ AK,

- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06).

The XOR of the Sequence Number (SQN) and the Anonymity Key (AK) is sent to the UE as a part of the Authentication Token (AUTN), see TS 33.102 [3]. If AK is not used, AK shall be treated in accordance with TS 33.102 [3], i.e. as 000…0.

The serving network name shall be constructed as specified in clause 6.1.1.4 of TS 33.501 [xx].

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

### 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, KASME, KAUSF, or GBA/ 5G GBA/ AKMA/ proprietary agreed key depending on the key agreement version selected. The following input string shall be used when the UE and the HSE derive the BEST UE-to-HSE user plane service keys KE2Menc and/or KE2Mint 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 (KE2Menc) | 0x01 |
| BEST integrity Key (KE2Mint) | 0x02 |
| BEST Intermediate Key (KIntermediate) | 0x03 |

For 3G key agreement, the input key shall be equal to the concatenation CK || IK of CK and IK.

For 4G key agreement, the input key shall be equal to KASME.

For 5G key agreement, the input key shall be equal to KHSE (see clause 5.1.0a).

For GBA and 5G GBA, the input key shall be equal to Ks\_(int/ext)\_NAF.

For AKMA, the input key shall be equal to KAF.

For proprietary key agreement, the proprietary key shall be used as the input key.

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

END OF CHANGE 7

START OF CHANGE 8

### 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 1Note 2 | Note 1Note 2Note 3 | Note 2Note 3 | Note 1Note 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 1Note 2 | Note 1Note 2Note 3 | Note 2Note 3 | Note 1Note 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. Two simultaneously existing sessions shall not have the same Session ID unless they correspond to the same UE.

**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.

END OF CHANGE 8

START OF CHANGE 9

### 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 3GPP 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.

If 128-NIA1 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-NIA2 is indicated in the HSE BEST protocol ID element, then the algorithm specified in 3GPP 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-NIA3 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.

CK This 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.

If 128-NEA1 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-NEA2 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-NEA3 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.

END OF CHANGE 9

START OF CHANGE 10

##### 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. The UE may also include a ‘BEST confidential service requested’ indication in the EMSDP Session Request command to indicate the UE is requesting a 'BEST user plane confidential service'. For UEs not supporting 5G authentication, if the UE is requesting a 'BEST user plane confidential service' then the Serving network information shall be present, else this information is optional. For UEs supporting 5G authentication, the Serving network information shall be present.

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 or SUCI 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.. |

SUCI TLV: This is a TLV that contains the 5G SUCI as follows:

Table 6.2.6.1.1-x: SUCI TLV

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Size | M / C / O | Value |
| SUCI TLV Tag | 1 byte | M | 0x |
| Length | 1 byte | M | Length of SUCI value (X) |
| SUCI value  | X bytes | M | according to TS 33.501 [xx]. |

The SUCI TLV shall be used if SUCI is supported by the UE, otherwise the IMSI TLV shall be used.

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 |
| Reserved for future use (set to 00) | BEST encryption algorithm 128-NEA1 supported | BEST encryption algorithm 128-NEA2 supported | BEST encryption algorithm 128-NEA3 supported | BEST integrity algorithm 128-NIA1 supported | BEST integrity algorithm 128-NIA2 supported | BEST integrity algorithm 128-NIA3 supported |
| BEST key agreement - 4G authentication supported | BEST key agreement - 5G authentication supported | BEST key agreement - GBA supported | BEST key agreement - 5G GBA supported | BEST key agreement - AKMA supported | BEST key agreement - Proprietary key agreement supported |  BEST confidential service requested | Reserved for future use (set to 00) |

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, "0001" = Release 15, "0010" = Release 16, "0011" = Release 17 and "0100" 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 only the 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, 128-EEA3, 128-NEA1, 128-NEA2 and 128-NEA3. 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-EIA2,128-EIA3, 128-NIA1, 128-NIA2 and 128-NIA3.

- Values:

'1' = Algorithm supported,

'0' = Algorithm not supported.

