

ICS 33.070.99

M 36

YD

中华人民共和国通信行业标准

YD/T 2913-2015

M2M 通信系统增强安全要求

Security aspects of network enhancement for
machine-type communications

2015-07-14 发布

2015-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 缩略语	2
4 M2M安全架构和安全需求	2
4.1 M2M安全架构	2
4.2 安全需求	3
5 Tsp接口安全技术要求	4
5.1 概述	4
5.2 双向鉴权	4
5.3 安全配置	4
6 MTC终端触发相关安全技术要求	5
6.1 概述	5
6.2 过滤设备触发SMS短消息的网络侧方案	5
7 安全连接技术要求	6
7.1 概述	6
7.2 MTC设备发起的安全连接	6
7.3 网络发起的安全连接	7
8 USIM与MTC设备绑定安全技术要求	7
8.1 基于UE的USAT应用配对概述	7
8.2 安全技术要求	7
附录A（资料性附录） M2M应用场景	9

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中兴通讯股份有限公司、中国信息通信研究院、华为技术有限公司、大唐电信科技产业集团。

本标准主要起草人：游世林、林兆骥、余万涛、崔媛媛、陈 璟、应江威、艾 明。

M2M 通信系统增强安全要求

1 范围

本标准规定了移动通信系统承载M2M业务时的触发安全、Tsp接口安全、安全连接以及USIM与MTC设备绑定4个方面的安全技术要求。

本标准适用于基于3GPP R12承载M2M业务的包括终端、智能卡和系统设备在内的端到端移动通信系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3GPP TS 23.040 短消息技术实现（Technical realization of the Short Message Service (SMS)）

3GPP TS 23.142 短消息增值业务：接口和信令流程（Value-added Services for SMS (VAS4SMS); Interface and signalling flow）

3GPP TS 23.204 3GPP IP接入下的短消息业务：阶段2（Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2）

3GPP TS 23.682 分组数据网络与应用下设备通讯的架构增强（Architecture Enhancements to facilitate communications with Packet Data Networks and Applications）

3GPP TS 29.368 MTC-IWF与SCS之间的Tsp接口协议（Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)）

3GPP TS 31.111 USIM应用工具箱（Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)）

3GPP TS 31.115 USIM应用工具箱安全包结构（Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications）

3GPP TS 31.116 USIM应用工具箱APDU结构，（Remote APDU Structure for (U)SIM Toolkit applications）

3GPP TS 33.220 通用认证架构(GAA)之通用自举架构，（Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)）

3GPP TS 33.223 通用认证架构(GAA)之通用自举架构推送功能（Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function）

ETSI TS 102. 225 智能卡：基于UICC应用的安全包结构（Smart Cards; Secured packet structure for UICC based applications）

ETSI TS 102. 226 智能卡：基于UICC应用的远程APDU结构（Smart cards; Remote APDU structure for UICC based applications）

3 缩略语

下列缩略语适用于本文件。

AVP	Attribute Value Pair	属性值对
CEA	Capabilities-Exchange-Answer	能力交换响应
CER	Capabilities-Exchange-Request	能力交换请求
ESP	Encapsulating Security Payload	封装安全有效负载
GPRS	General Packet Radio Service	通用分组无线业务
IKE	Internet Key Exchange	Internet密钥交换协议
MTC	Machine-Type Communication	机器类通信
MTC-IWF	MTC Interworking Function	机器类通信互联功能
PKI	Public key infrastructure	公钥基础设施
SCS	Service Capability Server	业务能力服务器
TLS	Transport Layer Security	传输层安全
UMTS	Universal Mobile Telecommunications System	通用移动通信系统
USAT	USIM Application Toolkit	USIM应用工具
USIM	UMTS Subscriber Identity Module	UMTS用户身份模块
UTRAN	UMTS Radio Access Network	UMTS无线接入网
UE	User Equipment	用户设备
UICC	UMTS Integrated Circuit Card	UMTS集成电路卡

