ETSI TS 133 163 V15.6.0 (2019-10)

LTE;
5G;
Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST)
(3GPP TS 33.163 version 15.6.0 Release 15)

Reference
RTS/TSGS-0333163vf60

Keywords
5G,LTE,SECURITY

ETSI

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

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

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

Important notice

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

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

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

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

Copyright Notification

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

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

Specifically:

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

1 Scope

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

These processes consist of:

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

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[14] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

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

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

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

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

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

UE-to-EAS: UE to Enterprise Application Server

3.2 Abbreviations

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

EAS Enterprise Application Server
HSE HPLMN Security Endpoint

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

4.1 Introduction

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

The following services are defined:

- BEST key agreement only service – This service is a battery efficient service for key agreement between a BEST compliant UE and the HSE or the EAS. The user plane for this service is provided by the application layer between the UE and the EAS and is out of scope of this specification.

- BEST user plane integrity protected service – This service is a battery efficient integrity protected user plane service for low throughput devices. This service includes the key agreement and includes integrity protected security over small data over NAS User Plane. The user plane for this service can be either terminated in the HSE (so called UE-to-HSE mode) or in the EAS (so called UE-to-EAS mode). Control messages are always terminated in the HSE.

- BEST user plane confidential service – This service is a battery efficient integrity and confidentiality protected user plane service for low throughput devices. The user plane for this service can be either terminated in the HSE (so called UE-to-HSE mode) or in the EAS (so called UE-to-EAS mode). Control messages are always terminated in the HSE.

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

4.2 BEST Framework Service Description

4.2.1 Architecture

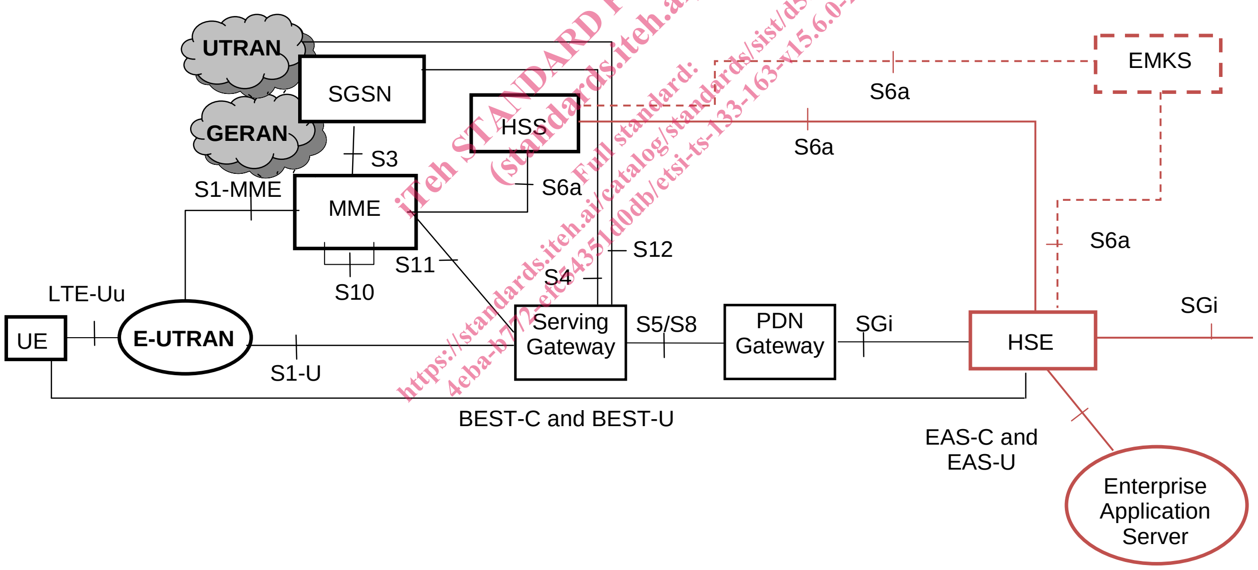

Figure 4.2.1-1: The architecture of the extended user plane protection service

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.

