33.050
M30

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T ××××—××××

M2M 应用通信协议技术要求

Technical requirements of M2M service communication protocol

××××-××-××发布　　××××-××-××实施

中华人民共和国工业和信息化部发布

目　录

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准是M2M业务系列标准之一，该系列标准的名称及结构预计如下：

— 《M2M业务总体技术要求》

— 《M2M应用通信协议技术要求》

— 《M2M业务平台设备技术要求》

— 《M2M业务终端设备技术要求》

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：中国移动通信集团公司、工业和信息化部电信研究院、中国电信集团公司、华为技术有限公司、中国联合网络通信集团有限公司、北京映翰通网络技术有限公司。

本标准主要起草人：刘玮、王红梅、刘越、肖青、牛亚文、王崇萍、魏晨光、赵立君、吴伟、王艺、诸瑾文、汪香君、张永靖、卞永刚、韩玲、孙利、韩传俊。

M2M 应用通信协议技术要求

1. 范围

本标准规定了M2M业务系统中的端到端通信协议。

本标准适用于M2M业务系统。

2. 术语、定义和缩略语

2.1. 术语、定义

下列术语、定义适用于本文件。

2.1.1

M2M

机器与机器或者人之间的通信。

2.1.2

M2M平台

M2M业务管理平台。

2.1.3

M2M应用

提供M2M业务的应用平台。

2.2. 缩略语

下列缩略语适用于本文件。

CDMA 2000	Code Division Multiple Access2000	码分多址2000技术
GPRS	General Packet Radio Service	通用无线分组业务
GSM	Global System for Mobile Communication	全球移动通信系统
M2M	Machine To Machine/Man	机器到机器/人
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access	时分同步的码分多址技术
USSD	Unstructured Supplementary Service Data	非结构化补充数据业务
WCDMA	Wideband Code Division Multiple Access	宽带码分多址技术

3. 协议概述

3.1. 总体概述

M2M 应用通信协议是为实现 M2M 业务中 M2M 终端设备与 M2M 平台之间、M2M 平台与 M2M 应用间的数据通信过程而设计的应用层协议。

M2M 应用通信协议分为两部分描述：M2M 终端设备与 M2M 平台之间的通信协议，以及 M2M 平台与 M2M 应用之间的通信协议，如图 1 所示。

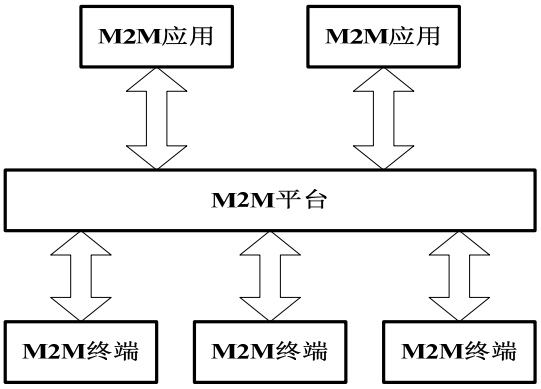


图 1　　M2M 终端接入 M2M 平台

3.2.　M2M 终端设备与 M2M 平台之间的通信协议

M2M 终端设备与 M2M 平台间的接口协议主要实现远程终端管理和应用数据转发功能。其中，远程终端管理包括 M2M 终端设备远程管理、远程维护、通讯接入等功能。应用数据转发主要包括 M2M 终端设备与 M2M 平台间的应用数据传输以及 M2M 终端设备之间借助 M2M 平台转发、路由所实现的端到端数据通信等功能。

M2M 终端可以通过多种通道类型接入 M2M 平台(如图 2)。典型的通道如下：

- 2.5G 通道（GPRS、CDMA 2000 1X）
- 3G 通道（WCDMA、CDMA200 EVDO、TD-SCDMA）
- WIFI 通道
- PSTN 通道
- 有线 IP 通道（ADSL 接入、光接入等）

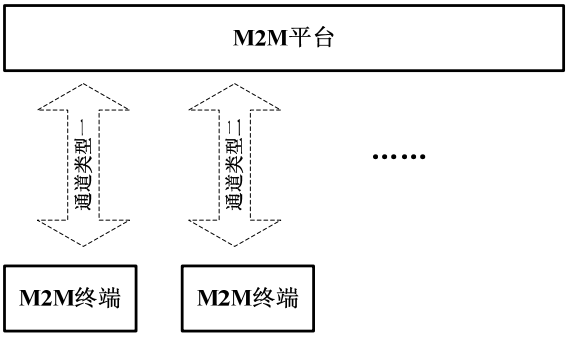


图 2　　M2M 终端接入 M2M 平台

上述不同类型的通道的差异性主要体现在 IP 承载能力和数据带宽两个方面。而这两点对接口协议的选择影响很大。首先，本标准主要针对能够承载 IP 协议的通道（PSTN 通道不在本要求考虑范围内）。其次，对于 2.5G 通道，由于带宽较小，接口协议必须考虑报文编码的效率。而对于带宽较高的有线通道，报文语法的灵活性和扩展性是关注重点，编码效率不是接口协议关注的重点。

本标准主要对上述协议进行相应描述，主要包括协议实现功能、交互机制、报文格式和安全考虑。

3.3. M2M 平台与 M2M 应用之间的通信协议

M2M 平台与 M2M 应用间的接口协议主要实现 M2M 平台与 M2M 应用之间的通信，以及 M2M 终端与 M2M 应用之间借助 M2M 平台转发、路由所实现的端到端数据通信。M2M 平台对应用系统提供了对 M2M 终端设备进行监控管理的能力；同时，通过实现本协议，M2M 终端设备与 M2M 应用之间可以通过 M2M 平台传递业务数据。

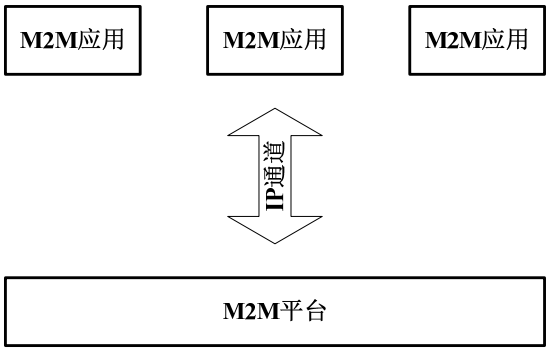


图 3 M2M应用接入M2M平台

M2M 平台和 M2M 应用之间的接口采用 IP 通道(如图 3)，带宽可以根据需要进行设置。因此，报文语法的灵活性和扩展性是关注重点，编码效率不是接口协议关注的重点。

本标准主要对上述协议进行相应描述，主要包括协议实现功能、交互机制、报文格式和安全考虑。

3.4. M2M 应用通信协议栈

M2M 应用通信协议栈结构如图 4 所示。

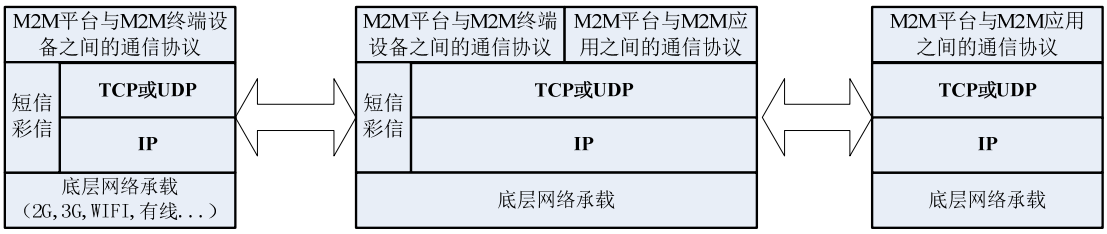


图 4 M2M应用通信协议栈结构

4. M2M 终端设备与 M2M 平台间协议

4.1. 协议报文描述

4.1.1. 协议报文结构

针对不同的 M2M 业务，例如视频类大数据量业务，考虑其他协议：如 http、Ftp 等，针对处理能力比较高的终端设备，不同带宽、不同业务类型可能采用的协议也不同。

本标准主要针对 M2M 终端设备与 M2M 平台之间的一个面向终端管理数据和小数据量业务数据的轻量级协议。

如无特殊声明，协议采用同步方式进行报文交互，每一个请求报文须有一个应答报文作为应答。报文由报文头和报文体构成。报文结构如图5所示。

图 5 报文结构图

在通用M2M终端设备与M2M平台间协议基础上，可以通过扩展TLV（TLV是带格式的的数字或不定长字符串或字节数组，它被用来动态扩展消息交互中的数据及参数）的方式来定义某一类或某一行业机器之间的通信语义，实现M2M终端设备与M2M平台间协议在该类M2M应用上的能力扩展。

TLV的结构如图6所示。其中T为TAG，表示该字符串的定义标签；L为LENGTH，表示该TLV扩展的有效数据或参数V的长度；V为VALUE，表示该数字或字符串或字节数组中有效数据的数值。

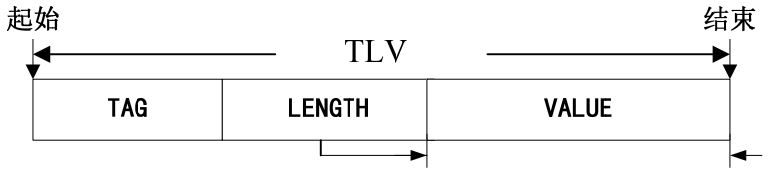


图 6 TLV的结构示意图

TLV与TLV组的区别如下：

项目	说明
TLV	带格式的的数字或不定长字符串或字节数组
TLV组	若干个首尾相连的TLV

4.1.1.1. 报文头

报文头是每个报文必要的公共部分，它描述了每个报文的最基本信息，其长度固定，包括报文总长度、终端设备序列号、版本号、命令代码、流水号、保留字6个字段。

4.1.1.2. 报文体

报文体是协议报文中承载交互数据的部分，其长度可变，格式不固定，甚至可以缺省，一般由内容体和摘要体构成。内容体一般由固定参数部分和可变TLV/TLV组部分构成。固定

参数部分的格式是各类报文所独有的，不同类型的报文其固定参数部分也不完全相同，某些类型的报文甚至缺省固定参数部分。摘要体是一个可选的TLV，用于报文完整性和来源身份合法性的验证。

4.1.2. 报文分类

根据报文是否采用安全机制，可将报文为四类：普通报文、接入安全验证报文、部分加密报文、完全加密报文。

- 普通报文，以明文方式传送的、未采用任何安全机制的、仅有报文头和报文体中的内容体报文。
- 接入安全验证报文，以明文方式传送的，除报文头和内容体之外，在报文体的最后携带了用于接入验证的摘要体的报文。
- 部分加密报文，对内容体中的某个或某几个TLV进行单独加密的，除报文头和内容体之外，在报文体的最后携带了用于接入安全验证的摘要体的报文。
- 完全加密报文，对整个内容体进行加密的，除报文头和内容体之外，在报文体的最后携带了用于接入安全验证的摘要体的报文。

4.1.3. 报文 TLV 的封装与超长报文的分割

由于受M2M终端设备处理能力以及承载方式所限，不可能在一个报文中封装无穷多的TLV，因此协议报文TLV的封装必须遵从以下规定：

1. 报文的总长度不能超过该通信方式下承载极限以及M2M终端设备和M2M平台的处理能力，如SMS为140字节，超长报文必须进行分包传输。
2. 报文中的TLV或TLV组必须是表示一个或几个完整的逻辑，不能把表示一个完整逻辑几个TLV拆分在几个非分包机制报文中传输。

4.1.4. 报文的字节顺序

报文采用网络字节序，即对于每个数据域先发送其高字节位。如0x12345678，在传输中依次送顺序为0x12，0x34，0x56，0x78。

4.2. 协议交互基本原则

M2M终端设备与M2M平台间的通信协议中采用了逻辑连接（以下简称连接）的概念。所谓连接是指M2M终端设备与M2M平台一次完整的报文交互过程，M2M终端设备以登录请求报文向M2M平台登录，其后M2M平台鉴权成功并发送登录应答报文为开始，以通信双方一端发起退出请求，另一端发出退出应答为结束，在逻辑连接中通信超时也视为连接结束。在此交互过程中，通信形式可以是SMS、基于数据通信的TCP或UDP方式，也可以是混合模式，即通信方式可在逻辑连接中切换。但需要注意的是，对于一对请求、应答，必须在同一通信方式下完成。

4.2.1. 长连接和短连接

采用基于IP的通信方式做承载时，根据M2M终端设备与M2M平台之间的IP链路连接是否一直存在，可分两种连接方式：长连接和短连接。

所谓长连接，指在一个连接过程中可以连续发送多个数据报文，如果没有数据报文发送，需要M2M终端设备发送心跳报文以维持此连接。短连接是指通信双方有数据交互时，就建立一个连接过程，数据发送完成后，则断开此连接过程。

所谓短连接，M2M终端设备平时处于下线，当本地有数据需要传输或达到定时上线时间等类似策略时，M2M终端设备作为客户端以“客户－服务器”方式建立连接，传送数据完成后，结束该连接。尽管是短连接，但是其操作流程与长连接基本一致，唯一的区别在于M2M终端设备不需要通过心跳报文来维持与M2M平台通信的链路一直存在，而是结束与M2M平台的数据传输之后，立即向M2M平台请求退出登录状态。短连接适用于数据量少，不需要一直在线的M2M应用或服务。

无论长连接，还是短连接，在采用 IP 方式时，都可以根据实际网络通信质量采用 TCP 或 UDP 方式。若网络通信质量较好时，可以优先选择 TCP 协议作为传输方式。

4.2.2. 同步交互和异步交互

在协议中，应答报文往往是表示应答方对请求方所发报文的正确接收或理解，而无法确认应答方对请求方命令的执行结果。因此，往往需要再发起一次数据交互以确认请求方的请求是否被应答方正确执行。

根据一次报文交互能否完成一个完整的逻辑事件，可以将报文分为同步交互报文和异步交互报文。若一次报文交互即可完成某个完整的逻辑事件，则该次报文交互的请求和应答报文即为同步交互报文；若一次报文交互只完成某个完整的逻辑事件的某一部分，还需要其它报文交互的配合才能完成该逻辑事件，则用于完成该逻辑事件的报文交互的请求和应答报文即为异步交互报文。与之对应，只需要一次报文交互即可完成的逻辑事件，称为同步交互事件；反之，则称为异步交互事件。

在 M2M 终端设备和 M2M 平台的数据交互中，异步交互事件多为涉及 M2M 终端设备参数设置的操作。

4.3. 协议功能及其交互

M2M 终端设备与 M2M 网络设备间可包含如下交互报文：终端设备注册、终端设备登录、终端设备登出、连接检测、终端信息上报、终端信息查询、远程控制、远程升级、终端参数配置、应用数据转发等。

4.3.1. 终端设备注册

终端设备必须配置终端设备编号，一个物理终端对应一个终端设备编号。终端编号的获取可以有多种方式：

- 终端在出厂时预置终端编号；
- 终端在安装时配置终端编号；

■ 终端在注册时平台对其分配编号；

终端设备必须在终端设备注册成功后方能投入正常使用。即 M2M 终端设备在未注册状态下，需要向 M2M 平台注册，才能使用 M2M 业务。因此 M2M 终端设备必须首先 M2M 平台注册。

M2M 终端设备注册主要分为两类：M2M 终端设备首次注册和 M2M 终端设备变更映射关系注册。

4.3.1.1. M2M 终端设备首次注册

M2M终端设备首次注册根据平台的安全机制配置可分为两类：配置安全机制的终端设备注册和没有配置安全机制的终端设备注册。

4.3.1.1.1. 配置安全机制的终端设备注册

配置安全机制的终端设备的注册又分为未预置密码和基础密钥的设备注册和已预置了接入密码和基础密钥的终端设备的注册。

4.3.1.1.1.1. 未预置接入密码和基础密钥

对于配置安全机制而未预置接入密码和基础密钥的M2M终端设备而言，其注册过程是一个异步交互事件，它包括三次报文交互：M2M终端设备提交注册信息、M2M平台下发接入密码和基础密钥、M2M终端设备首次登录。

第一次为M2M终端设备向M2M平台提交注册信息，M2M平台接收到后给予应答。

第二次为M2M终端设备通过M2M平台注册之后，M2M平台通过短信方式下发该M2M终端设备的接入密码，若M2M终端设备支持加密，同时一并下发基础密钥。

第三次为M2M终端设备首次登录M2M平台报文交互。若M2M终端设备在规定的时间内成功登录则完成注册过程。

配置安全机制而未预置接入密码和基础密钥的M2M终端设备注册过程如图7所示。

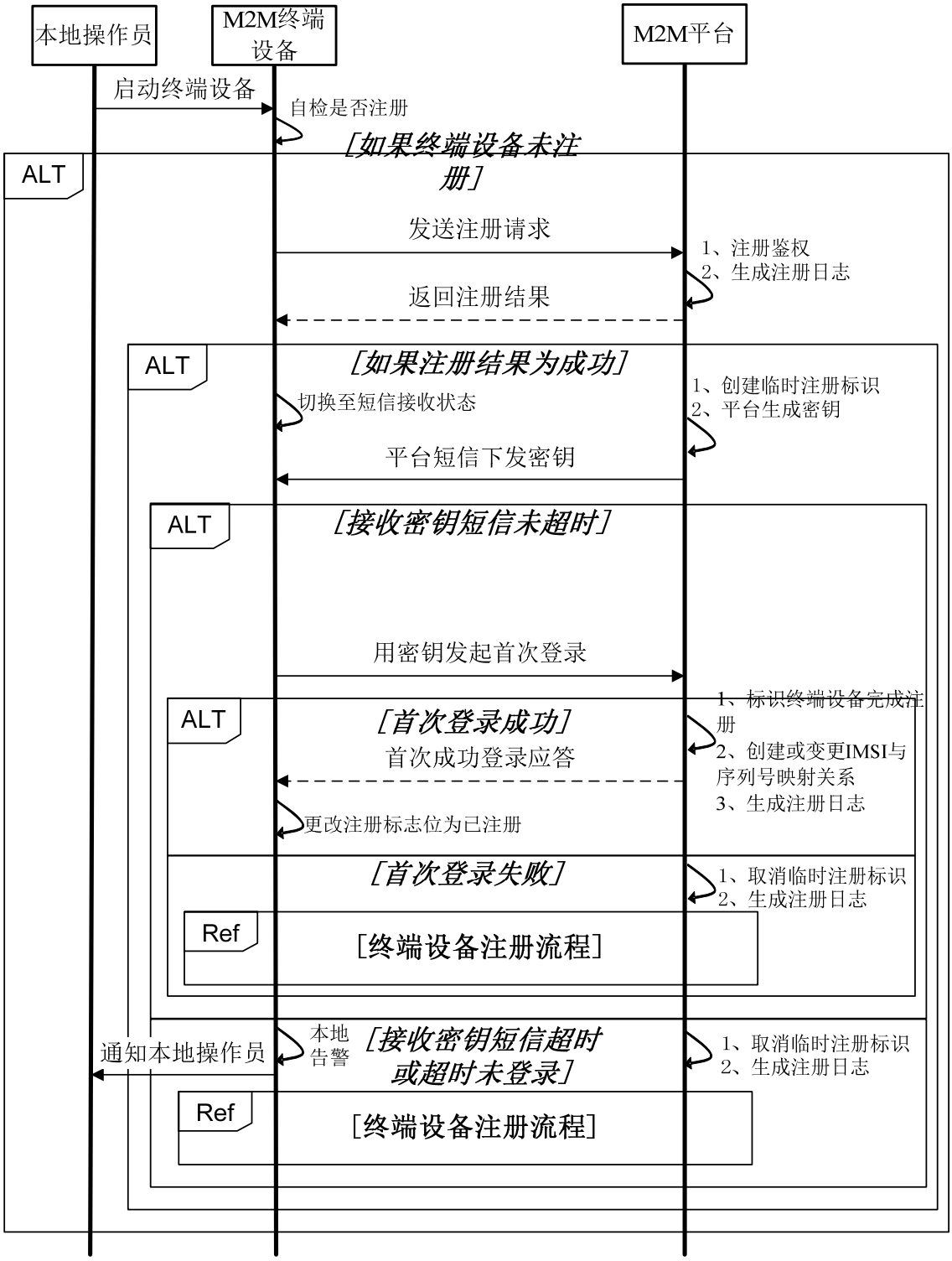


图 7 配置安全机制未预置接入密码和基础密钥的M2M终端设备注册流程图

a). 用户启动M2M终端设备。

b). M2M终端设备自检是否为非注册状态，如果为注册状态，结束该流程。

c). 如果为非注册状态，M2M终端设备发送注册请求到M2M平台，上报参数包括IMEI/MEID/ESN（可选项，如果此处上报，则M2M终端设备登录的时候无需上报）、IMSI、终端设备序列号等。

d). 注册鉴权，即M2M平台检测M2M终端设备上报的信息是否合法。

e). M2M平台根据鉴权结果向M2M终端设备返回注册结果，并生成注册日志。如果注册结果为成功，则在返回结果中包含分配给终端设备的序列号，并在平台创建或变更该序列号与IMSI、MSISDN或MDN的映射关系，同时生成临时注册标识。

f). 若M2M终端设备注册成功，M2M平台通过短信下发该M2M终端设备的接入密码和基础密钥。需要指出的是，由于是注册后首次下发接入密码，在此之前终端设备内没有存储任何安全密码或密钥，因此下发安全设置报文中可不携带接入安全验证的摘要体。

g). M2M终端设备在规定的时间内，利用接入密码发起首次登录，成功登录则完成注册。

4.3.1.1.1.2. 预置接入密码和基础密钥的 M2M 终端设备注册

对于配置安全机制且已预置接入密码和基础密钥的M2M终端设备而言，其注册过程也是一个异步交互事件。但是，相对于未预置接入密码和基础密钥的M2M终端设备，不需要M2M平台下发接入密码和基础密钥，它的注册过程仅包括两次报文交互：M2M终端设备提交注册信息、M2M终端设备首次登录。

与非预置接入密码和基础密钥的M2M终端设备注册流程不同的是，预置了终端设备序列号和接入密码(支持加密的终端设备同时还可预置基础密钥)M2M终端设备，除上报IMEI/MEID/ESN（可选，如果此处上报，则M2M终端设备登录的时候无需上报）、IMSI、终端设备序列号之外，还须上报相应的安全参数信息。

预置接入密码和基础密钥的M2M终端设备注册过程如图8所示。

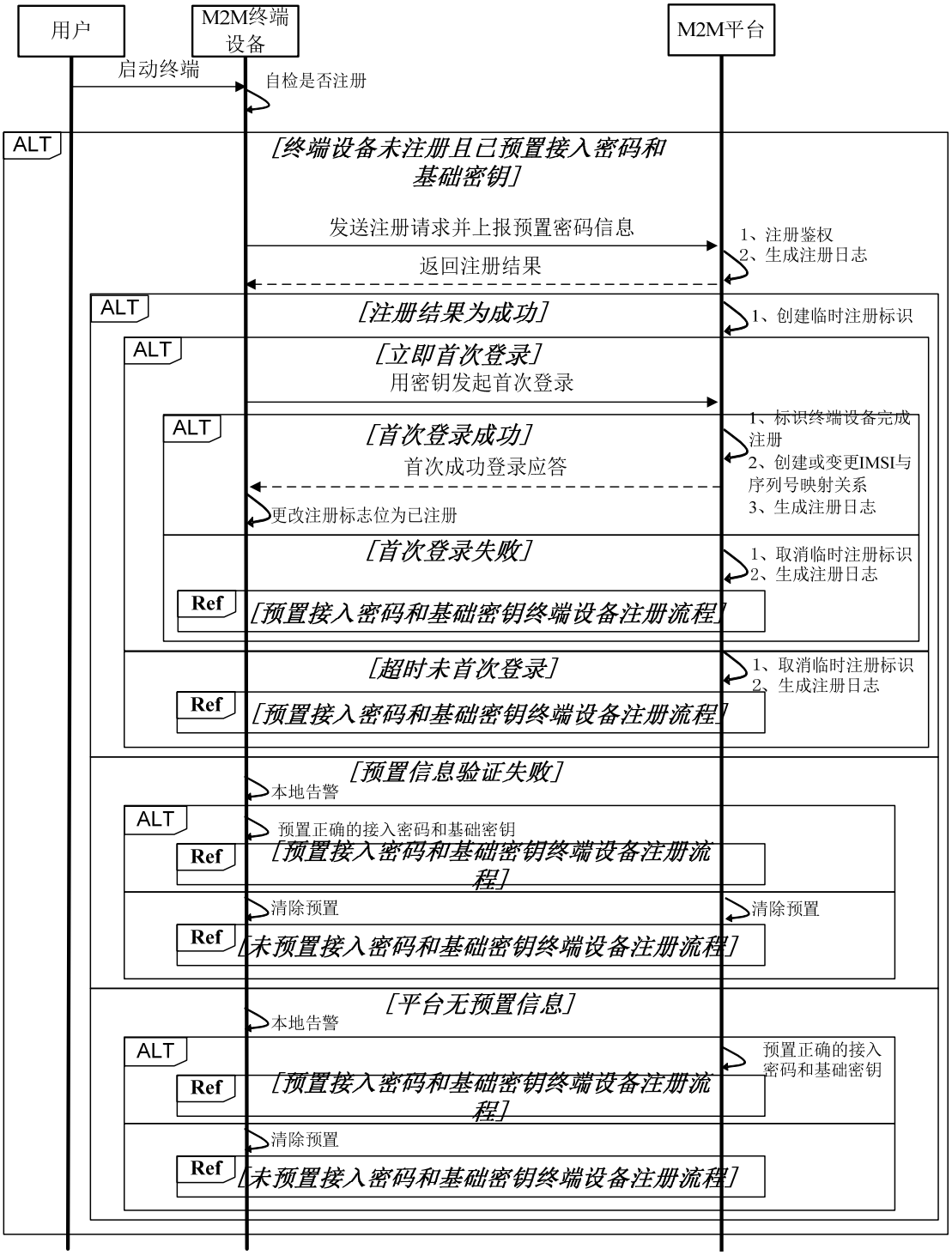


图 8 配置安全机制且预置接入密码和基础密钥的M2M终端设备注册流程图

对于因预置接入密码和基础密钥信息而注册失败可分为三种类型：

（1） 预置接入密码和基础密钥信息验证失败

对于该类型，可以本地人工重新预置正确的接入密码和基础密钥后，再由M2M终端设备发起新的“预置接入密码和基础密钥终端设备的注册流程”；也可以同时人工在M2M终端设备

和M2M平台都取消相关预置信息，再由M2M终端设备发起新“未预置接入密码和基础密钥终端设备的注册流程”。

（2） M2M平台无该终端设备的预置接入密码和基础密钥信息

对于该类型，可以在M2M平台输入该终端设备正确的接入密码和基础密钥后，再由M2M终端设备发起新的“预置接入密码和基础密钥终端设备的注册流程”；也可以同时人工在M2M终端设备取消相关预置信息，再由M2M终端设备发起新“未预置接入密码和基础密钥终端设备的注册流程”。

（3） M2M终端设备未上报预置接入密码和基础密钥信息

对于该类型，首先要人工本地确认 M2M 终端设备是否属于预置接入密码和基础密钥的终端设备。若是，则可以本地人工重新预置正确的接入密码和基础密钥后，再由 M2M 终端设备发起新的“预置接入密码和基础密钥终端设备的注册流程”；若不是，则在 M2M 平台都取消相关预置信息，再由 M2M 终端设备发起新“未预置接入密码和基础密钥终端设备的注册流程”。

4.3.1.1.2. 无配置安全机制的终端设备注册

对于无配置安全机制的终端设备的注册，平台则直接返回注册结果完成注册过程。无配置安全机制的终端设备注册如图 9 所示。

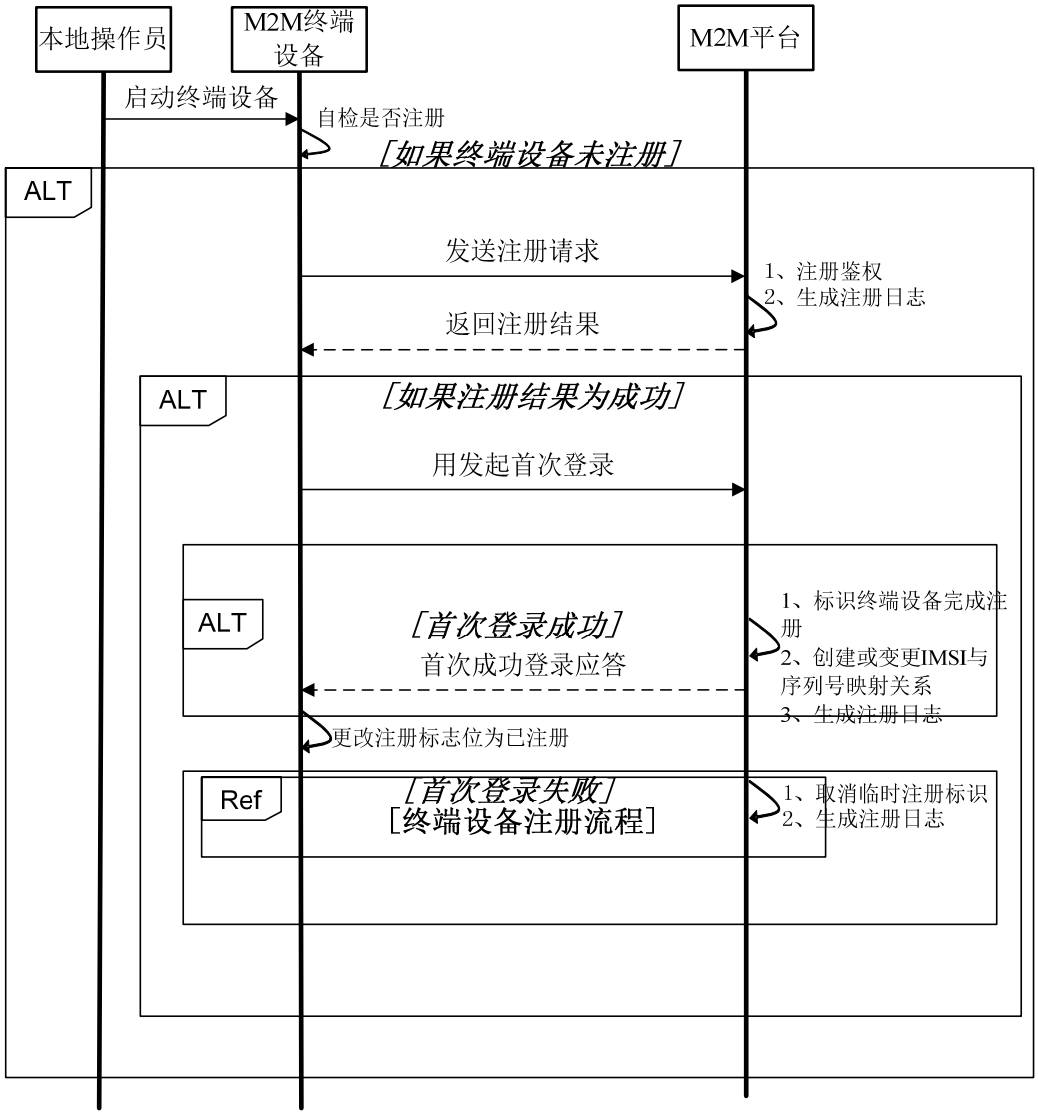


图 9 无配置安全机制的M2M终端设备注册流程图

4.3.1.2. M2M 终端设备变更映射关系注册

当M2M终端设备换卡时，需要向M2M平台提交映射关系变更请求，否则M2M终端设备将无法通过M2M平台的映射关系鉴权。

M2M终端设备变更映射关系属于同步交互事件。M2M终端设备变更映射关系如图10所示。

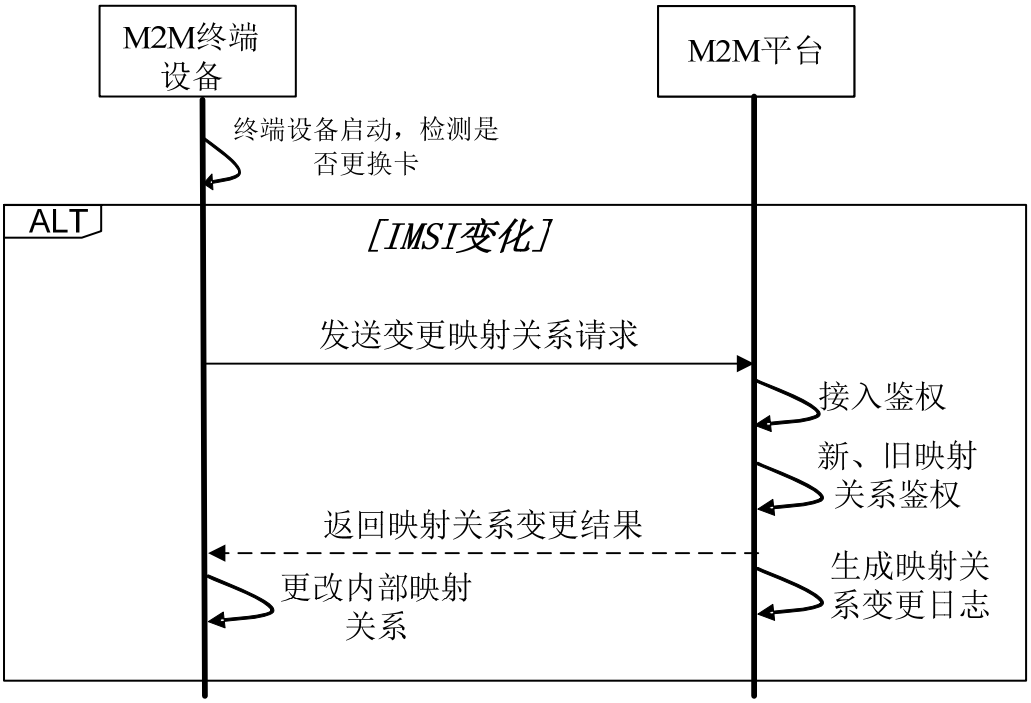


图 10 M2M终端设备变更映射关系

a). M2M终端设备启动，M2M终端设备自检是否被换卡，若IMSI无变化，则结束该流程。

b). 若IMSI变化，M2M终端设备发送变更映射关系请求到M2M平台。上报参数至少包括新IMSI、终端设备序列号，也可接入验证密码的摘要体(其中的IMEI、IMSI为变更前)。

c). M2M平台鉴权，即M2M平台检测M2M终端设备上报的信息是否合法。

d). M2M平台根据鉴权结果向M2M终端设备返回映射关系变更结果，如果映射关系变更成功，并变更该序列号与IMSI/MSISDN的映射关系。

此外，需要指出的是，对于没有通过摘要体的接入安全验证的映射关系变更请求报文，M2M平台直接丢弃，不做任何应答。

4.3.2. 终端设备登录

只有已注册的终端才能执行登录操作。终端与M2M平台通信之前，如果状态为未登录，则需要先登录M2M平台。终端登录平台后，才能执行各种通信交互操作。M2M平台不接受没有登录的终端发出的报文。因此，M2M终端在与M2M平台在进行数据交互之前，必须首先发送登录请求报文。

M2M终端设备登录M2M平台属于异步交互事件。M2M终端设备登录流程如图11所示。

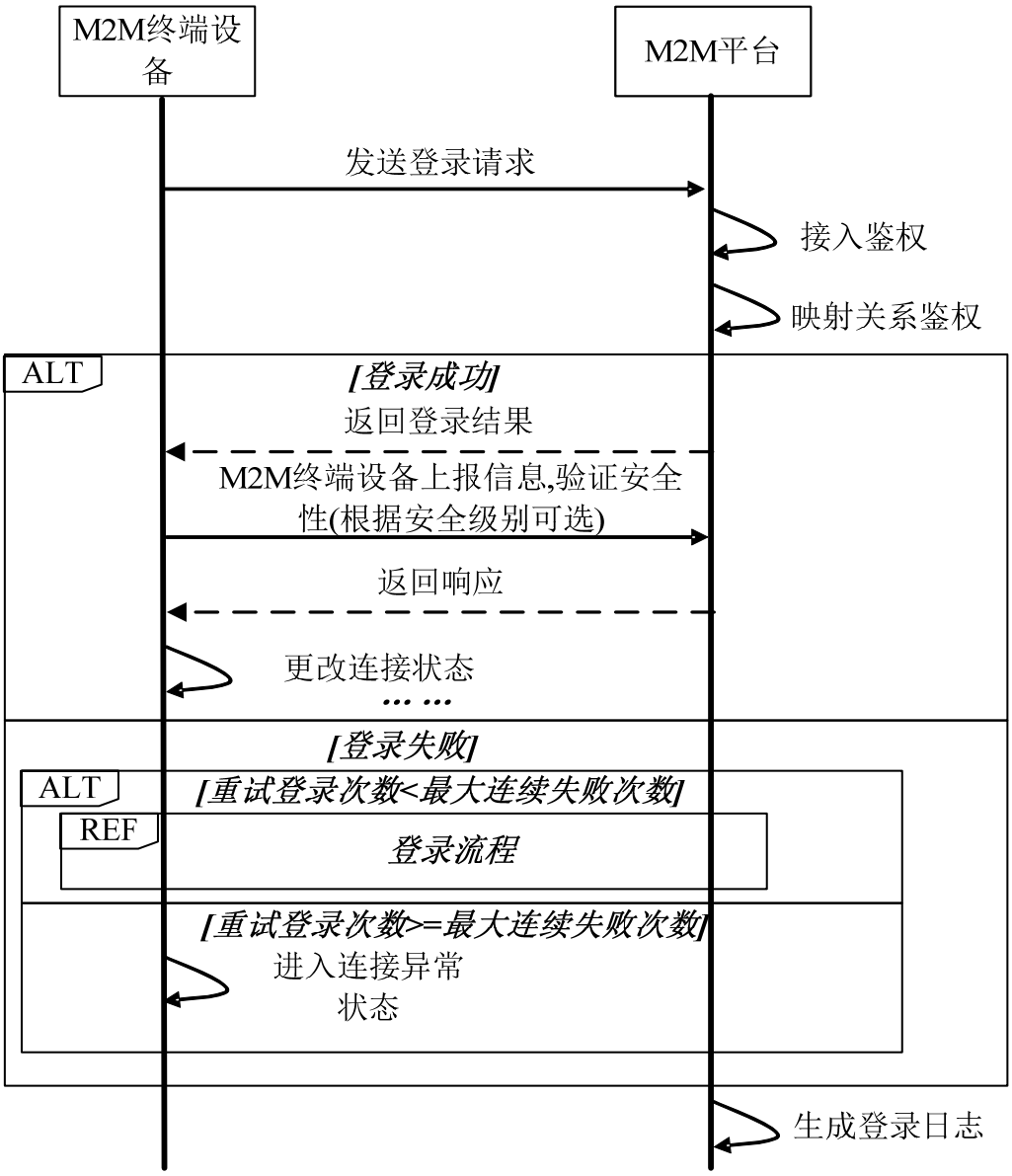


图 11 M2M终端设备登录流程图

a). M2M终端设备向M2M平台发送登录请求。登录上报参数包括：IMEI/MEID/ESN（可选）、终端设备软件版本号、M2M终端设备需与M2M平台同步的配置参数的校验以及其它可选参数。

b). M2M平台对M2M终端设备进行审核鉴权后，向M2M终端设备回送登录结果应答，并生成登录日志。M2M平台在拒绝了某个M2M终端设备的接入请求后，则会产生告警信息。

c). M2M终端设备登录成功后，根据安全级别的设定，对需要安全性验证的报文需要发送一个安全性验证报文，通过该报文中的特定的参数验证该连接的安全性。验证该次登录是否为非法的重放攻击。

d). M2M终端设备根据登录结果信息设置其状态。

1) 如果允许接入到 M2M 平台，M2M 终端设备处于工作激活状态，根据设定的工作方式工作；

2) 如果禁止接入到 M2M 平台，M2M 终端设备处于去活状态，通过指示灯告警。

其中，如果发送安全性验证报文，该报文中可以包含M2M终端设备认为需要上报的信息。终端也可以使用终端信息上报报文上报信息。如果发生配置参数校验失败的情形，终端需要

使用终端信息上报报文向M2M平台上报相应的配置参数的参数序列（含参数类型信息和当前值），也可以在安全性验证报文中进行发送。

对于M2M终端设备登录流程中的登录失败，不同于登录请求应答中定义的登录失败。在此登录失败的定义为：M2M平台返回的M2M终端设备的登录请求的应答报文超时，或M2M平台返回的M2M终端设备上报信息请求的应答报文超时。若M2M终端设备登录失败，M2M终端设备须再次尝试重新登录，直至达到最大连续失败上限。M2M终端设备登录最大连续失败次数设置为一个可配置参数。

4.3.3. 终端设备登出

当 M2M 终端不再需要现有连接传输数据时，主动通知 M2M 平台关闭连接。平台收到登出请求后，返回应答，并清除终端连接信息，记录日志。

M2M 平台也可强行要求 M2M 终端登出。终端收到控制请求后，也向平台发出登出报文。

当M2M终端设备与M2M平台之间处于通信故障状态时，终端和平台可以直接判定终端进入登出状态，也可以采用以下策略：先检测出通信故障的一方(即可能是M2M终端设备，也可能是M2M平台)向对方发送登出报文，并通过登出报文的状态字报告通信故障。登出由请求方发送后，请求方收到登出应答或接收超时后，释放该连接。