4 M2M 安全架构和安全需求

4.1 M2M 安全架构

备注：T5a、T5b和T5c接口在本标准不做要求。

图1定义了一个高层次的机器类通信安全架构。

层次A：MTC设备和3GPP网络之间机器类通信的安全可以进一步分为：

A1：MTC设备和无线接入网络之间机器类通信的安全；

A2：MTC设备和非接入层之间机器类通信的安全；

A3：MTC设备和非3GPP接入之间机器类通信的安全。

层次B：3GPP网络和SCS/MTC应用之间机器类通信的安全可以进一步分为：

B1：在间接模式下SCS和3GPP网络之间的机器类通信的安全。可以进一步细分为当SCS位于3GPP网络域内与3GPP网络域外的安全。

B2：在直接模式下MTC应用和3GPP网络之间的机器类通信的安全。

SCS和MTC应用之间的通信在本标准规定范围之外。

层次C：MTC设备和SCS/MTC应用之间机器类通信的安全可以进一步分为：

C1：在间接模式下MTC服务器和MTC设备之间的机器类通信的安全。

C2：在直接模式下MTC应用和MTC设备之间的机器类通信的安全。

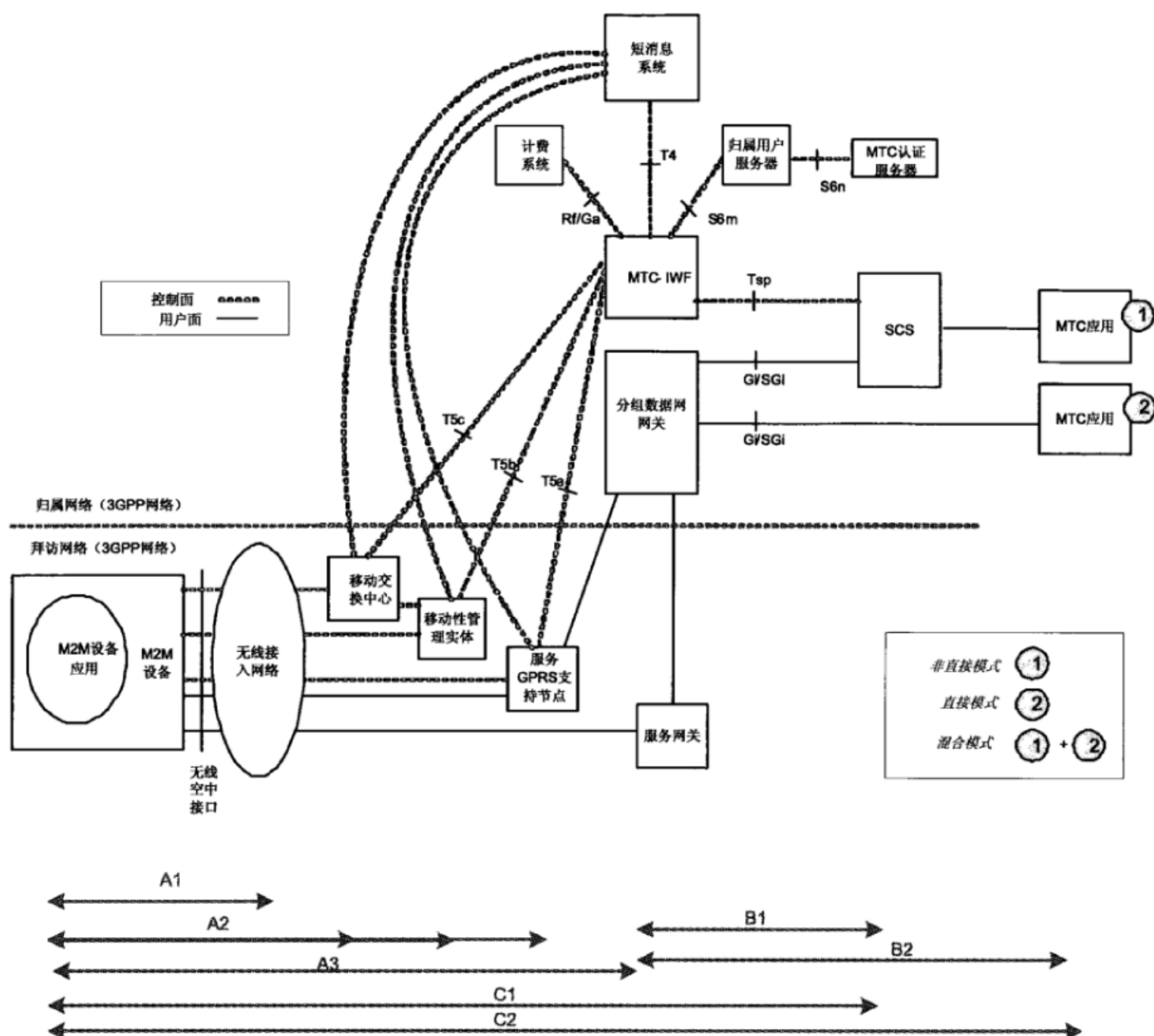


图1 3GPP M2M 安全架构

4.2 安全需求

4.2.1 MTC 安全需求

针对MTC的安全需求包括：M2M的优化不能降低优化前通讯系统的安全级别。

4.2.2 Tsp 接口安全需求

Tsp接口应符合如下安全需求：

- Tsp接口之间的通讯应提供完整性保护、重放攻击保护、机密性保护和隐私保护；
- Tsp接口之间的通讯应提供相互认证、鉴权；
- 相互认证的方式见3GPP TS 29.368；
- Tsp接口应使用完整性保护和重放攻击保护；
- Tsp接口应使用机密性保护；
- Tsp接口应使用隐私保护（比如：IMSI不能传递到非3GPP运营网络之外）。

4.2.3 MTC-IWF 安全需求

MTC-IWF 的安全需求与 Tsp 接口安全需求一致。

