ETSI TS 133 187 V12.2.0 (2015-04)

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements
(3GPP TS 33.187 version 12.2.0 Release 12)**

Reference
RTS/TSGS-0333187vc20

Keywords
GSM,LTE,SECURITY,UMTS

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

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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.

1 Scope

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 (MTCe) as per the use cases and service requirements defined in 3GPP TS 22.368 [2] and the architecture enhancements and procedures defined in 3GPP 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".

[7] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[8] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[9] 3GPP TS 23.204: "Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2".

[10] 3GPP TS 31.115: "Remote APDU Structure for (U)SIM Toolkit applications".

[11] 3GPP TS 31.116: "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[12] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications'.

[13] ETSI TS 102 226: "Smart cards; Remote APDU structure for UICC based applications'.

[14] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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 TR 21.905 [1].

3.2 Symbols

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

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

MTC	Machine-Type Communications
MTC-IWF	MTC Interworking Function

4 Security Requirements

4.1 Requirements on MTC

The security requirements for MTC include the following:

- MTC optimizations shall not degrade security compared to non-MTC communications 3GPP TS 22.368 [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.

5 General security procedures

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 Device Triggering

6.1 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 standardized indicator in the SM that can be used to distinguish a trigger SM from other types of SM, i.e. TP Protocol Id as specified in 3GPP TS 23.040 [5].
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 3GPP 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.

- Referring to the SMS architecture and function defined in 3GPP TS 23.040 [5] and 3GPP TS 23.204 [9], SMSs need to be delivered through SMS-SC. On the basis of the architecture of machine-type communication, for SMS based device trigger and 3GPP TS 23.040 [5], the SMS-SC can receive short message with the related sender and receiver"s identities from three paths, i.e. SME via Tsms interface or T4 interface or from SMS-IWMSC. Filtering SMS-delivered device trigger messages is network-based, so the fake triggering SMSs from an attacker shall be distinguished and blocked to be sent by SMS-SC on the network side. The following is how these three paths work for SMS-SC to receive short messages: 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.

- When SMS-SC receives short message which is forwarded by MTC-IWF via T4 interface, the SMS-SC ensures T4 interface is trusted and sends the short message, because the MTC-IWF can authenticate MTC server and ensure that only the authorized MTC Server can trigger the particular MTC devices.

- When the SMS-SC receives short messages from SMS-IWMSC, the SMS-SC shall also forward the SM to filtering infrastructure. Thus the SMS-SC can check if the SM is originated from an authorized SME by checking the receiver"s authorized sender list. If not, it should block the fake SM to be sent.

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 3GPP TS 23.682 [3] clause 5.2.1.

The normal UE is not allowed to send MO trigger SMSs to trigger MTC devices according to section 9.2.3.9 of 3GPP TS 23.040 [5], so SMS-SC shall distinguish and block the fake MO device trigger SMSs from normal UE"s subscription.

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 3GPP 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 (i.e. TP Protocol Id as specified in 3GPP TS 23.040 [5]).

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 an optional entity that may be present in the MT case only, 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. The best place for filtering infrastructure to associate with is SMS-SC which can filter SMs received from all paths.

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.

NOTE 4: There exists a scenario in which inter-PLMN SMC-SCs are directly connected, thus the implementation of Home Network Routing is not mandatory.

7 Security procedures for secure connection

7.1 Introduction

The Secure Connection is a feature with which the network operator is able to efficiently provide key material for securing the application protocol between UE and a SCS (indirect model) or between UE and a MTC Application Server (direct model).

GBA, as specified in 3GPP TS 33.220 [7], is used to bootstrap authentication and key agreement for application security based on the 3GPP AKA mechanism. GBA shall be used to establish the keys for a UE initiated Secure Connection.

An extension to GBA, called GBAPush, is defined in 3GPP TS 33.223 [8]. GBAPush is also used to establish keys for application security between two entities, but unlike GBA, it is initiated from the network. GBAPush shall be used to establish the keys for a network initiated Secure Connection.

Also other mechanisms (for example, using EAP-AKA authentication in scenarios which GBA cannot apply to) can be used to provide the MTC Secure Connection feature between the UE and SCS or between the UE and MTC Application Server. These mechanisms are regarded to be outside the scope of 3GPP specifications.

The implementation of Secure Connection feature in the ME and network is optional.

7.2 UE initiated secure connection

This solution is restricted to such UEs that support HTTP.

A UE-initiated Secure Connection shall be established using GBA as defined in 3GPP TS 33.220 [7].
GBA shall be used regardless if the Secure Connection is between the UE and SCS or between the UE and MTC Application Server. The SCS and the MTC Application Server shall act as NAFs. The Secure Connection key establishment using GBA is outlined as follows:

> The UE runs a GBA bootstrapping with the BSF via the Ub interface. This bootstrapping results in that the UE and BSF share a session key Ks and an identifier associated with the Ks, called B-TID. The UE next generates a Ks_(ext/int)_NAF key from key Ks, and establishes a connection with the intended NAF over the Ua interface. The NAF function is performed by the SCS in the indirect model, and by the MTC Application Server in the direct model. At the start of the communication, the UE provides the NAF with the B-TID. The NAF requests the Ks_(ext/int)_NAF, corresponding to the B-TID from the BSF. The UE and SCS/MTC Application Server can then protect the Ua application protocol (i.e. the Secure Connection) using the shared Ks_(ext/int)_NAF key.