M2M终端设备中止连接/退出系统属于同步交互事件。。

4.3.4. 连接检测

处于长连接模式时，如果终端长时间不发送数据到一定周期，M2M终端向M2M平台发送连接检测消息，表示M2M终端设备处于工作状态，M2M平台收到后给予应答。

M2M终端设备如果连续接收不到M2M平台的心跳应答信息的次数达到阈值，则M2M终端设备与M2M平台之间可能处于通信故障状态，M2M终端设备通过指示灯告警。M2M平台在规定时间内未接收到M2M终端设备的连接检测消息，表示M2M终端设备故障。

M2M平台如果连续接收不到平台的心跳报文，则M2M平台认为M2M终端设备与M2M平台之间可能处于通信故障状态。

M2M终端设备连接检测消息属于同步交互事件。

4.3.5. 终端信息上报

M2M终端设备可根据需要向M2M平台上报信息，M2M平台收到后给予应答。

M2M终端设备的上报信息是指由M2M平台管理的信息，例如配置信息、告警信息、统计信息等。M2M终端设备在检测到自身参数变化或根据M2M平台要求，可向M2M平台发送其配置参数；M2M终端设备在检测到外部状态变化、告警状态或采集信息超过设置的阀值后，向M2M平台发送告警信息；M2M终端设备按照平台的要求上报统计数据，终端设备要求能记录自身每月业务使用标志，并能向平台上报是否使用业务。此外，需要指出的是，对于由于某些因通信故障引用的告警信息，M2M终端设备可以在未登录的状态下直接采用短信方式向M2M平台上报告警。

M2M平台通过设置M2M终端设备的业务统计策略，M2M终端设备根据策略存储统计信息，并按照策略进行定时、周期上报统计信息等，上报成功后可按照策略在M2M终端设备将统计数据清零。此项功能可选。

M2M终端设备向M2M平台上报信息属于同步交互事件。

4.3.6. 终端信息查询

M2M平台在需要的时候可向M2M终端设备发送命令，要求其立即上报其工作状态或者配置参数，如位置、信号强度、通信方式等；M2M终端设备收到后给予应答。

M2M平台向M2M终端设备实时提取信息属于同步交互事件。M2M平台向M2M终端设备实时提取信息的流程如图12所示。

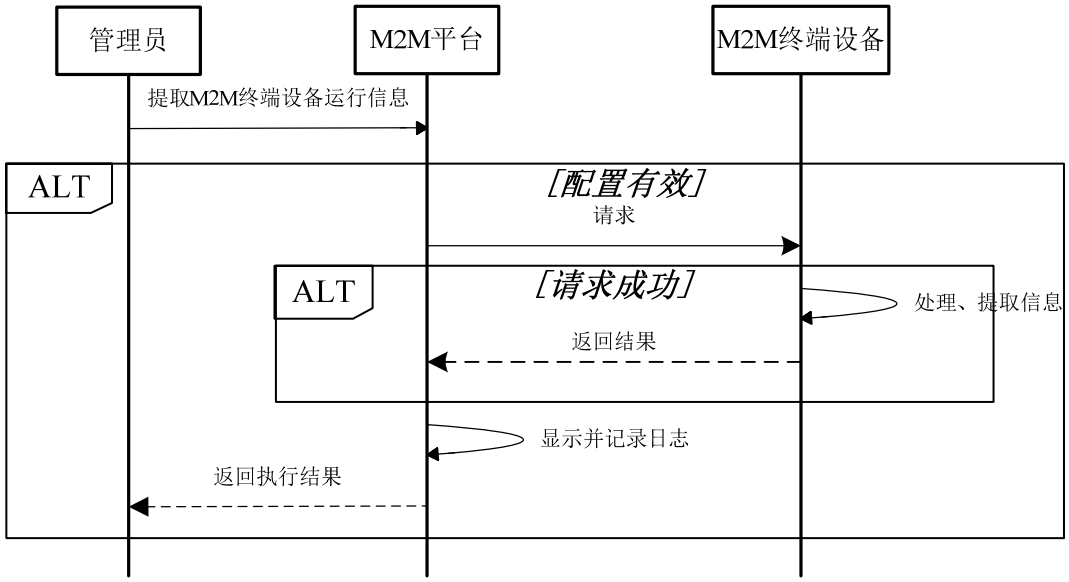


图 12 M2M平台向终端设备实时提取信息流程

当 M2M 平台请求提取参数中，有 M2M 终端设备不支持的参数时，直接报错，M2M 终端设备不处理，M2M 平台根据策略选择下一步操作。

4.3.7. 远程控制

M2M平台可以通过远程控制操作对M2M终端设备发送控制指令，控制终端设备重启、复位等操作。M2M终端设备收到后给予应答，并根据平台的要求触发相应的操作。

M2M平台对M2M终端设备的远程控制属于既有同步交互事件，也有异步交互事件。如果是异步交互事件，M2M终端设备需要向M2M平台上报远程控制的结果。

4.3.8. 远程升级

M2M终端设备可以通过M2M平台或第三方的升级服务器对其软件进行升级。下图给出了M2M终端设备软件远程下载升级的流程。M2M终端设备的软件下载升级可分为两个流程：升级通知和文件下载。

终端设备厂商将升级软件包发布到M2M平台上，或由第三方的升级服务器通知M2M平台有新的升级软件，由M2M平台接收到升级文件或通知后在平台上创建升级事务，并向M2M终端设备下发升级通知，通知终端设备下发升级服务器的地址和端口，以及升级相关的版本信息。M2M终端设备接收到升级通知后，根据其自身情况判断是否需要升级，并向M2M平台应答。

M2M终端设备软件下载通知流程如图13所示。

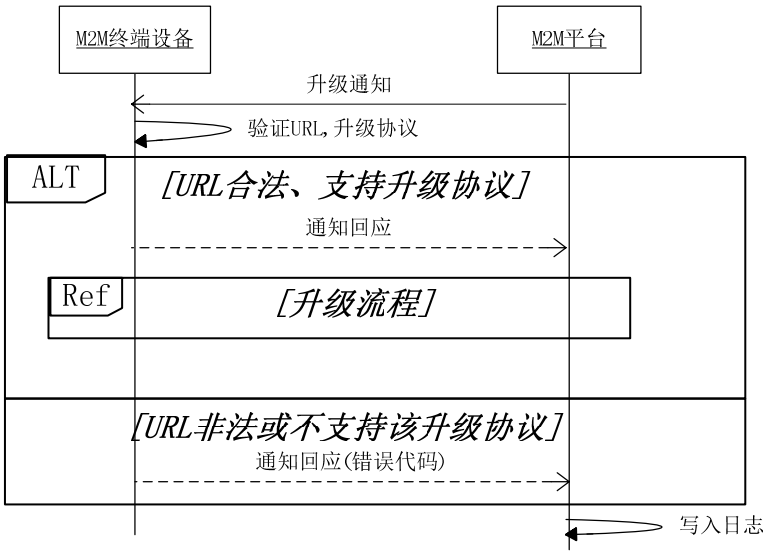


图 13 M2M终端设备软件下载通知流程

M2M终端设备如果需要升级其软件，则在其空闲时向M2M平台或第三方的升级服务器请求下载升级文件。下载协议可以采用ftp,http等标准协议，也可以采用如下描述的下载协议：

M2M平台或第三方的升级服务器在接收到下载请求后，给予应答并将升级文件分成多个数据块陆续装在应答数据报文中分批发送给M2M终端设备，直至全部升级文件接收完成。升级文件下载过程必须支持断点续传，即M2M终端设备可以暂时停止下载，先处理其它优先级较高的任务，待空闲时从上次下载的断点继续下载文件。M2M终端设备软件远程下载升级流程如图14所示。

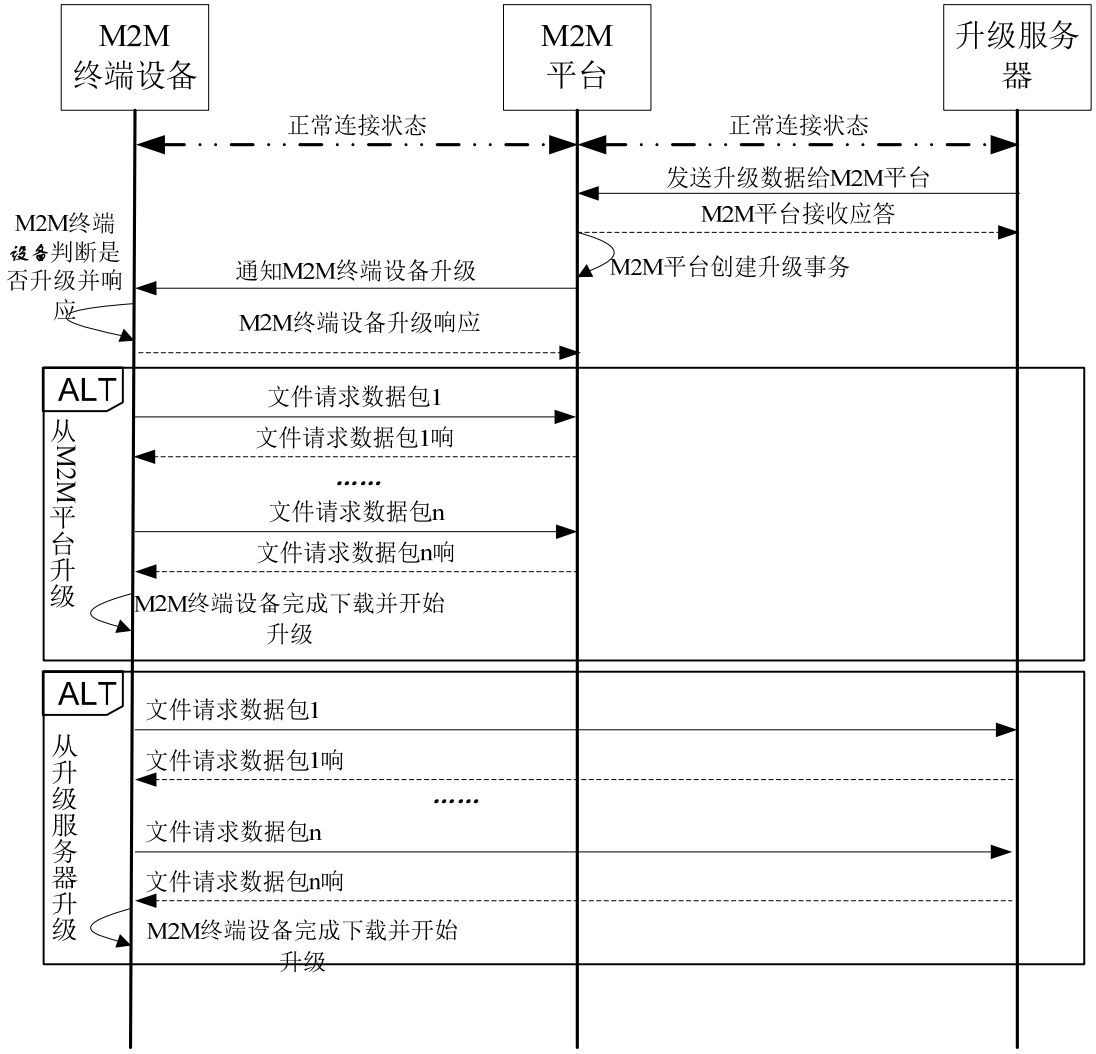


图 14 M2M终端设备软件远程下载升级

M2M终端设备从M2M平台或第三方下载服务器下载文件的具体流程如下：

a). M2M终端设备发送开始下载的请求报文。

b). M2M平台或第三方的升级下载服务器对M2M终端设备开始下载请求给予文件下载请求应答的报文，并根据下载请求返回下载文件的相应的数据块。

c). M2M终端设备对接收的数据块进行校验，并根据校验结果向M2M平台或第三方的升级下载服务器继续请求数据下载。

d). 当整个下载过程完成且整个文件的校验正确之后，M2M终端设备需要向M2M平台或第三方的升级下载服务器发送下载完成的通知。通知报文依然采用文件下载请求报文，下载状态设定为下载完成。

对于文件下载的异常处理：

- 文件下载过程中某个数据块下载失败

在文件下载过程中，若M2M终端设备对某个文件下载请求应答报文返回的文件数据块中内容的校验失败，则认为该数据块下载失败。M2M终端设备可以重新请求该部分的数据区；也可以仅请求该部分数据区中一部分连续的数据；甚至可以跳过该部分，而请求后续部分的数据。

- 文件下载失败

在文件下载过程中，若发生可导致整个下载过程失败的情况，如某部分数据区下次失败次数过多、整个下载文件校验失败、下载存储空间不足或溢出等，M2M终端设备则认为本次文件下载失败。M2M终端设备需要向M2M平台或第三方的升级下载服务器发送下载失败的通知。通知报文仍然采用文件下载请求报文，但报文状态设定为文件下载失败。具体的失败原因可向M2M平台告警。

4.3.9. 普通参数配置

普通参数配置可分为三种类型：终端请求参数配置，终端本地人工配制和平台设置终端参数。

4.3.9.1. 终端设备请求参数配置

M2M终端设备在某些情况下(比如终端设备的配置信息丢失或破坏)需要主动向平台请求配置信息。M2M平台收到请求后将配置数据下发给M2M终端设备。与M2M平台向M2M终端设备设置终端设备参数所不同的是,M2M终端设备在向M2M平台请求配置时,必须是在其空闲状态下,即M2M终端设备接收到M2M平台返回的参数立即可以应用参数配置。

终端设备向平台请求配置数据属于异步交互事件。M2M终端设备在获取参数配置生效后，需要向M2M平台上报参数，其流程如图15所示。

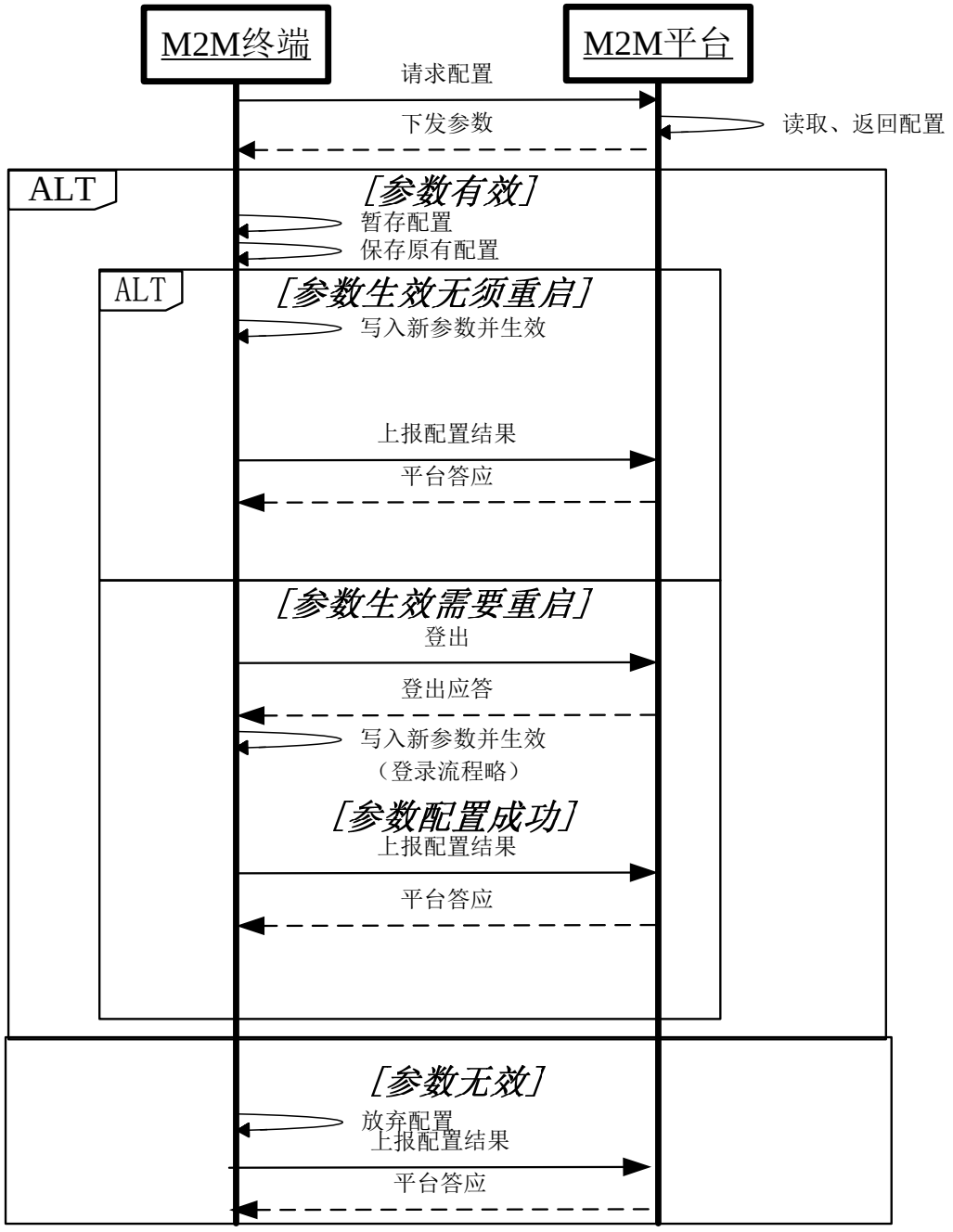


图 15 M2M终端设备向M2M平台请求配置数据流程

终端设备向平台请求配置数据过程如下：

a). M2M终端设备根据需要主动发起参数配置请求，M2M平台判断终端设备请求的参数中是否有不可识别的参数。若有，则向M2M终端设备返回数据请求无效的应答，并在应答报文中包含有不支持的参数；否则，则向M2M终端设备返回数据请求有效，并在应答报文中回复终端设备请求的参数序列。

b). 终端设备在接收到配置参数时，立即应用参数。与平台下发参数流程类似，终端设备应用向平台请求来配置参数也分为两种情况：

a) 新参数生效无需重启终端设备。首先将原有参数保存，然后写入新参数配置，则待新参数生效后且系统稳定运行后，向平台上报参数配置结果。

b) 新参数生效需要重启终端设备。首先将原有参数保存，然后写入新参数配置，并向M2M平台发送 带适当的“登出原因”的登出报文后，重启终端设备。终端设备重启后向登陆M2M平台后，应向M2M平台上报其应用配置结果。

当 M2M 终端设备接收到 M2M 平台返回的请求参数后，若其本地参数与 M2M 平台返回的参数一致，则无须应用；否则应立即应用。若应用参数，M2M 终端设备无须重启，则应用后立即向 M2M 平台上报其应用配置结果。

若 M2M 终端设备需要重启，则在应用参数前必须向 M2M 平台发起退出登录以更新 M2M 平台下发参数请求。

然后，M2M终端设备必须接收到M2M平台返回的退出登录应答后，才能应用配置参数。M2M终端设备重新登录后，应向M2M平台上报其应用配置结果。

4.3.9.2. M2M 终端设备本地人工配置参数

M2M终端设备可以在本地人工配置其参数，但在其参数生效之后，应立即向M2M平台上报其更新参数，以便M2M同步更新其参数配置。M2M终端设备应用本地人工配置参数上报过程，并与平台进行数据交互，其交互流程分为两种情况：

a). M2M在线的情况下，本地人工配置参数。

1) 若参数生效无须重启终端设备，则直接上报其配置参数。

2) 若参数生效必须重启终端设备，则先用带适当的“登出原因”的登出报文通知M2M平台需要应用本地配置参数退出登录。然后，待新参数生效，重新向M2M平台登录后，上报其配置参数。

b). M2M离线的情况下，本地人工配置参数。新参数生效后，M2M终端设备重新登录上M2M平台后，上报其更新的配置参数。

需要指出的是，上述本地人工配置M2M终端设备参数仅适用于普通参数的设置。

4.3.9.3. M2M 平台设置 M2M 终端参数

在M2M登录到M2M平台之后，M2M平台在需要的时候可向M2M终端设备发送参数设置命令，通过平台向M2M终端发送的参数设置报文设置终端设备的参数。M2M终端设备收到后给予应答。

M2M平台向M2M终端设备设置终端设备参数可以是同步交互事件，也可以属于异步交互事件。如果是异步交互事件，M2M终端设备在获取参数配置生效后，需要向M2M平台上报参数。（以下流程以异步交互事件模式为例进行说明）

M2M平台配置终端设备参数过程如下：

a). M2M终端设备在接收到M2M平台根据需要发起远程参数配置命令之后，判断在下发的参数中是否有不可识别的参数。若有不可识别的参数，则拒绝执行参数配置命令，向M2M平台返回数据无效的应答，并在应答报文中上报包含有不支持的参数信息。

b). 若终端设备支持下发的全部参数，则将参数暂存，并向M2M平台返回数据正确的应答；否则，则返回数据无效的应答。

c). 若终端设备因正在运行业务，无法立即应用参数，则需要以心跳间隔向M2M平台上报暂缓应用参数配置信息，直至可以应用参数配置为止。

d). 终端设备在应用参数配置时，分为两种情况：

1） 新参数生效无需重启终端设备：终端首先将原有参数保存，然后写入新参数配置，则待新参数生效后且系统稳定运行，向平台上报参数配置结果。

2） 新参数生效需要重启终端设备：终端首先将原有参数保存，然后写入新参数配置，并向M2M平台发送登出报文并且将登出原因设为“M2M终端设备应用平台下发新配置生效重启会话”，然后重启终端设备。终端设备重启后向登录M2M平台后，向M2M平台上报其应用配置结果。

M2M平台向终端设置参数过程如图16所示。需要注意的是，“暂缓应用配置信息”通知反复上报在此流程中为可选项，亦可以采用心跳的方式保持连接。

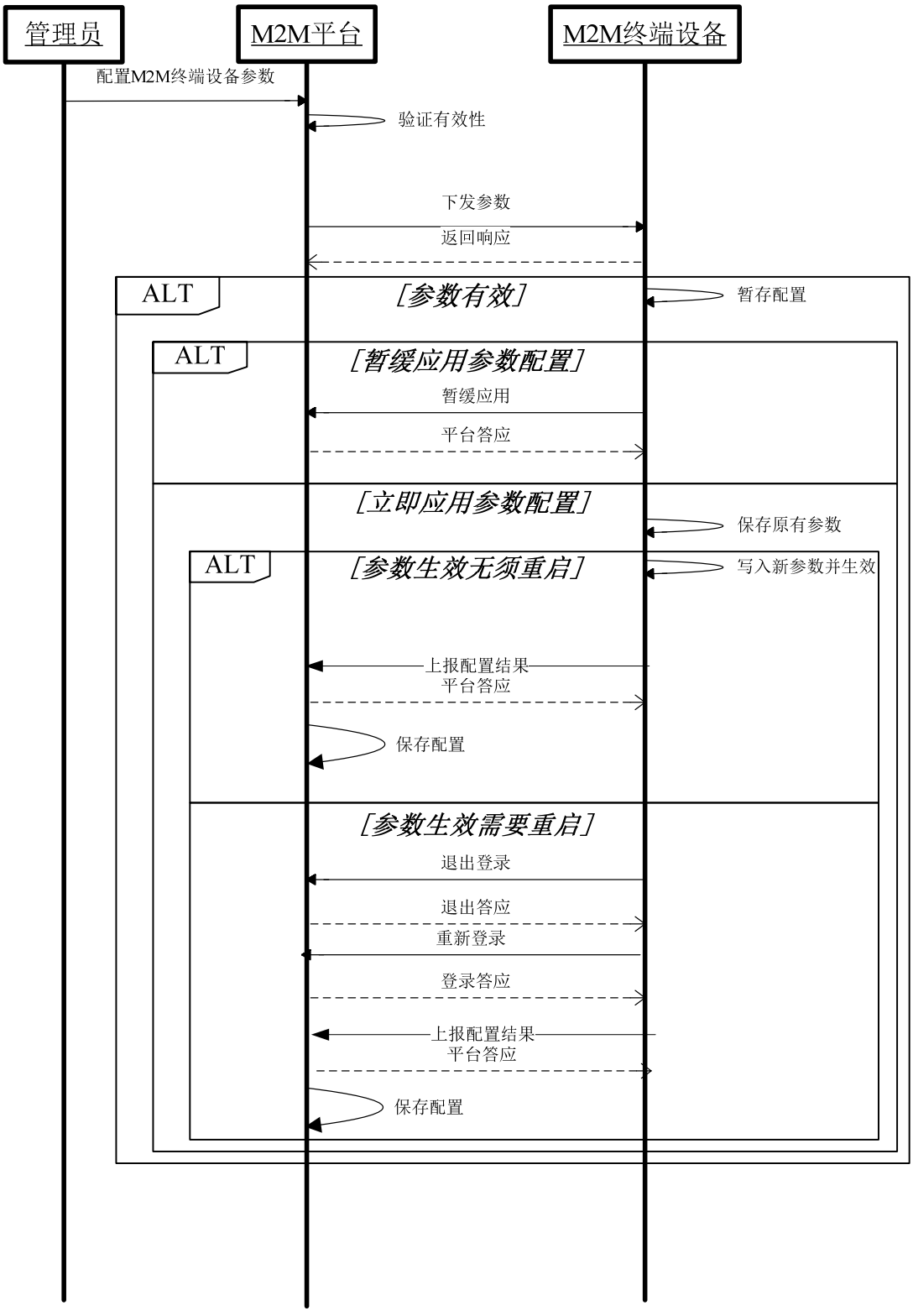


图 16 M2M平台向终端设备设置终端设备参数过程

M2M平台向M2M终端设备设置的参数需要终端设备立即应用，则必须在报文中携带参数指示终端为强制执行。

当M2M平台设置的参数中，有M2M终端设备不支持的参数时，终端返回失败应答的报文。

若M2M终端设备因正在运行业务，无法立即应用参数，且M2M平台不强制M2M终端设备立即应用，则M2M终端设备需要以心跳间隔向M2M平台上报暂缓应用参数配置信息，直至可以应用参数配置为止。

M2M终端设备应用参数，若无须重启，则应用后立即向M2M平台上报其应用配置结果，

若M2M终端设备需要重启，则在应用参数前必须向M2M平台发起退出登录以更新M2M平台下发参数请求。

然后，M2M终端设备必须接收到M2M平台返回的退出登录应答后，才能应用配置参数。M2M终端设备重新登录后，应向M2M平台上报其应用配置结果。

4.3.10. 安全参数设置

M2M平台在需要的时候可向M2M终端设备发送设置安全相关的参数的值，M2M终端设备也可以向M2M平台请求设置安全参数的值。M2M终端设备或M2M平台收到后给予应答。

M2M终端设备无权自行设置安全参数，必须向M2M平台请求设置；而M2M平台下发的接入密码和基础密钥若以明文发送则必须以短信的方式下给M2M终端设备。对于M2M平台设置SIM卡的PIN1码，M2M终端设备需要用存储在在本地原始PIN码校验通过后，再应用M2M平台下发的PIN码；若应用失败应向平台告警。

4.3.11. 业务数据转发

M2M终端设备在采集数据后，可以经由M2M平台向M2M应用或其它M2M终端设备发送。此数据报文既可由M2M终端设备发起，M2M平台确认(主动上报数据)；也可能由M2M平台发起，M2M终端设备确认。

业务数据转发可以有三种模式：第一种为网关模式，即所有的请求均需要对应的ACK反馈消息确认（如图17,图18）。第二种为路由器模式，即所有的请求均无需ACK反馈消息确认（如图19，图20）。第三种分段确认模式，即M2M终端与M2M平台之间的所有请求都有ACK馈消息确认，而M2M平台完成M2M终端设备的接收之后无需向M2M应用发送完成接收的消息（如图图21，图22）。可以根据实际应用情况选取其中1种或多种模式进行应用。

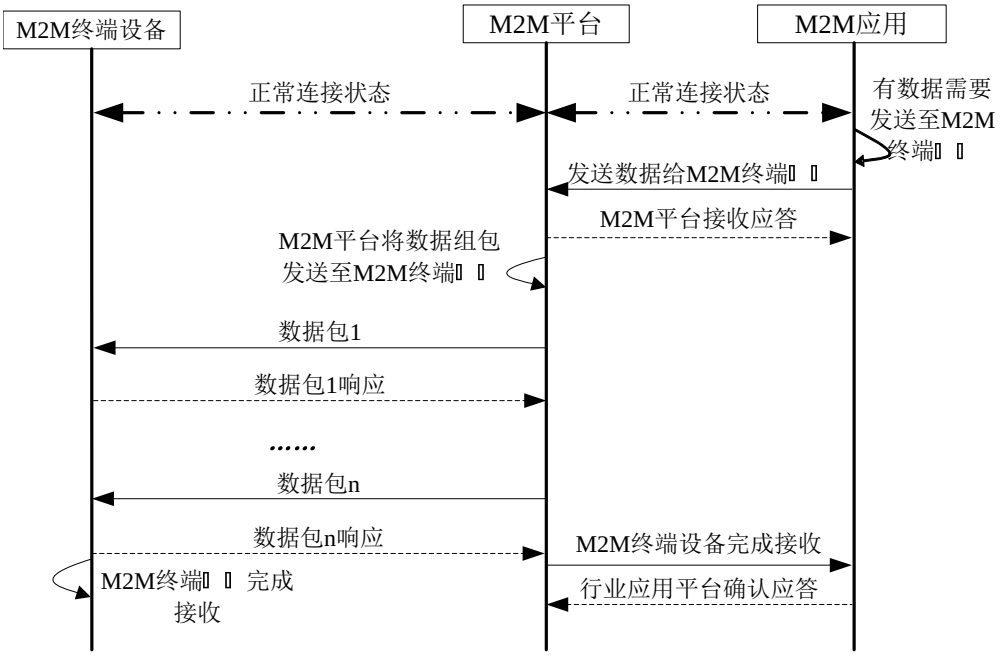


图 17 M2M应用向M2M终端设备数据透传（网关模式）

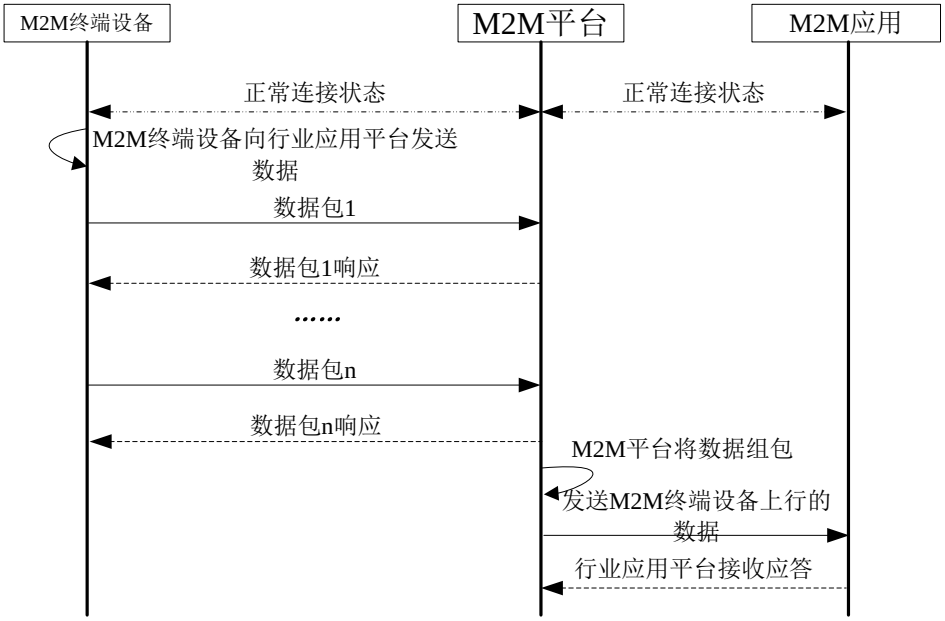


图 18 M2M终端设备向M2M应用数据透传（网关模式）

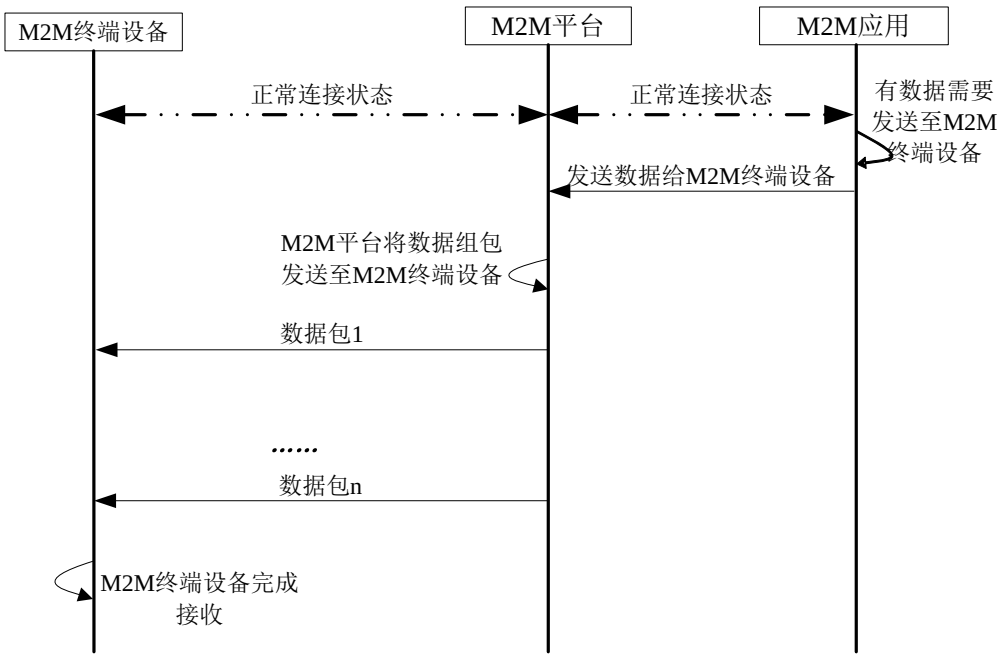


图 19 M2M应用向M2M终端设备数据透传（路由器模式）

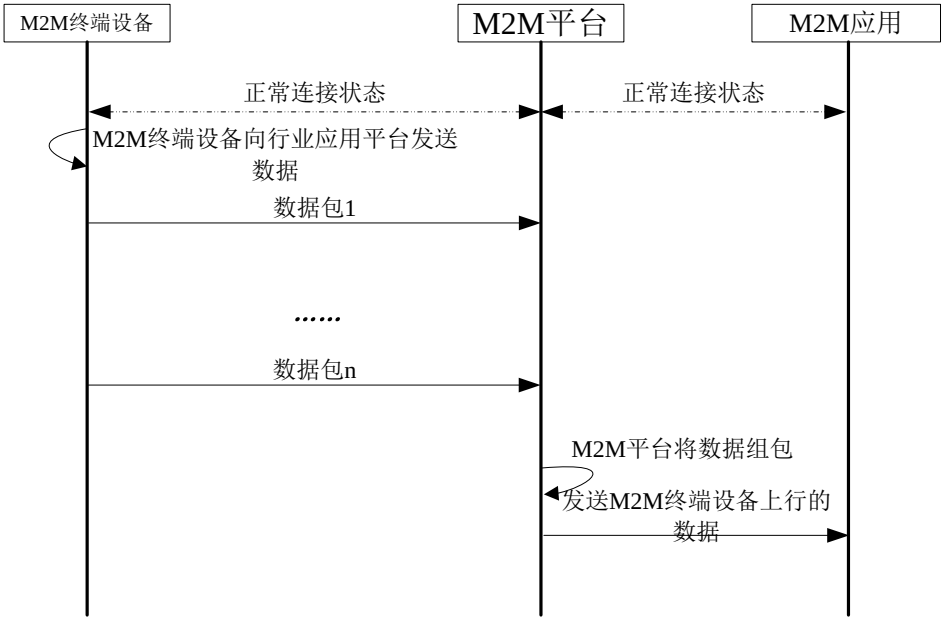


图 20 M2M终端设备向M2M应用数据透传（路由器模式）

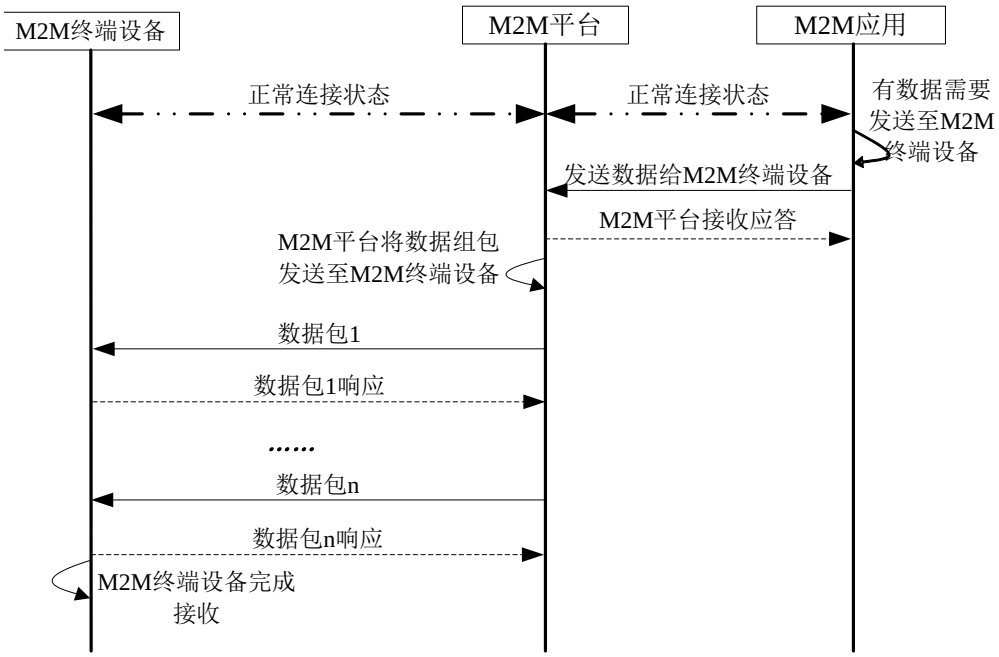


图 21 M2M应用向M2M终端设备数据透传（分段确认模式）

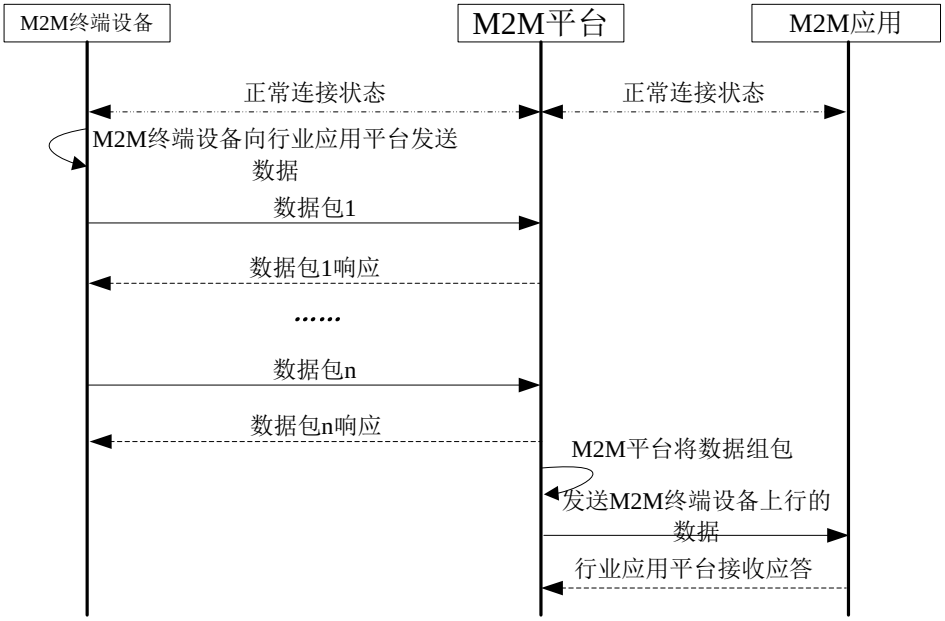


图 22 M2M终端设备向M2M应用数据透传（分段确认模式）

以上分别给出了M2M终端设备与M2M应用之间的数据透传的三种模式和流程。报文体数据对于M2M终端设备以及M2M平台是透明、不可或不需理解的业务流数据，M2M平台只是数据进行路由转发。

4.4. 协议安全机制

4.4.1. SIM 卡对 M2M 终端设备的认证

在M2M的实际应用中，M2M终端设备可能被置于非安全的环境下使用，为保证合法的M2M终端设备或合法的SIM卡不被用于M2M业务的非法接入， SIM卡必须具备对M2M终端设备的安全认证机制。即只有M2M终端设备拥有正确的PIN码才能启用合法的SIM卡，从而通过SIM卡接入到M2M业务系统。

在M2M系统中，只有使用合法的SIM卡的终端设备才能进入M2M系统，而SIM卡的合法性鉴权是由通信网络来保证的。因此，通过SIM卡对M2M终端设备的安全认证机制即可实现对M2M终端设备的安全认证。