5 Tsp 接口安全技术要求

5.1 概述

应使用在IETF RFC 3588中所定义的Diameter安全机制。

5.2 双向鉴权

本标准只针对如下部署方式的Tsp接口安全过程：MTC-IWF和SCS之间的Tsp接口上的DIAMETER消息应通过MTC-IWF所在的安全域中的至少一个DIAMETER代理（后文中称为“MTC-IWF侧代理”），和SCS所在的安全域中的一个DIAMETER代理（后文中称为“SCS侧代理”）。

注 1： 也可以有其他的部署方式，但不推荐使用Tsp接口。

MTC-IWF所在的安全域中的一个节点和SCS所在的安全域中的一个节点之间的双向鉴权应使用IETF RFC 3588所定义的TLS或IPsec，除非使用6.3.3中所定义的安全配置。

应遵循以下规则：

- 在MTC-IWF的安全域和SCS的安全域之间不能有存在中间DIAMETER代理的第三个安全域。
- 在MTC-IWF的安全域中，如果有MTC-IWF侧代理，则由MTC-IWF侧代理作为执行Tsp相关双向鉴权的节点；如果没有MTC-IWF侧代理，则由MTC-IWF作为执行Tsp相关双向鉴权的节点。
- 在SCS的安全域中，如果有SCS侧代理，则由SCS侧代理作为执行Tsp相关双向鉴权的节点；如果没有SCS侧代理，则由SCS作为执行Tsp相关双向鉴权的节点。
- 各节点应使用TLS或IPsec验证在CER/CEA消息中收到的标识（比如，证书中的名称）的节点标识。
- 域授权检查：一个收到Tsp相关DIAMETER消息的适当的节点应检查该消息的发出者，即在应用层指定的SCS（或MTC-IWF），是真正被授权通过其标识在之前的步骤中被验证的节点发送该消息的。这项检查可以通过与SCSs（或MTC-IWFs）相关联的本地表格结合其标识可以被接受域验证的初始安全域中的节点执行。执行该域授权检查的节点应是MTC-IWF或发到MTC-IWF的消息的MTC-IWF侧代理，以及SCS或发到SCS的消息的SCS侧代理。