It depends on the used Ua application protocol how the Ks_(ext/int)_NAF keys are used in order to protect the communication between the UE and the SCS or between the UE and the MTC Application Server.

7.3 Network initiated secure connection

A network-initiated Secure Connection shall be established using GBAPush as defined in 3GPP TS 33.223 [8].
GBAPush shall be used regardless if the Secure Connection is between the UE and SCS or between the UE and MTC Application Server. The SCS and the MTC Application Server shall act as Push NAFs.
The Secure Connection key establishment using GBAPush is outlined as follows:

> The pushNAF, i.e. the SCS in the indirect model and the MTC Application Server in the direct model, determines the need to use GBAPush in order to establish keys for application security (i.e. a Secure Connection) with the UE. The pushNAF then requests a GBA Push-Info (GPI) and a Ks_(int/ext)_NAF key from the BSF and then forwards the GPI to the UE. The UE processes the GPI and generates a Ks_(ext/int)_NAF key from it. The UE and pushNAF can protect the Ua application protocol (i.e. the Secure Connection) using the shared Ks_(ext/int)_NAF key.

If the pushNAF (SCS or MTC Application Server) does not have IP connectivity with the UE, the GPI can be sent in the Device Trigger to the UE via the Tsp in case of SCS is the pushNAF and via Tsms in case of MTC Application Server (acting as SME) is the pushNAF. In this case the GPI can serve two purposes: it can be used to provide keys for the application protocol (i.e. Secure Connection) and it can also be used protect the device trigger itself in an end-to-end manner.

If the pushNAF (SCS or MTC Application Server) has IP connectivity with the UE, the GPI can be sent within the application protocol that the MTC application uses and used to provide keys for the Secure Connection.

It depends on the used Ua application protocol how the Ks_(ext/int)_NAF keys are used in order to protect the communication between the UE and the SCS or between the UE and the MTC Application Server.

8 Security procedures for restricting the USIM to specific UEs

8.1 UE-based procedure with USAT application pairing

8.1.1 General

This clause specifies how the use of a USIM can be restricted to specific MEs thanks to UE-based solution relying on USAT application pairing. The solution is optional for implementation in the User Equipment and in the operator network.

To have USAT application pairing capable User Equipment, the ME shall support USAT, as specified in 3GPP TS 31.111 [14].

8.1.2 Security procedure

USAT application pairing is successful when the IMEI or IMEISV retrieved from the terminal matches the value or the range of values the UICC is configured with. USAT application pairing fails if the terminal does not support USAT command PROVIDE LOCAL INFORMATION.

An UE supporting USAT application pairing proceeds to Profile download as specified in 31.111 [14]. Then, the USIM requests IMEI(SV) using PROVIDE LOCAL INFORMATION proactive command. The ME sends the TERMINAL RESPONSE with its IMEI(SV).

The file EF_{IWL} stores the IMEI(SV) or range of value to which the USIM is bound.

The file EF_{IPS} stores the status of the last pairing check performed by the UICC. The UICC checks the combination of USIM and MTC ME and sets the status flag to 'OK' in case of successful pairing check. The UICC also stores in the file EF_{IPD} the IME(SV) value of the MTC ME. In case of unsuccessful pairing check, the USIM sets the status flag to 'KO' in the file EF_{IPS} and stores in the file EF_{IPD} the IME(SV) value of the unauthorized MTC ME.

The status flag of pairing check (with value 'OK or 'KO') stored in the file EF_{IPS} can be read by any terminal hosting the UICC. But, the IMEI(SV) value stored in the file EF_{IPD} is protected by ADM right, only the operator can retrieve this information. The information stored in the file EF_{IPD} provide a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the files EF_{IPS} and EF_{IPD} can be read out locally by the maintenance persons.

The UICC shall respond to any AUTHENTICATE command with error status words if:

- IMEI or IMEISV provided by the ME is not in the corresponding white list configured in the USIM (EF_{IWL})

Or

- ME has not provided either IMEI or IMEISV

If the AUTHENTICATE command had been executed before the pairing procedure has been successfully performed (in the case of pre-Rel-12 MEs), the UICC may need to trigger a network attachment procedure by sending a proactive command REFRESH(3G SESSION RESET).

UICC OTA mechanism (as specified in 3GPP TS 31.115 [10] / TS 31116 [11] and ETSI TS 102 225 [12] and TS 102 226 [13]) is used to update the file EF_{IWL} stored in the USIM. This mechanism provides dynamic management of the pairing to change the allowed combinations of USIM and MTC ME(s) by adding or removing authorized IMEI(SV) values or IMEI(SV) ranges the file EF_{IWL}.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2014-06	SA#64	SP-140318	001	1	Modification on clause 6.1 of TS 33.187	12.0.0	12.1.0
2015-03	SA#67	SP-150078	002	1	USAT Pairing update	12.1.0	12.2.0

History

Document history		
V12.1.0	October 2014	Publication
V12.2.0	April 2015	Publication