4.4.1.1. SIM 卡对 M2M 终端设备的安全认证

M2M终端设备基于SIM对M2M终端设备安全认证机制的安全接入M2M平台流程如图23所示。

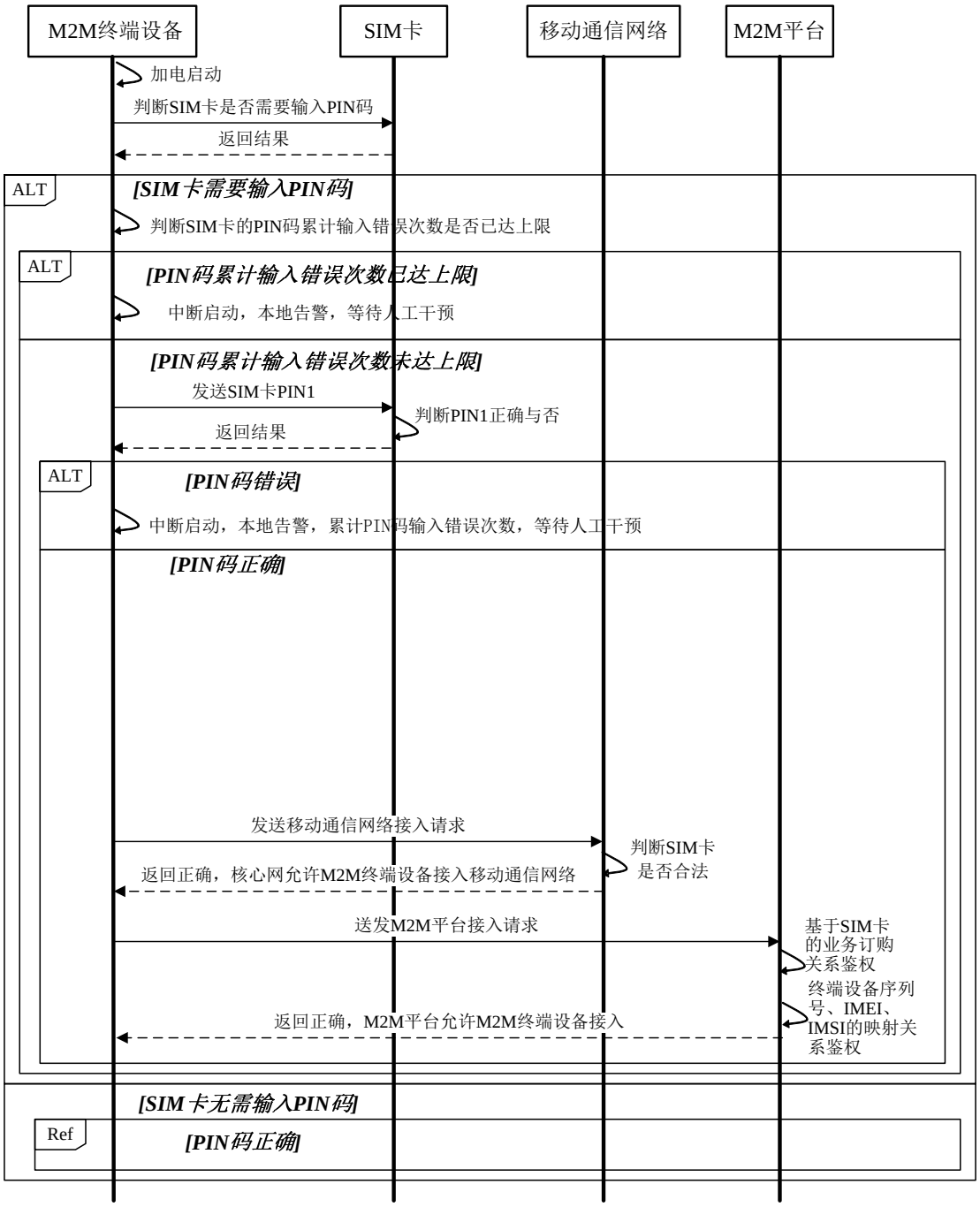


图 23 M2M终端设备基于SIM对M2M终端设备安全认证机制的安全接入M2M平台流程

1. M2M终端设备加电启动后，首先判断该SIM卡PIN码累计输入错误次数是否已达上限，若是，则停止启动，产生SIM卡PIN码累计输入错误已达上限的本地告警，防止SIM卡因为PIN码输入错误次数过多而锁死；否则，向SIM卡发送其PIN1码。SIM卡判断是否为正确的PIN1码，若正确则SIM卡允许M2M终端设备使用SIM卡；否则，则拒绝M2M终端设备使用本SIM卡，此时M2M终端设备应立即停止启动过程，产生SIM卡PIN码输入错误的本地告警，并累计该SIM卡PIN码输入错误次数。
2. M2M终端设备启动SIM卡后，接入移动通信网络。
3. M2M终端设备成功接入移动通信网络后，向M2M平台发起接入请求。
4. M2M平台对M2M终端设备的接入请求进行鉴权，判断是否允许M2M终端设备接入到M2M系统中。

4.4.1.2. M2M 平台设置 SIM 卡对 M2M 终端设备安全认证参数

M2M协议支持M2M平台通过相关指令设置M2M终端设备上的SIM卡相关安全机制，如SIM卡的PIN码和PUK码的密码设置变更或启用等，其流程如图24所示。

1. M2M平台根据业务需要选择采用明文模式或密文模式设置SIM卡对M2M终端设备安全认证参数。

- 明文模式
  a) M2M平台通过安全参数设置流程向M2M终端设备发送SIM卡对M2M终端设备安全认证参数变更通知，要求M2M终端设备进入短信通信模式等待接收SIM卡对M2M终端设备安全认证参数。
  b) M2M终端设备对接收到的安全参数设置报文进行鉴权。
  c) M2M终端设备通过M2M平台的请求报文鉴权后，向M2M平台返回应答，并进入短信模式等待。
  d) M2M平台接收到M2M终端设备返回的应答后，经过一段时间的时延，以短信方式向M2M终端设备下发SIM卡对M2M终端设备安全认证参数。
  e) M2M终端设备接收到SIM卡对M2M终端设备安全认证参数之后，立即将其妥善存储，并在条件允许的情况下尽可能向M2M平台返回接收成功应答。
- 密文模式
  a) M2M平台通过安全参数设置流程以密文模式向M2M终端设备发送SIM卡对M2M终端设备安全认证参数。
  b) M2M终端设备对接收到的SIM卡对M2M终端设备安全认证参数设置报文进行鉴权。
  c) M2M终端设备通过M2M平台的请求报文鉴权后，将接收到的参数进行解密，立即将其妥善存储，并向M2M平台返回接收成功应答。

2. 在成功接收SIM卡对M2M终端设备安全认证参数之后，M2M终端设备应立即向M2M平台发送退出登录请求，以更新SIM卡对M2M终端设备安全认证参数。

3. M2M平台返回退出登录请求应答。

4. M2M终端设备立即应用SIM卡对M2M终端设备安全认证参数。

5. M2M终端设备在SIM卡对M2M终端设备安全认证参数生效之后，立即重新向M2M平台发起登录请求。

6. M2M平台接收到M2M终端设备的登录请求之后，返回登录应答；并生成SIM卡对M2M终端设备安全认证参数设置成功的日志，同时保存新的M2M终端设备与SIM卡双向安全认证参数。

需要指出的是，对于SIM卡对M2M终端设备安全认证参数的操作，必须是M2M终端设备在M2M平台完成注册并获得其接入密码之后才能进行。对于首次下发PIN码并启用的情况，M2M终端设备应用本地事先存储的默认PIN码去进行PIN码启用过程中PIN码校验；而对于M2M终端设备再次接受M2M平台下发PIN码并启用的情况，M2M终端设备应使用已经存储在本地的上一次的PIN码去进行PIN码启用过程中的PIN码校验。此外，如果条件允许，M2M平台应在M2M终端设备登录之后，再次通过报文查询设置的安全认证参数，以确认该参数是否确实在M2M终端设备上生效；而对于M2M终端设备应用平台下发的安全参数失败，M2M终端设备需通知M2M平台。

此外，为保证SIM卡对M2M终端设备安全认证参数的一致性，简化相关操作，M2M协议不支持M2M终端设备发起的SIM卡对M2M终端设备安全认证参数变更操作，即M2M终端设备无权更改其SIM卡对M2M终端设备安全认证参数，必须通过M2M平台对其进行相关设置。

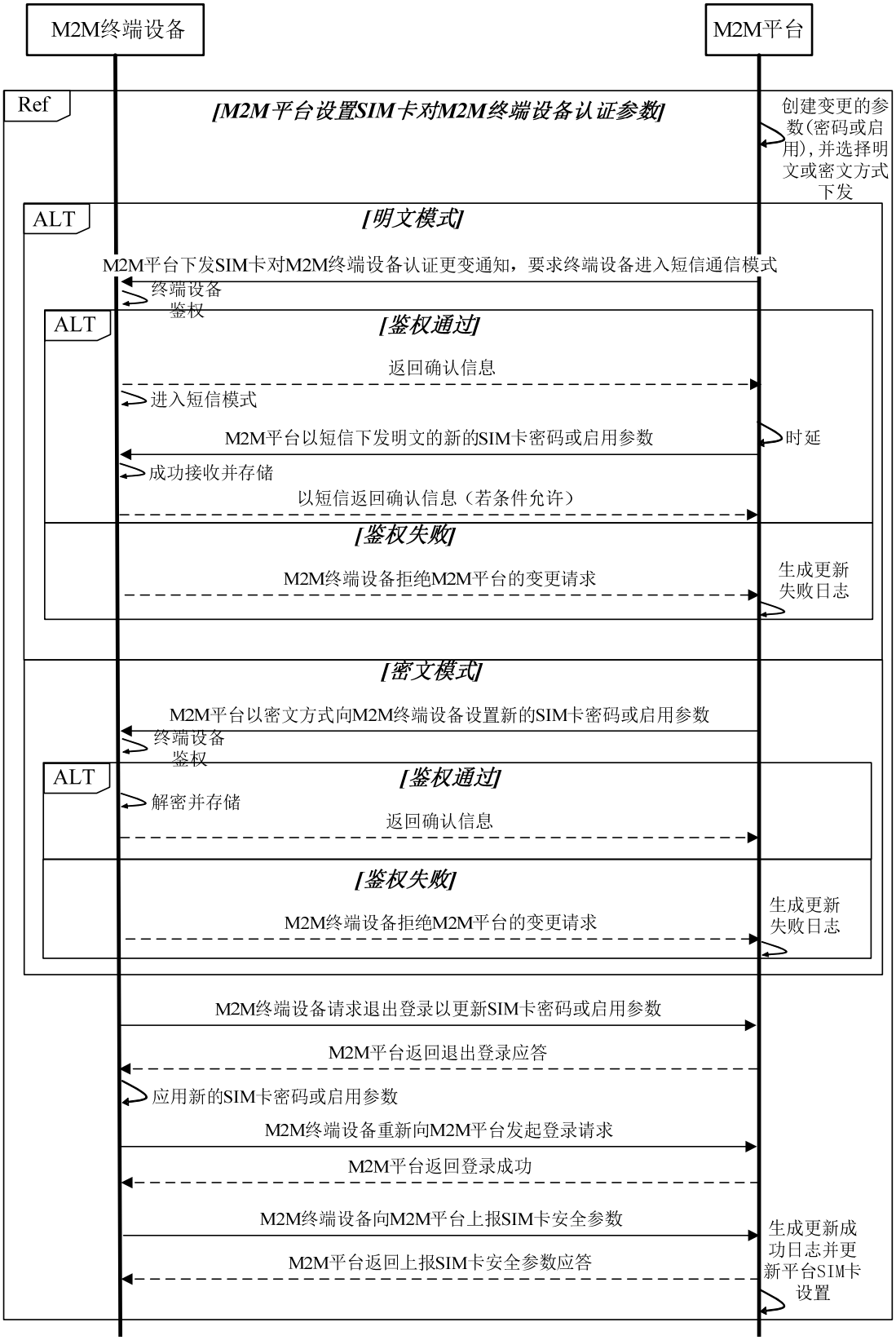


图 24 M2M 平台设置 SIM 卡对 M2M 终端设备安全认证参数流程

4.4.1.3. M2M 终端设备更换 SIM 卡

4.4.1.3.1. 启用 SIM 卡对 M2M 终端设备安全认证机制的终端设备更换 SIM 卡

对于启用SIM卡对M2M终端设备安全认证机制的M2M终端设备更换SIM卡时，必须先通过M2M平台取消其M2M终端设备上的安全机制，其具体流程如图25所示。

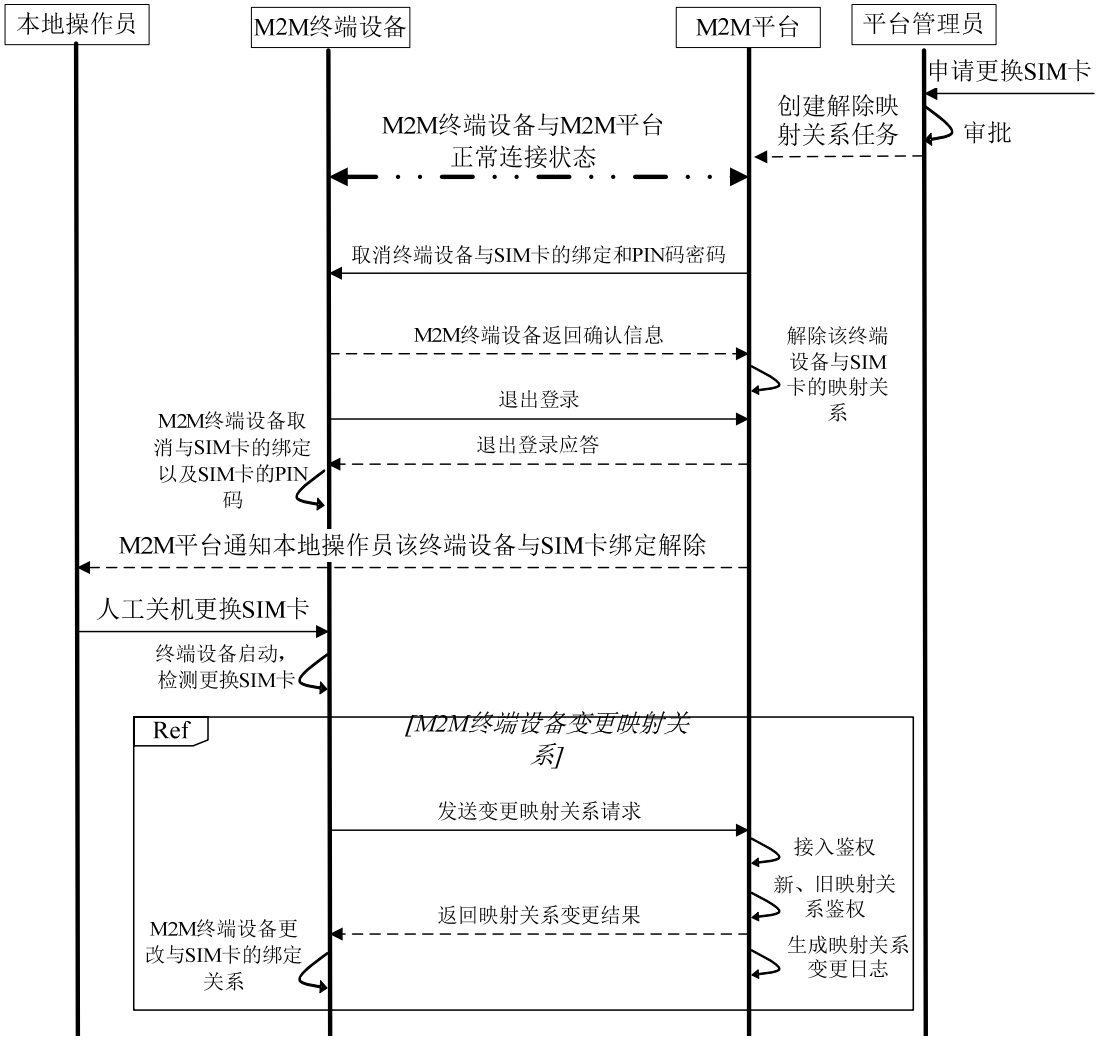


图 25 M2M终端设备更换SIM卡的流程

1. 在更换SIM卡申请获得批准之后，M2M平台创建解除映射关系的任务。
2. 在M2M终端设备正常连接情况下，M2M平台下发取消M2M终端设备与SIM卡绑定和PIN码密码的指令，M2M终端设备接收到后，向M2M平台返回接收成功的应答。M2M平台接收到M2M终端设备返回的该应答之后，在平台侧取消该M2M终端设备与原有SIM卡的绑定关系。

3. M2M终端设备向M2M平台发送退出登录以更新双向安全认证参数；M2M平台在接收到该退出登录请求后，向M2M终端设备返回退出登录应答并通知本地操作员该终端设备与SIM卡的绑定关系已经解除。
4. 本地操作员确认M2M终端设备已经解除与SIM卡的绑定关系之后，人工手动关机并更换SIM卡。
5. M2M终端设备加电启动之后，检测其已经更换SIM卡，则发起变更映射关系请求，具体参见附录B。

需要指出的是，M2M终端设备执行完“取消M2M终端设备与SIM卡绑定和PIN码密码”的命令之后，原SIM卡上所有的安全设置和PIN码的密码都必须被清除。

对于个别极端情况，可以直接本地人工清除SIM卡对M2M终端设备安全认证机制(参见“ 本地人工清除SIM卡对M2M终端设备安全认证参数”)，然后更换SIM卡，其流程参见下文“2. 未启用SIM卡对M2M终端设备安全认证机制的终端设备更换SIM卡”部分内容。

4.4.1.3.2. 未启用 SIM 卡对 M2M 终端设备安全认证机制的终端设备更换 SIM 卡(4.4.1.3.2)

对于未启用SIM卡对M2M终端设备安全认证机制的M2M终端设备更换SIM卡时，仅需人工关机更换SIM卡，M2M终端设备加电后自动向M2M平台发送变更映射关系请求,具体参见附录B。

4.4.1.4. 本地人工清除 SIM 卡对 M2M 终端设备安全认证参数

当M2M终端设备发生以下异常情况时，可以本地人工取消SIM卡对M2M终端设备安全认证参数：

1. M2M终端设备更换SIM卡后，因M2M终端设备绑定SIM卡的IMSI而无法正常启动。
2. SIM卡PIN码输入错误或输入错误累计次数达到上限。
3. SIM卡PIN码锁死，需要本地解锁。
4. 其它因SIM卡对M2M终端设备安全认证参数配置错误导致M2M终端设备无法正常登录M2M平台、无法正常工作、本地告警而需要本地人工干预的情况。

本地人工清除SIM卡对M2M终端设备安全认证参数流程如图26所示。

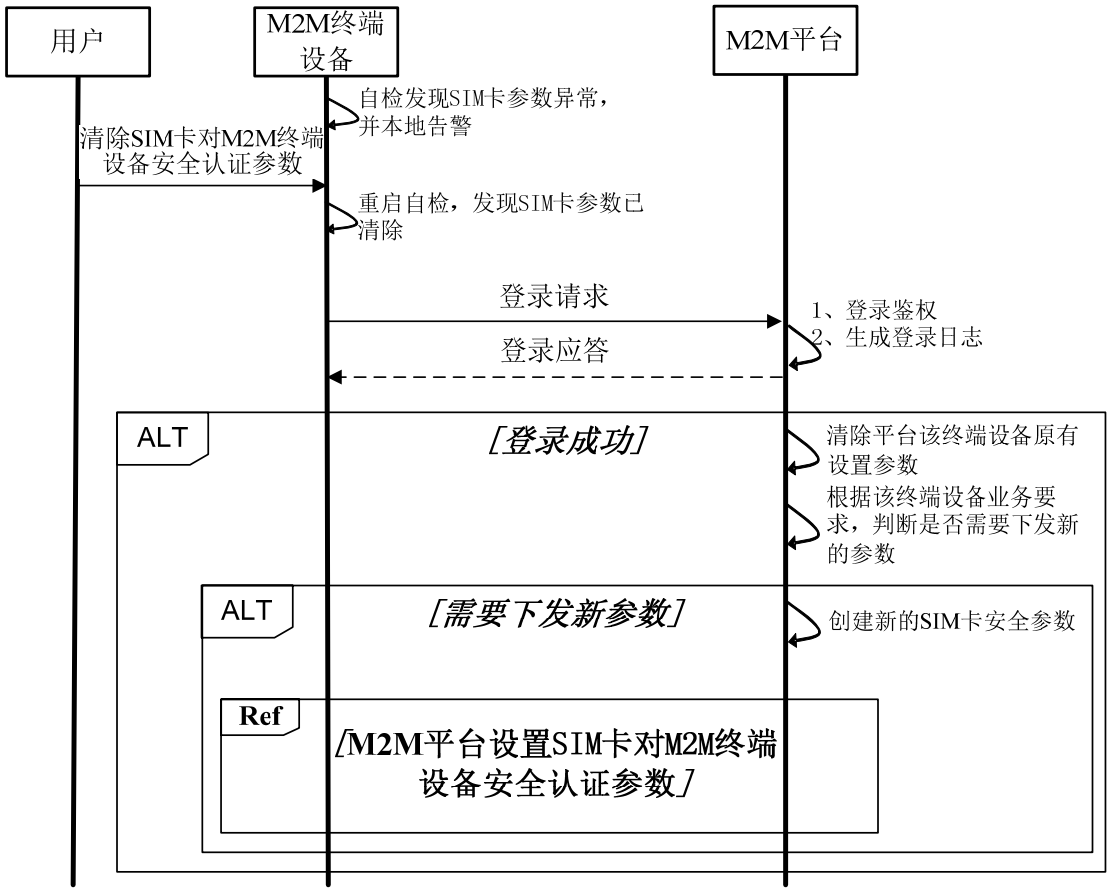


图 26 本地人工清除SIM卡对M2M终端设备安全认证参数流程

M2M终端设备本地人工设置SIM卡对M2M终端设备安全认证参数时，M2M终端设备必须对该操作进行本地鉴权，只有鉴权通过才能进行后续操作。鉴权内容包括：

- 身份鉴权，是指进行本地人工取消SIM卡对M2M终端设备安全认证参数操作必须拥有相应的操作权限。
- 终端设备状态鉴权，是指M2M终端设备的工作状态必须是异常或告警状态，正常工作或登录状态下即使身份鉴权通过也无法进行本地人工设置。

本地人工取消SIM卡对M2M终端设备安全认证参数后，M2M终端设备必须在登录请求中向M2M平台上报相关信息。M2M平台接收该上报信息之后，根据该M2M终端设备业务的要求，判断是否重新为该终端设备设置M2M终端设备与SIM卡双向安全认证参数，设置的流程参见“ M2M平台设置SIM卡对M2M终端设备安全认证参数”。

本地人工设置仅能够禁用SIM卡对M2M终端设备安全认证机制并将SIM卡的PIN码清除，不能重新设置M2M终端设备与SIM卡双向安全认证参数或PIN码。

对于某些极端情况下，必须本地人工设置M2M终端设备的PIN码和PUK码，因为涉及M2M平台与M2M终端设备参数配置一致性问题和安全因素，M2M协议不支持该操作。但可以通过人工的方式在M2M终端设备设置好PIN码和PUK码，并在M2M平台人工手动维护好相应数据，从而达到M2M平台与M2M终端设备参数配置一致性。

4.4.2. 终端设备与平台的数据交互安全

为保证M2M终端设备与M2M平台之间的数据交互安全，M2M终端设备与M2M平台间通信协议采用接入密码安全验证和报文摘要的方式，以实现在报文交互中对通信双方的身份验证并确保报文的完整性；采用报文内容加密的方式，以保证报文内容的安全性。

其中，终端是否使用加密，是否使用接入密码进行认证，应通过预配置在平台进行设置。

4.4.2.1. 通信安全性

M2M终端设备与M2M平台间的通信协议通过在报文之后增加接入密码安全验证并对整个消息体进行摘要处理，以实现M2M终端设备与M2M平台之间交互报文来源的身份验证并保证报文的完整性，从而确保M2M终端设备与M2M平台的通信安全。

终端和平台之间的报文设置摘要体（摘要体不加密），通过摘要体的校验确定是否是合法的通信报文。摘要体的计算方式如下：

加密函数(报文头+报文体+IMSI+接入密码)

M2M终端设备与平台利用接入密码与终端设备序列号可以有效验证彼此接收到的报文来源的身份的合法性：当接收方接收到任意一条报文时判断摘要体是否正确（根据计算公式进行计算的结果和接收到的报文的摘要体进行比较，判断），若正确则接收到的报文的完整性和来源真实性都合法；反之，接收到的报文非法。

若M2M终端设备或M2M平台接收到一条本该携带摘要体而没有携带的报文或摘要体校验错误，则会根据其自身安全设置，选择相应的操作。具体内容参见“安全验证失败的处理流程”。

需要指出的是，在短信通信模式下时，M2M报文默认不需要携带摘要。

4.4.2.2. 数据安全性

M2M 终端设备与 M2M 平台间的通信协议支持通过对内容体中的数据进行加密，以保证数据在传输过程中的安全性，加密报文可分为部分加密报文和完全加密报文。

协议支持通过对内容体中的数据进行加密，以保证数据在传输过程中的安全性。如前文所述，加密报文可分为部分加密报文和完全加密报文。报文发送方可根据其发送报文中数据安全性的要求，自行选择对哪些内容进行加密以及采用部分加密报文还是完全加密报文。对于部分加密报文，其经过加密后的部分只是内容体中一个参数，而在该参数中承载了需要加密的一个或几个原始参数；对于完全加密报文，则是将整个明文的内容体加密成一个密文格式的加密内容体，并以一个参数的形式在报文中呈现。当密文的长度超过一个M2M协议报文的最大长度，则必须将密文拆分成多个子段进行传送。

当M2M终端设备接收到经过加密的报文时，首先使用接入密码和IMSI对其携带的摘要体进行接入安全验证；若通过验证，则用其相应的密钥对报文中的加密的内容进行解密；最后，再执行报文所承载的命令。

当M2M平台接收到经过加密的报文时，首先根据该报文的报文头中的终端设备序列号选择该M2M终端设备的接入密码和IMSI对该报文携带的摘要体进行接入安全验证；若通过验证，则该M2M终端设备所对应的密钥对报文中的加密的内容进行解密；最后，再执行报文所承载的命令。

协议在加密、解密过程中使用到了两个密钥：基础密钥和会话密钥。

1. 基础密钥用于加密、解密会话密钥，不同的M2M终端设备由M2M平台分配不同的基础密钥；M2M平台负责统一分配和保存所有M2M终端基础密钥。基础密钥是M2M终端在M2M平台上成功注册之后，由M2M平台通过短信方式下发至终端设备，并可定期更新（也可采用预置的方式在终端和平台上进行加载） 。
2. 会话密钥，用于每次会话数据的加密解密，在M2M终端设备每次成功登录M2M平台之后，由M2M平台用基本密钥加密之后发至终端设备。M2M终端设备与M2M平台的每次会话均有M2M平台分配会话密钥，一次会话只允许持续一定的时间，如果超出该时间，M2M终端设备必须重新登录，分配新的会话密钥。否则，M2M平台将拒绝M2M终端设备的消息。

4.4.3. 密码与密钥的分发

4.4.3.1. 接入密码和基础密钥的分发与变更

M2M终端设备的接入密码和基础密钥是M2M安全机制的基础，M2M终端设备接入M2M系统前必须从M2M平台获取其接入密码，而具备数据加密功能的M2M终端设备还必须获取其基础密钥。

4.4.3.1.1. M2M 终端设备预置接入密码和基础密钥

在M2M终端设备向M2M平台注册前，其接入密码可以通过预置的方式与其终端设备序列号一并存入该终端设备；对于支持加密功能的M2M终端设备，可以同时预置其基础密钥。但是，必须将预置的终端设备序列号、接入密码、基础密钥等相应数据维护在M2M平台上，以便M2M终端设备注册时进行核对。

对于预置接入密码和基础密码的M2M终端设备在其向M2M平台注册时，必须向M2M平台上报其预置的终端设备序列号以及经过摘要处理的接入密码和基础密钥的相关信息。对于预置接入密码和基础密钥核对无效的M2M终端设备，M2M平台禁止其注册。

需要指出的是，由于无法确定M2M终端设备首次使用的确切时间，因此，对于预置的接入密码和基础密钥其有效期都需有一个预定值。待M2M终端设备首次成功登录M2M平台之后，由M2M平台根据该M2M终端设备的业务要求进行修改。

4.4.3.1.2. M2M 平台首次下发接入密码和基础密钥

M2M终端设备首次获取其接入密码和基础密钥的过程如图27所示。

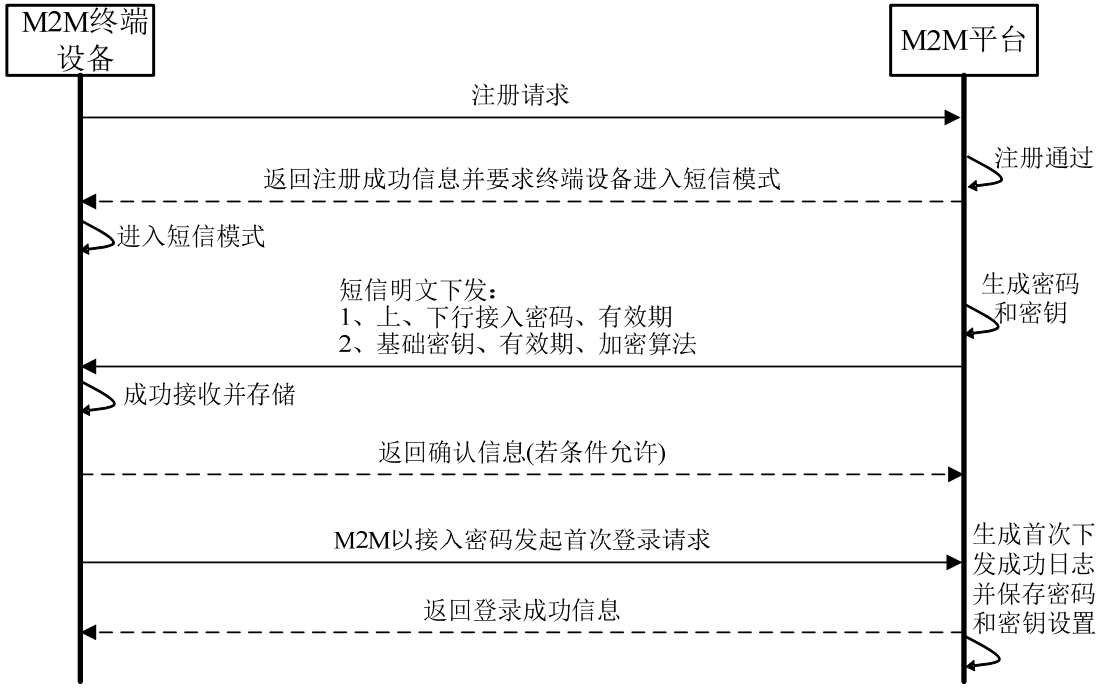


图 27 M2M终端设备首次获取其接入密码和基础密钥的流程

M2M终端设备通过其向M2M平台注册，进而首次获取其接入密码和基础密钥。其过程如下：

a). M2M终端设备向M2M平台发起注册请求。

b). M2M平台通过M2M终端设备的注册请求之后，会向其回复注册成功并要求其进入短信模式，准备接收平台下发的接入密码和基础密钥。

c). M2M终端设备接收到上述信息之后，立即进入短信通信模式。

d). M2M平台经过一定时延之后，通过短信向M2M终端设备发送M2M终端设备的接入密码和有效期信息， 若本终端设备支持数据加密功能，则M2M平台一并下发该M2M终端设备的基础密钥和基础密钥的有效期信息。

e). M2M终端设备接收到M2M平台下发的接入密码和基础密钥之后，立即将其妥善存储；并根据其是否具备短信业务订购关系向M2M平台返回接收应答（可选）。

f). M2M终端设备立即用首次接收到的接入密码向M2M平台发起登录请求，如要启用数据加密，则需要一并携带基础密钥的相关信息摘要。

g). M2M平台接收到M2M终端设备的首次登录请求之后，对其进行鉴权，鉴权通过后给登录成功应答，并在平台生成首次下发密码成功日志，同时保存密码或密钥。

需要指出的是，接入密码和基础密钥的首次下发，必须采用短信以明文的方式下发。

4.4.3.1.3. 请求变更

M2M终端设备在首次成功获取其接入密码和基础密钥之后，即可以安全的方式接入M2M平台。在此之后，M2M终端设备和M2M平台都可以向对方发起接入密钥或基础密钥请求变更。根据请求变更流程发起方的不同，该流程可为：M2M终端设备请求变更其接入密码或基础密钥和M2M平台主动变更终端设备的接入密码或基础密钥。

4.4.3.1.3.1. M2M 终端设备请求变更其接入密码或基础密钥

M2M终端设备请求变更接入密码与基础密钥的流程如图28所示。

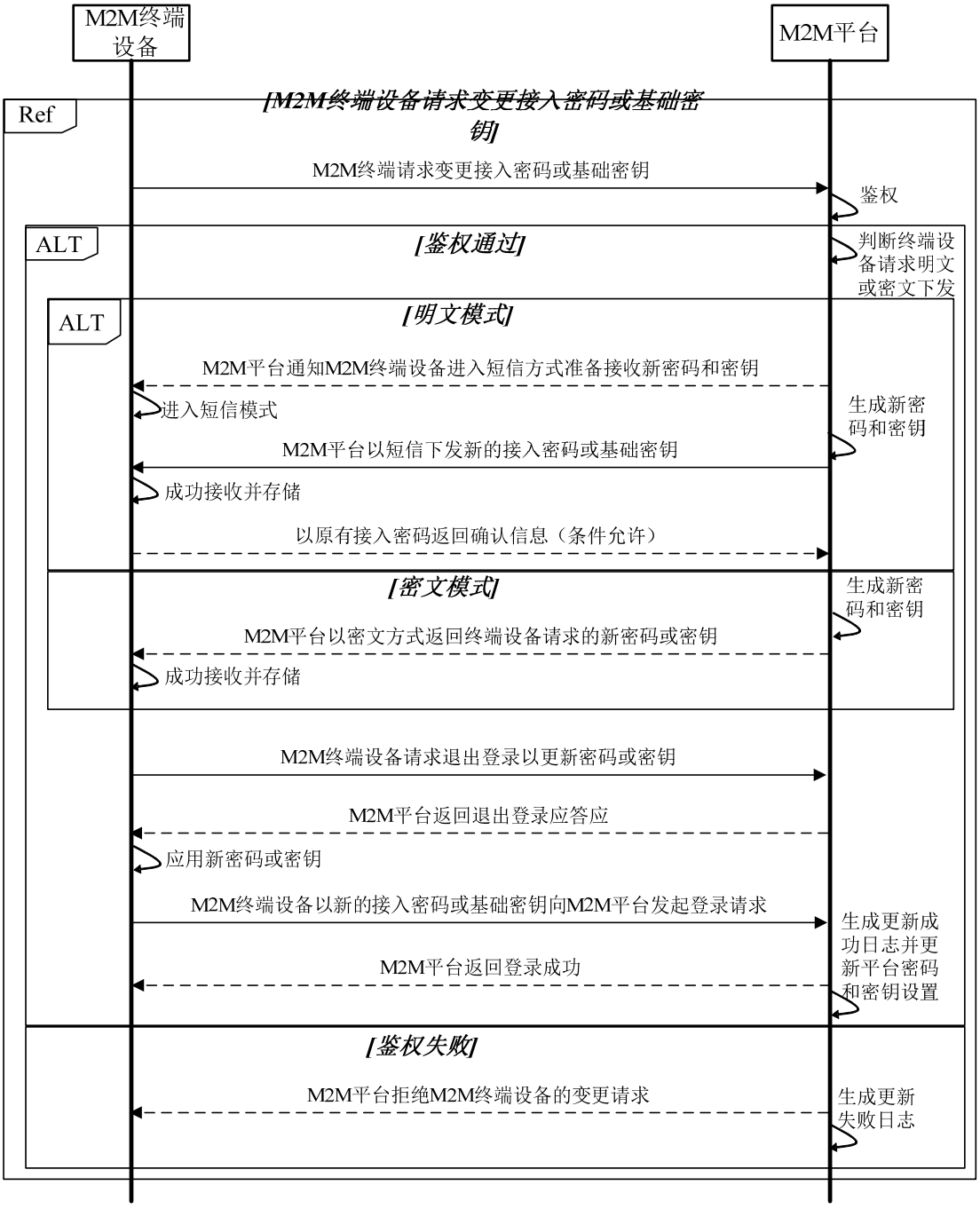


图 28 M2M终端设备请求接入密码、基础密钥变更流程

a). M2M终端设备向M2M平台发送请求变更接入密码或基础密钥。

b). M2M平台接收到请求之后，首先对请求进行鉴权，鉴权通过后再根据安全设置报文中的参数判断M2M终端设备是请求以明文还是密文方式下发接入密码或基础密钥。

1) 明文模式

i. M2M平台向M2M终端设备返回请求变更接受应答，要求其进入短信通信模式等待接收以短信方式下发的、包含有新的接入密码或基础密钥的安全设置报文，同时平台生成新接入密码或基础密钥准备下发。

ii. M2M平台经过一定时延后，以短信方式下发新的接入密码或基础密钥。

iii. M2M终端设备接收到新的接入密码或基础密钥之后，立即将其妥善存储，并在条件允许的情况下向M2M平台返回接收成功应答（可选）。

2) 密文模式

i. M2M平台向M2M终端设备返回请求变更接受应答，并在应答报文中以密文的方式下发新的接入密码或基础密钥。

c). 在成功接收新的接入密码或基础密钥之后，M2M终端设备应立即向M2M平台发送退出登录请求，以更新其接入密码或基础密钥；待接收到M2M平台的退出登录请求应答之后，立即应用新接入密码或基础密钥。

d). M2M终端设备在规定的时间内，以新的接入密码或基础密钥向M2M平台发起登录请求。

e). M2M平台接收到M2M终端设备的登录请求之后，返回登录应答；并生成接入密码或基础密钥更新成功的日志，同时保存新接入密码或基础密钥。

4.4.3.1.3.2. M2M 平台主动变更 M2M 终端设备的接入密码或基础密钥

M2M平台主动变更M2M终端设备的接入密码或基础密钥的流程如图29所示。

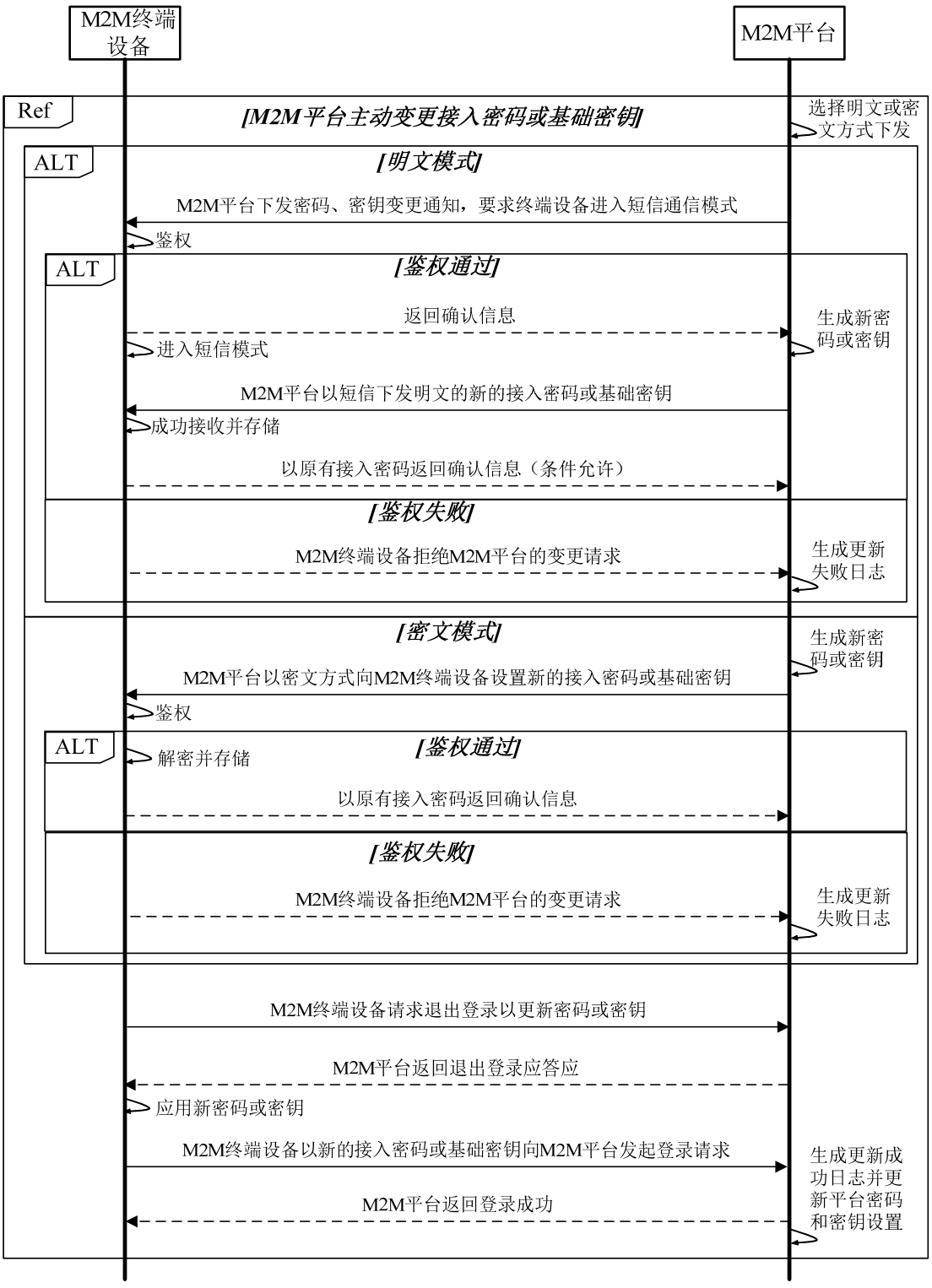


图 29 M2M平台主动变更M2M终端设备的接入密码或基础密钥流程

a). M2M平台选择是以明文或密文的方式下发新的接入密码或基础密钥。

a.1) 明文方式

a.1.1) M2M平台向M2M终端设备通过发送接入密码或基础密钥变更请求，要求M2M终端设备进入短信通信模式等待接收。

a.1.2) M2M终端设备对接收到的安全参数设置报文进行鉴权。

a.1.3) 鉴权通过后，M2M终端设备向M2M平台返回确认应答，并立即进入短信通信模式准备接收。

a.1.4) M2M平台接收到M2M终端设备的应答报文之后，立即生成新接入密码或基础密钥，经过一定时延后，以短信方式向M2M终端设备下发新的接入密码或基础密钥。

a.1.5) M2M终端设备接收到新的接入密码或基础密钥之后，立即将其妥善存储，并在条件允许的情况下向M2M平台返回接收成功应答（可选）。

a.2) 密文模式

a.2.1) M2M平台通过安全参数设置报文以密文的方式向M2M终端设备发送新的接入密码或基础密钥。

a.2.2) M2M终端设备对接收到的安全参数设置报文进行鉴权。

a.2.3) 鉴权通过后，M2M终端设备向M2M平台返回确认应答，并立即将新的接入密码或基础密钥妥善存储。

b). 在成功接收新的接入密码或基础密钥之后，M2M终端设备应立即向M2M平台发送退出登录请求，以更新其接入密码或基础密钥；待接收到M2M平台的退出登录请求应答之后，立即应用新接入密码或基础密钥。

c). M2M终端设备在规定的时间内，以新的接入密码或基础密钥向M2M平台发起登录请求。

d). M2M平台接收到M2M终端设备的登录请求之后，返回登录应答；并在生成接入密码或基础密钥更新成功的日志，同时保存新接入密码或基础密钥。

4.4.3.1.3.3. 接入密码或基础密钥请求变更的异常处理

需要指出的是，M2M终端设备无论以何种方式获取了新的接入密码或基础密钥，应立即向M2M平台发送退出登录以更新接入密码或基础密钥的请求，并必须得到M2M平台的退出登录应答。这是因为M2M平台和M2M终端设备只能通过退出登录的过程来确认双方在下一次登录报文交互中启用相同的接入密码或基础密钥，否则M2M平台和M2M终端设备则会因为双方的接入密码或基础密钥不一致而导致M2M终端设备无法正常登录。若在规定的时间内未接到M2M平台的应答，则M2M终端设备必须再次向M2M平台发送该退出登录请求，直至接收到M2M平台的退出登录应答。