注 2： 即使存在MTC-IWF侧代理，MTC-IWF也可以执行域安全检查，因为MTC-IWF侧代理在Record-Route AVP中包含验证过的标识（SCS侧的情况类似）。域授权检查的概念在以上的列举项中定义，而不是来自其他规范性文件。

5.3 安全配置

在TLS上支持Tsp是强制的。支持IKE/IPsec是可选的。

IKE、IPsec和TLS的安全配置应遵循以下规定：

- TLS实现和使用的配置应遵循3GPP TS 33.310附录E中的规定。双向鉴权应基于根据3GPP TS 33.310中6.1.3a节和6.1.4a节的配置的证书。用于这些证书的PKI的结构不在本标准范围内，因此本条中对证书的发出者的规定不适用。
- 如果支持IKE/IPsec，则实现IKEv2和基于根据3GPP TS 33.310配置的证书的双向鉴权是强制的。证书配置应遵循3GPP TS 33.310中6.1.3和6.1.4。用于这些证书的PKI的结构不在本标准范围内，因此本条中对证书的发出者的规定不适用。
- 如果支持IKE/IPsec，则IPsec ESP应根据3GPP TS 33.210中的配置实现。隧道模式是强制支持的。传输模式是可选支持的。

6 MTC 终端触发相关安全技术要求

6.1 概述

MTC 终端触发安全技术方案是基于 SMS 短消息传递的设备触发消息的过滤的相关技术要求。

6.2 过滤设备触发 SMS 短消息的网络侧方案

以下方案用于过滤基于 SMS 短消息传递的设备触发消息。

该方案依赖于短消息中的标准化标识，也就是 3GPP TS 23.040 中所定义的 TP Protocol ID，用于区分触发短消息和其它类型的短消息。

该方案进一步假设合法触发短消息的传递需要经过归属域网络中的 SMS-SC，以验证通过 Tsms 接口发送触发短消息的短消息实体身份是否合法；或者经过归属域网络中的 MTC-IWF，以验证通过 Tsp 接口发送触发 SM 的 SCS 身份是否合法。

归属域网络应该基于 3GPP TS 23.040，为发给归属域网络用户的短消息终呼实现归属网络路由，以保护这些用户免遭未经授权 SMS 触发消息的攻击（例如，支持 SMS 触发的终端中的签约）。归属网络路由应该能够将 SM 传递给 HPLMN 中的 SMS 路由器，而不是传递给目标 UE 的服务 MSC/VLR、SGSN、或者 MME。如果 SMS 路由器接收到的 SM 不是来自于归属域网络中的处理 SMS 触发消息的 SMS-SC，则 SMS 路由器会将该 SM 发送给过滤设施，从而过滤并阻止包含触发指示的短消息。

参考 3GPP TS 23.040 和 3GPP TS 23.204 所定义的 SMS 架构和功能，SMSs 的传输需要经过 SMS-SC。根据 M2M 机器类通信的架构，对于基于 SMS 的设备触发，SMS-SC 所接收的短消息包含了相关的发送者标识和接收者标识，这些短消息来自三条路径，即通过 Tsms 接口的短消息实体、T4 接口、SMS-IW MSC。过滤 SMS 触发消息是基于网络侧的，因此伪造的 SMS 触发消息应该被 SMS-SC 所识别并阻止。以下描述了 SMS-SC 如何处理来自于这三条路径的短消息。

