3GPP TS 33.187 V0.1.0 (2013-04)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of Machine-Type and other Mobile Data Applications Communications Enhancements; (Release 12)

Logos: *Use exactly one of the above lines. Delete the other two.*
Use the top line for documents which are specific to GERAN technology only.
Use the second line for documents which are specific to UTRAN technology only or to GERAN and UNTRAN techologies only.
*Use the third line for documents which relate to LTE technology (regardless of their applicability to GERAN or to UTRAN technologies) in Releases **prior to** Release 10.*

Keywords
<keyword[, keyword, …]>
Use the fourth line for documents which relate to LTE technology (regardless of their applicability to GERAN or to UTRAN technologies) in Release 10 onwards.

MCC selects keywords from stock list.

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

This clause shall start on a new page.

The present document specifies the security architecture enhancements (, i.e., enhancements to the security features and the security mechanisms) to facilitate Machine-Type and other mobile data applications communications enhancements as per the use cases and service requirements defined in TS 22.368 [2] and the architecture enhancements and procedures defined in TS 23.682 [3].

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 TS 22.368: "Service Requirements for Machine-Type Communications (MTC)".

[3] 3GPP TS 23.682: "Architecture Enhancements to facilitate communications with Packet Data Networks and Applications".

[4] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)".

[5] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[6] 3GPP TS 23.142: "Value-added Services for SMS (VAS4SMS); Interface and signalling flow".

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Clause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

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

Definition format (Normal)

<defined term>: *<definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

3.3 Abbreviations

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

Abbreviation format (EW)

<ACRONYM> <Explanation>

4 Security Requirements

<This section specifies the security requirements for Machine-Type and other mobile data applications Communications enhancements >

4.1 Requirements on MTC

The security requirements for MTC include the following:

- MTC optimizations shall not degrade security compared to non-MTC communications [2]

4.2 Requirements on Tsp Reference Point

The Tsp reference point shall fulfil the following requirements:

- integrity protection, replay protection, confidentiality protection and privacy protection for communication between the MTC-IWF and SCS shall be supported:
  - mutual authentication between two directly communicating entities in the security domains, in which MTC-IWF and SCS respectively reside, shall be supported;
  - the use of mutual authentication shall follow the provisions in TS 29.368 [4];
  - integrity protection and replay protection shall be used;
  - confidentiality protection should be used;
  - privacy shall be provided (e.g. IMSI shall not be sent outside the 3GPP operator domain).

4.3 Requirements on MTC-IWF

The functionality of the MTC-IWF includes the following:

- support ability to satisfy security requirements on Tsp reference point in clause 4.2 of the present specification.

5 General Security Procedures

<This section specifies the general security procedure>

5.1 Security Procedures for Tsp Interface Security

The security procedures for the Tsp interface are specified in TS 29.368 [4].

6 Security Procedures for Small Data and Device Trigger Enhancements (SDDTE)

6.1 Security procedures for Device Triggering

6.1.1 Network based solution for filtering SMS-delivered device trigger messages

The following solution may be implemented to filter SMS-delivered device trigger messages. This solution relies on the fact that there is a standardised indicator in the SM that can be used to distinguish a trigger SM from other types of SM. The solution further assumes that legitimate trigger SMs are delivered via either a SMS-SC in the HPLMN that can verify the identity of the SME sending a legitimate trigger SM over Tsms, or via an MTC-IWF in the HPLMN that can verify the identity of the SCS sending a legitimate trigger SM over Tsp.

The HPLMN shall implement Home Network Routing according to TS 23.040 [5] for Mobile Terminated SMs destined for all HPLMN subscribers that need protection against unauthorised SMS-delivered device trigger messages (e.g. all subscriptions that may be used in MEs that support SMS-delivered device triggering). Home Network Routing shall have the effect of forcing the delivery of the SM to an SMS Router in the HPLMN rather than to the serving MSC/VLR, SGSN or MME of the destination UE. If an SM received by the SMS Router does not originate from the SMS-SC in the HPLMN that handles SMS-delivered device trigger messages, then the SMS Router shall forward the SM to infrastructure that shall filter and block all SMs that contain a trigger indication.