M2M终端设备在得到M2M平台的退出登录应答之后，必须立即以新的接入密码或基础密钥向M2M平台发起登录请求。若M2M终端设备在规定的时间未收到M2M平台的登录应答（包括登录成功或失败），则必须再次向M2M平台发起登录，直至接收到登录应答。若重新登录次数达到上限，或接收到M2M平台安全参数错误拒绝登录的应答，则取消已经应用的、新的接入密码或基础密钥，以原先的接入密码或基础密钥向M2M平台发起登录。

若在规定的时间内，M2M平台未接到M2M终端设备以新的接入密码或基础密钥发起的登录请求，则需要向M2M终端设备发送远程控制指令，控制其立即进行登录。若在此之后的一定时间内，M2M终端设备仍然未向M2M平台发起登录，则产生接入密码或基础密钥更新未立即生效告警，并将M2M终端设备的接入密码或基础密钥恢复到更新前的状态，以便M2M终端设备以旧的接入密码或基础密钥进行登录。

此外，M2M平台以明文模式向M2M终端设备下发新的接入密码或基础密钥，由于其通信承载方式采用的是短信，而短信的存储转发机制会造成在传输过程中不可预测的时延或丢包。因此，M2M平台以短信向M2M终端设备发送新的接入密码或基础密钥之后一定的时间内，若一直未接收到M2M终端设备发送的退出登录以更新接入密码或基础密钥的请求，则平台可以再

次以短信向M2M终端设备发送新的接入密码或基础密钥，直至接收到M2M终端设备发送的退出登录以更新接入密码或基础密钥的请求。

4.4.3.2. 会话密钥的分发与变更

对于支持数据通信加密功能的M2M终端设备，在其登录过程中必须向M2M平台申请会话密钥以用于登录之后的数据加密。

M2M终端设备的会话密钥的分发与变更流程如图30所示。

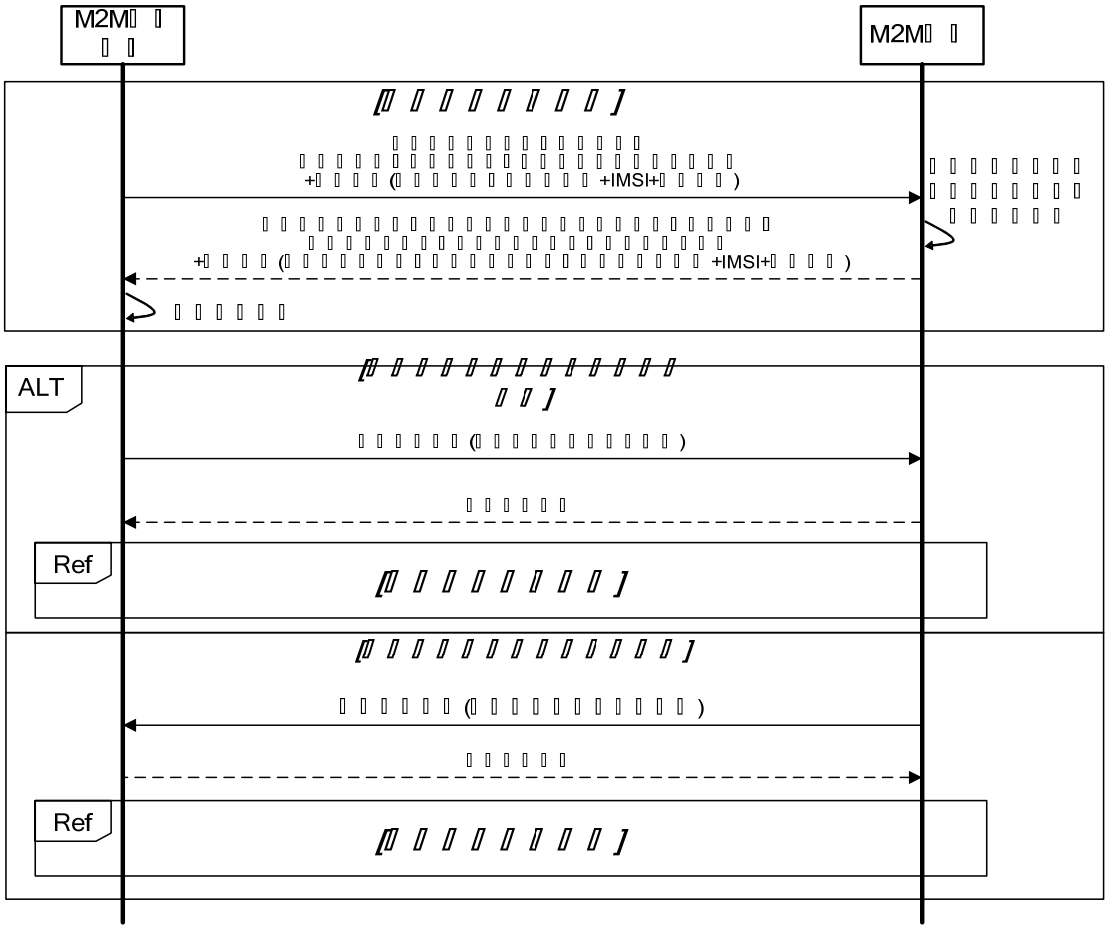


图 30 会话密钥的分发与变更

a). M2M终端设备发起登录请求，并在登录请求报文中向M2M平台请求会话密钥。登录报文的格式如下：

登录报文头＋登录报文体(包含基本密钥相关信息的摘要值)+加密函数(登录报文头＋登录报文体+IMSI+接入密码)

b). M2M平台对M2M终端设备的登录请求进行鉴权，通过鉴权后生成会话密钥并返回登录应答，登录应答报文格式如下：

登录应答报文头＋登录应答报文体(包含加密的会话密钥)+加密函数(登录应答报文头＋登录报应答文体+IMSI+下行接入密码)

c). M2M终端设备成功接收到会话密钥之后，立即妥善存储，并在下一次报文交互中用会话密钥对数据进行加密。

d). 当会话过期之后，M2M平台或M2M终端设备都可向对方发送退出登录以更新会话密钥。

4.4.4. 本地人工清除终端设备与平台的数据交互安全设置

当M2M终端设备发生因接入密码和基础密码配置错误导致M2M终端设备无法正常登录M2M平台、无法正常工作、本地告警而需要本地人工干预的情况时，可以本地人工清除M2M终端设备接入密码和基础密钥及相关设置。

本地人工清除M2M终端设备的接入密码和基础密钥时，M2M终端设备必须对该操作进行本地鉴权，只有鉴权通过才能进行后续操作。鉴权内容包括：

- 身份鉴权，是指进行本地人工清除M2M终端设备的接入密码和基础密钥操作必须拥有相应的操作权限。
- 终端设备状态鉴权，是指M2M终端设备的工作状态必须是异常或告警状态，正常工作或登录状态下即使身份鉴权通过也无法进行本地人工设置。

本地人工设置仅能够清除M2M终端设备的接入密码和基础密钥及其相关设置参数，不能本地人工重新设置M2M终端设备的接入密码和基础密钥。

本地人工清除M2M终端设备的接入密码和基础密钥及其相关设置参数后，M2M终端设备必须重新向M2M平台申请本终端设备的接入密码和基础密钥。由于安全信息已经被清除，M2M平台无法正常验证M2M终端设备的合法性，因此，M2M终端设备必须通过注册报文上报相关信息，申请获得新的基础密钥和会话密钥。M2M平台接收该上报信息之后，重新为该终端设备设置接入密码和基础密钥及其相关设置参数。

4.4.5. 安全验证失败的处理流程

- 当报文的接入密码摘要验证失败时：

  1. 若是请求报文，接收方直接丢弃安全验证失败的报文，不做任何响应。
  2. 若是应答报文，接收方直接丢弃安全验证失败的报文，并认为未接收到应答方的应答报文，超时未接收到应答报文则进入超时重发流程。

- 当报文的解密失败时：可采用两种方式之一进行处理：
  1. 在报文头中设置标识位标志解密失败。
  2. 在应答报文的响应码中返回解密失败（响应码不进行加密。）

4.4.6. 通信过程中的异常与重发

M2M终端设备与M2M平台之间的通信不可避免会发生丢包或超时的情况。因此，为保证数据的可靠传输，协议采用丢包重发机制。根据丢包和超时发生的频度，M2M终端设备与M2M平台之间的通信异常可分为两种情况：偶发异常和通信故障。

4.4.6.1. 偶发异常

偶发异常主要指M2M终端设备与M2M平台之间的通信过程中的偶然的、突发的、非持续的丢包情况。图31给出了偶发异常情况下M2M终端设备与M2M平台之间数据丢包与重发的交互过程。

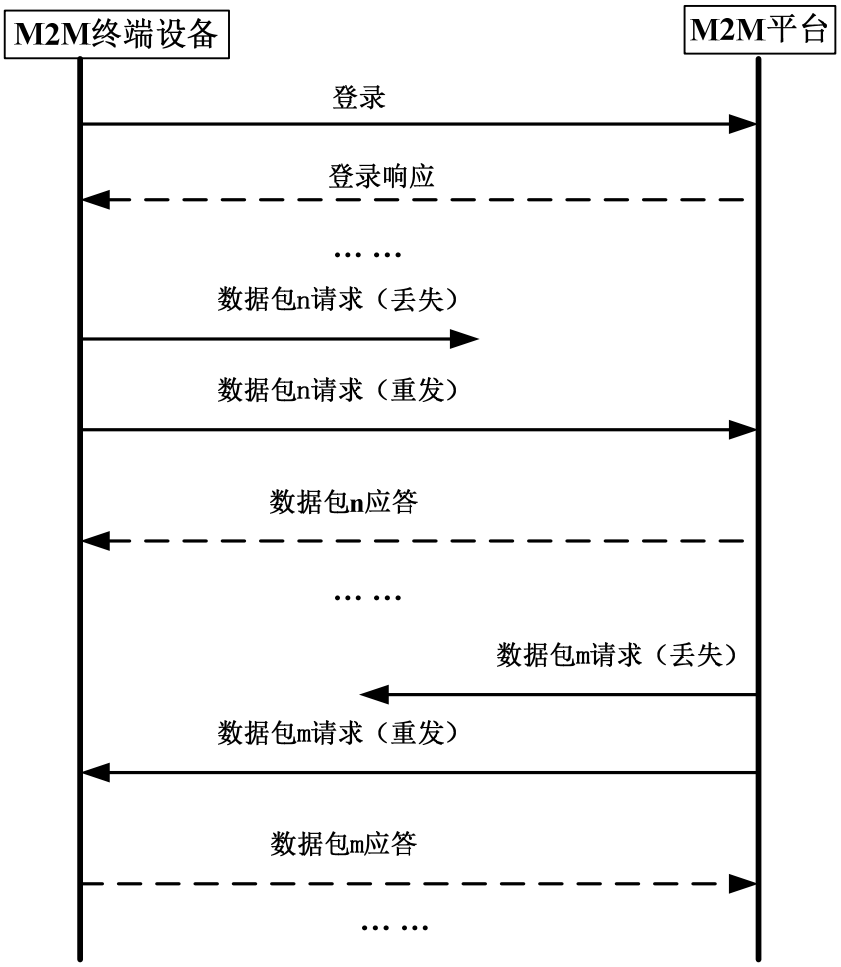


图 31 偶然的丢包和重发

通信过程中，丢包情况大致有以下两种：

1.请求方的数据请求报文在通信过程中未到达应答方就已经丢失，此时请求方应在应答超时后决定是否重发；（由预先设置的参数决定）。

2．当请求方的数据请求报文到达应答方后，应答方动作后的应答报文在传送过程中未到达请求方即丢失，则请求方应在应答超时后决定是否重发。（由预先设置的参数决定）。

应答方无需关心请求方的报文内容，只需拷贝该报文的流水号到应答包中。对于收到两个报文实际内容相同的数据包，此时应答方由于不关心序号是多少，处理的机制完全按照两个不同的数据包处理，即都作回复处理，这样做可简化处理。如图32所示：

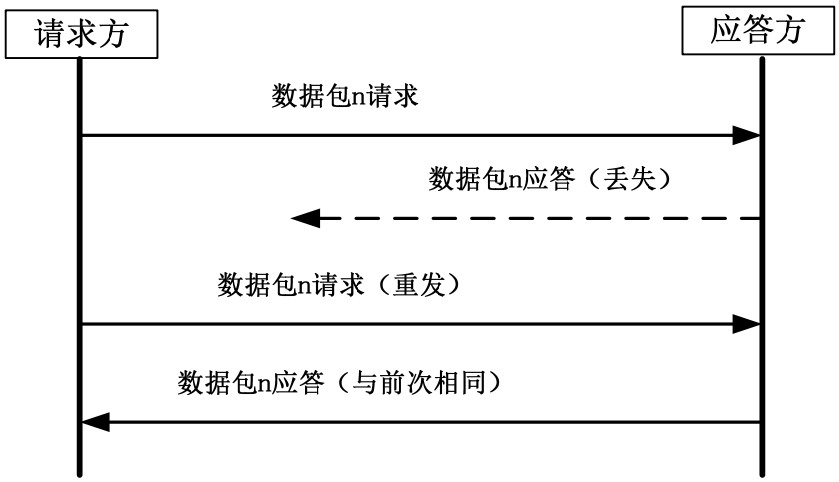


图 32 对于数据包重复接收的处理

4.4.6.2. 通信故障

当丢包、超时连续出现或比率较大时，则M2M终端设备与M2M平台之间处于通信故障状态。先检测出通信故障的一方(即可能是M2M终端设备，也可能是M2M平台)向已知的对端IP发送LOGOUT报文，并通过LOGOUT报文的状态字(参见LOGOUT定义中的“2:通信故障断开”)报告通信故障。LOGOUT由请求方发送后，请求方收到LOGOUT_ACK或接收超时后，释放该连接。如果LOGOUT报文或LOGOUT_ACK报文在传送的过程中丢失，请求方在接收LOGOUT_ACK超时后，释放该连接，而应答方也可在无数据包传输一段时间后检测出该连接无效。然后M2M终端设备可以根据自身需要决定是否再重新发起连接。

LOGOUT报文是一个可选数据包，在应用条件许可的情况下，可以进行LOGOUT交互，从而有助于M2M平台对终端设备通信状态的管理。如果应用不具备该条件，可不支持LOGOUT过程。

5. M2M 平台与 M2M 应用间协议

5.1. 协议交互机制

5.1.1. M2M 应用向 M2M 平台登陆

交互流程如图33所示。

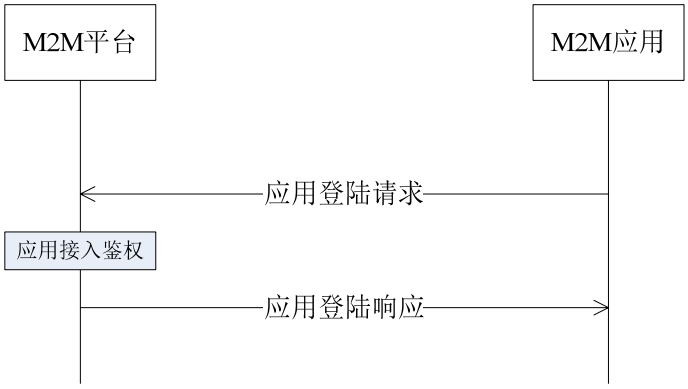


图 33 M2M应用登陆交互流程

流程描述如下：

（1） M2M应用向M2M平台发送应用登陆请求；

（2） M2M平台接收到请求后，对登陆请求进行鉴权，鉴权成功后向M2M应用返回应用登陆响应；

（3） M2M应用登陆成功后，可以进行后续报文的交互。

5.1.2. M2M 应用向 M2M 平台登出

交互流程如图34所示。

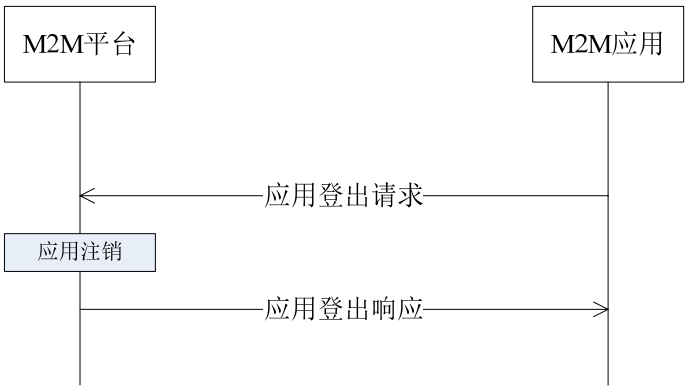


图 34 M2M应用登出交互流程

流程描述如下：

（1） M2M应用向M2M平台发送应用登出请求；

（2） M2M平台接收到请求后，设置M2M应用为登陆状态，返回响应；

（3） M2M应用登陆成功后，对于长连接方式，M2M应用和M2M平台均可断开连接。

5.1.3. 终端设备信息查询

M2M应用可以查询M2M终端设备的各种信息。该查询功能可以分为两种：一种是M2M平台转发查询，即通过M2M平台转发，由M2M平台对M2M终端设备进行实时信息查询，M2M再将查询结果返回给应用。另一种是M2M平台直接查询，即M2M应用直接读取M2M平台上存储的M2M终端设备的信息。

M2M终端设备信息查询应支持批量查询的功能。

5.1.3.1. M2M 平台转发查询

交互流程如图35所示。

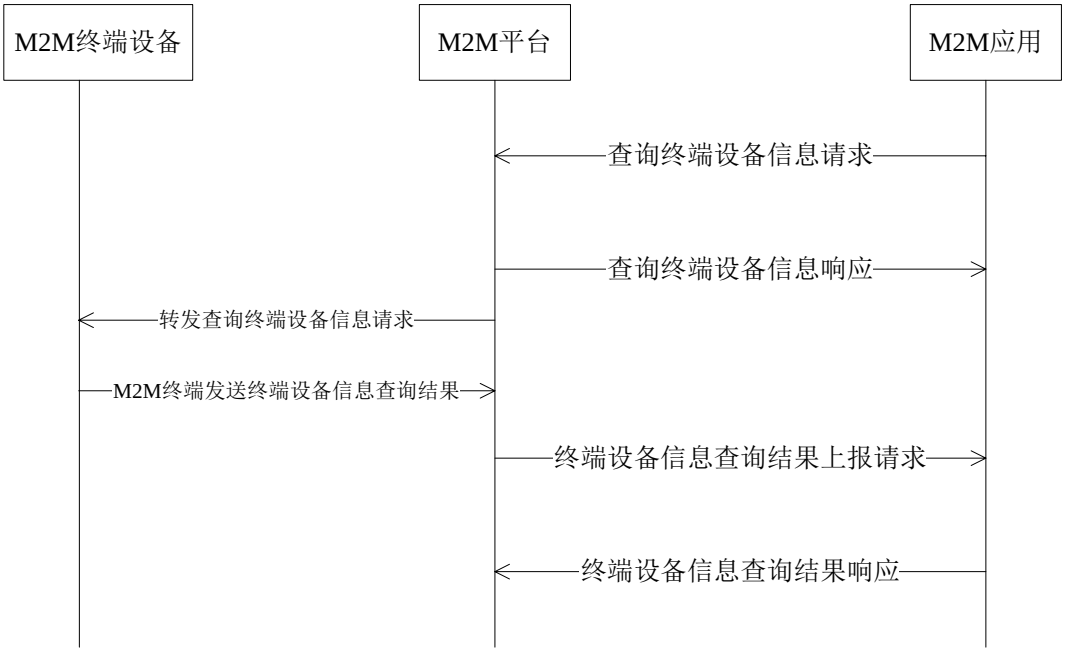


图 35 查询M2M终端设备信息交互流程（M2M平台转发查询）

交互流程描述如下：

（1） M2M应用向M2M平台发送查询终端设备信息请求;

（2） M2M平台反馈查询终端设备信息响应到M2M应用，该应答只表示收到该请求，并转发请求到指定终端设备；

（3） M2M终端设备向M2M平台上报终端设备信息查询结果，M2M平台通过终端设备信息查询结果上报请求到M2M应用；

（4） M2M应用返回响应。

5.1.3.2. M2M 平台直接查询

交互流程如图36所示。

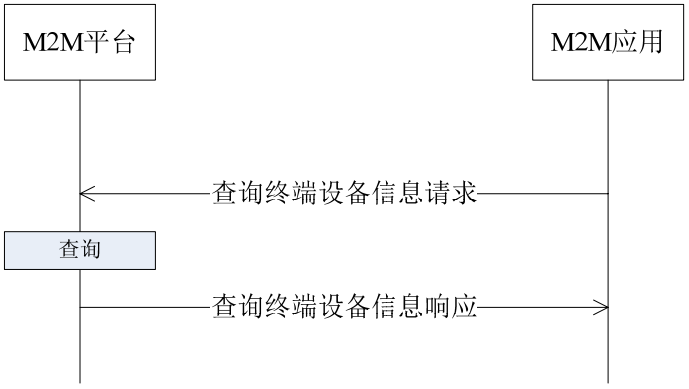


图 36 查询终端设备信息交互流程（M2M平台直接查询）

流程描述如下：

（1） M2M应用向M2M平台发送查询终端信息请求；

（2） M2M平台接收到请求后，相应配置信息、统计信息(如果统计信息存储在平台数据库中，则M2M平台向数据库发起查询请求)、监控信息，通过响应报文将查询到的信息返回给M2M应用。