4.3 Procedures between the UE and the HSE

4.3.1 Overview of BEST procedures

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

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

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

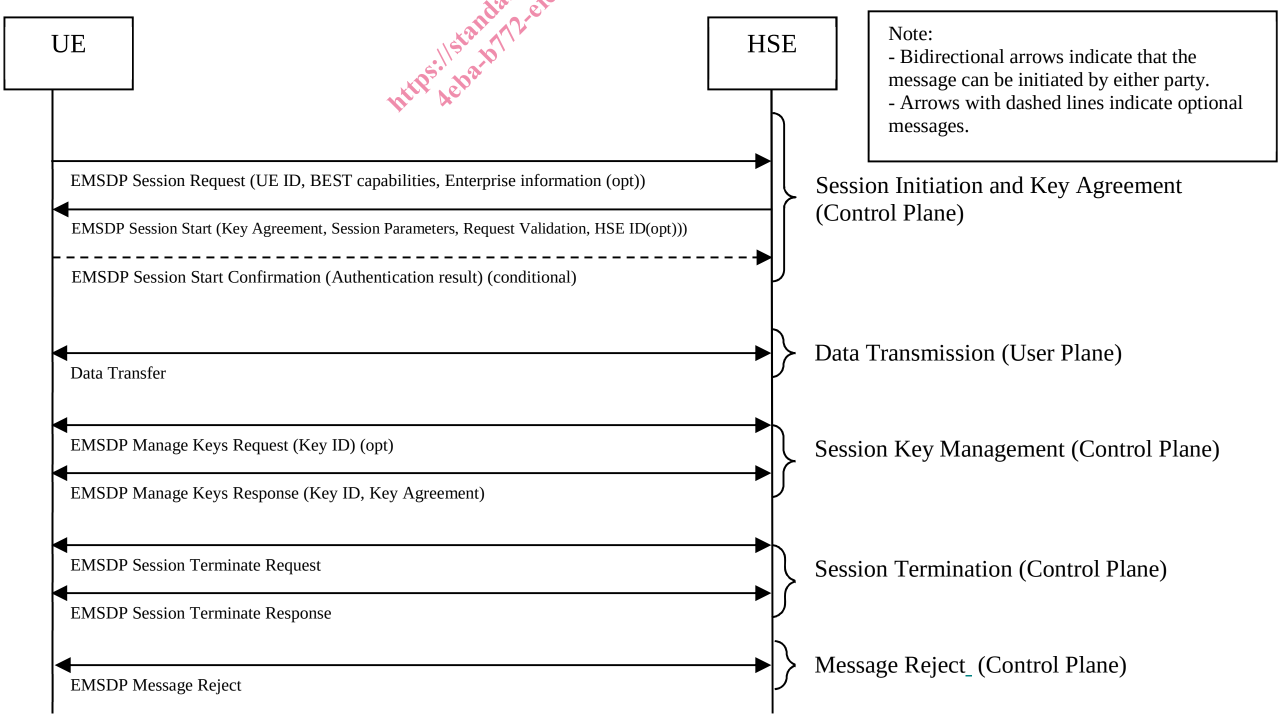

Figure 4.3.1-1: Generalised BEST service flow

4.3.2 BEST Session Initiation and Key Agreement

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

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

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

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

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

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

4.3.3 BEST Session Key Management

At any time during the BEST session, either the UE or the HSE may trigger a re-negotiation of the keys being used for the BEST service using the EMSDP Manage Keys Request and Response exchange.

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

4.3.4 BEST Session Termination

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

4.3.5 BEST Message Reject

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

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

4.4 Procedures between the HSE and the EAS

4.4.1 Message Exchange Overview

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

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

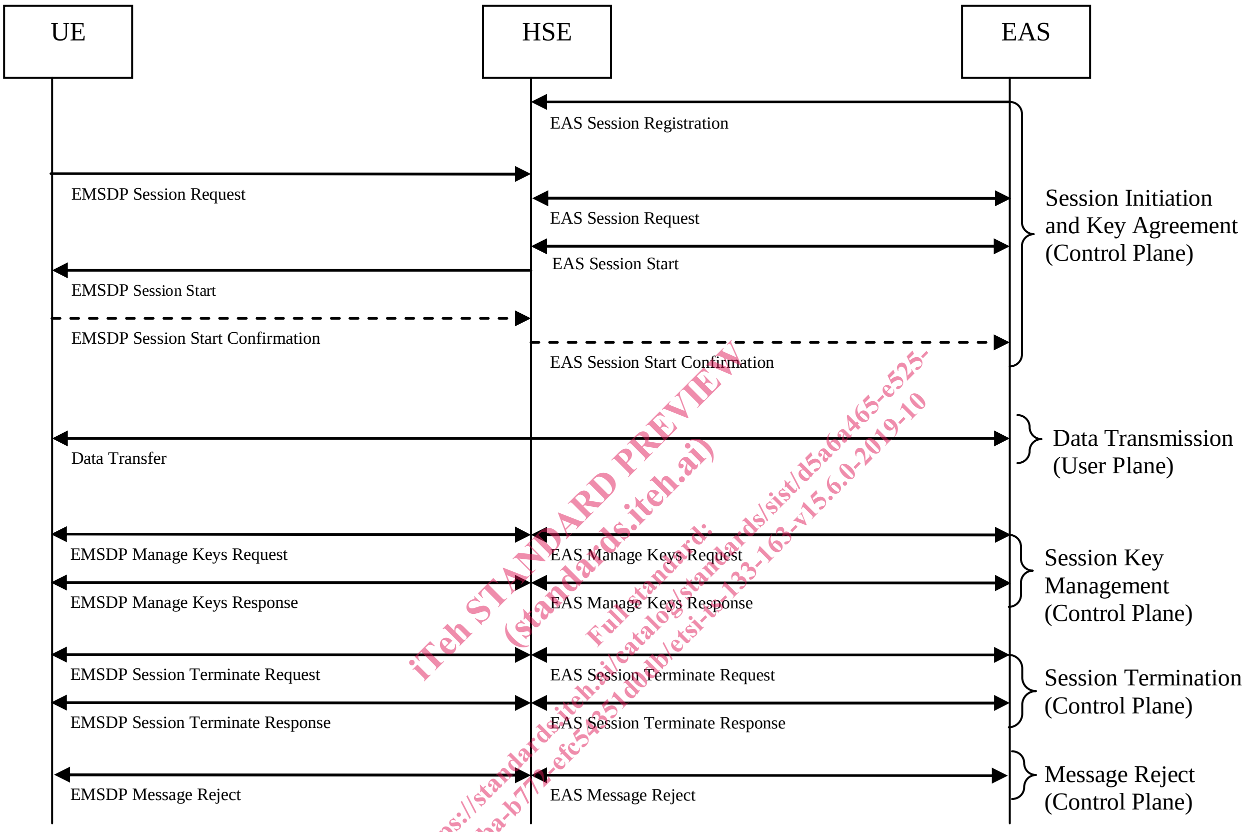

Figure 4.4.1-1: Generalised BEST EAS service flow

4.4.2 EAS Registration for BEST Service

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

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

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

4.4.3 Key Request

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