- 如果 HPLMN 中处理 SMS 触发消息的 SMS-SC 所接收的 SM 不是来自于 T4 接口，则应该将该 SM 发送给过滤设施。

- 如果过滤设施所接收的 SM 包含触发指示并且不是源于一个授权发送触发 SMs 的可信 SME，则阻止该 SM。

- 如果过滤设施所接收的 SM 包含触发指示并且源于一个授权发送触发 SMs 的可信 SME，则将触发请求 SM 发送给 SME 所授权发送的特定 UEs。本标准不定义过滤设施如何决定可信 SME 是否允许将设备触发 SM 发送给特定的 UE。

- 如果 SMS-SC 所接收的 SM 来自于 T4 接口的 MTC-IWF，则 SMS-SC 认为 T4 接口是可信的并继续发送该 SM，因为 MTC-IWF 能认证 MTC 服务器并且能保证只有授权了的 MTC 服务器才可以触发特定的 MTC 设备。

- 如果 SMS-SC 所接收的 SM 来自于 SMS-IW MSC，则 SMS-SC 应该将 SM 发送给过滤设施。这样，SMS-SC 可以通过检查接收方的授权发送方列表，来决定 SM 是否来自于一个授权的 SME。如果不是，SMS-SC 阻止该伪造触发 SM 的发送。如果 MTC-IWF 接收的触发请求来自于 Tsp 接口，则 MTC-IWF 应该过滤并阻止来自非可信 SCS 的触发 SM，3GPP TS 23.682 的 5.2.1 节描述了具体流程。

根据 3GPP TS 23.040 的 9.2.3.9 节，普通 UE 不允许发送起呼触发短消息来触发 MTC 设备，因此 SMS-SC 应该根据普通 UE 的签约信息来区分并阻止伪造的 MO 设备触发 SMSs。

根据运营商策略，可信源可以被授权发送触发消息给任何 UE。为了防止源欺骗，需要保护用来传

输触发消息的接口，特别应该保护 Tsmc、Tsp、和 T4 接口。3GPP TS 23.682 的 4.3.3.1 节中定义了 Tsp 接口安全，Tsmc 接口的安全机制不在本标注研究范围内。可以根据 3GPP TS 23.142 定义的架构来过滤非法 SMS。当过滤实体接收到 SM 后，它能够基于包含在 SM 中的触发指示（即，3GPP TS 23.040 定义的 TP Protocol ID）来识别 SM 是否为触发 SM。

上述解决方案中的过滤功能分布于 SMS 路由器上的过滤设施、SMS-SC 上的过滤设施、以及 MTC-IWF 上的过滤设施。这说明过滤功能需要由能够在本地连接接口上验证 SM 源的实体所激活。同时 SMS 路由器只仅仅是 MT 场景下的一个可选实体，它没有能力验证 Tsp 和 Tsm 接口上的消息源，因此只在 SMS 路由器上实现过滤功能是不足的。实现过滤功能设施的最好位置是 SMS-SC，因为它可以过滤来自三条路径的 SMs。

解决方案旨在防止未授权实体发送大量的触发消息给大量的 MTC 设备而造成对核心网的分布式拒绝服务攻击。但是，本方案只是防止了 SMS 应用层威胁，而没有能够防止网络内部节点或网络信令链接遭受威胁或攻击者滥用所带来的攻击（例如，欺骗的 MAP_Forward_Short_Message 包含一个触发指示并通过 SS7 连接发送给目标 UEs）。如果需要消除这种攻击或者 HPLMN 不支持归属网络路由，那么本章的安全解决方案是不足的，因此需要在网络侧的 MTC 应用和 UE 的 MTC 应用之间，实现某种端到端的密码保护机制来保护触发消息。但这种解决方案可能由应用层来提供而不在本标准范围之内。将来的 3GPP 版本可能还会引入这种密码保护触发消息的解决方案。