5.1.4. 终端设备状态告警

交互流程如图37所示。

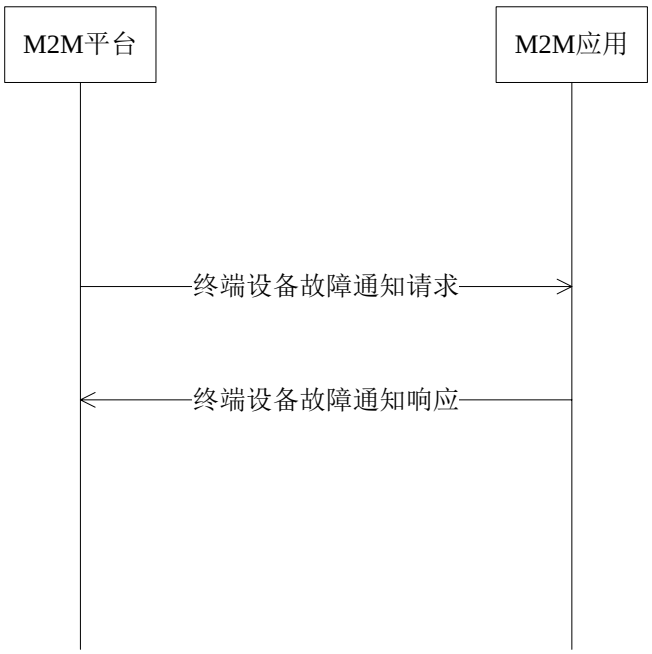


图 37 M2M终端设备状态告警交互流程

交互流程描述如下：

（1） M2M平台检测到M2M终端设备状态异常，向M2M应用发送终端设备故障通知请求；

（2） M2M应用返回响应。

5.1.5. 终端设备通知

终端设备通知分为终端设备注册通知，终端设备登录通知和终端设备登出通知。

5.1.5.1. 终端设备注册通知

交互流程如图38所示。

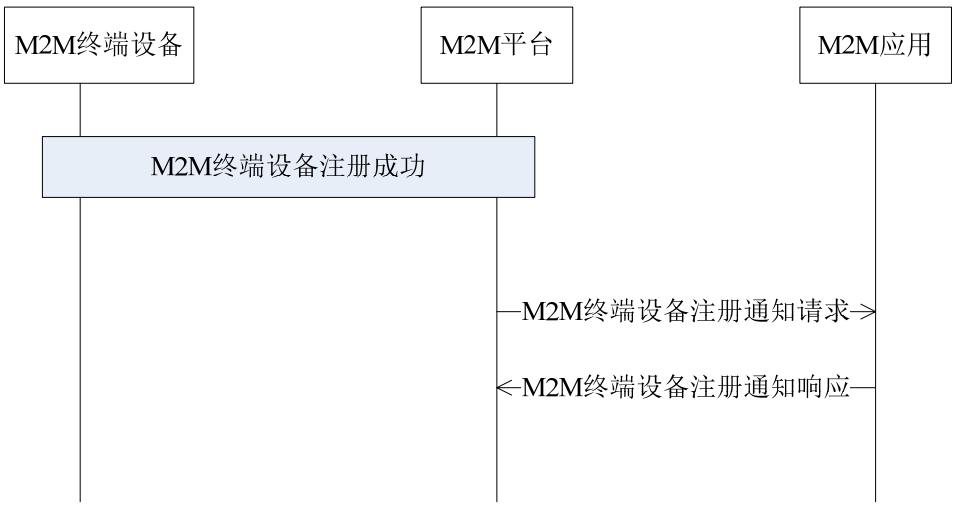


图 38 M2M终端设备注册交互流程

交互流程描述如下：

（1） M2M终端设备在M2M平台注册成功后，M2M平台向M2M应用发送终端设备注册通知请求；

（2） M2M应用返回响应。

5.1.5.2. 终端设备登录通知

交互流程如图39所示。

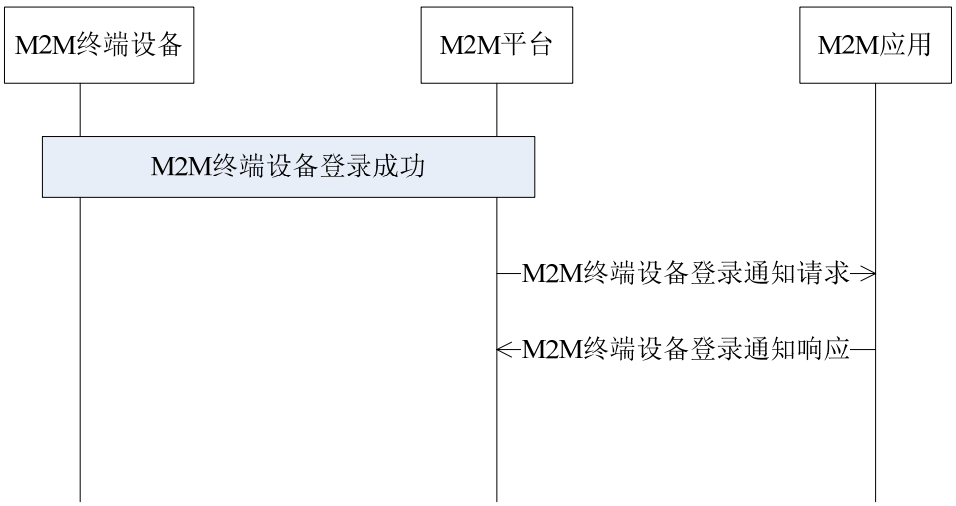


图 39 M2M终端设备登录通知交互流程

交互流程描述如下：

（1） M2M终端设备在M2M平台登录成功后，M2M平台向M2M应用发送终端设备登录通知请求；

（2） M2M应用返回响应。

5.1.5.3. 终端设备登出通知

M2M终端设备在M2M平台退出登录时，M2M平台向对应的M2M应用发送该M2M终端设备的退出登录信息。交互流程如图40所示。

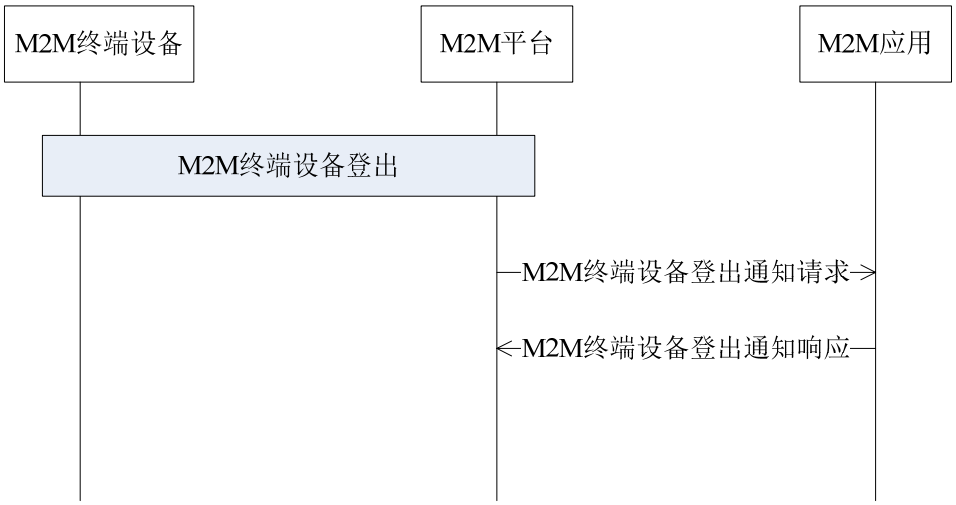


图 40 M2M终端设备登出通知交互流程

交互流程描述如下：

（1） M2M终端设备在M2M平台登录退出后，M2M平台向M2M应用发送终端设备登录退出通知请求；

（2） M2M应用返回响应。

5.1.6. 远程控制终端设备

交互流程如图41所示。

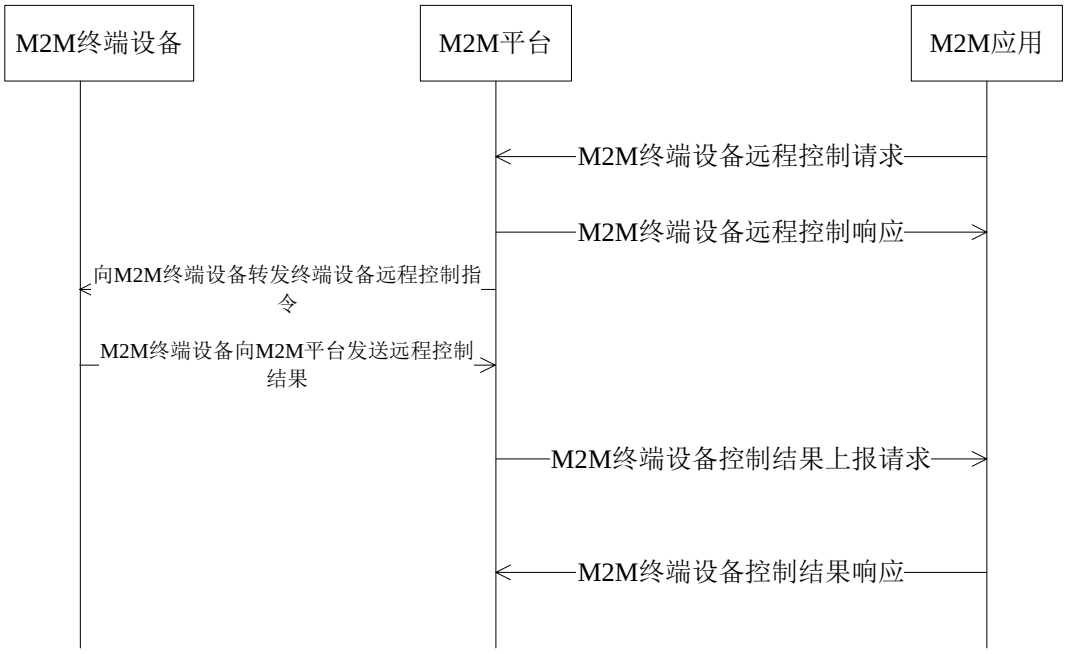


图 41 M2M终端设备远程控制流程

交互流程描述如下：

（1）M2M应用向M2M平台发送M2M终端设备远程控制请求；

（2）M2M平台接收请求后返回响应，该应答只表示收到该请求，M2M平台向M2M终端设备转发远程控制指令；

（3）M2M终端设备执行远程控制指令，向M2M平台上报远程控制指令执行结果；

（4）M2M平台向M2M发起M2M终端设备远程控制结果上报请求；

（5）M2M应用返回响应。

另外，不是所有的远程控制都对M2M应用开放。M2M应用只能操作对其开放的远程控制功能。

5.1.7. 终端设备远程更新

交互流程如图42所示。

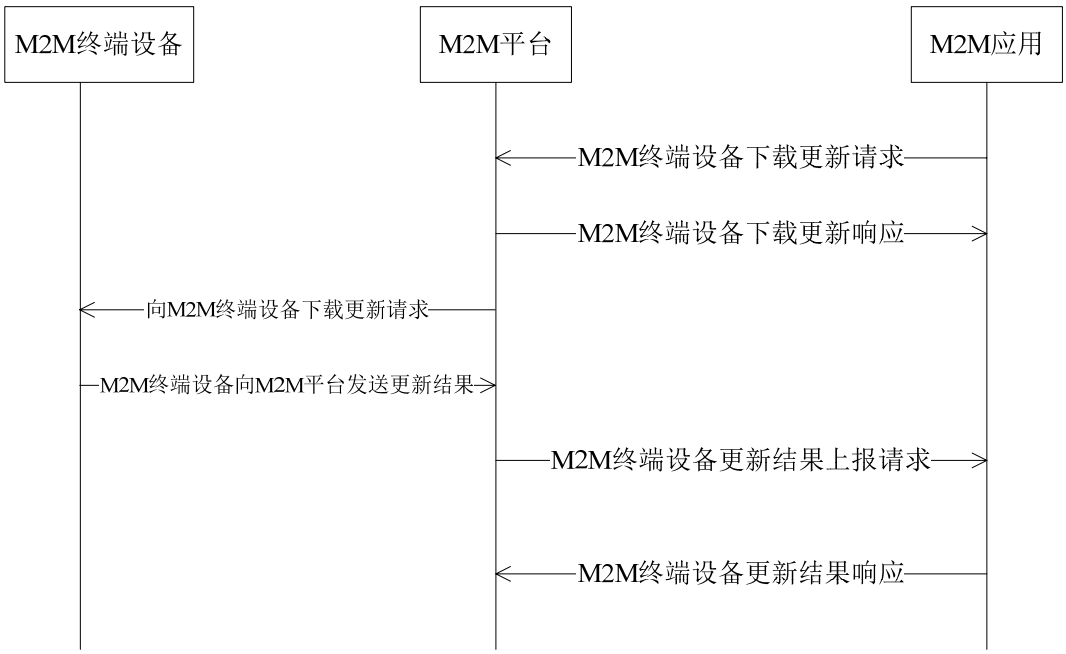


图 42 M2M终端设备远程更新流程

交互流程描述如下：

（1）M2M应用向M2M平台发送M2M终端设备下载更新请求；

（2）M2M平台接收请求后返回响应，M2M平台向M2M终端设备转发下载更新请求；

（3）M2M终端设备下载更新请求，向M2M平台上报下载更新结果；

（4）M2M平台向M2M应用发起M2M终端设备更新结果上报请求；

（5）M2M应用返回响应。

5.1.8. 链路检测

交互流程如图43所示。

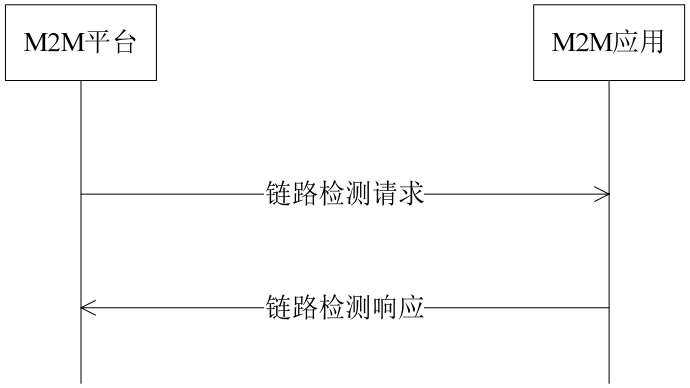


图 43 链路检测交互流程

交互流程描述如下：

（1）M2M平台定时向M2M应用发送链路检测请求；

（2）M2M应用接收到请求后返回链路检测响应。

5.1.9. 业务数据上传和下发

见4．3．11的相关内容。

5.1.10. 安全参数设置

交互流程如图44所示。

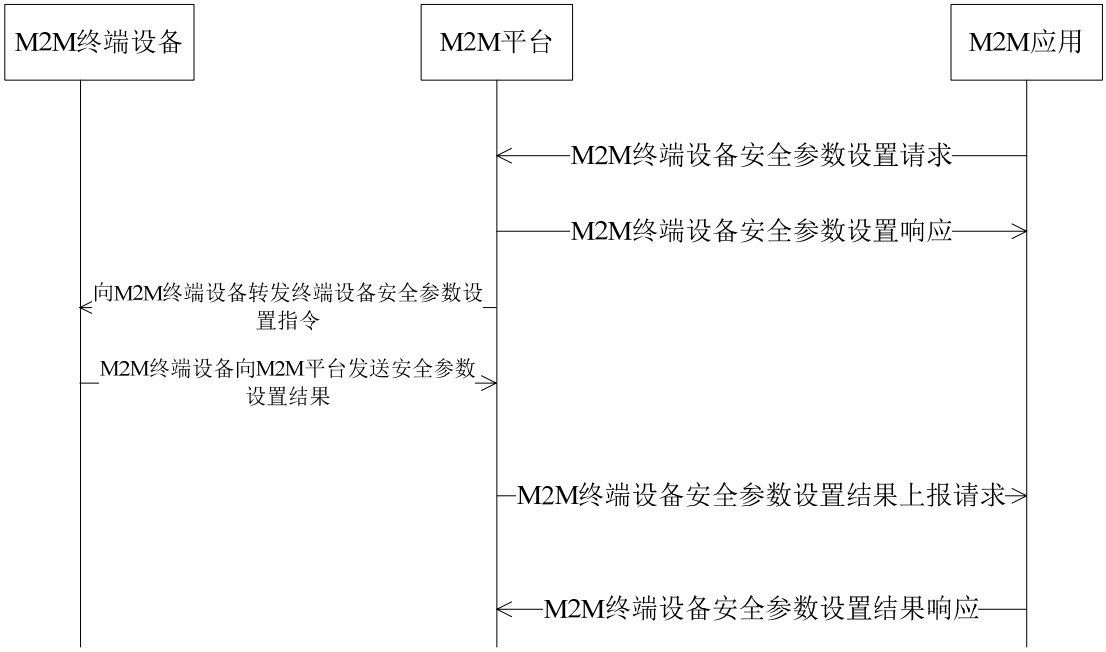


图 44 M2M终端设备安全参数设置流程

交互流程描述如下：

（1） M2M应用向M2M平台发起M2M终端设备安全参数设置请求；

（2） M2M平台接收并处理请求，返回响应；

（3） M2M平台向M2M终端设备转发安全参数设置指令；

（4） M2M终端设备执行安全参数设置指令，向M2M平台上报安全参数设置结果；

（5） M2M平台向M2M应用转发安全参数设置结果，发起安全参数设置结果上报请求；

（6） M2M应用返回响应。

5.1.11. 终端设备参数设置

终端设备参数设置可以分为两类：M2M应用设置终端参数和终端设备请求参数配置。

5.1.11.1. M2M 应用设置终端参数

交互流程如图45所示。

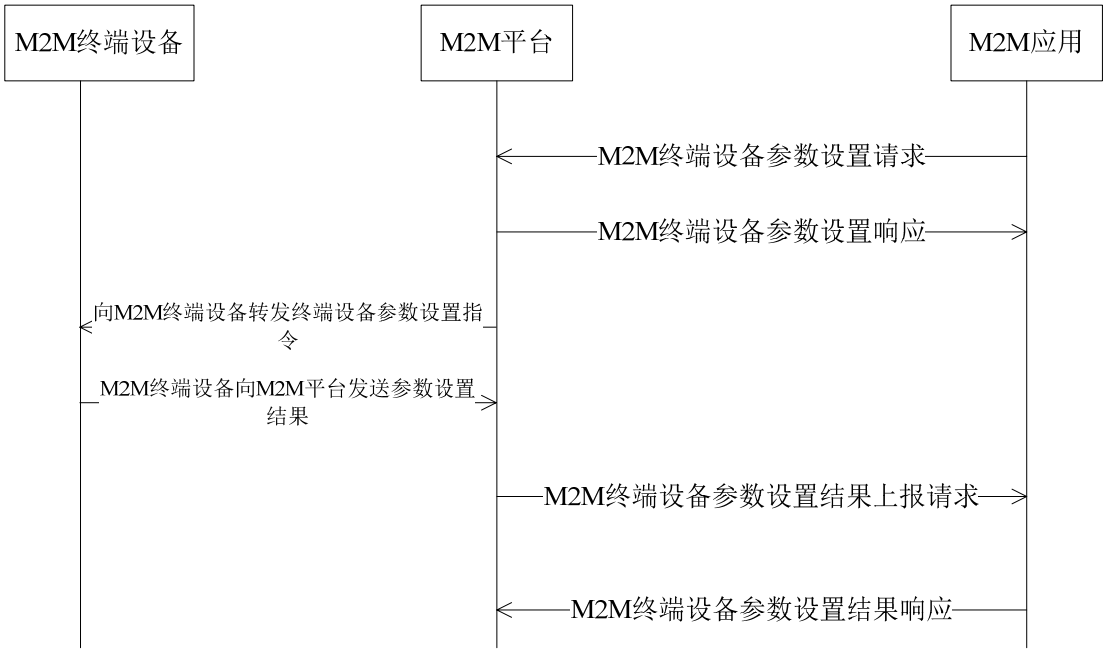


图 45 M2M应用设置终端设备参数流程

交互流程描述如下：

（1） M2M应用向M2M平台发起M2M终端设备安全参数设置请求；

（2） M2M平台接收并处理请求，返回响应；

（3） M2M平台向M2M终端设备转发参数设置指令；

（4） M2M终端设备执行参数设置指令，向M2M平台上报参数设置结果；

（5） M2M平台向M2M应用转发参数设置结果，发起参数设置结果请求；

（6） M2M应用返回响应。

5.1.11.2. 终端设备请求参数设置

交互流程如图46所示。

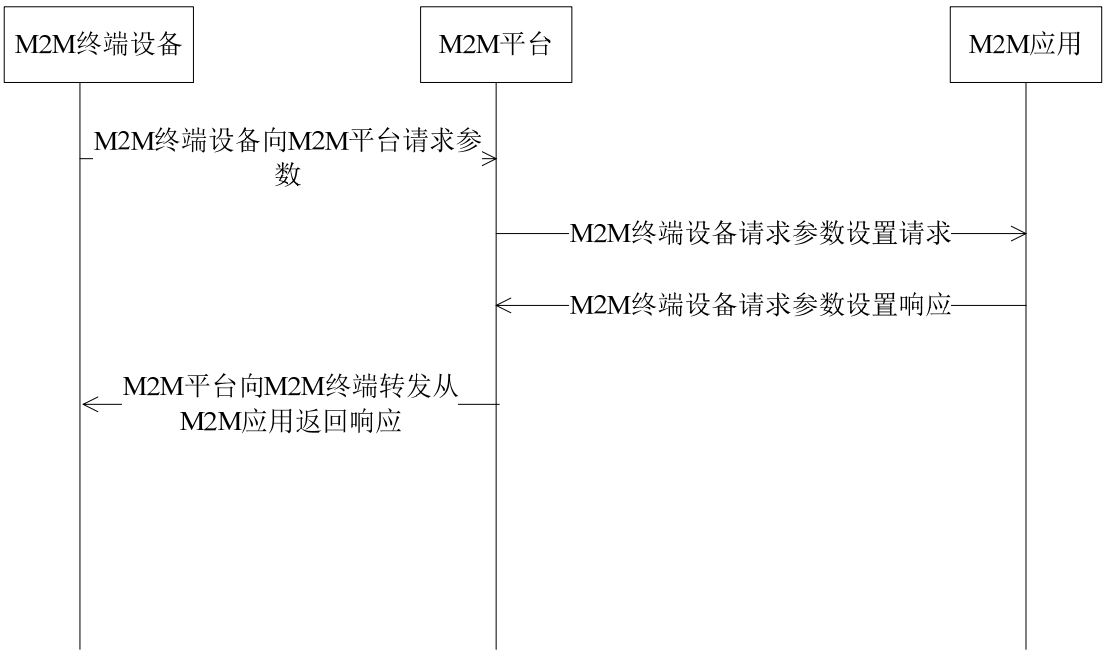


图 46 M2M终端设备请求参数设置交互流程

交互流程描述如下：

（1） M2M终端设备向M2M平台请求终端参数设置，M2M平台向M2M应用发起终端设备请求参数设置请求；

（2） M2M应用终端参数信息通过响应报文返回给M2M平台；

（3） M2M平台转发终端参数信息到M2M终端设备。

5.1.12. 终端设备上报信息

交互流程如图47所示。

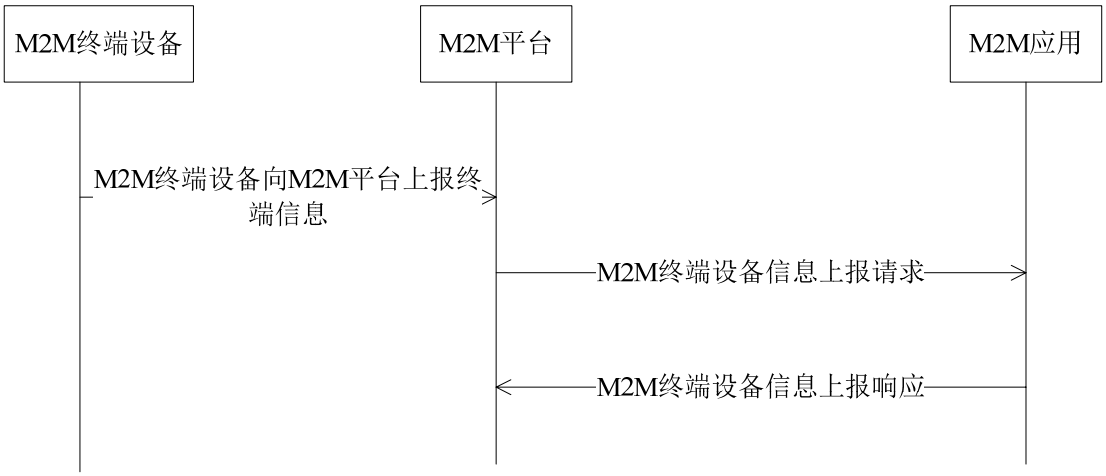


图 47 M2M终端设备信息上报交互流程

交互流程描述如下：

（1） M2M终端设备向M2M平台上报告警信息、配置信息和统计信息，M2M平台向M2M应用发起终端设备终端设备信息上报请求，转发信息；

（2） M2M应用接收并处理请求，向M2M平台返回终端设备信息上报响应。

5.1.13. 基本密钥过期通知

交互流程如图48所示。

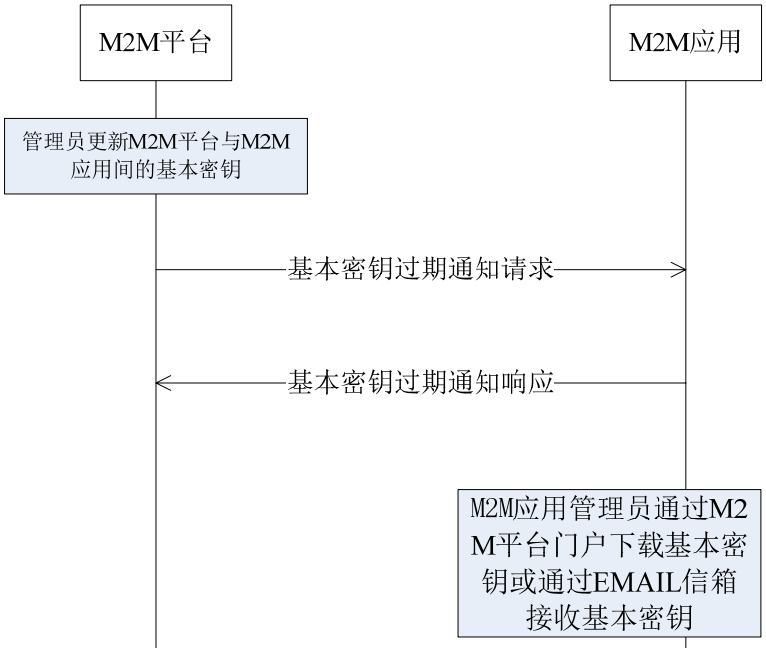


图 48 基本密钥过期通知交互流程

交互流程描述如下：

（1） M2M平台的系统管理人员修改M2M平台和M2M应用间通信的基本密钥,M2M平台向M2M应用发起基本密钥过期通知请求；

（2） M2M应用接收并处理请求，向M2M平台返回基本密钥过期通知响应；

（3） M2M应用管理员应通过M2M平台的门户下载基本密钥或通过EMAIL信箱接收基本密钥。

5.2. 协议安全机制

5.2.1. 数据安全性

M2M平台与M2M应用之间的交互消息均要求携带摘要字段，摘要字段将消息头、消息体、用户名、密码作为输入。

其中用户名和密码由M2M平台为M2M应用分配，M2M应用发往M2M平台的消息以及M2M平台发往M2M应用的消息，均要求用上述算法计算摘要。

M2M应用和M2M平台的交互包含两种密钥：

1. 基础密钥，不同的M2M应用由M2M平台分配不同的基础密钥；M2M平台负责统一分配和保存所有M2M应用密钥。M2M应用的密钥通过Email的方式由M2M平台发送给各M2M应用。

2. 会话密钥，M2M应用与M2M平台的每次会话均有M2M平台分配会话密钥。一次会话只允许持续一定的时间，如果超出该时间，M2M应用必须重新登录，分配新的会话密钥。否则M2M平台将拒绝M2M应用的消息。

基础密钥用于M2M应用向M2M平台登录启动新会话时加密消息体，以及M2M平台返回会话密钥时用于加密消息体。M2M应用需要先向M2M平台登录，登录消息包含M2M平台分配的用户名和密码，并用基础密钥加密（3DES算法）。M2M平台为本次会话分配会话密钥，并用基础密钥加密后返回给M2M应用。然后在会话中，双方用会话密钥加密和解密消息体。

消息交互流程如图49：

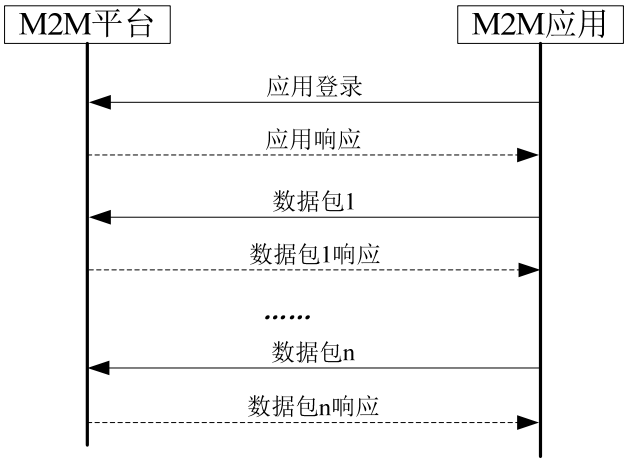


图 49 M2M应用与M2M平台的消息交互

M2M应用首先向M2M平台进行登录，由M2M平台分配并返回会话密钥。在后续的消息交互的数据包中，双方通过会话密钥加密消息体。

5.2.2. 网络安全性

M2M平台接口采用如下的手段保证和M2M应用之间通信的网络安全：IP鉴权及业务ID控制列表。

1. M2M应用接入M2M平台时需提供其业务系统出访IP和URL（根据其业务特性确定）；
2. M2M平台为M2M应用的每一个业务分配一个全局唯一的业务ID；
3. M2M平台侧防火墙配置安全策略，只有有效的IP和业务ID才能够访问M2M平台；
4. M2M应用端配置相应策略，以拒绝非M2M平台的接口调用；
5. 建议M2M应用和M2M平台之间采用VPN通道。

附录 A
（资料性附录）
M2M 终端设备与 M2M 平台之间的协议报文结构

M2M终端设备与M2M平台之间的协议报文由报文头和报文体构成。其结构如图50所示。

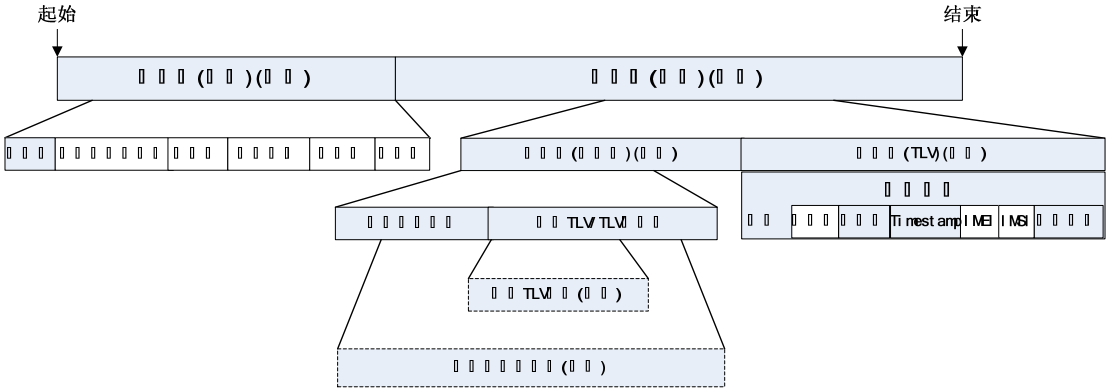


图 50 协议报文的结构图

1） 报文头结构

表A-1 报文头结构

	字段	长度(字节)	备注
报文头	报文总长度	2	
	终端设备序列号	16	
	报文协议版本	2	
	命令类型代码	2	Command ID
	报文流水号	4	从0x00000000到0xFFFFFFFF
	保留字	2	

报文字段说明：

- 报文总长度：整个报文的长度；对于承载同一信息的报文，带有摘要体的报文长度要比不携带摘要体的报文长度多20个字节。
- 终端设备序列号：终端设备的唯一标识，由平台统一分配管理。
- 报文协议版本：标识报文发送方使用的报文协议版本，接收方可根据该编号进行相应的处理或拒绝。协议版本用两个字节表示，高字节作为主版本号，低字节作为次版本号。版本号均为二进制表示的数字，例如2.1版本表示为00000010 00000001。
- 命令类型代码：标识该报文所要执行或应答的监控管理命令，如：远程配置、下载更新、数据采集等，即Command ID。
- 报文流水号：唯一标识发送方发出的每一次报文请求。接收方回复请求时，将该流水号原样返回。发送方各自维护自己的流水号(从0x00000000至0xFFFFFFFF)，每发出一次请求，下一次报文请求的流水号自动循环递增，当流水号达到0xFFFFFFFF时，下一个报文的流水号循环重新回到0x00000000。

- 保留字：保留字由两个字节构成。通常第一个字节可用于安全标识，第二个字节暂无定义，补0x00。安全标识：用于在报文头中标识该终端设备及报文的相关安全信息，以及对上一报文的安全验证的结果。例如某终端设备支持加密、启用加密、本报文启用接入密码校验、本报文启用加密，且上一报文接入密码验证正确、解密正确、没有遗漏接入密码和加密，则表示为1111 0000 0000 0000。

表A-2 报文头安全标识说明

从高至低的位数(二进制)	描述
终端设备及报文安全标识	
第1位 ■□□□ □□□□	M2M终端设备上行报文中： 本终端设备支持加密标识位 0——不支持 1——支持 M2M平台下行报文中： 无定义，为0
第2位 □■□□ □□□□	M2M终端设备上行报文中： 本终端设备启用加密标识位 0——未启用 1——启用 M2M平台下行报文中： 无定义，为0
第3位 □□■□ □□□□	本报文接入密码校验(摘要体)启用标识 0——未启用 1——启用
第4位 □□□■ □□□□	本报文加密、分包类型标识位 0——未加密或部分加密或未分包 1——完全加密或分包 该标识位用于判断报文中的固定参数部分是否携带固定参数，即固定参数是否被放于完全加密体或分包体的TLV中。
上一报文的安全验证结果标识	
第5位 □□□□ ■□□□	上一报文接入密码校验结果标识位 0——正确 1——错误
第6位 □□□□ □■□□	上一报文是否遗漏摘要体标识位 0——否 1——是 该标识用于接收方判断接收到的报文是不是需要携带接入密码以验证其来源的真实性。若遗漏则意味着该报文存在安全风险，有可能截获后再仿冒发回。
第7位 □□□□ □□■□	上一报文解密结果标识位 0——正确 1——错误
第8位	上一报文内存溢出标识位。

□□□□ □□□■	0——未溢出 1——溢出 ● 用于报文接收方标识接收到的上一报文是否报文长度超过其处理能力。 ● 当报文长度超过接收方内存空间或处理能力时，接收方将原报文的报文头作为报文内存溢出通知返回报文发送方，但必须更改其安全标识的内存溢出标识位。 ● 当报文发送方接收到接收方返回的报文内存溢出通知后，若发送的上一报文是请求报文，则减少该报文中承载的TLV或采用分包机制再重新发送；若发送的上一报文是应答报文，则必须采用分包机制重发上一报文。

2) 报文体结构

报文体由内容体和摘要体构成。

2.1) 内容体

内容体一般由固定参数部分和可变TLV/TLV部分组构成。固定参数部分的格式是各类报文所独有的，不同类型的报文其固定参数部分也不完全相同，某些类型的报文甚至缺省固定参数部分。

内容体可以通过数据加密以保证其在传输过程中的安全性。对于内容体的加密，既可以对整个内容体进行加密，也可以对某个或某几个TLV进行单独加密；而加密结果也以特定的TLV在报文中表示。

2.2) 摘要体

摘要体是一个可选的TLV，用于报文完整性和来源身份合法性的验证。其V值示例格式如下：

V(Value)=加密函数(报文头+内容体+Timestamp+IMEI+IMSI+分配给终端设备的接入密码)

其中：

报文头：报文头部分，28字节长度；

内容体：报文体中内容体部分，不定长度；

Timestamp：4字节长度，每次逻辑连接时由M2M平台生成一个时间戳(注册请求报文及注册应答报文等连接建立前的报文固定为0x00000000)；

IMEI：存储于通信模组中的国际移动设备识别码；

IMSI：存储于SIM卡中的国际移动用户识别码；

分配给终端设备的接入密码：M2M平台下发M2M终端设备的安全密码。

3) 四种类型报文的区别

根据报文是否采用安全机制，可将报文为四类：普通报文、接入安全验证报文、部分加密报文、完全加密报文。四种类型报文的区别如表A-3所示：

表A-3 报文类型

项目	报文头	报文体	
		内容体	摘要体

普通报文			
有/无	有	可选	无
加密	无加密	无加密	/
格式	未启用安全标识		/
接入安全验证报文			
有/无	有	可选	必选
加密	无加密	无加密	无加密
格式	启用安全标识		TLV T=0xE021 L=0x0010 V=加密函数(报文头+内容体+Timestamp+IMEI+IMSI+接入密码)
部分加密报文			
有/无	有	必选	必选
加密	无加密	部分TLV加密	无加密
格式	启用安全标识	加密部分为TLV T=0xE043 L=不定长 V=加密算法(某个或某几个TLV)	TLV T=0xE021 L=0x0010 V=加密函数(报文头+内容体+Timestamp+IMEI+IMSI+接入密码)
完全加密报文			
有/无	有	必选	必选
加密	无加密	整个内容体完全加密	无加密
格式	启用安全标识	整个内容体为一个TLV T=0xE042 L=不定长 V=加密算法(全部内容体)	TLV T=0xE021 L=0x0010 V=加密函数(报文头+内容体+Timestamp+IMEI+IMSI+接入密码)

附录 B
（资料性附录）
M2M 终端设备与 M2M 平台之间的协议交互机制

1） M2M终端设备注册

1.1）M2M终端设备首次注册

1.1.1） 配置安全机制且未预置接入密码和基础密钥的M2M终端设备注册中

M2M平台分配终端设备序列号的注册报文格式为：

REGISTER						REGISTER		
	8 0		0x0008			OPERATION 0x00	IMEI	IMSI

M2M终端设备预置终端设备序列号的注册报文格式为：

REGISTER						REGISTER		
	8 0		0x0008			OPERATION 0x01	IMEI	IMSI

注册成功的报文格式为：

REGISTER_ACK						REGISTER_ACK	
	上报的原序列号		0x8008			RESULT 0x00	TERMINAL ID 分配/预置的终端序列号

注册失败的报文格式为：

REGISTER_ACK						REGISTER_ACK	
	上报的原序列号		0x8008			RESULT 0x02~0x08	TERMINAL ID 上报的原序列号

M2M终端设备注册成功，M2M平台通过短信下发该M2M终端设备的接入密码和基础密钥的报文格式为：

SECURITY_CONFIG						SECURITY_CONFIG						
			0x000E			OPERATION 0x00	TLV 0xE025	TLV 0xE027	TLV 0xE028	TLV 0xE02A	TLV( ) 0xE036	TLV( ) 0xE038

M2M终端设备在规定的时间内，利用接入密码发起首次登录，成功登录则完成注册。无须会话密钥的登录报文格式为：

LOGIN						LOGIN			
			0x0001		X X 1 0 0 0 0 0		CRC32	TLV	TLV 0xE021

需要会话密钥的登录报文格式为：

LOGIN						LOGIN				
			0x0001		1 1 1 0 0 0 0 0		CRC32	TLV	TLV 0xE03A	TLV 0xE021

1.1.2) 配置安全机制且预置接入密码和基础密钥的 M2M 终端设备注册

仅预置接入密码的M2M终端设备注册报文格式为：

REGISTER□ □ □						REGISTER□ □ □					
□ □ □	□ □ □ □ □ □ □ □ *后8位不全为0*	□ □ □ □	□ □ □ □ ***0x0008***	□ □ □	□ □ □	OPERATION ***0x03***	TLV ***0xE026***	TLV ***0xE029***	TLV ***0xE03A***	IMEI	IMSI

预置接入密码和基础密钥的M2M终端设备注册报文格式为

REGISTER□ □ □						REGISTER□ □ □					
□ □ □	□ □ □ □ □ □ □ □ *后8位不全为0*	□ □ □ □	□ □ □ □ ***0x0008***	□ □ □	□ □ □	OPERATION ***0x03***	TLV ***0xE026***	TLV ***0xE029***	TLV ***0xE03A***	IMEI	IMSI

注册成功的报文格式为：

REGISTER_ACK□ □ □						REGISTER_ACK□ □ □	
□ □ □	□ □ □ □ □ □ □ □ *预置的终端序列号*	□ □ □ □	□ □ □ □ ***0x8008***	□ □ □	□ □ □	RESULT ***0x09***	TERMINAL ID *预置的终端序列号*

注册失败的报文格式为：

REGISTER_ACK□ □ □						REGISTER_ACK□ □ □	
□ □ □	□ □ □ □ □ □ □ □ *预置的终端序列号*	□ □ □ □	□ □ □ □ 0x8008	□ □ □	□ □ □	RESULT ***0x02~0x08, 0x0A~0x0F***	TERMINAL ID *预置的终端序列号*

1.2） M2M终端设备变更映射关系

若IMSI变化，M2M终端设备发送变更映射关系请求的报文格式：

REGISTER□ □ □						REGISTER□ □ □			
□ □ □	□ □ □ □ □ □ □ □	□ □ □ □	□ □ □ □ ***0x0008***	□ □ □	□ □ □	OPERATION ***0x02***	□ IMEI	□ IMSI	□ □ □ TLV ***0xE021(□ IMEI□ □ IMSI)***

注意：此时摘要体中Timestamp固定为0x00000000。

映射关系变更成功返回的应答报文格式为：

REGISTER_ACK□ □ □						REGISTER_ACK□ □ □		
□ □ □	□ □ □ □ □ □ □ □	□ □ □ □	□ □ □ □ ***0x8008***	□ □ □	□ □ □	RESULT ***0x01***	TERMINAL ID	□ □ □ TLV ***0xE021(原IMEI、原IMSI)***

注意：此时摘要体中Timestamp固定为0x00000000。

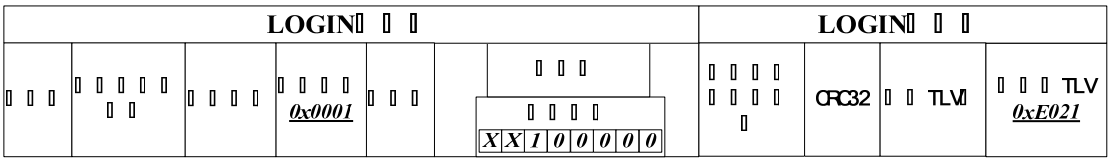
通过摘要体的接入安全验证，但映射关系变更失败返回的应答报文格式为：

REGISTER_ACK□ □ □						REGISTER_ACK□ □ □		
□ □ □	□ □ □ □ □ □ □ □	□ □ □ □	□ □ □ □ ***0x8008***	□ □ □	□ □ □	RESULT ***0x02~0x08***	TERMINAL ID	□ □ □ TLV *0xE021(原IMEI、原IMSI)*

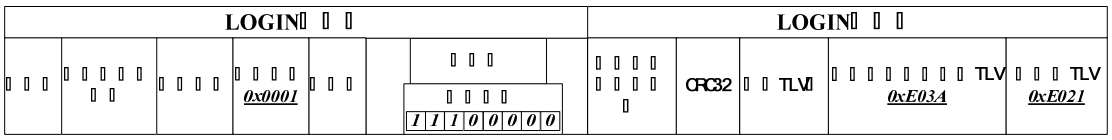
注意：此时摘要体中Timestamp固定为0x00000000。

2） 终端设备登陆

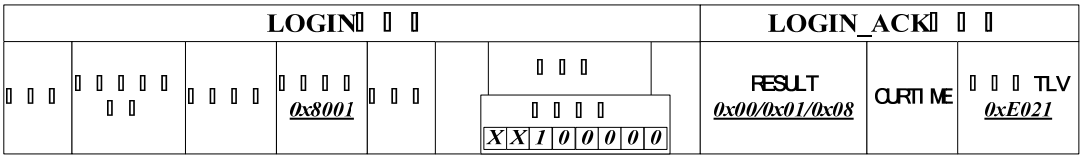
M2M终端设备向M2M平台发送登录请求，无须会话密钥的登录请求报文格式为：



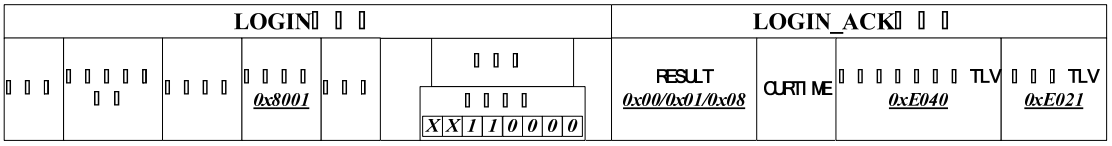
M2M 终端设备向 M2M 平台发送登录请求，需要会话密钥的登录请求报文格式为：



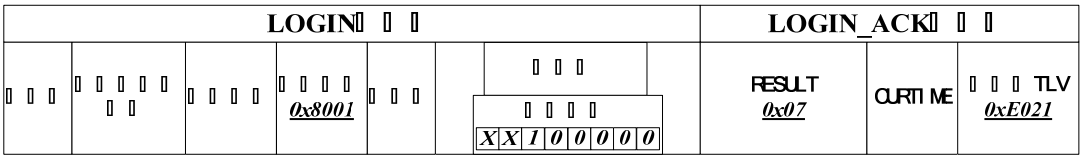
无须会话密钥的登录成功应答报文格式为：



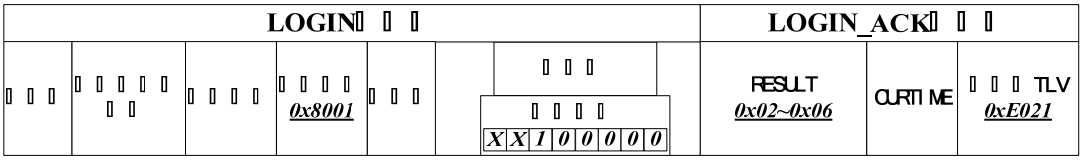
需要会话密钥的登录成功应答报文格式为：



登录成功但基础密钥校验失败的应答报文格式为：

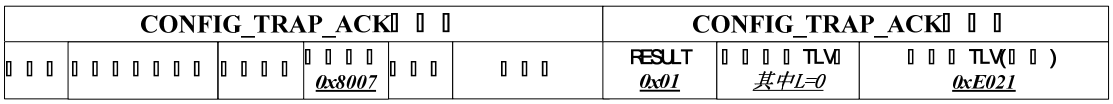


登录失败应答报文格式为：



3) 终端设备上报

当M2M平台不支持M2M终端设备上报的TLV时，其返回失败应答的报文格式为：



4) M2M终端设备信息提取

M2M平台向M2M终端设备实时提取信息的报文格式为：

CONFIG_TRAP_ACK□ □ □						CONFIG_TRAP_ACK□ □ □		
□ □ □	□ □ □ □ □ □ □ □	□ □ □ □	□ □ □ □ *0x8007*	□ □ □	□ □ □	RESULT *0x01*	□ □ □ □ TLV□ *其中L=0*	□ □ □ TLV(□ □) *0xE021*

M2M终端设备返回失败应答的报文格式为：

CONFIG_GET_ACK□ □ □						CONFIG_GET_ACK□ □ □		
□ □ □	□ □ □ □ □ □ □	□ □ □ □	□ □ □ □ *0x8005*	□ □ □	□ □ □	RESULT *0x01*	□ □ □ □ TLV□ *其中L=0*	□ □ □ TLV(□ □) *0xE021*

5） 参数配置

5.1）终端设备请求参数配置

M2M终端设备向M2M平台请求参数的报文格式为：

CONFIG_REQ□ □ □						CONFIG_REQ□ □ □	
□ □ □	□ □ □ □ □ □ □	□ □ □ □	□ □ □ □ *0x000A*	□ □ □	□ □ □	□ □ □ TLV□ *其中L=0*	□ □ □ TLV(□ □) *0xE021*

M2M平台返回M2M终端设备请求参数的应答报文格式为：

CONFIG_REQ_ACK□ □ □						CONFIG_REQ_ACK□ □ □		
□ □ □	□ □ □ □ □ □ □	□ □ □ □	□ □ □ □ *0x800A*	□ □ □	□ □ □	RESULT *0x00*	□ □ □ □ □ TLV□	□ □ □ TLV(□ □) *0xE021*

当M2M平台不支持M2M终端设备请求参数的TLV时，其返回失败应答的报文格式为：

CONFIG_REQ_ACK□ □ □							CONFIG_REQ_ACK□ □ □		
□ □ □	□ □ □ □ *0x800A*	□ □ □	□ □ □ □	□ □ □ □	□ □ □	□ □ □ □ □ □ □	RESULT *0x01*	□ □ □ □ TLV□ *其中L=0*	□ □ □ TLV(□ □) *0xE021*

当M2M终端设备接收到M2M平台返回的请求参数后，若其本地参数与M2M平台返回的参数一致，则无须应用；否则应立即应用。若应用参数，M2M终端设备无须重启，则应用后立即向M2M平台上报其应用配置结果，其报文格式如下：

CONFIG_TRAP□ □ □							CONFIG_TRAP□ □ □		
□ □ □	□ □ □ □ *0x0007*	□ □ □	□ □ □ □	□ □ □ □	□ □ □	□ □ □ □ □ □ □	□ □ □ □ □ □ □ □ □ □ □ □ TLV *0x4010*	□ □ □ □ □ □ CRC32 TLV *0x4012*	□ □ □ TLV(□ □) *0xE021*

M2M终端设备需要重启时，在应用参数前必须向M2M平台发起退出登录以更新M2M平台下发参数请求，其报文格式如下：

LOGOUT□ □ □						LOGOUT□ □ □	
□ □ □	□ □ □ □ □ □ □ □	□ □ □ □	□ □ □ □ *0x0002*	□ □ □	□ □ □	LOGOUTREASON *0x07*	□ □ □ TLV(□ □) *0xE021*

5.2）M2M平台设置M2M终端参数

M2M平台向M2M终端设备设置的参数需要终端设备立即应用，则必须在报文中携带平台参数配置选项的TLV 0x4009且其值为0x01，其报文格式如下：

CONFIG_SET□ □ □						CONFIG_SET□ □ □		
□ □ □	□ □ □ □ □ □ □ □	□ □ □ □	□ □ □ □ *0x0006*	□ □ □	□ □ □	□ □ □ □ □ □ TLV *0x4009*	□ □ □ □ TLV□	□ □ □ TLV(□ □) *0xE021*

当M2M平台设置的参数中，有M2M终端设备不支持的TLV时，其返回失败应答的报文格式为：

CONFIG_SET_ACK						CONFIG_SET_ACK		
			0x8006			RESULT 0x01	TLV 其中L=0	TLV( ) 0xE021

若M2M终端设备因正在运行业务，无法立即应用参数，且M2M平台不强制M2M终端设备立即应用，则M2M终端设备需要使用CONFIG_TRAP和0x4010定义的TLV组以心跳间隔向M2M平台上报暂缓应用参数配置信息，直至可以应用参数配置为止。其报文格式如下：

CONFIG_TRAP						CONFIG_TRAP	
			0x0007			TLV 0x4010	TLV( ) 0xE021

M2M终端设备应用参数，若无须重启，则应用后立即向M2M平台上报其应用配置结果，其报文格式如下：

CONFIG_TRAP						CONFIG_TRAP		
			0x0007			TLV 0x4010	CRC32 TLV 0x4017	TLV( ) 0xE021

若M2M终端设备需要重启，则在应用参数前必须向M2M平台发起退出登录以更新M2M平台下发参数请求，其报文格式如下：

LOGOUT						LOGOUT	
			0x0002			LOGOUTREASON 0x07	TLV( ) 0xE021

然后，M2M终端设备必须接收到M2M平台返回的退出登录应答后，才能应用配置参数。M2M终端设备重新登录后，应向M2M平台上报其应用配置结果。

6） 安全参数设置

SIM卡对M2M终端设备安全认证相关参数操作的相关报文如下：

（1） M2M平台设置M2M终端设备绑定或取消绑定当前SIM卡的报文格式：

SECURITY_CONFIG						SECURITY_CONFIG		
			0x000E			OPERATION 0x00	SIM TLV 0xE00D	TLV 0xE021

（2） M2M平台设置但未改变M2M终端设备的启用SIM卡PIN1码的报文格式：

明文(短信方式)：

SECURITY_CONFIG						SECURITY_CONFIG		
			0x000E			OPERATION 0x00	SIM PIN TLV 0xE001	TLV 0xE021

密文：

SECURITY_CONFIG						SECURITY_CONFIG		
			0x000E			OPERATION 0x00	TLV (0xE043) SIM PIN TLV 0xE001	TLV 0xE021

（3） M2M平台设置并改变M2M终端设备的启用SIM卡PIN1码的报文格式：

明文(短信方式)：

SECURITY_CONFIG						SECURITY_CONFIG			
			0x000E			OPERATION 0x00	SIM PIN1 TLV 0xE001	SIM PIN1 TLV 0xE003	TLV 0xE021

密文：

SECURITY_CONFIG						SECURITY_CONFIG			
			0x000E			OPERATION 0x00	TLV (0xE043) SIM PIN1 TLV 0xE001	TLV (0xE043) SIM PIN1 TLV 0xE003	TLV 0xE021

（4） M2M平台以明文读取M2M终端设备的SIM卡密码及其启用状态报文格式：

SECURITY_CONFIG						SECURITY_CONFIG			
			0x000E			OPERATION 0x02	SIM PIN1 TLV 0xE002 L=0	SIM PIN1 TLV 0xE003 L=0	TLV 0xE021

返回应答格式：

SECURITY_CONFIG						SECURITY_CONFIG			
			0x000E			OPERATION 0x02	SIM PIN1 TLV 0xE002	SIM PIN1 TLV 0xE003	TLV 0xE021

（5） M2M平台以密文读取M2M终端设备的SIM卡密码及其启用状态报文格式：

SECURITY_CONFIG						SECURITY_CONFIG			
			0x000E			OPERATION 0x01	SIM PIN1 TLV 0xE001 L=0	SIM PIN1 TLV 0xE003 L=0	TLV 0xE021

返回应答格式：

SECURITY_CONFIG_ACK						SECURITY_CONFIG_ACK			
			0x800E			RESULT 0x00	TLV (0xE043) SIM PIN1 TLV 0xE001	TLV (0xE043) SIM PIN1 TLV 0xE003	TLV 0xE021

（6） M2M平台设置SIM卡密码启用与否报文格式：

SECURITY_CONFIG						SECURITY_CONFIG		
			0x000E			OPERATION 0x00	SIM PIN1 TLV 0xE003	TLV 0xE021

附录 C
（资料性附录）
M2M 平台与 M2M 应用之间的协议描述

1） 协议接口描述

本协议支持两种连接方式：

1、 基于HTTP的标准WEB Service方式。M2M应用和M2M平台采用WSDL（Web Services Description Language）来对接口进行描述。WSDL是用来定义Web服务的属性以及如何调用它的一种XML语言。一个完整的WSDL服务描述是由一个服务接口和一个服务实现文档组成的。通过查阅Web服务的WSDL文档，开发者可以知道Web提供了哪些方法和如何用正确的参数调用他们。因为WSDL包含了对服务接口的完整描述，所以可以使用它来创建能简化服务访问的存根，该存根为一段Java代码（假设使用Java），它自动生成了访问Web服务的类。如果需要访问Web服务，只需调用该类中对应的方法即可，而不用在客户端程序中再写入配置信息。要求通信双方作为WEB Service服务端时，应实现HTTP会话的超时机制。即一定时间内，如果客户端没有新的HTTP请求，则服务端主动断开连接。会话维持的时间要求可配置。

2、 长连接。M2M应用可以选择采用长连接和M2M平台交互，以提高效率。消息格式的定义和WEB Service方式一致。

2） 消息结构

2.1) WEB Service方式消息格式

所有的协议数据单元PDU由如下表的消息头和消息体组成：

PDU组成	描述
Message Header	消息头
Message BODY	消息体
Message HASH	消息摘要

消息头、消息体和摘要体在xml中的表现形式如下：

```
<?xml version=”1.0” encoding=”UTF-8”?>
<MsgName >
  <Head>
    <Attribute1>消息头属性一</Attribute1>
    <Attribute2>消息头属性二</Attribute2>
    <Attribute3>消息头属性三</Attribute3>
  </Head>
  <BODY>加密后的消息体</BODY>
  <HASH>消息摘要</HASH>
</MsgName>
```

未加密的消息体也是一个完整的xml文件，如下例所示：

```
<?xml version="1.0"?>
<BODY>
  <Attribute1>消息体属性一</Attribute1>
  <Attribute2>消息体属性二</Attribute2>
  <Attribute3>消息体属性三</Attribute3>
</BODY>
<HASH>消息摘要</HASH>
```

本标准报文为文本格式，对于二进制内容，应进行BASE64编码。
加密后的消息体通过BASE64编码放入BODY标签。

2.2) 长连接方式消息格式

PDU组成	**描述**
Message Length	消息长度
Message Header	消息头
Message BODY	消息体
Message HASH	消息摘要，计算方法为： 加密函数(消息头+3DES(消息体)+用户名+密码)