- BEST Key agreement mechanisms supported by the UE: a flag for each supported key agreement method: 4G authentication, 5G authentication, GBA, 5G GBA, AKMA and proprietary key agreement.

- Values:

'1' = Algorithm supported,

'0' = Algorithm not supported.

- BEST confidential service requested – an indication from the UE that it would like the BEST user plane data to be confidentiality protected.

- Values:

'1' = BEST confidential service requested,

'0' = BEST confidential service not requested.

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:

- If no indication is given, 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.

- If indicated, perform a 4G 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 to derive KASME and subsequently use KASME 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.

- If indicated, perform a 5G 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 to derive KHSE (depending on the authentication method selected) and subsequently use KHSE 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. The derivation of KHSE is described in clause 5.1.0a. 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.

- If indicated, perform a GBA based authentication. After establishing the agreed key (see clause 5.1.1), the UE uses this key 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 indicated, perform a 5G GBA based authentication. After establishing the agreed key (see clause 5.1.1), the UE uses this key 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 indicated, perform a AKMA based authentication. After establishing the agreed key (see clause 5.1.1), the UE uses this key 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 indicated, perform a proprietry based authentication. After establishing the agreed key (see clause 5.1.1), the UE uses this key 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.

- 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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| BEST HSE configuration TLV Tag = '04' |
| Length of Best protocol ID contents = x bytes |
| BEST Service Activated | BEST encryption algorithm GEA4 to be used | BEST encryption algorithm GEA5 to be used | BEST encryption algorithm UEA1 to be used | BEST encryption algorithm UEA2 to be used | BEST encryption algorithm EEA0 to be used | BEST encryption algorithm 128-EEA1 to be used | BEST encryption algorithm 128-EEA2 to be used |
| BEST signalling plane protocol identifier |
| BEST user plane protocol identifier |
| BEST encryption algorithm 128-EEA3 to be used | BEST integrity algorithm GIA4 to be used | BEST integrity algorithm GIA5 to be used | BEST integrity algorithm UIA1 to be used | BEST integrity algorithm UIA2 to be used | BEST integrity algorithm 128-EIA1 to be used | BEST integrity algorithm 128-EIA2 to be used | BEST integrity algorithm 128-EIA3 to be used |
| Reserved for future use (set to 00) | UE triggered key refresh supported | Local BEST configuration management allowed |  Reserved for future use (set to 0000) |
| New Session Required | Use EAS UP Keys | EMSDP MAC length | Size of EMSDP Data Length |
| Reserved for future use (set to 00) | Authentication method | BEST encryption algorithm 128-NEA1 to be used | BEST encryption algorithm 128-NEA2 to be used | BEST encryption algorithm 128-NEA3 to be used | BEST integrity algorithm 128-NIA1 to be used | BEST integrity algorithm 128-NIA2 to be used | BEST integrity algorithm 128-NIA3 to be used |
| BEST key agreement - 4G authentication required | BEST key agreement - 5G authentication required | BEST key agreement - GBA required | BEST key agreement - 5G GBA required | BEST key agreement - AKMA required | BEST key agreement - Proprietary key agreement required | Reserved for future use (set to 00) |

- 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, 128-EEA3, 128-NEA1, 128-NEA2, and 128-NEA3. 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, 128-EIA3, 128-NIA1, 128-NIA2, and 128-NIA3. 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.

- Authentication method – 1 bit that indicates which authentication method was selected by the UDM.

- Values:

'0' = 5G AKA was selected,

'1' = EAP-AKA' was selected.

- BEST Key Agreement Method - 6 bits that indicate which one of the key agreement methods to use, the bit set indicates the relevant method from the following methods: 4G authentication, 5G authentication, GBA, 5G GBA, AKMA and proprietary key agreement. At most one of the BEST Key Agreement Method values shall be set to 1 and the BEST Key Argeement Method set shall be one of the supported BEST Key Agreement Methods indicated in the preceeding Sesssion Request.