存在不同网络的短信中心直接连接的场景，因此部署归属网络路由不是强制的。

7 安全连接技术要求

7.1 概述

MTC 安全连接特征就是运营商能够为保护 MTC 设备和 SCS 之间（非直接模式下）或者 MTC 设备和 MTC 应用之间（直接模式下）的应用协议安全提供密钥材料。

GBA，如 3GPP TS 33.220 所描述的，用于针对基于 3GPP AKA 机制的应用安全的自举认证和密钥协商。GBA 应被用于为一个 MTC 设备发起的安全连接建立密钥。

作为 GBA 的扩展，GBAPush 在 3GPP TS 33.223 中进行了定义。GBAPush 也用于为两个实体间的应用安全建立密钥。

其他机制（例如，在不能应用 GBA 的场景中使用 EAP-AKA）可以用于为 MTC 设备和 MTC 服务器之间或者 MTC 设备和 MTC 应用服务器之间提供安全连接特征。这些机制被认为不在本标准范围内。

在 ME 和网络之间的安全连接特征实现是可选的。

7.2 MTC 设备发起的安全连接

UE 发起的安全连接仅适用于支持 HTTP 协议的 MTC 设备。

一个 MTC 设备发起的安全连接应通过 3GPP TS 33.220 定义的 GBA 方式建立。

MTC 设备与 MTC 服务器或者 MTC 设备与 MTC 应用服务器之间的安全连接都应使用 GBA 方式。MTC 服务器和 MTC 应用服务器应作为 NAF 服务器使用。通过 GBA 方式建立安全连接密钥的过程具体如下：

MTC 设备与 BSF 通过 Ub 接口执行 GBA 自举过程。自举过程使得 MTC 设备和 BSF 获得一个共享密钥 Ks 和与该共享密钥 Ks 关联的一个标识 B-TID。MTC 设备接着基于 Ks 生成一个 Ks_(ext/int)_NAF 密钥，并通过 Ua 接口与目标 NAF 建立一个连接。在非直接模式下，NAF 功能由 MTC 服务器执行，在直接模式下，NAF

功能由MTC应用服务器执行。开始通信时，MTC设备向NAF提供B-TID。NAF向BSF请求B-TID关联的Ks_(ext/int)_NAF密钥。这样，MTC设备与MTC服务器/MTC应用服务器就可以使用Ks_(ext/int)_NAF密钥保护Ua应用协议（即安全连接）。

如何使用Ks_(ext/int)_NAF密钥保护MTC设备与MTC服务器之间或MTC设备与MTC应用服务器之间的通信依赖于使用的Ua应用协议。

7.3 网络发起的安全连接

一个网路发起的安全连接应通过3GPP TS 33.223定义的GBAPush方式建立。

MTC设备与MTC服务器或者MTC设备与MTC应用服务器之间的安全连接都应使用GBAPush方式。MTC服务器和MTC应用服务器应作为PushNAF服务器使用。通过GBAPush方式建立安全连接密钥的过程具体如下：

PushNAF服务器，即非直接模式下的MTC服务器和直接模式下的MTC应用服务器，决定使用GBAPush为其与MTC设备之间的应用安全（即一个安全连接）建立密钥。PushNAF然后从BSF请求一个GBA Push-Inf (GPI) 和一个Ks_(ext/int)_NAF密钥，并进一步将GPI发送到MTC设备。MTC设备处理GPI并生成一个Ks_(ext/int)_NAF密钥。这样MTC设备和PushNAF可以使用共享的Ks_(ext/int)_NAF密钥保护Ua应用协议（即安全连接）。

如果PushNAF（MTC服务器或MTC应用服务器）与MTC设备之间无IP连接，GPI可以在触发信息中发送到MTC设备。在MTC服务器作为PushNAF的情况下作为触发信息的GPI通过Tsp接口发送。在MTC应用服务器作为PushNAF的情况下作为触发信息的GPI通过Tsms接口发送。GPI可以有两个用途：GPI可以为应用协议（即安全连接）提供密钥；GPI可以用于以端到端的方式保护触发信息。