附录 D
（资料性附录）
M2M 终端设备与 M2M 平台之间命令代码定义

消息类型	Command_id	说明
LOGIN	0x0001	M2M终端设备向M2M平台发送的登录包
LOGIN_ACK	0x8001	M2M平台向M2M终端设备发送的连接登陆应答
LOGOUT	0x0002	M2M终端设备与M2M平台之间发送的断开连接
LOGOUT_ACK	0x8002	M2M终端设备与M2M平台之间发送的断开连接应答
HEART_BEAT	0x0003	M2M终端设备向M2M平台发送的维持过程连接
HEART_BEAT_ACK	0x8003	M2M平台向M2M终端设备发送的维持过程连接回应
TRANSPARENT_DATA	0x0004	可以双向传输的透明数据
TRANSPARENT_DATA_ACK	0x8004	对可以双向传输的透明数据包的应答
CONFIG_GET	0x0005	M2M平台向M2M终端设备发送的读取M2M终端设备的配置信息
CONFIG_GET_ACK	0x8005	M2M终端设备向M2M平台发送的应答包，上报配置信息
CONFIG_SET	0x0006	M2M平台向M2M终端设备发送的设置命令包或者设置参数
CONFIG_SET_ACK	0x8006	M2M终端设备向M2M平台发送的设置应答
CONFIG_TRAP	0x0007	M2M终端设备向M2M平台上报的TRAP信息，包括告警信息。
CONFIG_TRAP_ACK	0x8007	M2M平台对M2M终端设备上报告信息的应答。
REGISTER	0x0008	M2M终端设备向M2M平台发送的注册包
REGISTER_ACK	0x8008	M2M平台向M2M终端设备发送的注册应答
CONFIG_REQ	0x000A	M2M终端设备向M2M平台发起请求配置参数
CONFIG_REQ_ACK	0x800A	M2M平台向M2M终端设备发送的请求配置参数的应答
REMOTE_CTRL	0x000B	M2M平台向M2M终端设备发送的远程控制包
REMOTE_CTRL_ACK	0x800B	M2M终端设备向M2M平台发送的远程控制应答包
DOWNLOAD_INFO	0x000C	M2M平台发起下载更新通知
DOWNLOAD_INFO_ACK	0x800C	M2M终端设备对M2M平台发起下载更新通知的应答

消息类型	Command_id	说明
FILE_REQ	0x000D	M2M终端设备向M2M平台发送文件下载请求
FILE_REQ_ACK	0x800D	M2M平台向M2M终端设备发送文件下载请求应答
SECURITY_CONFIG	0x000E	M2M终端设备安全参数设置请求
SECURITY_CONFIG_ACK	0x800E	M2M终端设备安全参数设置请求应答
TRANSPARENT_CMD	0x000F	可以双向传输的透明命令请求
TRANSPARENT_CMD_ACK	0x800F	可以双向传输的透明命令请求的应答

附录 E
（资料性附录）
TLV 说明

a) TLV格式说明

名称	长度(字节)	取值范围	说明
TAG	2	0x0001~0x0FFF	配置参数相关内容
		0x1001~0x1FFF	软件升级相关内容
		0x2001~0x2FFF	终端设备统计相关内容
		0x3001~0x3FFF	终端设备监控相关内容
		0x4001~0x4FFF	控制参数相关内容
		0x5001~0x7FFF	平台预留
		0x8001~ 0xDFFF	厂家预留
		0xE001~0xFFFF	安全控制相关内容
Length	2	SMS： 0x0000 ~ 0x0064 分组域承载： 0x0000 ~ 0x0400	表示 value 长度，不包括标签、长度的内容
Value	SMS： 0~100 分组域承载技术： 0~1024		内容

b) TAG配置参数相关内容

标签值	数据类型	数据长度(字节)	标签说明
0x0001	字符串	≤16	分组域承载网络拨号号码
0x0002	字符串	≤32	M2M平台网络接入点名称(APN)
0x0003	字符串	≤32	分组域承载网络拨号用户名
0x0004	字符串	≤32	分组域承载网络拨号密码
0x0005	字符串	≤20	短信中心号码
0x0006	字符串	不定长	业务应用服务器的传输密钥
0x0007	字符串	≤20	M2M平台短信特服号
0x0008	字符串	≤64	M2M平台的URL地址
0x0009	数字	4	M2M平台的IP地址
0x000A	数字	4	M2M平台的端口 第1~2字节为UDP端口，第3~4字节为TCP端口。当端口值为0x0000时无效，即：若value值为0x14730000则表示只设置UDP端口，没有设置TCP端口。
0x000B	字符串	≤20	业务应用短信中心号码
0x000C	字符串	≤64	业务应用服务器的URL地址
0x000D	数字	4	业务应用服务器IP地址不用

标签值	数据类型	数据长度(字节)	标签说明
0x000E	数字	4	业务应用服务器端口 第1~2字节为UDP端口，第3~4字节为TCP端口。当端口值为0x0000时无效，即：若value值为0x14730000则表示只设置UDP端口，没有设置TCP端口。不用
0x000F			保留（备用业务应用服务器的URL地址） 备用通道做报警
0x0010	数字	4	DNS地址
0x0011	数字	4	心跳间隔(PERIOD)，单位：秒 0x0000——不发送心跳 默认心跳间隔为30秒
0x0012	字符串	≤20	业务应用非结构化补充数据业务短信特服号码
0x0013	字符串	≤32	M2M应用网络接入点名称(APN)
0x0014	数字	4	备用DNS地址
0x0025	数字	不定长	M2M终端设备需与M2M平台登录同步的核心配置参数TLV的TAG值，按TAG升序排列
0x0026	数字	2	短信接收超时时间，单位：秒
0x0027	数字	1	最大登录重试次数参数 0x01~0xFE——1~254次 0x00——不重试 0xFF——一直重试
0x0028	数字	不定长	默认的终端设备所属EC或SI的业务代码EC Code
0x0029	数字	1	最大注册重试次数，0～255，0表示一直重试
0x002A	数字	8	登录失败重试间隔参数 第1~4字节：登录失败最小重试间隔，单位：秒 第5~8字节：登录失败最大重试间隔，单位：秒
0x002B	数字	8	注册失败重试间隔参数 第1~4字节：注册失败最小重试间隔，单位：秒 第5~8字节：注册失败最小重试间隔，单位：秒
0x002C	数字	不定长	用户扩展参数类TLV的TAG标识，按TAG升序排列。 该TLV定义了用户使用了哪些自定义参数类TLV，且该类自定义TLV，终端设备掉电/断电不易失。
0x002D	数字	不定长	用户扩展状态类、临时数据类TLV的TAG标识，按TAG升序排列。 该TLV定义了用户使用了哪些自定义状态类、临时数据类TLV对于该类TLV，终端设备掉电/断电不保存。
0x002E	字符串	不定长	MSISDN号，即手机号。
个性化参数			

标签值	数据类型	数据长度(字节)	标签说明
0x0101	数字	2	本地串口波特率设置，Value取值范围： 0——默认波特率9600 1——300 2——600 3——1200 4——2400 5——4800 6——9600 7——19200 8——38400 9——57600 10——115200 < 255， 定制波特率 其他无效
0x0102	数字	1	本地串口工作方式数据位： Value取值范围： 0：8位 5、6、7、8分别表示5、6、7、8bit 默认为8bit 其余保留
0x0103	数字	1	本地串口停止位，Value取值范围： 0 表示1位停止位， 1表示1.5位停止位 2表示2位停止位 其余保留，缺省为0
0x0104	数字	1	本地串口校验: 0表示无校验 1表示奇校验 2表示偶校验 3表示mark 4表示space 其余保留
0x0105	数字	2	本地串口扫描间隔， Value取值范围(单位100ms)： 1~100 其余无效
0x0106	数字	2	保留

标签值	数据类型	数据长度(字节)	标签说明
0x0107	数字	4xN	非注册与登录数据报文应答超时参数 第1字节：通信方式 0x01:SMS 0x02、0x03、0x05:分组域承载 0x04:MMS 第2字节：时间单位 0x00：秒 0x01：分 0x02：小时 第3~4字节：超时门限值
0x0108	数字	1	非注册与登录传输失败最大允许重发次数， value取值范围(单位 次)：1~254 0x00——不重发 0xFF——一直重发
0x0109	数字	3	设置门限：1-速度，2-载重量，3-电流，其它-保留给集团客户定义，门限值：2字节，M2M终端设备检测到数据超过门限后将发送告警，如车辆速度等。

c) 软件下载升级相关内容

标签值	数据类型	数据长度(字节)	标签说明
0x1000	数字	1	升级方式下载协议 0x00——M2M应用通信协议 0x01——HTTP 0x02——FTP 其它待定
0x1001	字符串	不定长	下载升级服务器的URL地址 即DOWNLOAD_INFO中的DownAddURL字段
0x1002	字符串	不定长	下载升级服务器的IP地址
0x1003	数字	2	下载升级服务器端口
0x1004	字符串	不定长	下载升级服务器登陆密码
0x1005	字符串	不定长	下载文件的版本号
0x1006	数字	4	下载文件的总长度
0x1007	数字	2	整个下载文件的CRC16校验
0x1008	数字	4	整个下载文件的CRC32校验
0x1009	数字	2	升级事务TRANS_ID，8位16进制数
0x100A	字符串	12	下载文件的发布日期 YYYYMMDDHHMM，如：200808031736 YYYY——年，如：2008 MM——月，如：08 DD——日，如：03 HH——小时，采用24小时制，如：17 MM——分钟，如：36

0x100B	数字	1	强制立即下载并升级参数，用于M2M平台或第三方下载升级服务器控制M2M终端设备是否立即强制下载并升级。 0x00——非强制，由M2M终端设备自行决定在何时发起下载及升级过程 0x01——强制，无论M2M终端设备目前是否在执行其它操作，必须发起下载，下载完成后并立即升级
0x100C	字符串	8	当前软件本版号

d) 终端设备统计相关内容

标签值	数据类型	数据长度(字节)	标签说明
累加统计条件参数			
0x2001	数字	1	累加统计信息上报条件参数： 0x00——定时立即上报，即M2M终端设备依据TLV 0x2002所设置的定时时间向M2M平台上报统计数据； 0x01——周期上报，即M2M终端设备以TLV 0x2003所设置的时间间隔周期性向M2M平台上报统计数据； 0x02——每月业务首次使用上报，即M2M终端设备每月首次向M2M应用系统发送数据时，向M2M平台上报统计数据； 其他保留。 注： 1. 该TLV通过CONFIG_SET、CONFIG_REQ、CONFIG_GET来进行设置、读取。 2. 控制M2M终端设备通过CONFIG_TRAP上报TLV 0x2004、0x2008~0x200E，以实现累加数据统计上报功能
0x2002	数字	4	定时上报时间(单位：秒) 从1970-1-1 00:00:00到定时上报时刻的秒数
0x2003	数字	4	周期上报的周期值，单位：秒
0x2004	数字	1	本月使用M2M应用业务标志： 0x00——未使用 0x01——使用
0x2005	数字	1	上报后是否清零终端设备统计数据参数 0x00——上报后不清零终端设备统计数据 0x01——上报后清零终端设备统计数据
0x2006	数字	4	开始统计的时间参数 从1970-1-1 00:00:00到开始统计的时刻的秒数。

标签值	数据类型	数据长度(字节)	标签说明
			(1) 如果有该参数，则以此时间作为统计开始的时间。 (2) 如果该参数为全0，即0x00000000，则统计数据的起始时间为执行平台发出清除终端设备统计数据或终端设备依据TLV 0x2005的设置上报完统计数据自动清除原有统计数据后的时间。如果第一次统计(从未清除过终端设备统计数据)为终端设备首次运行时间。 (3) 如果该参数为全F，即0xFFFFFFFF，则终端设备不进行数据统计。
0x2007	数字	4	结束统计的时间 从1970-1-1 00:00:00到结束统计的时刻的秒数。 该参数可选。 (1) 如果有该参数，则以此时间作为统计结束的时间； (2) 如果该参数为全F，即0xFFFFFFFF，则没有统计结束时间；
0x2008	数字	4	终端设备发送短信成功条数(单位：条)
0x2009	数字	4	终端设备发送短信失败条数(单位：条)
0x200A	数字	4	终端设备接收短信条数(单位：条)
0x200B	数字	4	终端设备分组域承载数据通信流量(单位：字节)
0x200C	数字	4	终端设备非结构化补充数据业务成功条数(单位：条)
0x200D	数字	4	终端设备非结构化补充数据业务失败条数(单位：条)
0x200E	数字	4	终端设备接收非结构化补充数据业务条数(单位：条)
分类统计条件参数			
0x2011	数字组合信息	12	短信业务统计设置参数： 启用开关(第1字节)： 0x00——关闭 0x01——开启 统计周期数值(第2~3字节)：0x0000~0xFFFF 统计周期单位(第4字节)： 0x00——无效 0x01——分钟 0x02——小时 0x03——天

标签值	数据类型	数据长度(字节)	标签说明
			0x04——周 0x05——月 0x06——年 周期统计起始时间点(第5~8字节)： 从1970-1-1 00:00:00到当前的秒数 周期统计结束时间点(第9~12字节)： 从1970-1-1 00:00:00到当前的秒数，取0xFFFFFFFF表示无结束统计时间
0x2012	数字组合信息	12	短信业务统计信息自动上报参数： 自动上报启用开关(第1字节)： 0x00——关闭 0x01——开启 上报周期数值(第2~3字节)：0x0000~0xFFFF 上报周期单位(第4字节)： 0x00——无效 0x01——分钟 0x02——小时 0x03——天 0x04——周 0x05——月 0x06——年 周期上报起始时间点(第5~8字节)： 从1970-1-1 00:00:00到当前的秒数 周期上报结束时间点(第9~12字节)： 从1970-1-1 00:00:00到当前的秒数，取0xFFFFFFFF表示无结束上报时间
0x2013	数字组合信息	8×n字节(n最大为90)	M2M交互类短信统计： n条统计记录，各记录之间顺序排序，每条记录格式如下： 时间戳： 4字节，1970-1-1 0:0:0的秒数 短信发送条数：2字节； 短信接收条数：2字节；
0x2014	数字组合信息	8×n字节(n最大为90)	业务交互类短信统计： n条统计记录，各记录之间顺序排序，每条记录格式如下： 时间戳： 4字节，1970-1-1 0:0:0的秒数 短信发送条数：2字节；

标签值	数据类型	数据长度(字节)	标签说明
			短信接收条数：2字节；
0x2015	数字组合信息	12	分组域承载业务统计设置参数： 启用开关(第1字节)： 0x00——关闭 0x01——开启 统计周期数值(第2~3字节)：0x0000~0xFFFF 统计周期单位(第4字节)： 0x00——无效 0x01——分钟 0x02——小时 0x03——天 0x04——周 0x05——月 0x06——年 周期统计起始时间点(第5~8字节)： 从1970-1-1 00:00:00到当前的秒数 周期统计结束时间点(第9~12字节)： 从1970-1-1 00:00:00到当前的秒数，取0xFFFFFFFF表示无结束统计时间
0x2016	数字组合信息	12	分组域承载业务统计信息自动上报参数： 自动上报启用开关(第1字节)： 0x00——关闭 0x01——开启 上报周期数值(第2~3字节)：0x0000~0xFFFF 上报周期单位(第4字节)： 0x00——无效 0x01——分钟 0x02——小时 0x03——天 0x04——周 0x05——月 0x06——年 周期上报起始时间点(第5~8字节)： 从1970-1-1 00:00:00到当前的秒数 周期上报结束时间点(第9~12字节)：

标签值	数据类型	数据长度(字节)	标签说明
			从1970-1-1 00:00:00到当前的秒数，取0xFFFFFFFF表示无结束上报时间
0x2017	数字组合信息	12×n字节(n最大为90)	M2M交互类分组域承载业务流量统计： n条统计记录，各记录之间顺序排序，每条记录格式如下： 时间戳：4字节，1970-1-1 0:0:0的秒数 分组域承载发送字节数：4字节； 分组域承载接收字节数：4字节；
0x2018	数字组合信息	12×n字节(n最大为90)	业务交互类分组域承载流量统计： n条统计记录，各记录之间顺序排序，每条记录格式如下： 时间戳：4字节，1970-1-1 0:0:0的秒数 分组域承载发送字节数：4字节； 分组域承载接收字节数：4字节；
0x2019	数字组合信息	12	非结构化补充数据业务统计设置参数： 启用开关(第1字节)： 0x00——关闭 0x01——开启 统计周期数值(第2~3字节)：0x0000~0xFFFF 统计周期单位(第4字节)： 0x00——无效 0x01——分钟 0x02——小时 0x03——天 0x04——周 0x05——月 0x06——年 周期统计起始时间点(第5~8字节)： 从1970-1-1 00:00:00到当前的秒数 周期统计结束时间点(第9~12字节)： 从1970-1-1 00:00:00到当前的秒数，取0xFFFFFFFF表示无结束统计时间
0x201A	数字组合信息	12	非结构化补充数据业务统计信息自动上报参数： 自动上报启用开关(第1字节)： 0x00——关闭 0x01——开启 上报周期数值(第2~3字节)：0x0000~0xFFFF

标签值	数据类型	数据长度(字节)	标签说明
			上报周期单位(第4字节)： 0x00——无效 0x01——分钟 0x02——小时 0x03——天 0x04——周 0x05——月 0x06——年 周期上报起始时间点(第5~8字节)： 从1970-1-1 00:00:00到当前的秒数 周期上报结束时间点(第9~12字节)： 从1970-1-1 00:00:00到当前的秒数，取0xFFFFFFFF表示无结束上报时间
0x201B	数字组合信息	8×n字节(n最大为90)	M2M交互类非结构化补充数据业务统计： n条统计记录，各记录之间顺序排序，每条记录格式如下： 时间戳： 4字节，1970-1-1 0:0:0的秒数 非结构化补充数据业务发送条数：2字节； 非结构化补充数据业务接收条数：2字节；
0x201C	数字组合信息	8×n字节(n最大为90)	业务交互类非结构化补充数据业务统计： n条统计记录，各记录之间顺序排序，每条记录格式如下： 时间戳： 4字节，1970-1-1 0:0:0的秒数 非结构化补充数据业务发送条数：2字节； 非结构化补充数据业务接收条数：2字节；

e) 终端设备监控相关内容

标签值	数据类型	数据长度(字节)	标签说明
0x3001		2	通信协议版本，第1个字节为主版本号，第2个字节为次版本号，只要主版本匹配即可建立通信过程
0x3002		16	终端设备序列号，唯一标识该M2M终端设备
0x3004		8	终端设备软件版本号
0x3005		4	4字节。上一次心跳延时，单位秒
0x3006		4	4字节，Cellular ID，终端设备所在小区标识(高16位表示LAC，低16位表示CI)
0x3007		1	1字节，本地信号场强，0－100
0x3008		1	终端设备参数初始化通知标识： 0x00——关闭 0x01——启用

标签值	数据类型	数据长度(字节)	标签说明
			用于M2M终端设备通知M2M平台将其除终端设备序列号及注册状态标识之外的所有参数恢复到出厂默认状态。
0x3009	整形	4	系统时间， 当前系统时间：从1970-1-1 00:00:00到当前的秒数
0x300A			保留
0x300B	数字	1	Alarm_Status，1个字节，告警状态： 0x00——正常 0x01——告警
0x300C	数字	1	Alarm_Type，1个字节告警信息类型 0x01——通讯告警 0x02——终端设备硬件告警 0x03——终端设备软件告警
0x300D	数字组合信息	2×n	Alarm_Code，双字，表示告警原因的告警代码，一次告警可上报多个告警原因。。 0x0001——短信方式连接入服务器失败(通讯告警) 0x0002——非结构化补充数据业务方式连接入服务器失败(通讯告警) 0x0003——分组域承载方式连接入服务器失败(通讯告警) 0x0004——分组域承载无法打开(通讯告警) 0x0005——GPS模块故障(终端设备硬件告警) 0x0006——终端设备自检测故障(终端设备硬件告警) 0x0007——短信提交信息超时(通讯告警) 0x0008——终端设备电源故障(终端设备硬件告警) 0x0009——超门限告警(终端设备硬件告警) 0x000A——终端设备升级失败(终端设备软件告警) 0x000B——信号强度弱(终端设备硬件告警) 0x000C——拨号失败(终端设备硬件告警) 0x000D——误码过多(终端设备软件告警) 0x000E——M2M业务平台连接失败(通讯告警) 0x000F——未收到平台服务器的任何数据包 0x0010——与平台协议版本不匹配 0x0011——内存出错 0x0012——应用文件损坏 0x0013——业务应用服务器平台无法访问 0x0014——监控平台无法访问 0x0015——打印机异常 0x0016——扫描枪异常 0x0017——POS刷卡器异常 0x0018——IC卡感应器异常 0x0019——密码小键盘异常

标签值	数据类型	数据长度(字节)	标签说明
			0x001A——外接话机异常 0x001B——升级失败告警 0x001C——短信接收超时 其他——系统保留 其值的形式为：0x0001000A000B
0x300E	数字组合信息	不定长	RestoreAlarm，为已恢复的故障编码合集，如：0x0001000A000B
0x300F	数字组合信息	不定长	DEVS：终端外设的状态。 外设类型采用2个字节编码，允许扩展，目前系统预留了如下外设编码： 0x0001——PRN：打印机 0x0002——SCAN：扫描枪 0x0003——POS：POS刷卡器 0x0004——IC：IC卡感应器 0x0005——KEY：密码小键盘 本TAG针对终端外设，1为启用，0为禁用，2为故障。值的格式： **VALUE的格式：** 设备ID，2字节 | 1字节，表示启用或禁用
0x3010	数字组合信息	不定长	DEV：终端设备支持的外设： 外设类型采用2个字节编码，允许扩展，目前系统预留了如下外设编码： 0x0001——PRN：打印机 0x0002——SCAN：扫描枪 0x0003——POS：POS刷卡器 0x0004——IC：IC卡感应器 0x0005——KEY：密码小键盘 0x0006——PHONE：外接话机 DEV的值为外设编码的序列，无间隔。 **举例：** 0x000100020003
0x3011	数字	4	4个字节，终端设备上报丢包数
0x3012	数字组合信息	5	M2M终端设备下载、升级文件失败告警 **VALUE的格式：** 左起高位第1~4字节：升级事务ID(DOWNLOAD_INFO.DownAddURL.TRANS_ID) 左起高位第5字节：失败原因 0x00——无法连接下载地址 0x01——终端设备缓存不足无法开始下载 0x02——下载过程中内存溢出 0x03——下载过程中连接超时 0x04——完整的下载文件CRC校验失败 0x05——终端设备升级文件失败

备注：当终端设备检测到终端设备故障，则上报故障信息，当所有故障恢复后才上报终端设备正常信息。

f) 控制参数相关内容

标签值	数据类型	数据长度(字节)	标签说明

标签值	数据类型	数据长度(字节)	标签说明
0x4001	数字	1	控制命令TLV，以REMOTE_CTRL报文下发，用以控制M2M终端设备执行相关操作，定义如下： 0x00——终端设备业务停用(终端设备停止EC应用服务，但保持与M2M平台连接)； 0x01——终端设备业务恢复(终端设备恢复EC应用服务)； 0x02——终端设备重启； 0x03——远程唤醒(终端设备未与M2M平台连接，激活终端设备重新登录M2M平台)； 0x04——上报统计数据(用于M2M平台控制终端设备立即向M2M平台上报TLV 0x2004、0x2008~0x200E中的当前累加统计数据)； 0x05——业务统计累计清零(用于M2M平台控制M2M终端设备立即清除所存储的业务统计数据)； 0x06——上报监控信息(用于M2M平台控制终端设备立即向M2M平台上报所监控的信息)； 0x07——上传业务数据(用于M2M平台控制终端设备立即向业务平台上报业务数据)； 0x08——上报M2M应用连接的通信方式(即0x4005，0x4006)； 0x09——切换APN，由M2M应用切换到M2M平台； 0x0A——恢复出厂设置，除终端设备序列号及注册状态标识之外的所有参数恢复到出厂默认状态。 0x0B——上报核心配置参数(当终端设备收到该命令后通过CONFIG_TRAP上报0x0025定义的核心同步参数)。 0x0C——切换APN，由M2M平台切换到M2M应用； 0x0D——以启用会话密钥加密方式重新登录M2M平台 注： 1. 对于该TLV，M2M平台与终端设备仅作为控制状态参数，无须存储其当前TLV值。

标签值	数据类型	数据长度(字节)	标签说明
0x4002		1	M2M终端设备当前连接M2M平台方式： 0x00——UDP 短连接； 0x01——UDP 长连接； 0x02——TCP 短连接 0x03——TCP 长连接 0x04——SMS 0x05——非结构化补充数据业务
0x4003		1	数据传送方式 0x00——管理流-业务流并行模式，默认 0x01——管理流-业务流分离模式
0x4005		1	采集(统计、监控、业务)数据传送方式： 0x01——SMS； 0x02——非结构化补充数据业务； 0x03——分组域承载 0x04——其他；
0x4006		2	第1字节表示M2M应用基于IP时的传输层连接模式： 0x00——UDP模式； 0x01——TCP模式； 第2字节表示M2M应用基于IP时的应用层协议： 0x00——透明传输 0x01——HTTP 0x02——FTP 0x03——SOAP 0xA0~0xFF为厂商自定义 此TLV一般用于数据流直接与M2M应用交互的应用
0x4007	BIN_STR	不定长	用户数据标识

标签值	数据类型	数据长度(字节)	标签说明
0x4008	数字	不定长	未完全加密分包机制参数(分包机制参见附录C)。 第1~2字节——分包事务的TANS_ID，为分包机制发起方临时生成的随机数 第3~4字节——子包总数 第5~6字节——子包序号 第7字节——操作类型 0x00——开始分包交互 0x01——接收方请求第5~6字节定义的子报文 0x02——发起方异常中止分包交互，第5~6字节为异常中止前发送的子报文序号 0x03——接收方异常中止分包交互，第5~6字节为异常中止时接收的子报文序号 第8字节以后——子包所承载的TLV，但摘要体的TLV不能放到该TLV中
0x4009	数字	1	平台参数配置选项： 0x00——非强制执行，终端设备接到后，无须停止一切操作，立即应用参数，可根据其业务暂缓执行 0x01——强制执行，终端设备接到后，停止一切操作，立即应用参数
0x4010		5	终端设备执行平台参数配置(安全参数)、远程控制选项： 第1字节——终端 设备执行平台参数配置的结果 0x00——已经执行 0x01——暂缓执行 0x02——参数应用失败，系统无法正常工作，返回原先配置 第2~5字节——参数配置报文的流水号(注：对于分包交互的参数配置报文，则报文流水号为第一包的报文流水号)
0x4011	数字	0	终端设备应用本地人工配置参数生效上报通知标识，用于M2M终端设备在CONFIG_TRP中通知本终端设备应用了本地人工配置的参数。 该TLV无VALUE值。
0x4012		16	M2M终端设备/EC请求平台转发报文或应用数据的目的终端设备的序列号
0x4013		16	M2M终端设备/EC接收到平台转发报文或应用数据的来源终端设备的序列号
0x4014		不定长	M2M终端设备请求平台转发报文或应用数据的目的EC的代码

标签值	数据类型	数据长度(字节)	标签说明
0x4015		不定长	M2M终端设备收到平台转发报文或应用数据来源的EC的代码
0x4016		不定长	透传的控制命令的固定参数部分
0x4017		4	配置参数TLV的CRC32校验，按TAG的递增排序，用于平台下发终端设备参数配置结果的校验。
0x4021			控制终端设备的外设。 外设类型采用2个字节编码，允许扩展，目前系统预留了如下外设编码： 0x0001——PRN：打印机 0x0002——SCAN：扫描枪 0x0003——POS：POS刷卡器 0x0004——IC：IC卡感应器 0x0005——KEY：密码小键盘 本TAG针对终端外设，1为启用，0为禁用。值的格式： 设备ID，2字节 | 1字节，表示启用或禁用

g) 安全控制相关内容

标签值	数据类型	数据长度(字节)	标签说明
PIN1相关参数TLV (0xE001~0xE003)			
0xE001	字符串	8	SIM PIN1(必须是8位的数字)
0xE002	数字	16	SIM PIN1的安全摘要 加密函数(终端设备序列号+IMEI+IMSI+PIN1) 注：“+”表示字符串首尾连接
0xE003	数字	1	SIM PIN1启用参数，1位16进制数： 0x00——不启用 0x01——启用
PIN2相关参数TLV (0xE004~0xE006)			
0xE004	字符串	8	SIM PIN2(必须是8位的数字)
0xE005	数字	16	SIM PIN2的安全摘要 加密函数(终端设备序列号+IMEI+IMSI+PIN2) 注：“+”表示字符串首尾连接
0xE006	数字	1	SIM PIN2启用参数，1位16进制数： 0x00——不启用 0x01——启用
PUK1相关参数TLV (0xE007~0xE009)			
0xE007	字符串	8	SIM PUK1(必须是8位的数字)
0xE008	数字	16	SIM PUK1的安全摘要 加密函数(终端设备序列号+IMEI+IMSI+PUK1) 注：“+”表示字符串首尾连接

标签值	数据类型	数据长度(字节)	标签说明
0xE009	数字	1	SIM PUK1启用参数，1位16进制数： 0x00——不启用 0x01——启用
PUK2相关参数TLV (0xE00A~0xE00C)			
0xE00A	字符串	8	SIM PUK2(必须是8位的数字)
0xE00B	数字	16	SIM PUK2的安全摘要 加密函数(终端设备序列号+IMEI+IMSI+PUK2) 注：“+”表示字符串首尾连接
0xE00C	数字	1	SIM PUK2启用参数，1位16进制数： 0x00——不启用 0x01——启用
M2M终端设备与SIM卡映射或绑定相关参数TLV			
0xE00D	数字	1	启用SIM卡绑定参数 0x00——不启用 0x01——启用 0x02——M2M平台清除M2M终端设备的SIM卡全部安全参数，M2M终端设备接收到该Value之后，首先清除与SIM卡的绑定关系，若SIM卡设置了PIN码密码则清除PIN码的密码。
0xE00E	字符串	16	IMEI
0xE00F	字符串	16	加密函数(IMEI)
0xE010	字符串	16	原IMEI
0xE011	字符串	16	加密函数(原IMEI)
0xE012	字符串	15	IMSI
0xE013	字符串	16	加密函数(IMSI)
0xE014	字符串	15	原IMSI
0xE015	字符串	16	加密函数(原IMSI)
0xE016	字符串	16	加密函数(终端设备序列号+IMEI+IMSI) 注：“+”表示字符串首尾连接
0xE017	字符串	16	原映射关系 加密函数(终端设备序列号+原IMEI+原IMSI) 注：“+”表示字符串连接
0xE018	数字	2	PIN1码输入错误次数上限和累计输入错误次数，2字节16进制数，左起依次表示为： 第1字节——PIN1码输入错误次数上限，取值范围0x01~0xFF 第2字节——PIN1码累计输入错误次数，取值范围0x01~0xFF

标签值	数据类型	数据长度(字节)	标签说明
0xE019	数字	2	PIN2码输入错误次数上限和累计输入错误次数，2字节16进制数，左起依次表示为： 第1字节——PIN2码输入错误次数上限，取值范围0x01~0xFF 第2字节——PIN2码累计输入错误次数，取值范围0x01~0xFF
0xE01A	数字	2	PUK1码输入错误次数上限和累计输入错误次数，2字节16进制数，左起依次表示为： 第1字节——PUK 1码输入错误次数上限，取值范围0x01~0xFF 第2字节——PUK 1码累计输入错误次数，取值范围0x01~0xFF
0xE01B	数字	2	PUK2码输入错误次数上限和累计输入错误次数，2字节16进制数，左起依次表示为： 第1字节——PUK 2码输入错误次数上限，取值范围0x01~0xFF 第2字节——PUK 2码累计输入错误次数，取值范围0x01~0xFF
SIM卡相关参数保留TLV(0xE01C~0xE01F)			
M2M终端设备密码本地清除TLV			
0xE020	数字	1	M2M终端设备密码本地人工清除上报参数，8位2进制数，左起依次表示为： 第1位——PIN1 第2位——PIN2 第3位——PUK1 第4位——PUK2 第5位——上行接入密码 第6位——下行接入密码 第7位——基础密钥 第8位——无定义，取0 各位0,1分别表示如下意义： 0——未清除该位所表示的密码 1——已清除该位所表示的密码
接入密码相关参数(0xE021~0xE013)			
0xE021	字符串	16	接入安全验证的摘要体内容： 加密函数(报文头 + 内容体 + Timestamp + IMEI + IMSI + 接入密码)

标签值	数据类型	数据长度(字节)	标签说明
0xE022	数字	1	接入密码启用参数，1位16进制数 0x00——全部报文都不启用 0x01——全部报文都启用(默认值) 0x02——部分报文启用，含有特定命令字的报文 0x03——部分报文启用，含有特定TLV的报文 0x04——部分报文启用，含有特定命令字的报文或含有特定TLV的报文 0x05——部分报文启用，含有特定命令字的报文并含有特定TLV的报文
0xE023	字符串	不定长	须启用接入密码验证的命令字的Command_id。 因请求与应答是成对处理的，故只填请求报文的Command_id即可。
0xE024	字符串	不定长	须启用接入密码验证的TLV的TAG。
上行接入密码相关参数			
0xE025	字符串	8	上行接入密码(必须是8位的数字、大小写英文字母) 用于平台验证上行报文是否本终端设备所发送，只能为可见ASCII字符，
0xE026	字符串	16	上行接入密码的安全摘要 加密函数(上行接入密码的TLV 0xE025+上行接入密码有效期的TLV 0xE027)
0xE027	日期	4	上行接入密码有效期 从1970-1-1 00:00:00到当前的秒数 东8时区 北京
下行接入密码相关参数			
0xE028	字符串	8	下行接入密码(必须是8位的数字、大小写英文字母) 用于终端设备验证下行报文是否平台所发送，只能为可见ASCII字符，必须满8位(该值只支持SECURITY_CONFIG指令)
0xE029	字符串	16	下行接入密码的安全摘要 加密函数(下行接入密码的TLV 0xE028+下行接入密码有效期TLV 0xE02A)
0xE02A	日期		下行接入密码有效期 从1970-1-1 00:00:00到当前的秒数东8时区 北京
接入密码相关参数保留TLV (0xE02B~0xE02F)			
加密的相关参数			
0xE031	数字	1	终端设备是否支持加密，2位16进制数： 0x00——不支持 0x01——支持

标签值	数据类型	数据长度(字节)	标签说明
0xE032	数字	1	终端设备是否启用报文加密，2位16进制数： 0x00——全部报文都不启用 0x01——全部报文都启用 0x02——部分报文启用，含有特定命令字的报文 0x03——部分报文启用，含有特定TLV的报文 0x04——部分报文启用，含有特定命令字的报文或含有特定TLV的报文 0x05——部分报文启用，含有特定命令字的报文并含有特定TLV的报文
0xE033	字符串	不定长	须启用加密的命令字的Command_id。 因请求与应答是成对处理的，故只填请求报文的Command_id即可。
0xE034	字符串	不定长	须启用加密的TLV的TAG。
0xE035	数字	1	加密算法： 0x00——无 0x01——DES 0x02——3DES (CBC，K1=K3) 0x03——AES 0x04——RAS
基础密钥相关参数			
0xE036	字符串	不定长	基础密钥(必须为数字、大小写英文字母)，该密钥用于解密每次登录协商中所得的会话密钥。 注：若采用非对称加密，则此处为基础密钥的公钥。
0xE037	字符串	不定长	基础密钥的私钥(必须为数字、大小写英文字母) 。 注：非对称加密时，此参数有效，否则L=0。
0xE038	日期		基础密钥的有效期 从1970-1-1 00:00:00到当前的秒数 东8时区北京
0xE039	数字	1	基础密钥采用的加密算法 0x00——DES 0x01——3DES 0x02——AES 0x03——RAS
0xE03A	字符串	16	基本密钥相关信息的摘要值，即将0xE036、0xE037、0xE038、0xE039所表示的TLV组成字符串后做加密函数计算 对于本版协议： 加密函数(0xE036+0xE038)

标签值	数据类型	数据长度(字节)	标签说明
会话密钥相关参数			
0xE03B	字符串	不定长	会话密钥(必须为数字、大小写英文字母)，该密钥用于加密解密会话的报文 注：若采用非对称加密，则此处为会话密钥的公钥。
0xE03C	字符串	不定长	会话密钥的私钥(必须为数字、大小写英文字母) 。 注：非对称加密时，此参数有效，否则L=0
0xE03D	日期		会话密钥的有效期 从1970-1-1 00:00:00到当前的秒数 东8时区北京
0xE03E	数字	1	会话密钥采用的加密算法 0x00——DES 0x01——3DES 0x02——AES 0x03——RAS
0xE03F	字符串	16	会话密钥相关信息的摘要值，即将0xE03B、0xE03C、0xE03D、0xE03E所表示的TLV组成字符串后做加密函数计算 对于本版协议： 加密函数(0xE03B+0xE03D)
0xE040	字符串	不定长	用基础密钥加密的会话密钥的加密体 对于本版协议： 加密(0xE03B+0xE03D)
0xE041	数字	1	报文安全验证失败回复参数： 0x00——丢弃，不做任何回复 0x01——回复原报文的报文头，但更改其安全验证结果信息
0xE042	字符串	不定长	在完全加密模式下，用会话密钥加密的内容体的加密体
0xE043	字符串	不定长	在部分加密模式下，用会话密钥加密某个或某几个TLV

标签值	数据类型	数据长度(字节)	标签说明
0xE044	字符串	不定长	被分割成若干子包的用会话密钥加密的报文的加密体 第1~2字节——加密分包事务的TANS_ID，为分包机制发起方临时生成的随机数 第3~4字节——子包总数 第5~6字节——子包序号 第7字节——操作类型 0x00——开始分包交互 0x01——接收方请求第5~6字节定义的子报文 0x02——发起方异常中止分包交互，第5~6字节为异常中止前发送的子报文序号 0x03——接收方异常中止分包交互，第5~6字节为异常中止时接收的子报文序号 第8字节以后——加密子包所承载的加密数据，但摘要体的TLV不能放到该TLV中