If an SM received by the SMS-SC in the HPLMN that handles SMS-delivered device trigger messages does not originate from the T4 interface, then the SMS-SC shall forward the SM to filtering infrastructure. If an SM received by the filtering infrastructure contains a trigger indication, and does not originate from a trusted SME that is authorised to send trigger SMs, then the SM shall be blocked. If an SM received by the filtering infrastructure contains a trigger indication, and does originate from a trusted SME that is authorised to send trigger SMs, then the filtering infrastructure shall only allow trigger requests to be sent to particular UEs that the trusted SME is authorised to send to. It is outside the scope of this specification how the filtering infrastructure shall determine if a trusted SME is allowed to send a device trigger to a particular UE.

If a trigger request received by the MTC-IWF originates from the Tsp interface, then the MTC-IWF shall filter and block the trigger unless it originates from a trusted SCS that is authorised to send trigger requests. The procedure is described in TS 23.682[3] clause 5.2.1.

NOTE 1: Depending on operator policy, a trusted source may be authorized to send trigger messages to any UE.

In order to protect against source spoofing, the interfaces used to transport trigger messages shall be suitably secured. In particular, the Tsms, Tsp and T4 interfaces shall be secured. Tsp interface security is specified in TS 23.682 [3] clause 4.3.3.1. The security mechanisms for the Tsms interface are outside the scope of this specification.

Filtering of SMS can be performed according to the architecture specified in TS 23.142 [6]. When the filtering entity receives an SM, it can identify if the SM is a trigger SM based on some trigger indication contained in the SM (e.g. port address number).

NOTE 2: In the above solution filtering is distributed between filtering infrastructure associated with the SMS Router, filtering infrastructure associated with the SMS-SC, and the filtering functions within the MTC-IWF. This reflects the fact that the filtering needs to be invoked by an entity which can verify the source of the SM on a locally connected interface. Whilst the SMS Router is inthe path of all SMs towards MTC devices, it does not have the capability to verify the original source of messages on the Tsp or Tsms interfaces, and therefore a solution where only the SMS Router invokes filtering is not sufficient.

NOTE 3: The solution in this clause aims to protect against unauthorised entities sending potentially high volumes of trigger messages to large numbers of MTC devices to cause a Distributed Denial of Service (DDoS) attack against the core network. However, the solution only provides protection against SMS application level threats; it does not protect against attacks where network internal nodes or network signalling links are compromised or abused by an attacker (e.g. spoofing of MAP_Forward_Short_Message operations containing trigger indications towards target UEs on an SS7 connection). If such attacks need to be mitigated, or if Home Network Routing is not supported by the HPLMN, then the solution specified in this clause is not sufficient and some form of end-to-end cryptographic protection of trigger messages is needed between the MTC Application in the network and the MTC Application in the UE. Such solutions may be provided at an application level outside the scope of 3GPP specifications. A solution to cryptographically protect trigger messages may be introduced in a future 3GPP Release.

6.2 Security procedures for Small Data Transmission

<This section specifies the small data transmission security procedure>

7 Security Procedures for UE Power Consumption Optimisation (UEPCOP)

<This section specifies the security procedure for UE power consumption optimization >

8 Security Procedures for Secure Connection

<This section specifies the security procedure for Secure Connection >

9 Security Procedures for Restricting the USIM to specific UEs

<This section specifies the security procedure for USIM binding to specific UEs>

10 Privacy Concerns on MTC

<This section specifies the procedure for Privacy Concerns>

Annexes are only to be used where appropriate:

Annex <A> (normative): <Normative annex title>

Annex <X> (informative): Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2013-04					*Initial version and addition of contributions agreed in SA3#71 meeting*	*-*	*0.1.0*