如果PushNAF（MTC服务器或MTC应用服务器）与MTC设备之间有IP连接，GPI可以在MTC应用使用的应用协议中发送，并为安全连接提供密钥。

如何使用Ks_(ext/int)_NAF密钥保护MTC设备与MTC服务器之间或MTC设备与MTC应用服务器之间的通信依赖于使用的Ua应用协议。

8 USIM 与 MTC 设备绑定安全技术要求

8.1 基于 UE 的 USAT 应用配对概述

本章针对如何绑定USIM与MTC设备进行了明确说明。该解决方案在UE和运营商网络中是可选的。为使UE有USAT应用配对能力，ME应支持USAT（USAT在3GPP TS 31.111中规定）。

8.2 安全技术要求

当从终端取回的IMEI或IMEISV与经USAT配置的UICC的值或值的范围匹配时，USAT应用配对成功。如果终端不支持USAT命令PROVIDE LOCAL INFORMATION,USAT应用配对失败。

UICC重置后，在选择USIM应用前，USIM将PIN置于死锁状态。USAT配对成功后，PIN可处于解锁状态或禁用状态。支持USAT应用配对的UE进行Profile下载，该过程具体如3GPP TS 31.111所规范。USIM随即发送一个主动命令PROVIDE LOCAL INFORMATION以请求UE的IMEI(SV)。然后，在开始USIM初始化过程前，UE发送携带IMEI(SV)的TERMINAL RESPONSE消息。

文件EF_{IMEISV}保存IMEI(SV)或者与USIM绑定的值的范围。

文件EF_{pairing}保存由UICC执行的最后配对检查的状态。UICC检查USIM和MTC设备之间的组合，并在配对检查成功的情况下将状态标记设置为‘OK’。UICC也在EF_{pairing}文件中存储MTC设备的IMEI(SV)值。在配对检查失败时，USIM将状态标记设置为‘OK’，并在EF_{pairing}文件中存储未授权MTC设备的IMEI(SV)值。

保存在EF_{pairing}文件中的配对检查的状态标记（其值为‘OK’或‘KO’）可以由任何安装该UICC的终端读取。但是，保存在EF_{pairing}文件中的IMEI(SV)值，通过ADM权利保护，只有运营商可以获取其信息。保存在EF_{pairing}文件中的信息提供了一种检测USIM与MTC设备之间组合改变的机制。存储在EF_{pairing}文件中的信息由维护人员在本地读取。

UICC OTA机制（在3GPP TS 31.115、3GPP TS 31.116和ETSI TS 102.225、ETSI TS 102.226中规范）用于更新保存在USIM中的EF_{pairing}文件。该机制通过增加或删除EF_{pairing}文件中的授权IMEI(SV)值或IMEI(SV)范围，对USIM与MTC设备(s)的组合变更提供动态管理。

附 录 A
(资料性附录)
M2M 应用场景

以下列出几种常见的M2M应用，对于本标准不限定以下应用。

A.1 智能抄表

用户家里安装了智能电力抄表系统，无需电力公司工作人员每个月上门抄电表和收电费，用户每个月的电能消费信息会根据一定的策略每隔一段时间或在固定的日子里上传到电力公司的网络系统中，电力公司直接根据用户的智能电表上传的消费数据从用户账户中扣除消费的款项，当账户余额不足时通过短消息或自动发送电子邮件的方式通知用户。电力公司还可以根据每个时间段内的电力消耗情况自动调节电力价格，用户可以实时获得电力价格变化信息，当电价较高时减少电器的使用，这样不仅可以为用户节约用电成本，还可以平滑用电高峰，避免出现电力供应不足的现象。

对于这种智能电表，用户和电力公司共同拥有，用户和电力公司都希望数据的准确性，都希望不被攻击者篡改。因此智能电表向电力公司发送数据需要受到安全保护，当数据被破坏时，需要同时通知用户和电力公司。