附录 F
（资料性附录）
分包交互机制

当M2M终端设备与M2M平台的交互指令中TLV组总长度超过其承载方式的容量时，应采取分包交互机制。

分包交互机制的基本原则：

a) 分包交互机制下的子报文仍采用原有命令字，但在报文头的安全标识位的第4位标识为“1”。

b) 原报文中由非TLV固定参数和非摘要体TLV组成的内容体被看作是排列好的完整的数据，被从左起高位依次分割成若干待传送的数据，并被对应的子报文的0x4008的TLV所承载。

c) 为最大限度利用每个子报文的承载能力，减少子报文的总数目，一个TLV可以被拆分到多个子报文序号相临的子报文中。

d) 每个子报文的报文流水号按本协议对报文流水号的规定递增。

e) 应答方判断出请求方的子包错误时，中止分包交互状态，并在当前子包应答中通知请求方异常退出分包交互。

f) 子包全部完整接收完成后，再执行报文所承载的命令。

g) 分包机制遵从M2M终端设备与M2M平台之间的协议报文协议对于报文的所有规定。

基于上述原则，M2M终端设备与M2M平台之间的协议报文报文的拆分如图52所示。

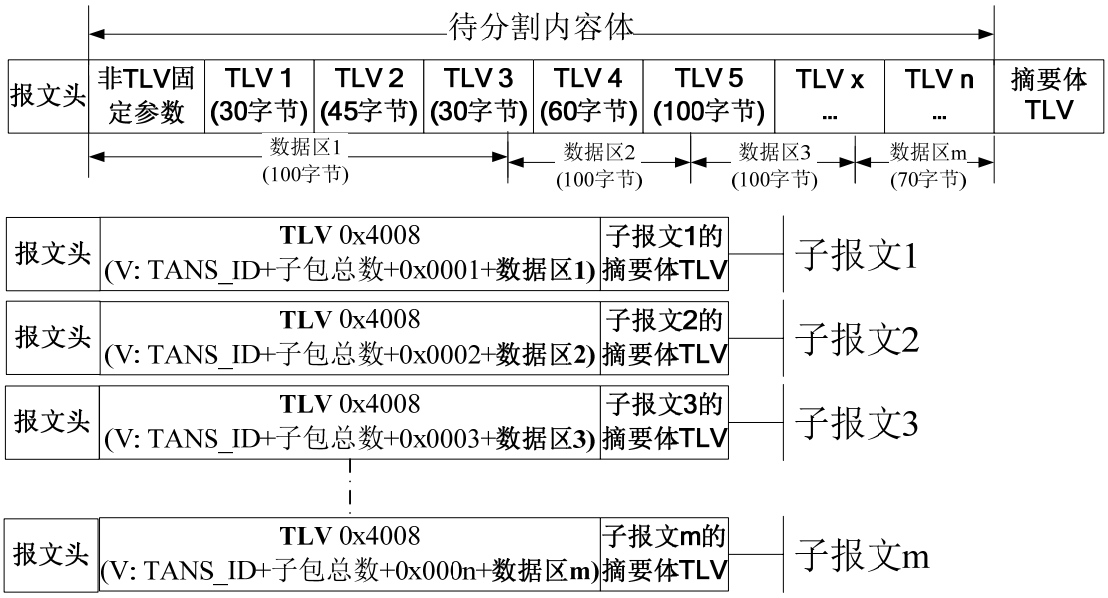


图52 M2M终端设备与M2M平台之间的协议报文报文的拆分示意图

分包交互机制下的指令交互流程：

情况1：请求方的TLV组无需分包，但答应方指令中TLV组过长需要分包，如图53所示。

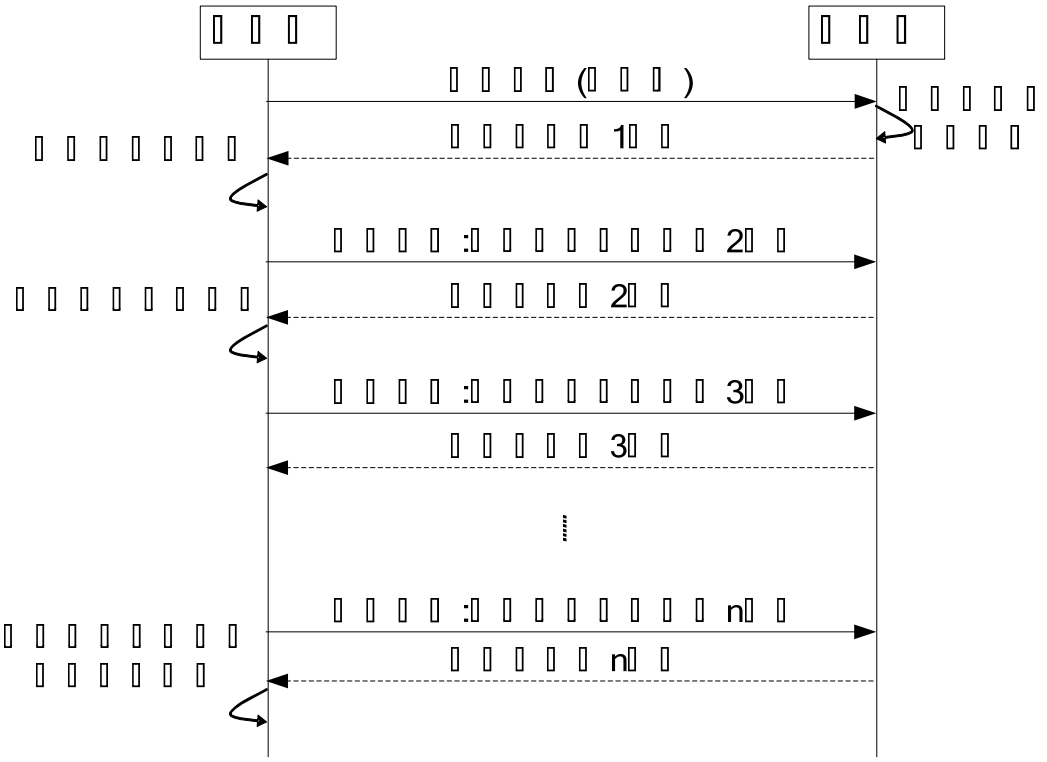


图53 情况1

情况2：请求方的TLV组需要分包，则答应方必须分包应答，如图54所示。

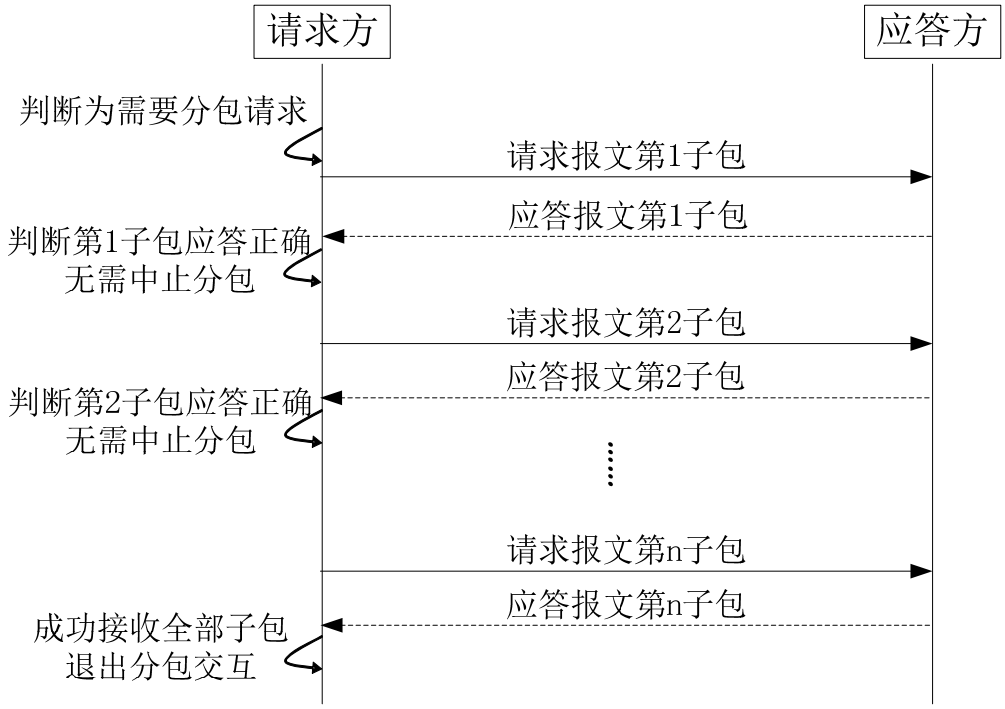
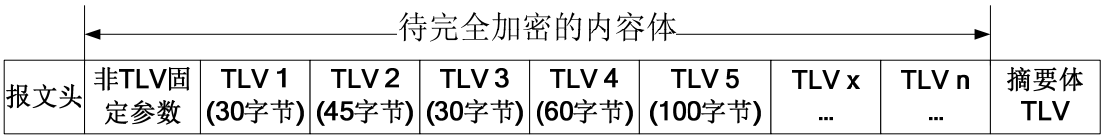


图54 情况2

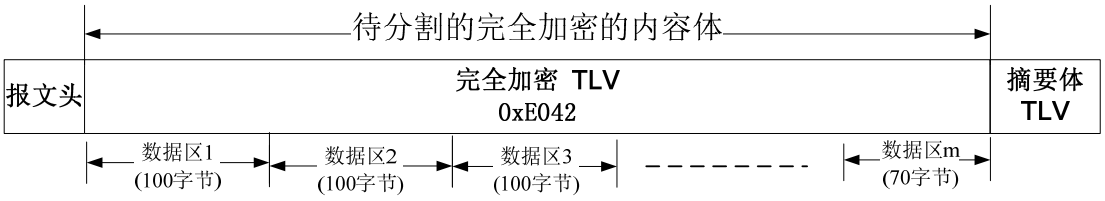
发送配置参数时，终端设备检测到任何一个无效的参数配置，返回“1－数据无效”，终端设备不进行参数配置操作，之前收到的参数也不进行参数配置操作。平台修订参数后全部重发配置参数包。

需要指出的是，在加密模式下，分包机制先将完全加密后的报文内容分割成若干子加密体，然后采用0xE044定义的TLV承载子加密体。接收时，待各个子加密体接收完成，并顺序拼接后再对拼接后的加密体进行解密处理。

原始报文



加密报文



分包报文

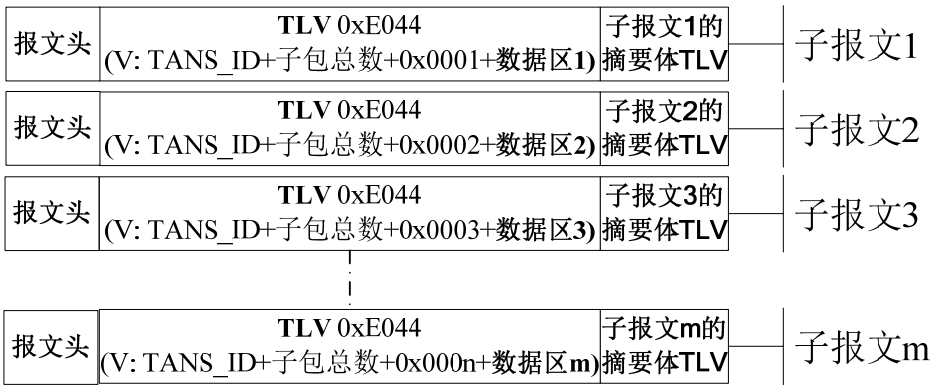


图1 M2M终端设备与M2M平台之间的协议报文报文的完全加密拆分示意图

附录 G
（资料性附录）
M2M 终端设备与 M2M 平台间的协议报文定义

a) 终端设备注册请求及响应报文

用于 M2M 终端设备向 M2M 平台发送注册请求，以及 M2M 平台反馈给 M2M 终端设备的注册请求响应。

(1)REGISTER 报文体定义

REGISTER，单向上行请求命令字，用于M2M终端设备向M2M平台发送注册请求，或请求变更“序列号－IMEI－IMSI”的映射关系。

REGISTER报文体定义如下：

	字段名	字节数	描述
固定部分	OPERATION	1	注册操作的类型，16 进制数 0x00——终端设备注册，申请平台分配序列号 0x01——终端设备注册，终端设备已经预置序列号 0x02——终端设备申请“序列号－IMEI－IMSI”映射关系变更 0x03——终端设备注册，终端设备已经预置序列号和接入密码和基础密钥 0x04——本地人工清除或遗失终端设备的密码和密钥上报
	IMEI	16	定长字段，16字节，对于15字节的IMEI号，则后面补0x00。
	IMSI	15	IMSI号码(String)
	当OPERATION=0x03时，必选TLV部分		
	0xE026	20	上行接入密码的安全摘要(预置接入密码时上报)
	0xE029	20	下行接入密码的安全摘要(预置接入密码时上报)
	0xE03A	20	基本密钥相关信息的摘要值(预置基础密钥时上报)
	当OPERATION=0x04时，必选TLV部分		
	0xE020	1	M2M终端设备密码本地人工清除上报参数，8位2进制数，左起依次表示为： 第1位——PIN1 第2位——PIN2 第3位——PUK1 第4位——PUK2 第5位——上行接入密码 第6位——下行接入密码 第7位——基础密钥 第8位——无定义，取0 各位0,1分别表示如下意义： 0——未清除该位所表示的密码 1——已清除该位所表示的密码
可选	**当OPERATION=0x02时，必选TLV部分**		

	0xE021	20	接入验证摘要值： 加密函数(REGISTER报文+0x00000000+原IMEI+原IMSI+上行接入密码)

如果消息头中终端设备序列号的第9~16位为全0，则是终端设备向平台申请序列，平台根据一定算法计算出序列号的后八位，并将产生的序列号返回给终端设备。

如果终端设备本身已预置序列号，则注册报文中该端序列号的第9~16位不全为0，则平台需导入或配置终端设备序列号数据。

REGISTER报文头中的加密标识本终端设备支持加密，则是通知M2M平台本终端设备支持加密(参见“接入密码和基础密钥的分发与变更”)。

(2)REGISTER_ACK 报文体定义

REGISTER_ACK，单向下行应答命令字，用于M2M平台对M2M终端设备注册请求的应答。

REGISTER_ACK报文体定义如下：

字段名		字节数	描述
固定部分	RESULT	1	返回注册结果，16 进制数 0x00——注册成功，终端设备必须进入短信模式准备接收平台下发的接入密码和基础密钥 0x01——映射关系变更成功 0x02——注册/映射关系变更失败，无法验证 IMSI 订购关系，要求 M2M 终端设备改为短信注册 0x03——注册/映射关系变更失败，非法的 MSISDN/IMSI，无该 SIM 卡订购关系 0x04——注册/映射关系变更失败，MSISDN/IMSI 冲突，该 SIM 卡对应终端设备正在线工作 0x05——注册/映射关系变更失败，非法终端设备序列号 0x06——注册/映射关系变更失败，终端设备序列号冲突，该序列号对应的终端设备正在线工作 0x07——注册/映射关系变更失败，IMEI 冲突，该 IMEI 所对应的终端设备正在线工作 0x08——注册/映射关系变更失败，通信协议版本不兼容 0x09——注册成功，终端设备预置的接入密码和基础密钥有效，立即发起首次登录。 0x0A——注册失败，终端设备预置的接入密码校验信息验证无效。 0x0B——注册失败，终端设备预置的基础密钥校验信息验证无效。 0x0C——注册失败，终端设备预置的接入密码和基础密钥验证都无效。 0x0D——注册失败，M2M 平台无终端设备预置的接入密码校验信息。 0x0E——注册失败，M2M 平台无终端设备预置的基础密钥。

			0x0F——注册失败，M2M 平台无终端设备预置的接入密码和基础密钥。 0x10——注册失败，M2M 终端设备未上报预置的接入密码校验信息。 0x11——注册失败，M2M 终端设备未上报预置的基础密钥校验信息。 0x12——注册失败，M2M 终端设备未上报预置的接入密码和基础密钥校验信息。 0x13—注册成功，不需要下发接入密码，终端直接登录 其他：保留。
	TERMINAL ID	16	注册/映射关系变更成功，平台返回分配/预置的终端设备序列号； 注册/映射关系变更失败，平台返回终端设备上报的终端设备序列号。
安全认证部分	**当REGISTER.OPERATION=0x02时，必选TLV部分**		
	0xE021	20	接入验证的摘要值： 加密函数(REGISTER_ACK 报文+0x00000000+原 IMEI+原 IMSI+下行接入密码)

当M2M终端设备处于业务流－管理流分离模式下，M2M平台要求M2M终端设备改为短信注册时，M2M终端设备判断业务平台连接状态是否正常，如正常，则不立即转到短信模式，以不影响业务应用为原则。

M2M终端设备切换到短信模式下后，在指定超时范围（TAG：0x0026）内，未接收到平台的短信，则切换回原有通信方式，并以CONFIG_TRAP格式上报错误（TAG: 0x300D, Alarm_Code:0x001C)。

b) 终端设备登录及登录响应报文

用于 M2M 终端设备向 M2M 平台发送登录，以及 M2M 平台反馈给 M2M 终端设备的登录请求响应。

LOGIN，单向上行请求命令字，用于M2M终端设备向M2M平台发送登录请求。若终端设备启用会话加密功能，则必须在登录请求中携带会话密钥请求的相关TLV。

LOGIN报文体定义如下：

字段名		字节数	描述
固定部分	Terminal Soft-Version	8	终端设备软件版本号，定长字段，8字节，ASCII码表示，不足位补0x00。
	终端设备配置参数的CRC32校验	4	由TLV 0x0025定义的M2M终端设备需与平台同步的配置参数TLV组的CRC32校验和：按TLV 的TAG值按由小到大排序后，对整个TLV组进行CRC32计算。 M2M平台通过对比平台存储的用户定制配置参数的CRC32校验和以及终端设备上报的本地配置参数CRC32校验和，判断终端设备的配置参数内容与平台存储的信息是否一致。
可选部分	**可选TLV组部分**		
	0x0011		**心跳间隔**

<table>
<tr><td rowspan="10"></td><td>0x0107</td><td></td><td>数据包应答超时，见附录</td></tr>
<tr><td>0x0108</td><td></td><td>传输失败最大允许重发次数，value取值范围(单位 次)：1~5
0：表示不重发</td></tr>
<tr><td>0x3006</td><td></td><td>Cellular ID，终端设备所在小区标识(高16位表示LAC，低16位表示CI)</td></tr>
<tr><td>0x3007</td><td></td><td>SigIntensity，本地信号场强，0~100</td></tr>
<tr><td>0x3010</td><td></td><td>终端设备外设
外设类型采用2个字节编码，允许扩展，目前系统预留了如下外设编码：
0x0001——PRN：打印机
0x0002——SCAN：扫描枪
0x0003——POS：POS刷卡器
0x0004——IC：IC卡感应器
0x0005——KEY：密码小键盘
0x0006——PHONE：外接话机
DEV的值为外设编码的序列，无间隔，例如：
<table>
<tr><td>TAG</td><td>Len</td><td>Value</td></tr>
<tr><td>0x3010</td><td>6</td><td>0x000100020003</td></tr>
</table>
表示三个外设编号分别为0x0001， 0x0002， 0x0003</td></tr>
<tr><td colspan="3">若启用会话加密，必选TLV部分</td></tr>
<tr><td>0xE03A</td><td>20</td><td>加密函数(基础密钥的相关信息)</td></tr>
<tr><td colspan="3">若本地人工清除M2M终端设备与SIM卡的双向安全认证机制必选TLV</td></tr>
<tr><td>0xE020</td><td>5</td><td>M2M终端设备密码本地人工清除上报参数，8位2进制数，左起依次表示为：
第1位——PIN1
第2位——PIN2
第3位——PUK1
第4位——PUK2
第5位——上行接入密码
第6位——下行接入密码
第7位——基础密钥
第8位——无定义，取0
各位0,1分别表示如下意义：
0——未清除该位所表示的密码
1——已清除该位所表示的密码</td></tr>
<tr><td>安全认证部分</td><td>0xE021</td><td>20</td><td>接入验证摘要值：
加密函数(LOGIN报文+0x00000000+IMEI+IMSI+上行接入密码)</td></tr>
</table>

LOGIN_ACK，单向下行应答命令字，用于M2M平台对M2M终端设备登录请求的应答。

LOGIN_ACK报文体定义如下：

字段名		字节数	描述
消息体	RESULT	1	登录结果，16 进制数

			0x00——登录成功 0x01——登录成功，但 CRC32 不一致需要上报配置 0x02——登录失败，非法映射关系 0x03——登录失败，非法终端设备序列号； 0x04——登录失败，终端设备序列号冲突，上报的序列号在线； 0x05——登录失败，通信协议版本不兼容； 0x06——登录失败，终端设备没有注册； 0x07——登录成功，基础密钥校验失败，无法发送会话密钥 0x08——登录成功，M2M 平台准备更新密码或密钥或其它配置参数，M2M 终端设备需要保持长连接 0x09——登录失败，未上报基础密钥校验 0xE03A。 其他：保留。
	CURTIME	4	当前系统时间：从1970-1-1 00:00:00到当前的秒数，该字段作为M2M平台与M2M终端设备的时间同步可选手段，同时在一个连接过程中安全摘要部分（0xE021）中的Timestamp即为此值
可变部分	**若启用会话加密，必选TLV组部分**		
	0xE040	20	用基础密钥加密的会话密钥的加密体 加密(0xE03B+0xE03D)
安全认证部分	0xE021	20	接入验证摘要值： 加密函数(LOGIN_ACK报文+Timestamp+IMEI+IMSI+下行接入密码) Timestamp=本报文中的CURTIME

M2M终端设备登录成功收到成功登录响应后，必须立即发送一个CONFIG_TRAP报文，通过CONFIG_TRAP报文的安全认证TLV，验证该M2M终端设备的此次连接是否合法。

c) 终端设备登出及登出响应报文

用于M2M终端设备或M2M平台告知对方终端设备退出登录请求，表示要结束此次会话过程，并表明结束过程的原因。登出响应报文用于M2M平台反馈给M2M终端设备的登出请求响应。

LOGOUT，双向上下行请求命令字，用于M2M终端设备或M2M平台告知对方终端设备退出登录请求，表示要结束此次会话过程，并表明结束过程的原因。

LOGOUT报文体定义如下：

字段名	字节数	描述

固定部分	LOGOUTREASON	1	退出登录原因，16 进制数 0x00——M2M 终端设备正常退出，进入等待激活模式； 0x01——M2M 终端设备正常退出，准备升级软件； 0x02——与 M2M 平台通信故障断开连接； 0x03——M2M 终端设备应用本地新配置生效，准备重启会话； 0x04——心跳超时； 0x05——M2M 终端设备故障退出，进入等待激活模式 0x06——M2M 终端设备故障断开连接会话，终端设备故障解决后自动重新登录 M2M 平台； 0x07——M2M 终端设备应用平台下发新配置生效重启会话； 0x08——会话密钥超时，重新登录 0x09——M2M 终端设备退出登录，准备更新接入密码或基础密钥 0x0A——M2M 终端设备退出登录，准备更新 SIM 卡安全参数 其他：保留。
安全认证部分	**可选 TLV 部分**		
	0xE021	20	接入验证摘要值： 加密函数(LOGOUT 报文+Timestamp+IMEI+IMSI+上/下行接入密码)

备注：等待激活模式为M2M终端设备等待M2M平台下发指令让其重新登录M2M平台。

LOGOUT_ACK，双向上下行应答命令字，用于M2M终端设备或M2M平台对退出登录请求的应答。

LOGOUT_ACK报文涉及一些参数配置生效退出登录的流程，为确保应答方的真实性，必须携带接入验证摘要体。

安全认证部分	**可选TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上/下行接入密码)

d) 链路检测请求及链路检测响应

HEART_BEAT，单向上行请求命令字，用于M2M终端设备向M2M平台告知连接状态的请求。在长连接模式时，由于要维持过程，必须发送维持连接包以维持连接，M2M终端设备在没有实际数据达到预先设置的间隔值时，发送HEART_BEAT报文以维持当前过程。对于短连接模式，终端设备根据其业务需要，也可向M2M平台发送心跳报文以表明终端设备处于工作状态，便于平台对终端设备的监控和管理。

HEART_BEAT报文体定义如下：

字段名	字节数	描述

可变部分	可选TLV组部分		
	0x3006		CELLULAR ID，终端设备所在小区标识(高16位表示LAC，低16位表示CI)
	0x3007		SIGINTENSITY，本地信号场强，0~100
	0x3005		上一次心跳延时
	0x3011		终端设备上报丢包数

需要指出的是，HEART_BEAT报文不需要携带接入验证的摘要体。但可根据其携带的TLV自行选择是否进行数据加密。此外，因心跳报文多数用于保持链路的连结状态，为保证报文交互逻辑的清晰，一般情况下不建议心跳报文携带承载应用数据的TLV/TLV组。若需定时向M2M平台上报相关数据可使用CONFIG_TRAP报文实现。

e) 信息上报及信息上报响应

用于M2M终端设备向M2M平台上报信息的请求，上报信息主要包括告警信息、统计信息、配置信息等。信息上报响应用于M2M平台反馈给M2M终端设备的信息上报响应。

CONFIG_TRAP，单向上行请求命令字，用于M2M终端设备向M2M平台上报信息的请求，上报信息主要包括告警信息、统计信息、配置信息等。

CONFIG_TRAP报文体定义如下：

字段名		字节数	描述
可变部分	可选TLV组部分		
	上报终端设备监控内容，格式参见附录B(4)终端设备监控相关内容。		
	上报故障信息，参见附录B(4)终端设备监控相关内容，0x300D(告警原因代码)		
	已恢复的故障编码合集，参见附录B(4)，0x300E		
	参见附录B：(1)配置参数相关内容		
	上报统计信息，参见附录B：(3)终端设备统计相关内容		
	对于需要分包的请求， TLV组的第1个TLV必须为分包机制参数。		
安全认证部分	安全TLV部分		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

注：一个CONFIG_TRAP报文体中可以同时包含告警、统计或者是配置信息。同时也可以包含0x3006、0x3007、0x3003等终端设备相关属性信息。

CONFIG_TRAP_ACK，单向下行应答命令字，用于M2M平台对M2M终端设备上报信息请求的应答。

CONFIG_TRAP_ACK报文体定义如下：

字段名		字节数	描述
固定部分	RESULT	1	返回状态字，16进制数 0x00——数据正确； 0x01——数据无效； 其他：失败，原因待定。
可	可选TLV组部分		

	TLV组		可选。如果M2M平台发现有不认识的TLV的TAG，直接报“数据无效”，M2M平台不处理，返回不支持的TLV，TLV中L为0。 对于分包的应答， TLV组的第1个TLV必须为分包机制参数。
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

f) 配置请求及配置请求响应

用于M2M终端设备向M2M平台请求配置信息，以及M2M平台反馈给M2M终端设备的配置请求响应。

CONFIG_REQ，单向上行请求命令字，用于M2M终端设备向M2M平台请求配置信息。

CONFIG_REQ报文体定义如下：

字段名		字节数	描述
可变部分	**TLV组**		
	参见附录B，所请求配置信息TLV中的L为0。 对于分包请求， TLV组的第1个TLV必须为分包机制参数。		
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

CONFIG_REQ_ACK，单向下行应答命令字，用于M2M平台对M2M终端设备设置参数请求的应答，平台返回查询。

CONFIG_REQ_ACK报文体定义如下：

字段名		字节数	描述
固定部分	RESULT		应答结果代码，16进制数 0x00——接收成功 0x01——数据无效 其他：失败，原因待定。
可变部分	**返回的TLV组部分**		
	平台返回参数配置，为TLV序列，参见附录B(1)配置参数相关内容。如果终端设备发现有不认识的TLV的TAG，直接报“数据无效”，终端设备不处理，返回不支持的TLV，TLV中L为0。 对于需要分包的应答， TLV组的第1个TLV必须为分包机制参数。		

安全认证部分	安全TLV部分		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

g) 终端设备信息获取及信息获取响应

用于M2M平台读取M2M终端设备的相应配置信息、统计信息、监控信息请求，以及M2M终端设备反馈给M2M平台的终端设备信息上报响应。

CONFIG_GET，单向下行请求命令字，用于M2M平台通过TAG读取M2M终端设备的相应配置信息、统计信息、监控信息请求。

CONFIG_GET报文体定义如下：

字段名	字节数	描述
可变部分	可选TLV组部分	
	终端设备监控内容，格式参见附录B(4)终端设备监控相关内容。TLV中的L为0	
	故障信息，参见附录B：(4)终端设备监控相关内容，0x300D(告警代码)， TLV中的L为0	
	配置信息，参见附录B：(1)配置参数相关内容， TLV中的L为0	
	统计信息，参见附录B：(3)终端设备统计相关内容， TLV中的L为0	
	注：对于分包请求， TLV组的第1个TLV必须为分包机制参数。	
安全认证部分	安全TLV部分	
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

注：一个CONFIG_GET报文体中可以同时包含监控、统计或者是配置信息。

CONFIG_GET_ACK，单向上行应答命令字，用于M2M终端设备对M2M平台查询终端设备配置请求的应答，返回M2M平台查询的TLV组所对应的内容。

数据体定义：

字段名	字节数	描述
固定部分	RESULT	应答结果代码，16进制数 0x00——接收成功 0x01——数据无效 其他：失败，原因待定。
可变部分	返回的TLV组部分	
	按监控模块的要求上传参数、状态或统计信息。如果终端设备发现有不认识的TLV的TAG，直接报“数据无效”，终端设备不处理，返回不支持的TLV，TLV中L为0。 对于需要分包的应答， TLV组的第1个TLV必须为分包机制参数。	

安全认证部分	安全TLV部分		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

h) 终端设备设置及终端设备设置响应

用于M2M平台通过指令设置M2M终端设备的某些参数的请求，以及M2M终端设备反馈给M2M平台的参数设置响应。

CONFIG_SET，单向下行请求命令字，用于M2M平台通过指令设置M2M终端设备的某些参数的请求。

CONFIG_SET报文定义如下：

字段名		字节数	描述
可变部分	TLV组		TLV组，参见附录B 注： 1、对于需要分包的请求， TLV组的第1个TLV必须为分包机制参数，即0x4008。 2、对于某些需要立即应用参数场合，用0x4009的TLV来强制要求终端设备立即中断所有操作，应用参数配置。如TLV组中无该TLV，则默认为非强制执行。
安全认证部分	安全TLV部分		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

CONFIG_SET_ACK，单向上行应答命令字，用于M2M终端设备对平台设置参数请求的应答。

CONFIG_SET_ACK报文定义如下：

字段名		字节数	描述
固定部分	RESULT		应答结果代码，16进制数 0x00——接收成功 0x01——数据无效 其他：失败，原因待定。
可变部分	可选TLV组部分		
	TLV组		如果终端设备发现有不认识的TLV的TAG，直接报“数据无效”，终端设备不处理，返回不支持的TLV，TLV中L为0。 对于分包的应答，TLV组的第1个TLV必须为分包机制参数。

安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

注：当配置参数完全正确时，终端设备才认为数据正确，返回“0－接收成功”。如果配置参数中有无效数据，则返回“1－数据无效”，终端设备不进行参数配置操作。

i) 远程控制及远程控制响应

用于M2M平台对M2M终端设备发送控制指令的请求，控制终端设备重启、复位等操作，以及M2M终端设备反馈给M2M平台的对控制指令的响应。

REMOTE_CTRL，单向下行请求命令字，用于M2M平台对M2M终端设备发送控制指令的请求，控制终端设备重启、复位等操作。

REMOTE_CTRL报文定义如下：

字段名		字节数	描述
可变部分	**可选TLV组部分**		
	TLV组		TLV组部分，TLV中TAG定义，参见附录B：(5)下行控制相关内容
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

REMOTE_CTRL_ACK，单向上行应答命令字，用于M2M终端设备对M2M平台远程控制指令请求的应答，返回TLV形式的M2M终端设备的配置内容。

REMOTE_CTRL_ACK报文定义如下：

字段名		字节数	描述
固定部分	RESULT		应答结果代码 0x00——接收成功 0x01——数据无效 其他：失败，原因待定。
可变部分	**可选TLV组部分**		
	TLV组		命令无效的TAG组，参见附录B(5)如果终端设备发现有不认识的TLV的TAG，直接报“数据无效”，返回不支持的TLV，L=0
安	**安全TLV部分**		

	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

注：对于数据采集类指令，终端设备采用CONFIG_TRAP上传采集数据，包括统计数据、监控信息、业务数据等。

j) 应用数据传输及应用数据传输响应

用于实现端到端的应用数据连接，即M2M终端设备或M2M应用经由M2M平台向对方发送应用数据请求及响应。用于业务数据下发和业务数据上传。

TRANSPARENT_DATA，双向上下行请求命令字，用于实现端到端的应用数据连接，即M2M终端设备或M2M应用经由M2M平台向对方发送应用数据请求。在业务流－管理流并行模式下，由M2M平台实现M2M终端设备与M2M应用业务服务器、M2M终端设备与M2M终端设备之间的双向的透明数据数据转发。

M2M平台如果从M2M终端设备收到该报文，则根据透传类型和源/目的地址来获取目的信息，把用户数据转发给相应目的EC应用或目的M2M终端设备；如果从EC应用收到该报文，则根据终端设备序列号来分发信息到相应的M2M终端设备。

TRANSPARENT_DATA报文定义如下：

字段名		字节数	描述
固定部分	CRC16	2	本子包用户数据USER_DATA部分的CRC16校验
	必选TLV		
	Destination /Source Address(EC Code /Terminal ID)	不定长	来源或目的地址(EC业务代码或终端设备序列号)： 目的应用的EC业务码 (TLV 0x4014) 来源应用的EC业务码 (TLV 0x4015) 目的终端设备的序列号 (TLV 0x4012) 来源终端设备的序列号 (TLV 0x4013)
可变部分	**可选TLV**		
	SUB_BLOCK	不定长	可选TLV，分包相关参数，参见0x4008的TLV定义。
	USER_DATA	不定长	M2M终端设备与EC应用服务器之间的交互数据(TAG 0x4007) 当采用SMS作为承载方式时，用户数据必须小于等于78字节；而无线分组业务作为承载传输时，建议小于等于1024字节。 注：当采用分包的时候，该字段将包含在SUB_BLOCK(TLV 0x4008)中。
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上/下行接入密码)

TRANSPARENT_DATA_ACK，双向上下行应答命令字，用于M2M终端设备或M2M平台向对方发送应用数据请求的应答。

TRANSPARENT_DATA_ACK报文定义如下：

字段名		字节数	描述
固定部分	RESULT	1	应答结果标识 0x00——M2M平台接收成功，CRC16校验成功，并转发 0x01——M2M平台接收成功，CRC16校验成功，但目的终端设备或应用平台离线，转发失败 0x02——M2M平台接收成功，CRC16校验成功，但目的地址错误或非法，转发失败 0x03——M2M成功接收平台，CRC16校验成功，但请求方无权限，转发失败 0x04——M2M平台接收失败，CRC16校验失败，数据无效 0x05——M2M终端设备接收成功，CRC16校验成功 0x06——M2M终端设备接收失败，CRC16校验失败，数据无效
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上/下行接入密码)

k) 软件更新请求及软件更新响应

用于M2M平台向M2M终端设备发送软件升级通知请求及M2M终端设备反馈给M2M平台的软件升级响应。

DOWNLOAD_INFO，单向下行请求命令字，用于M2M平台向M2M终端设备发送软件升级通知请求。

DOWNLOAD_INFO报文定义如下：

字段名		字节数	描述
固定部分	DownAddURL (0x1001)	不定长	URL格式： 协议://下载服务器IP地址:端口号/下载文件描述?参数列表集合 说明： 支持协议： HTTP/M2M应用通信协议 参数列表集合格式： 参数名=参数值&参数名=参数值&……&参数名=参数值 必要参数： TRANS_ID(升级事务ID，8位16进制字符串，如：1AFBDC01，表示0x1AFBDC01) FILE_SIZE (文件长度，10进制) CRC(CRC16/32校验，4位或8位16进制字符串，如：1AF0或1AF0F78B，采用CRC16还是CRC32由文件下载提供方根据下载文件的大小自行选择) VER_DSC(通知终端设备升级的版本号，参见LOGIN中的版本号描述)

			其它参数可由厂商、EC、下载升级服务提供商自定义。此外，参数名也可以用“附B TLV说明”的“(2) 软件下载升级相关内容”中定义的TLV的TAG来表示。 例如： ://61.135.68.199:9000/KKK001?TRANS_ID=1AFBDC01&FILE_SIZE=3429838&CRC16=1AF0&VER_DSC=LH-V001 注：当M2M终端设备收到该TLV时，需要将该TLV分解后填入对应的TLV()
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

DOWNLOAD_INFO_ACK中，单向上行应答命令字，用于M2M终端设备对M2M平台软件升级通知请求的应答。

DOWNLOAD_INFO_ACK报文体定义如下：

字段名		字节数	描述
固定部分	RESULT	1	应答结果代码 0x00——已是最新版本，不需更新； 0x01——立即准备更新； 0x02——终端设备正在执行业务，暂缓更新； 0x03——终端设备不支持升级协议； 0x04——URL参数无效； 0x05——终端设备缓存不足无法下载 其他：失败，原因待定。
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

l) 文件下载请求及文件下载响应

用于M2M终端设备向M2M平台请求下载文件，及M2M平台反馈给M2M终端设备的文件下载响应。

FILE_REQ，单向上行请求命令字，用于M2M终端设备采用M2M应用通信协议向M2M平台请求下载文件。

FILE_REQ报文体定义如下：

字段名		字节数	描述
固定部分	TRANS_ID	4	升级事务ID 该值为DOWNLOAD_INFO.DownAddURL中定义的升级事务ID的16进制表示
	STATUS	1	终端设备文件下载状态：

			0x00——开始下载。第一次请求下载的状态，用以通知M2M平台或第三方下载服务器：本终端设备开始下载； 0x01——下载中。正常下载中的状态，用来通知M2M平台或第三方下载服务器：从上次数据块下载CRC校验失败到上一下载完成的数据块为止未再次发生下载失败，继续请求后续的数据块。 0x02——下载完成。通知M2M平台或第三方下载服务器：本终端设备已经完成下载文件的全部数据分组的下载，并且CRC校验成功。 0x03——文件下载失败。用于通知M2M平台或第三方下载服务器：整个文件下载失败，下载中止。
	FILE_READ_POINT	4	请求下载文件读取位置的偏移地址。 STATUS=0x00时，一般为0x00000000，但可以从任何位置开始 STATUS=0x02/0x03时，为0xFFFFFFFF。
	FILE_BLOCK_SIZE	2	下载文件读取长度。 STATUS=0x02/0x03时，为0x0000。
	安全TLV部分		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上行接入密码)

FILE_REQ_ACK，单向下行应答该命令字，用于M2M平台对M2M终端设备请求下载文件的应答。

FILE_REQ_ACK报文体定义如下：

字段名		字节数	描述
固定部分	TRANS_ID	4	升级事务 ID
	STATUS	1	M2M 平台对 M2M 终端设备下载文件请求的应答状态： 0x00——正常或确认 0x01——非法的 TRANS_ID 0x02——非法的 FILE_READ_POINT 0x03——非法的 FILE_BLOCK_SIZE，M2M 平台继续发送正常的文件长度。
	CRC16	2	对下载文件数据块 FILE_BLOCK 中内容的 CRC16 校验。 FILE_BLOCK_SIZE=0x00000000 时，该值为 0x0000。
	FILE_READ_POINT	4	下载文件读取位置。 STATUS=0x00/0x03 时，为文件下载请求的读取位置即 FILE_REQ.FILE_READ_POINT 的值； STATUS=0x01/0x02 时，为 0xFFFFFFFF；

	FILE_BLOCK_SIZE	2	下载文件读取长度。 STATUS=0x00 时，为文件下载请求的读取长度即 FILE_REQ.FILE_BLOCK_SIZE 的值 STATUS=0x01/0x02 时，该值为 0x0000； STATUS=0x03 时，该值实际发送数据包的长度。
	FILE_BLOCK	FILE_BLOCK_SIZE 所表示的长度	由 FILE_READ_POINT 和 FILE_BLOCK 确定的数据包的内容。 FILE_BLOCK_SIZE=0x0000 时，项该无值。
	安全 TLV 部分		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+下行接入密码)

m) 安全参数配置请求及安全参数配置响应

用于M2M终端设备或M2M平台请求对终端设备安全参数的配置请求及响应。

SECURITY_CONFIG，双向上下行请求命令字，用于M2M终端设备或M2M平台请求对终端设备安全参数的配置请求。

SECURITY_CONFIG报文体定义如下：

字段名		字节数	描述
固定部分	OPERATION	1	0x00——平台设置终端设备安全参数(若安全参数中包含密码或密钥，以明文方式必须为短信方式，密文可用任意方式) 0x01——平台读取终端设备安全参数，要求终端设备以密文方式返回 0x02——平台读取终端设备安全参数的摘要信息，要求终端设备以明文方式返回 0x03——平台下发安全参数更新通知，要求终端设备进入短信模式，准备接收明文安全参数 0x04——终端设备上报安全参数(即可用明文方式，也可用密文方式；但以明文方式时，不能直接上报密码或密钥，只能上报密码或密钥的摘要值) 0x05——终端设备请求以明文更新安全参数 0x06——终端设备请求以密文更新安全参数 0x07——终端设备请求启用各类安全参数
可变部分	**可选TLV组**		
	当OPERATION=0x00时， 设置的安全参数的TLV：密码或密钥值、启用标识、有效期；		
	当OPERATION=0x01时， 读取的安全参数的TLV：密码或密钥值、启用标识、有效期，其中L=0		
	当OPERATION=0x02时， 读取的安全参数的TLV：密码或密钥值的摘要、启用标识、有效期，其中L=0		
	当OPERATION=0x03时，		

	要更新的安全参数的TLV，其中L=0		
	当OPERATION=0x04时， 上报的安全参数的TLV：加密的密码或密钥值、密码或密钥值的安全摘要、启用标识、有效期		
	当OPERATION=0x05/0x06时， 请求的安全参数的TLV：密码或密钥值的安全摘要、启用标识、有效期，其中L=0		
	当OPERATION=0x07时， 启用的安全参数的启用标识的TLV		
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上/下行接入密码)

需要指出的是，在注册后首次下发接入密码时，在此之前 M2M 终端设备内没有存储任何安全密码或密钥，因此下发安全设置报文中无须携带接入安全验证的摘要体。

SECURITY_CONFIG_ACK，双向上下行应答命令字，用于M2M终端设备或M2M平台对终端设备安全参数操作的应答。

SECURITY_CONFIG_ACK报文体定义如下：

字段名		字节数	描述
固定部分	RESULT	1	操作应答代码 0x00——终端设备或平台接受请求 0x01——错误，解密失败 0x02——错误，有不支持的TLV 0x03——平台拒绝终端设备启用或更新安全参数，仅对OPERATION=0x05/0x06/0x07的请求有效 0x04——错误，SIM卡的相关密码摘要校验错误，仅对SIM类参数操作有效 0x05——错误，M2M终端设备不支持加密功能 0x08——错误，终端设备采用会话加密方式登录
可变部分	**可选TLV组**		
	RESULT=0x00	SECURITY_CONFIG.OPERATION=0x00，无TLV组	
		SECURITY_CONFIG.OPERATION=0x01，以密文返回读取的TLV组	
		SECURITY_CONFIG.OPERATION=0x02，返回读取的TLV组	
		SECURITY_CONFIG.OPERATION=0x03，无TLV组，M2M终端设备接收后进入短信模式接收密码或密钥	
		SECURITY_CONFIG.OPERATION=0x04，无TLV组	
		SECURITY_CONFIG.OPERATION=0x05，无TLV组，M2M终端设备接收后进入短信模式接收密码或密钥	
		SECURITY_CONFIG.OPERATION=0x06，返回加密的安全参数	
		SECURITY_CONFIG.OPERATION=0x07，无TLV组	
	RESULT=0x0	无TLV组	

	1		
	RESULT=0x02	返回不支持的TLV，其中L=0	
	RESULT=0x03	返回拒绝的安全参数的启用标识TLV，其中L=0	
	RESULT=0x04	无TLV组	
	RESULT=0x05	无TLV组	
安全认证部分	**安全TLV部分**		
	0xE021	20	接入验证摘要值： 加密函数(报文+Timestamp+IMEI+IMSI+上/下行接入密码)

