**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211412-r1***

**e-meeting, 17 - 28 May 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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***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 can be 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 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, or 5G) 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 and 5G AKA have been included. * 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. * Derivation of UE-to-HSE keys and Intermediate Key has been updated for 3G, 4G, and 5G keys based derivations. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Without this change, BEST cannot be applied to 5GS networks. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 4.2.1, new 4.2.2, 4.3.1, 4.3.2, 4.6.1.1, 4.6.2.2, 5.1.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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".

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.

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.

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, and 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 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 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 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. Nudm\_UEAuthentication\_Get Request over SBA interface** – The HSE shall use the SBA interface to the UDM/ARPF to request one or more 5G HE authentication vectors using the UE SUCI.

**4. Nudm\_UEAuthentication\_Get Response over SBA interface** – The UDM/ARPF uses the SBA interface to the HSE to return the requested 5G HE authentication vectors. The UDM/ARPF shall select 5G AKA as the selected authentication method.

Editor's note: how UDM/ARPF knows when to select 5G AKA as selected authentication method is FFS.

**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 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

### 5.1.1 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, or KAUSF, 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 KAUSF.

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

END OF CHANGE 7