A.2 健康医疗

用户老张（被监测者）患有高血压，他可通过随身携带的便携式血压检测设备测出个人采样数据，然后，收集、整理测得的数据，将其通过无线近距离通信方式发送到网络终端，再由网络终端发送到医疗健康监测业务服务器。医院的相关工作人员通过网络可实时了解发送过来的数据，并根据患者基本情况及既往病史得出诊断结论，对患者进行健康指导。当监护数据超出由医生设定的某一阈值时，系统会实时地将当前的血压信息发送给预先设置的联系人，例如其主治医生张医生和女儿小张。而当血压超过一个由医生设定的更大的阈值时，除了及时发送当前的血压信息外，还会提供老张当前的位置信息，同时还会向最近的急救中心发送警报信息，并通知其主治医生，同时向其女儿小张发送信息通知其父亲处于危急状况。另外，被监测者以及授权的联系人可以查看病人的历史数据，对其进行分析，通过网络给病人发送健康指导信息。

患者在候诊大厅候诊时，可以将末梢终端（如心电监测仪、血压计、血糖仪等设备）接在身体上，测出当时的相关体征信息，将此数据传送到医疗健康监测业务系统中。就诊时，医生就可以直接了解患者的体征信息，再根据患者的电子健康档案信息（包括患者基本信息、既往病史、历史就诊记录等，患者之前已经在系统中建立个人电子健康档案），即可快速得出病情结论及诊断方式，对患者进行健康指导。当患者住院以后，医生查房时，可以利用PDA或者具有无线上网功能的电脑连接系统服务器，从中了解患者之前的体征信息、既往病史和实施监护记录，指导患者下一步治疗方案。对于重症监护患者，ICU设有中心监护站，医生在监护站远程实时直接观察所有监护的病床患者体征，使重危病人得到早期而又准确的诊断，紧急而又恰当的处理。

对于健康医疗，数据的安全性更加重要，涉及个人隐私，有些数据只能医生或者病人家属知道，有些数据需要病人同时知道，比如血压，如果病人知道血压高了，需要吃降压药，有利于帮助病人及时降压。

A.3 智能家居

当小张下班回家时，大门的门禁设备识别他的脸，并探测到他口袋里的电子钥匙将门自动打开。当小张进入或者离开一个房间时家庭控制中心（Home Central Control, HCC）就会相应地自动打开或者关闭这个房间的电灯。HCC结合室内外温度、网上的天气预报以及用户的偏好等信息触发并自动调节暖气系统。

当HCC检测到异常情况，比如煤气泄露就会向小张的移动终端同时向他发送警告消息，并将电源自动切断。小张在办公室收到这一警告消息，他连接上HCC并点击“Home repairs”按钮，煤气公司就会收到HCC提供的详细信息。煤气公司派来的修理工带有专业的无线ID卡，HCC检测到这一信息并识别出无线卡的合法性才让修理工进入小张的房子，修理工可以通过冰箱上的视频面板与小张进行交流。当修理工完成修理以后保险公司会自动接收到来自HCC的损坏报告。

针对于智能家居，安全性和隐私性都非常重要，一旦被攻击，用户的财产甚至人生安全都会受到威胁。

A.4 智能物流

在物流行业中，需要将M2M设备放置到货物或者车辆上，用户能根据M2M的信息跟踪货物或者装载货物的车辆。

针对于物流行业，安装在货物上M2M设备属于一个短期的，或者也可以重复利用的，因此其安全性策略需要根据其特性制定，而针对装载在车辆上的M2M设备针对于物流公司非常重要，需要防止相关的M2M设备被篡改和攻击。

中华人民共和国
通信行业标准
M2M 通信系统增强安全要求
YD/T 2913-2015

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本：880 × 1230 1/16 2015 年 12 月第 1 版
印张：1 2015 年 12 月北京第 1 次印刷
字数：25 千字

15115 · 832

定价：10 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492