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

Key agreement TLV:

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 or X+1 or Y+1 or Z+1 |
| 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] |
| B-TID | X bytes | C | See 4.4.7 in 3GPP TS 33.220 [13] |
| A-KID | Y bytes | C | See 4.4.2 in 3GPP TS 33.535 [yy] |
| Pre-Agreed Key Identifier | Z bytes | C | Alphanumeric string |
| NOTE 1: For 3G/4G/5G key agreement, RAND IE and AUTN IE shall be present, B-TID, A-KID, and Pre-Agreed Key Identifier shall not be present.NOTE 2: For GBA and 5G GBA, B-TID shall be present, RAND IE, AUTN IE, A-KID, and Pre-Agreed Key Identifier shall not be present.NOTE 3: For AKMA, A-KID shall be present, RAND IE, AUTN IE, B-TID, and Pre-Agreed Key Identifier shall not be present.NOTE 4: For proprietary key agreement, Pre-Agreed Key Identifier shall be present, RAND IE, AUTN IE, B-TID, and A-KID shall not be present. |

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.

If BEST key agreement - 4G authentication required is indicated in the BEST HSE configuration TLV and if the Length is not set to 1 then RAND IE and AUTN IE shall be present in the Key Agreement TLV. In this case, B-TID, A-KID, and Pre-Agreed Key Identifier shall not be present in the Key Agreement TLV.

If BEST key agreement - 5G authentication required is indicated in the BEST HSE configuration TLV and if the Length is not set to 1 then RAND IE and AUTN IE shall be present in the Key Agreement TLV. In this case, B-TID, A-KID, and Pre-Agreed Key Identifier shall not be present in the Key Agreement TLV.

If BEST key agreement - GBA required is indicated in the BEST HSE configuration TLV and if the Length is not set to 1 then B-TID shall be present in the Key Agreement TLV set to a value that identifies the key generated by the GBA key agreement used for this purpose. In this case, RAND IE, AUTN IE, A-KID, and Pre-Agreed Key Identifier shall not be present in the Key Agreement TLV.

If BEST key agreement - 5G GBA required is indicated in the BEST HSE configuration TLV and if the Length is not set to 1 then B-TID shall be present in the Key Agreement TLV set to a value that identifies the key generated by the 5G GBA key agreement used for this purpose. In this case, RAND IE, AUTN IE, A-KID, and Pre-Agreed Key Identifier shall not be present in the Key Agreement TLV.

If BEST key agreement - AKMA required is indicated in the BEST HSE configuration TLV and if the Length is not set to 1 then A-KID shall be present in the Key Agreement TLV set to a value that identifies the key generated by the AKMA key agreement used for this purpose. In this case, RAND IE, AUTN IE, B-TID, and Pre-Agreed Key Identifier shall not be present in the Key Agreement TLV.

If BEST key agreement - Proprietary Key agreement required is indicated in the BEST HSE configuration TLV and if the Length is not set to 1 then Pre-Agreed Key Identifier shall be present in the Key Agreement TLV set to a value that identifies the Proprietary key to be used. In this case, RAND IE, AUTN IE, B-TID, and A-KID shall not be present in the Key Agreement TLV.

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 | C | As returned by the USIM. |
| XRES | X bytes | C | As returned by the USIM. |
| Proprietary Key agreement response | X bytes | O | Proprietary response |

If the response is associated with a 4G key agreement from the HSE then RES shall be present.

If the response is associated with a 5G key agreement from the HSE then XRES shall be present.

If the response is associated with a Proprietary key agreement from the HSE then Proprietary Key agreement response may be present.

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.

END OF CHANGE 10

START OF CHANGE 11

##### 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 | M |
| AUTS TLV | C |

Where:

Rejection details TLV: Contains the rejection reason. If the rejection reason is "Authentication ReSync required" and the key agreement method used is either 4G key agreement or 5G key agreement, then the Rejection details TLV and the AUTS TLV shall be present. For all other reasons only 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"

 '0A' = "No pre-agreed key available using the indicated key agreement method and identifier"

 '0B' = "Key agreement method not supported"

 '0C' = "Key agreement error - unspecified reason"

 '0D' = "UE temporary error – try again later"

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 |

END OF CHANGE 11