附录 H
（资料性附录）
M2M 平台与 M2M 应用间的协议消息定义

a) M2M 应用向 M2M 平台注册

M2M应用需要连接M2M平台时，必须通过本接口向M2M平台注册。

调用名称：TAppLogin

M2M应用向M2M平台发起的注册请求(P_APP_LOGIN_Req)

参数标识	TAppLoginReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TAppLoginReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>消息体为空</BODY> <HASH>消息摘要</HASH> </TAppLoginReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16

M2M平台对M2M应用注册请求的应答信息(P_APP_LOGIN_Resp)

参数标识	TAppLoginRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TAppLoginRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TAppLoginRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18

SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> <CONVKEY>会话密钥</CONVKEY> <EXPIRATION>会话有效期</EXPIRATION> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回注册结果 0：注册成功 1：无该用户名 2：密码和用户名不匹配 3：加密的消息体错误 其他：保留。	String	2
CONVKEY	本次会话密钥	String	16
EXPIRATION	本次会话有效期（单位分钟），采用相对时间。	整形	4

b) M2M 应用向 M2M 平台注销

M2M应用需要退出M2M平台时，必须通过本接口登出M2M平台。

调用名称：TAppLogout

M2M应用向M2M平台发起的退出登录请求(P_APP_LOGOUT_Req)

参数标识	TAppLogoutReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TAppLogoutReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TAppLogoutReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <USERNAME>用户名</USERNAME> <PASSWORD>密码</PASSWORD> </BODY>		

名称	说明	数据类型	长度（字节）
USERNAME	应用系统登录M2M平台的用户名	String	12
PASSWORD	应用系统登录M2M平台的密码	String	12

M2M平台对M2M应用注册请求的应答(P_APP_LOGOUT_Resp)

参数标识	TAppLoginRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TAppLoginRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TAppLoginRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回注册结果 0：退出成功 2：无该用户名 3：密码和用户名不匹配 4：加密的消息体错误 其他：保留。	String	2

c) 终端设备信息获取

M2M 应用通过本接口读取 M2M 终端设备的相应配置信息、统计信息、监控信息。该接口为异步接口，M2M 应用向 M2M 平台发出请求后，M2M 平台的应答只表示收到该请求。M2M 终端设备通过 T_TERMINFO_GET_RESULT 消息向 M2M 应用上报 M2M 应用所请求的终端设备信息。

调用名称：TTermInfoGet

M2M应用请求M2M终端设备消息（T_TERMINFO_GET_Req）

参数标识	TTermInfoGetReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermInfoGetReq>

	<HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermInfoGetReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMLIST> <TERMID>终端设备序列号</TERMID> …… </TERMLIST> <FILTER> <TERMIDRANGE start=终端设备序列号起始号码 end=终端设备序列号终止号码/> <MODEL>终端设备型号</MODEL> <PRODUCTOR>终端设备厂家</PRODUCTOR> <REGISTDATE start=起始日期 end=终止日期/> <AREA>终端设备安装的地区</AREA> </FILTER> <MONITOR> <TAG id=终端设备监控内容TAG/> …… </MONITOR> <ALARM> <TAG id=300D/> </ALARM> <CONFIG> <TAG id=配置项TAG/> …… </CONFIG> <STATISTIC> <TAG id=统计项TAG/> …… </STATISTIC> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**

TERMLIST	需要操作的终端设备序列号列表。该标签和FILTER标签互斥。	String	不定长
FILTER	过滤条件，即需要进行操作的终端设备的选择条件。该标签和TERMLIST互斥。FILTER包含如下几个子元素： TERMIDRANGE：终端设备序列号的起始号段，包含开始和终止号码两个子元素； MODEL：终端设备型号编码； PRODUCTOR：终端设备厂家代码； REGISTDATE：终端设备上线注册的日期范围； AREA：安装终端设备的地区。采用电话区号。	String	不定长
MONITOR	需要采集的终端设备监控内容，为4位16进制字符串（附录A（4）终端监控相关内容），可重复使用。	String	4
ALRAM	要求采集的故障信息，固定值为300D。在请求消息中最多出现一次。	String	4
CONFIG	需要采集的配置信息，为4位16进制字符串（参见附录A：（1）配置参数相关内容），可重复使用	String	4
STATISTIC	需要采集的统计数据，为4位16进制字符串（参见附录A：（3）终端统计相关内容），可重复使用。	String	4

M2M平台对M2M应用请求M2M终端设备消息的响应消息（T_TERMINFO_GET_Resp）

参数标识	TTermInfoGetRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermInfoGetRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermInfoGetRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			

消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回结果代码。 0——M2M 平台接受请求 1——M2M 平台拒绝请求 2——该应用未登录 其他：失败，原因待定。	String	2

d) 终端信息查询结果

M2M终端在处理应用下发的T_TERMINFO_GET请求后，返回处理结果，M2M平台转发该处理结果给应用系统。返回信息包括告警信息、统计信息、配置信息。一个T_TERMINFO_GET_RESULT包体中可以同时包含告警、统计或者是配置信息。同时也可以包含0x3006、0x3007、0x3003等终端相关属性信息。此外，还应包含终端不支持的TAG信息。

T_TERMINFO_GET_RESULT包头中的消息序号SID应与对应的T_TERMINFO_GET包头中的SID一致。

调用名称：TTermInfoGetResultM2M平台转发M2M终端设备上报信息的请求消息(T_TERMINFO_GET_RESULT_Req)

参数标识	TTermInfoGetResultReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermInfoReportReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermInfoGetResultReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端设备序列号</TERMID> <MONITOR> <TAG id=终端设备监控内容TAG>终端设备监控数据</TAG> …… </MONITOR> <ALARM> <CODE>故障代码1</CODE>		

	…… </ALARM> <RECOVERY> <CODE>已恢复的故障代码1</CODE> …… </RECOVERY > <CONFIG> <TAG id=配置项TAG>配置项的值</TAG> …… </CONFIG> <STATISTIC> <TAG id=统计项TAG>统计值</TAG> …… </STATISTIC> <INVALIDATE> <MONITOR> <TAG id=终端设备监控内容TAG/> …… </MONITOR> <CONFIG> <TAG id=配置项TAG/> …… </CONFIG> <STATISTIC> <TAG id=统计项TAG/> …… </STATISTIC> </INVALIDATE> </BODY>

名称	说明	数据类型	长度（字节）
TERMID	终端设备序列号	String	16
MONITOR	终端设备返回的终端设备监控数据的TAG，包含一个VALUE子节点，为该TAG的值。（附录A（4）终端设备监控相关内容）。消息中可重复使用MONITOR。	String	4 VALUE长度与监控数据TAG有关
ALARM	终端设备返回故障代码列表（参见附录A（4）终端设备监控相关内容，0x300D（报警代码））。	String	CODE值的长度为4
RECOVERY	终端设备返回已恢复的故障代码列表（参见附录A（4）终端设备监控相关内容，0x300D（报警代码））。	String	CODE值的长度为4
CONFIG	终端设备返回的配置数据（参见附录	String	4

	A:（1）配置参数相关内容），可重复使用		VALUE长度与配置数据TAG有关
STATISTIC	终端设备返回的统计数据（参见附录A:（3）终端设备统计相关内容），可重复使用	String	4 VALUE长度与配置数据TAG有关

M2M应用对M2M平台转发M2M终端设备上报信息的请求消息的响应消息(T_TERMINFO_GET_RESULT_Resp)

参数标识	TTermInfoGetResultRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermInfoGetResultRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermInfoGetResultRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	0：数据正确； 1：数据无效； 其他：失败，原因待定。	String	2

e) 查询终端设备信息接口

M2M应用通过本接口，从M2M平台的数据库中查询M2M终端设备的相应配置信息、统计信息、监控信息。该接口为同步接口，M2M应用向M2M平台发出请求后，M2M平台从数据库记录中查询被请求终端设备的信息，然后返回给M2M应用。

调用名称：PTermInfoQuery

查询终端设备信息请求(P_TERMINFO_QUERY_Req)

参数标识	PTermInfoQueryReq
消息格式	<?xml version="1.0" encoding="UTF-8"?>

	<PTermInfoQueryReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PTermInfoQueryReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端设备序列号</TERMID> <MONITOR> <TAG id=终端设备监控内容TAG/> …… </MONITOR> <ALARM> <TAG id=终端设备监控内容TAG/> </ALARM> <CONFIG> <TAG id=配置项TAG/> …… </CONFIG> <STATISTIC> <TAG id=统计项TAG/> …… </STATISTIC> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端设备序列号	String	16
MONITOR	需要采集的终端设备监控内容，为4位16进制字符串（附录A（4）终端设备监控相关内容），可重复使用。	String	4
ALRAM	要求采集的故障信息，固定值为300D。在请求消息中最多出现一次。	String	4
CONFIG	需要采集的配置信息，为4位16进制字符串（参见附录A：（1）配置参数相关内容），可重复使用	String	4
STATISTIC	需要采集的统计数据，为4位16进制字符串	String	4

	（参见附录A：（3）终端设备统计相关内容），可重复使用。		

查询终端设备信息响应（P_TERMINFO_QUERY_Resp）

参数标识	PTermInfoQueryRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PTermInfoQueryRsp > <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PTermInfoQueryRsp >		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端设备序列号</TERMID> <MONITOR> <TAG id=终端设备监控内容TAG>终端设备监控数据</TAG> …… </MONITOR> <ALARM> <CODE>故障代码1</CODE> …… </ALARM> <RECOVERY> <CODE>已恢复的故障代码1</CODE> <CODE>已恢复的故障代码2</CODE> …… </RECOVERY > <CONFIG> <TAG id=配置项TAG>配置项的值</TAG> …… </CONFIG> <STATISTIC> <TAG id=统计项TAG>统计值</TAG> …… </STATISTIC>		

	</BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端设备序列号	String	16
MONITOR	终端设备返回的终端设备监控数据TAG，包含一个VALUE子节点，为该TAG的值。（附录A（4）终端设备监控相关内容）。消息中可重复使用MONITOR。	String	4 VALUE长度与监控数据TAG有关
ALARM	终端设备返回故障代码列表（参见附录A（4）终端设备监控相关内容，0x300D（报警代码））。	String	CODE值的长度为4
RECOVERY	终端设备返回已恢复的故障代码列表（参见附录A（4）终端设备监控相关内容，0x300D（报警代码））。	String	CODE值的长度为4
CONFIG	终端设备返回的配置数据（参见附录A：（1）配置参数相关内容），可重复使用	String	4 VALUE长度与配置数据TAG有关
STATISTIC	终端设备返回的统计数据（参见附录A：（3）终端设备统计相关内容），可重复使用	String	4 VALUE长度与配置数据TAG有关

f) 终端设备状态告警

M2M平台在检测出终端出现故障时，通过本接口向M2M应用通报终端设备故障。

调用名称：PTermFaultNotify

M2M平台发送终端设备故障通知请求消息(P_TERM_FAULT_NOTIFY_Req)

参数标识	PTermFaultNotifyReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PTermFaultNotifyReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PTermFaultNotifyReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			

消息体格式	<BODY> <TERMID>终端设备序列号</TERMID> <ERRCODE>故障代码</ERRCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端设备序列号（出现故障的终端设备序列号）	String	16
ERRCODE	故障代码。可已有一到多个ERRCODE标签。故障代码定义如下： 01：终端设备与M2M平台链路中断 02：终端设备长时间无消息 03：终端设备消息格式错误，无法解析 04：终端设备序列号冲突（即序列号与注册时的MSISDN不符）	整型	2

响应消息(P_TERM_FAULT_NOTIFY_Resp)

参数标识	PTermFaultNotifyRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PTermFaultNotifyRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </PTermFaultNotifyRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
本消息无消息体。			

g) 查询统计信息

M2M应用通过本接口，从M2M平台的数据库中查询统计数据。该接口为同步接口，M2M应用向M2M平台发出请求后，M2M平台从数据库记录中查询被请求终端的信息，然后返回给M2M应用。

调用名称：PStatisticQuery

查询统计信息请求(P_STATISTIC_QUERY_Req)

参数标识	PStatisticQueryReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PStatisticQueryReq>

	<HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> <BODY>加密后的消息体</BODY> </PStatisticQueryReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMCOUNT> <PRODUCER>终端设备厂家</PRODUCER> <AREA>地区编码</AREA> <DATE>查询的日期</DATE> <MONTH>查询的月份</MONTH> </TERMCOUNT> <TERMFAULT> <PRODUCER>终端设备厂家</PRODUCER> <AREA>地区</AREA> <TERMMODEL>终端设备型号</TERMMODEL> <ERRCODE>故障代码</ERRCODE> <DATE>查询的日期</DATE> <MONTH>查询的月份</MONTH> </TERMFAULT> <TERMSTATUS> <PRODUCER>终端设备厂家</PRODUCER> <AREA>地区</AREA> <TERMMODEL>终端设备型号</TERMMODEL> <TS>终端设备序列号</TS> </TERMSTATUS> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMCOUNT	终端设备数量统计数据查询，可返回产生业务终端设备数量、已注册终端设备数量、当日新增终端设备数量。 TERMCOUNT包含如下几个子元素： PRODUCER：终端设备厂家 AREA：终端设备所在的区域 DATE：查询的日期，如果使用该元素，则	String	不定长

	M2M平台返回该天的统计量； MONTH：查询的月份，如果使用该元素，则M2M平台返回该月的统计量； 以上子元素作为查询的组合过滤条件，调用方可选择使用这些子元素。		
TERMFAULT	查询终端设备上报的故障情况。 TERMFAULT包含如下几个子元素： PRODUCER：终端设备厂家 AREA：终端设备所在的区域 TERMMODEL：终端设备型号 ERRCODE：故障代码 DATE：查询的日期，如果使用该元素，则M2M平台返回该天的统计量； MONTH：查询的月份，如果使用该元素，则M2M平台返回该月的统计量； 以上子元素作为查询的组合过滤条件，调用方可选择使用这些子元素。	String	不定长
TERMSTATUS	对终端设备状态进行统计。TERMSTATUS包含如下几个子元素： PRODUCER：终端设备厂家 AREA：终端设备所在地区 TERMMODEL：终端设备型号 TS：终端设备序列号 以上子元素作为查询的组合过滤条件，调用方可选择使用这些子元素。	String	4

查询统计信息响应（P_STATISTIC_QUERY_Resp）

参数标识	PStatisticQueryRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PStatisticQueryRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PStatisticQueryRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			

消息体格式	<BODY> <TERMCOUNT_RESULT> <WORKING>产生业务的终端设备数量</WORKING> <REGISTED>已注册的终端设备数量</REGISTED> <DATENEW>当日新增终端设备数量</DATENEW> <MONTHNEW>当月新增终端设备数量</MONTHNEW> <TOTAL>累计终端设备数量</TOTAL> </TERMCOUNT_RESULT> <TERMFAULT_RESULT> <DATENUM>当日产生终端设备数量</DATENUM> <MONTHNUM>当月产生终端设备数量</MONTHNUM> <TOTAL>故障终端设备总数</TOTAL> </TERMFAULT_RESULT> <TERMSTATUS_RESULT> <NORMAL>状态正常终端设备数量</NORMAL> <EXCEPTION>状态异常终端设备数量</EXCEPTION> <FORBIDDEN>已禁用的终端设备数量</FORBIDDEN> </TERMSTATUS_RESULT> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMCOUNT_RESULT	根据请求的查询条件得到的终端设备统计数量。TERMCOUNT_RESULT包含以下几个子元素： WORKING：产生业务的终端设备数量 REGISTED：已注册的终端设备数量DATENEW：当日新增终端设备数量 MONTHNEW：当月新增终端设备数量 TOTAL：累计终端设备数量	String	不定长
TERMFAULT_RESULT	根据请求的查询条件得到的故障终端设备数量。TERMFAULT_RESULT包含如下几个子元素： DATENUM：查询日期当日产生故障的终端设备数量 MONTHNUM：查询月份当月产生终端设备数量 TOTAL：故障终端设备总数	String	不定长
TERMSTATUS_RESULT	根据请求的查询条件得到的不同状态的终端设备数量。 TERMSTATUS_RESULT包含如下	String	不定长

	几个子元素： NORMAL：状态正常终端设备数量 EXCEPTION：状态异常终端设备数量 FORBIDDEN：已禁用的终端设备数量		

h) 查询单个终端设备统计信息

应用通过本接口，从M2M平台的数据库中查询单个终端的统计数据。该接口为同步接口，应用向M2M平台发出请求后，M2M平台从数据库记录中查询被请求终端的信息，然后返回给应用。

调用名称：PTermStatisticQuery

查询单个终端统计信息请求（P_TERM_STATISTIC_QUERY_Req）

参数标识	PTermStatisticQueryReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PTermStatisticQueryReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PTermStatisticQueryReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <DATERANGE start=起始时间 end=终止时间/> <ALARMCOUNT/> <LOGINCOUNT/> <LASTLOGIN/> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
DATERANGE	统计时间段。该元素有两个属性： （1） start：统计起始时间； （2） end：统计终止时间		0
ALARMCOUNT	终端发生的告警次数		0

LOGINCOUNT	终端登录次数		0
LASTLOGIN	终端最后一次登录时间		0

查询单个终端设备统计信息响应(P_TERM_STATISTIC_QUERY_Resp)

参数标识	PTermStatisticQueryRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PTermStatisticQueryRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PTermStatisticQueryRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <ALARMCOUNT>终端告警次数</ALRAMCOUNT> <LOGINCOUNT>终端登录次数</LOGINCOUNT> <LASTLOGIN>最后一次登录时间</LASTLOGIN> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
ALARMCOUNT	终端发生的告警次数	整数	4
LOGINCOUNT	终端登录次数	整数	4
LASTLOGIN	终端最后一次登录时间	整数	4

i) 终端设备远程控制

应用通过本接口对终端发送控制指令，控制终端重启、复位等操作。该接口为异步接口，应用向M2M平台发出请求后，M2M平台的应答只表示收到该请求。M2M平台接收到该消息之后，将其转换成WMMP-T协议的REMOTE_CTRL发送给M2M终端，M2M终端响应该控制消息后，M2M平台通过T_TERM_CTRL_RESULT接口转发给应用。

调用名称：TTermCtrl

请求消息(T_TERM_CTRL_Req)

参数标识	TTermCtrlReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermCtrlReq>

	<HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermCtrlReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMLIST> <TERMID>终端设备序列号</TERMID> …… </TERMLIST> <FILTER> <TERMIDRANGE start=终端序列号起始号码 end=终端设备序列号终止号码/> <MODEL>终端型号</MODEL> <PRODUCTOR>终端厂家</PRODUCTOR> <REGISTDATE start=起始日期 end=终止日期/> <AREA>终端安装的地区</AREA> </FILTER> <REMOTECTRL> <TAG id=远程控制指令TAG/> …… </REMOTECTRL> <LOGOUT>强制终端设备登出的原因</LOGOUT> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMLIST	需要操作的终端序列号列表。该标签和FILTER标签互斥。	String	不定长
FILTER	过滤条件，即需要进行操作的终端的选择条件。该标签和TERMLIST互斥。FILTER包含如下几个子元素： TERMIDRANGE：终端序列号的起始号段，包含开始和终止号码两个子元素； MODEL：终端型号编码；	String	不定长

	PRODUCTOR：终端厂家代码； REGISTDATE：终端上线注册的日期范围； AREA：安装终端的地区。采用电话区号。		
REMOTECTRL	远程控制指令TAG，为4位16进制字符串（参见附录A（5）下行控制相关内容）。可重复使用。 REMOTECTRL与LOGOUT指令互斥，在本消息中只能出现一个。	String	4
LOGOUT	0：正常退出，进入等待激活模式； 1：准备升级；（此项一般由M2M终端发起） 2：故障断开； 3：应用新配置；（此项一般由M2M终端发起）； 4：心跳超时； 5：故障退出，进入等待激活模式 其他：保留。 LOGOUT指令与REMOTECTRL指令互斥，在本消息中只能出现一个。	String	2

响应消息(T_TERM_CTRL_Resp)

参数标识	TRemoteCtrlRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TRemoteCtrlRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TRemoteCtrlRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> <REMOTECTRL>无效远程控制指令TAG</REMOTECTRL>		

	</BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回结果代码。 0——M2M 平台接受请求 1——M2M 平台拒绝请求 2——该应用未登录 其他：失败，原因待定。	String	2

j) 终端设备对远程控制执行结果通知

终端响应应用下发的远程控制指令后,M2M平台通过本接口向应用转发终端的响应结果。T_TERM_CTRL_RESULT包头中的消息序号SID应与对应的T_TERM_CTRL包头中的SID一致。

调用名称：TTermCtrlResult

M2M平台转发终端的远程控制响应请求消息(T_TERM_CTRL_RESULT_Req)

参数标识	TTermCtrlResultReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermCtrlResultReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermCtrlResultReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <RESULTCODE>返回结果代码</RESULTCODE> <REMOTECTRL> <TAG id=无效远程控制指令TAG/> …… </REMOTECTRL> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
RESULTCODE	响应结果代码 0——接收成功并执行控制指令 1——数据无效 2——接收成功，有无效命令	String	2

	其他：失败，原因待定		
REMOTECTRL	终端不能处理的无效远程控制指令TAG（参见附录A（5）下行控制相关内容）。可重复使用。	String	4

响应消息(T_TERM_CTRL_RESULT_Resp)

参数标识	TRemoteCtrlResultRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TRemoteCtrlResultRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </TRemoteCtrlResultRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
TRemoteCtrlResultRsp包是对TRemoteCtrlResultReq包请求的确认，无消息体			

k) 终端设备远程更新

应用通过本接口向终端发送下载更新通知。该接口为异步接口，应用向M2M平台发出请求后，M2M平台的应答只表示收到该请求。终端响应该通知消息后，M2M通过T_DOWNLOAD_RESULT接口转发给应用。

调用名称：TDownloadNotify

下载更新通知请求消息 (T_DOWNLOAD_Req)

参数标识	TDownloadNotifyReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> < TDownloadNotifyReq > <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TDownloadNotifyReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为	String	18

	YYYYMMDDHHmmssnnnn		
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMLIST> <TERMID>终端序列号</TERMID> …… </TERMLIST> <FILTER> <TERMIDRANGE start=终端序列号起始号码 end=终端序列号终止号码/> <MODEL>终端型号</MODEL> <PRODUCTOR>终端厂家</PRODUCTOR> <REGISTDATE start=起始日期 end=终止日期/> <AREA>终端安装的地区</AREA> </FILTER> <DOWNLOADURL>下载地址</DOWNLOADURL> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMLIST	需要操作的终端序列号列表。该标签和FILTER标签互斥。	String	不定长
FILTER	过滤条件，即需要进行操作的终端的选择条件。该标签和TERMLIST互斥。FILTER包含如下几个子元素： TERMIDRANGE：终端序列号的起始号段，包含开始和终止号码两个子元素； MODEL：终端型号编码； PRODUCTOR：终端厂家代码； REGISTDATE：终端上线注册的日期范围； AREA：安装终端的地区。采用电话区号。	String	不定长
DOWNLOADURL	下载地址	String	1024

下载更新响应消息(T_DOWNLOAD_Resp)

参数标识	TDownloadNotifyRsp
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TDownloadNotifyRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID>

	</HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TDownloadNotifyRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</ RESULTCODE > </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回结果代码。 0——M2M 平台接受请求 1——M2M 平台拒绝请求 2——该应用未登录 其他：失败，原因待定。	String	2

l) 终端设备软件更新结果通知

终端响应应用下发的下载通知消息后,M2M平台通过本接口向应用转发终端的响应结果。T_DOWNLOAD_RESULT包头中的消息序号SID应与对应的T_DOWNLOAD包头中的SID一致。

调用名称：TDownloadNotifyResult

M2M平台转发终端对下载通知响应的请求 (T_DOWNLOAD_RESULT_Req)

参数标识	TDownloadNotifyResultReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TDownloadNotifyResultReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TDownloadNotifyResultReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY>		

	<TERMID>终端序列号</TERMID> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>

名称	说明	数据类型	长度（字节）
TERMID	终端序列号	String	16
RESULTCODE	响应结果代码 0：已是最新版本，不需更新 1：立即准备更新 2：终端正在执行业务，暂缓更新 3：数据无效 其他：失败，原因待定。	String	2

M2M应用对M2M平台转发终端对下载通知响应的应答消息 (T_DOWNLOAD_RESULT_Resp)

参数标识	TDownloadNotifyResultRsp
消息格式	<?xml version="1.0" encoding="UTF-8"?> <DownloadNotifyResultRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </TDownloadNotifyResultRsp>

名称	说明	数据类型	长度（字节）
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
TDownloadNotifyResultRsp包是对TDownloadNotifyResultReq包请求的确认，无消息体			

m) 终端设备安全参数设置

应用通过本接口向终端发送终端安全参数配置。该接口为异步接口，应用向M2M平台发出请求后，M2M平台的应答只表示收到该请求。终端响应该通知消息后，M2M通过T_SECURITY_CONFIG_RESULT接口转发给应用。

调用名称：TSecurityConfig

请求消息(T_SECURITY_CONFIG_Req)

参数标识	TSecurityConfigReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TSecurityConfigReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID>

<table>
<tr><td></td><td colspan="3"></HEAD>
<BODY>加密后的消息体</BODY>
<HASH>消息摘要</HASH>
</TSecurityConfigReq></td></tr>
<tr><td>名称</td><td>说明</td><td>数据类型</td><td>长度（字节）</td></tr>
<tr><td>SID</td><td>消息流水号</td><td>String</td><td>16</td></tr>
<tr><td>TIMESTAMP</td><td>系统时间戳，格式为YYYYMMDDHHmmssnnnn</td><td>String</td><td>18</td></tr>
<tr><td>SERVICEID</td><td>业务应用标识</td><td>String</td><td>16</td></tr>
<tr><td colspan="4">未加密的消息体格式</td></tr>
<tr><td>消息体格式</td><td colspan="3"><BODY>
<TERMID>终端序列号</TERMID>
<OPERATION>对终端的操作</OPERATION>
<SECURITY>
<TAG id=安全项TAG>安全项配置的值</TAG>
……
<TAG id=E021>(SECURITY_CONFIG报文+接入密码)的摘要值</TAG>
</SECURITY>
</BODY></td></tr>
<tr><td>名称</td><td>说明</td><td>数据类型</td><td>长度（字节）</td></tr>
<tr><td>TERMID</td><td>需要操作的终端的序列号</td><td>String</td><td>16</td></tr>
<tr><td>OPERATION</td><td>0x00——平台以明文设置终端安全参数（M2M平台只能通过短信方式下发）
0x01——平台以密文设置终端安全参数(任何通信方式)
0x02——平台读取终端安全参数
0x03——平台下发安全参数更新通知,要求终端进入短信模式,准备接收明文安全参数
0x04——终端上报安全参数
0x05——终端请求以明文更新安全参数
0x06——终端请求以密文更新安全参数
0x07——终端启用各类安全参数</td><td>Intiger</td><td>3</td></tr>
<tr><td rowspan="4">SECURITY</td><td colspan="2">可选安全相关参数（参见附录A（6），安全控制相关内容）：</td><td rowspan="4">String</td><td rowspan="4">不定长</td></tr>
<tr><td>OPERATION=0x00</td><td>设置的安全参数为表示密码或密钥值、启用标识、有效期的TLV</td></tr>
<tr><td>OPERATION=0x01</td><td>经过加密的安全参数</td></tr>
<tr><td>OPERATION=0x02</td><td>读取的安全参数为表示密码或密钥值的摘要、启用标识、有效</td></tr>
</table>

		期的TLV，其中L=0		
	OPERATION=0x03	要更新的安全参数的TLV		
	OPERATION=0x04	上报的安全参数为表示密码或密钥值的安全摘要、启用标识、有效期的TLV		
	OPERATION=0x05/0x06	请求的安全参数为表示密码或密钥值、启用标识、有效期的TLV，其中L=0		
	OPERATION=0x07	启用的安全参数的启用标识的TLV		
	TAG id=E021： (SECURITY_CONFIG报文+接入密码)的摘要值： MD5(SECURITY_CONFIG报文+上行接入密码)		String	16

响应消息(T_SECURITY_CONFIG_Resp)

参数标识	TSecurityConfigRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TSecurityConfigRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TSecurityConfigRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</ RESULTCODE > </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回结果代码。 0——M2M 平台接受请求 1——M2M 平台拒绝请求 2——该应用未登录	String	2

	其他：失败，原因待定。		

n) 终端设备安全参数配置结果通知

终端响应应用下发的安全参数配置消息后，M2M平台通过本接口向应用转发终端的响应结果。

T_SECURITY_CONFIG_RESULT包头中的消息序号SID应与对应的T_SECURITY_CONFIG包头中的SID一致。

调用名称：TSecurityConfigResult

请求消息(T_SECURITY_CONFIG_RESULT_Req)

参数标识	TSecurityConfigResultReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TSecurityConfigResultReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TSecurityConfigResultReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <RESULTCODE>返回结果代码</RESULTCODE> <SECURITY> <TAG id=安全项TAG>安全项配置的值</TAG> …… <TAG id=E021>(SECURITY_CONFIG_RESULT报文+接入密码)的摘要值</TAG> </SECURITY> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
RESULTCODE	响应结果代码 操作应答代码 0x00——终端或平台接受请求 0x01——错误，终端基本标识的安全摘要校验错误	String	2

	0x02——错误，有不支持的TLV 0x03——拒绝终端启用安全参数，仅对OPERATION=4的请求有效 0x04——错误，终端 其他：失败，原因待定。			
SECURITY	RESULTCODE = 0x00	OPERATION=0x00	无SECURITY段	
		OPERATION=0x01	无SECURITY段	
		OPERATION=0x02	返回的终端安全参数TAG	
		OPERATION=0x03	无SECURITY段	
		OPERATION=0x04	无SECURITY段	
		OPERATION=0x05	无SECURITY段，M2M终端接收后进入短信模式接收密码	
		OPERATION=0x06	返回加密的安全参数TAG	
		OPERATION=0x07	无SECURITY段	
	RESULTCODE = 0x01	无SECURITY段		
	RESULTCODE = 0x02	返回不支持的TAG，格式为<TAG id=安全项TAG/>		
	RESULTCODE = 0x03	返回拒绝的安全参数的启用标识TAG，格式为<TAG id=安全项TAG/>		

响应消息(T_SECURITY_CONFIG_RESULT_Resp)

参数标识	TSecurityConfigResultRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TSecurityConfigResultRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </TSecurityConfigResultRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
TDownloadNotifyResultRsp包是对TDownloadNotifyResultReq包请求的确认，无消息体			

o) 终端设备注册通知

终端向M2M平台注册成功后，M2M平台根据终端的订购关系，向为该终端提供业务的应用系统发送终端注册通知消息。

调用名称：TRegist

请求消息(T_REGIST_Req)

参数标识	TRegistReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TRegistReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TRegistReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <IMEI>终端的IMEI号</IMEI> <IMSI>终端的IMSI号</IMSI> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号（即终端注册后，平台为其分配的序列号，或终端预置的合法序列号）	String	16
IMEI	终端的IMEI号。长度16字节或15字节	String	16或15
IMSI	终端的IMSI号	String	15

响应消息(T_REGIST_Resp)

参数标识	TRegistRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TRegistRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TRegistRsp>		
名称	**说明**	**数据类型**	**长度（字节）**

SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回注册结果 0：注册成功 1：登录成功，但需要下发配置 2：应用拒绝该终端的注册 其他：保留。	String	2

p) 终端设备登录通知

当终端在M2M平台注册成功，并登录到M2M平台时，M2M平台根据终端的订购关系，向相应的应用系统发送该终端的登录信息。

调用名称：TLogin

请求消息(T_LOGIN_Req)

参数标识	TLoginReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TLoginReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TLoginReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <IMEI>终端的IMEI号</IMEI> <IMSI>终端的IMSI号</IMSI> <TERMVER>终端版本号</TERMVER> <CONFIGCRC>终端配置参数的CRC32校验</CONFIGCRC>		

	<PARAM>终端上报的参数TAG1 <VALUE>参数值</VALUE> </PARAM> <PARAM>终端上报的参数TAG2 <VALUE>参数值</VALUE> </PARAM> …… </BODY>

名称	说明	数据类型	长度（字节）
TERMID	终端序列号	String	16
IMEI	终端的IMEI号。长度16字节或15字节	String	16或15
IMSI	终端的IMSI号	String	15
TERMVER	终端版本号	String	8
CONFIGCRC	终端全部配置信息 CRC32 校验和：校验值为终端所有配置参数，如果参数没有配置，则无需校验；按TLV的 TAG 值由小到大排序后，对整个 TLV 组进行 CRC32 计算。 M2M平台通过对比平台存储的用户定制配置参数的CRC32校验和以及终端上报的本地配置参数CRC32校验和，判断终端的配置参数内容与平台存储的信息是否一致。 本字段应填写CRC32校验和的16进制编码，共8个字符。	String	8
PARAM	终端上报M2M平台和应用的可选参数值，参见下表（终端登录时上报的参数）。可重复使用。	String	4 VALUE长度为不定长，与PARAM相关

终端登录时上报的参数：

终端登录时上报的可选参数		
参数 TAG	**字节数**	注释
0106	2	**心跳间隔（可选参数）**
0107	1	数据包响应超时，见附录（可选参数）
0108	1	传输失败最大允许重发次数,value 取值范围（单位 次）：1~5 0：表示不重发。 （可选参数）
3006	4	Cellular ID，终端所在小区标识（高 16 位表示 LAC，低 16 位表示 CI）（可选）
3007	1	SigIntensity，本地信号场强，0－100（可选）
3010		终端外设，（可选字段） 外设类型采用 2 个字节编码，允许扩展，目前系统预留了如下外设编码：

		0x0001——PRN：打印机 0x0002——SCAN：扫描枪 0x0003——POS：POS 刷卡器 0x0004——IC：IC 卡感应器 0x0005——KEY：密码小键盘 0x0006——PHONE：外接话机 DEV 的值为外设编码的序列，无间隔，例如： TAG | Len | Value 0x3010 | 6 | 0x000100020003 表示三个外设编号分别为 0x0001, 0x0002, 0x0003

响应消息(T_LOGIN_Resp)

参数标识	TLoginRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TLoginRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TLoginRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回注册结果 0：登录成功，不需要下发配置 1：登录成功，但需要下发配置 2：非法 MSISDN/IMSI 3：非法终端序列号； 4：终端序列号冲突：上报的序列号已有对应的其它终端正在平台正常工作且 IMSI/MSISDN 不同； 5：通信协议版本不兼容； 6：终端没有 REGIST（注册） 其他：保留。	String	2

q) 终端设备登出通知

终端在M2M平台退出登录时，M2M平台根据终端的订购关系，向相应的应用系统发送该终端的退出登录信息。

调用名称：TLogout

请求消息(T_LOGOUT_Req)

参数标识	TLogoutReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TLogoutReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TLogoutReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <LOGOUTREASON>终端退出登录原因</LOGOUTREASON> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
LOGOUTREASON	0：正常退出，进入等待激活模式； 1：准备升级；（此项一般由 M2M 终端发起） 2：故障断开； 3：应用新配置；（此项一般由 M2M 终端发起）； 4：心跳超时； 5：故障退出，进入等待激活模式 其他：保留。	String	16

响应消息(T_LOGOUT_Resp)

参数标识	TLogoutRsp
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TLogoutRsp> <HEAD>

	<SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </TLogoutRsp>

名称	说明	数据类型	长度（字节）
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
TLogoutRsp包是对TLogoutReq包请求的确认，无消息体。			

r) 链路检测

如果M2M应用采用长连接方式和M2M平台交互，则由M2M平台定期向应用系统发送链路检测包以维持链路。如果M2M应用连续3个包没有应答，则M2M平台可以认为链路失效，可断开链路。

调用名称：PLinkCheck

链路检测请求(P_LINKCHECK_Req)

参数标识	PLinkCheckReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PLinkCheckReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </PLinkCheckReq>

名称	说明	数据类型	长度（字节）
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
本消息没有消息体。			

链路检测响应(P_LINKCHECK_Resp)

参数标识	PLinkCheckRsp
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PLinkCheckRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP>

	<SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </PLinkCheckRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
本消息无消息体。			

s) 业务数据上传

终端设备和M2M应用之间可以通过本接口进行双向的透明数据传输。终端设备可以通过本接口将数据发送至M2M平台，由M2M平台转发给M2M应用。

调用名称：TTransparentDataUp

请求消息(T_TRANSPARENT_DATA_UP_Req)

参数标识	TTransparentDataUpReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTransparentDataUpReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTransparentDataUpReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <DATA>应用数据</DATA> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
DATA	终端向应用发送的应用数据。如果应用需要发送二进制数据，可以采用BASE64编码。	String	不限

响应消息(T_TRANSPARENT_DATA_UP_Resp)

参数标识	TTransparentDataUpRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTransparentDataUpRsp > <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTransparentDataUpRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</ RESULTCODE > </BODY>		
名称	**说明**	**名称**	**说明**
RESULTCODE	返回结果代码。 0——应用系统接受请求 1——应用系统拒绝请求 其他：失败，原因待定。	RESULTCODE	

t) 业务数据下发

应用和终端之间可以通过本接口进行双向的透明数据传输。企业应用服务器可以通过本接口将数据发送至M2M终端（必要的话，M2M终端再转发给它连接的下端设备）。

调用名称：TTransparentDataDown

请求消息(T_TRANSPARENT_DATA_DOWN_Req)

参数标识	TTransparentDataDownReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTransparentDataDownReq > <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTransparentDataDownReq>		
名称	**说明**	**数据类型**	**长度（字节）**

SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMLIST> <TERMID>终端序列号</TERMID> …… </TERMLIST> <FILTER> <TERMIDRANGE start=终端序列号起始号码 end=终端序列号终止号码/> <MODEL>终端型号</MODEL> <PRODUCTOR>终端厂家</PRODUCTOR> <REGISTDATE start=起始日期 end=终止日期/> <AREA>终端安装的地区</AREA> </FILTER> <DATA>应用数据</DATA> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMLIST	需要操作的终端序列号列表。该标签和FILTER标签互斥。	String	不定长
FILTER	过滤条件，即需要进行操作的终端的选择条件。该标签和TERMLIST互斥。FILTER包含如下几个子元素： TERMIDRANGE：终端序列号的起始号段，包含开始和终止号码两个子元素； MODEL：终端型号编码； PRODUCTOR：终端厂家代码； REGISTDATE：终端上线注册的日期范围； AREA：安装终端的地区。采用电话区号。	String	不定长
DATA	应用向终端发送的应用数据。如果应用需要发送二进制数据，可以采用BASE64编码。	String	不限

响应消息(T_TRANSPARENT_DATA_DOWN_Resp)

参数标识	TTransparentDataDownRsp
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTransparentDataDownRsp > <HEAD>

	<SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTransparentDataDownRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</ RESULTCODE > </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回结果代码。 0——M2M 平台接受请求 1——M2M 平台拒绝请求 2——该应用未登录 其他：失败，原因待定。	String	2

u) 业务数据下发结果通知

M2M平台在完成将T_TRANSPARENT_DATA_DOWN消息中数据向终端发送，并获得确定结果后，通过本接口向M2M应用返回处理结果。

T_TRANSPARENT_DATA_DOWN_RESULT 包头中的消息序号SID应与对应的T_TRANSPARENT_DATA_DOWN包头中的SID一致。

调用名称：TTransparentDataDownResult

请求消息(T_TRANSPARENT_DATA_DOWN_RESULT_Req)

参数标识	TTransparentDataDownResultReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTransparentDataDownResultReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTransparentDataDownResultReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16

TIMESTAMP	系统时间戳,格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端序列号</TERMID> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端序列号	String	16
RESULTCODE	响应结果代码 0——成功下发给终端 1——终端不在线 2——终端无应答 3——终端接收异常 其他：失败，原因待定。	String	2

响应消息(T_TRANSPARENT_DATA_DOWN_RESULT_Resp)

参数标识	TTransparentDataDownResultRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTransparentDataDownResultRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTransparentDataDownResultRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
本消息无消息体			

v) 终端参数设置

M2M应用通过本接口发送指令设置M2M终端设备的某些参数。该接口为异步接口，M2M应用向M2M平台发出请求后，M2M平台的应答只表示收到该请求。终端设备响应该参数设置请求后，M2M平台通过CONFIG_SET_RESULT接口向M2M应用转发终端设备处理结果。

调用名称：TConfigSet

终端设备参数设置请求(T_CONFIG_SET_Req)

参数标识	TConfigSetReq

消息格式	<?xml version="1.0" encoding="UTF-8"?> <TConfigSetReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TConfigSetReq >		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMLIST> <TERMID>终端设备序列号</TERMID> …… </TERMLIST> <FILTER> <TERMIDRANGE start=终端设备序列号起始号码 end=终端设备序列号终止号码/> <MODEL>终端设备型号</MODEL> <PRODUCTOR>终端设备厂家</PRODUCTOR> <REGISTDATE start=起始日期 end=终止日期/> <AREA>终端设备安装的地区</AREA> </FILTER> <CONFIG> <TAG id=配置项TAG>配置项的值</TAG> …… </CONFIG> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMLIST	需要操作的终端设备序列号列表。该标签和FILTER标签互斥。	String	不定长
FILTER	过滤条件，即需要进行操作的终端设备的选择条件。该标签和TERMLIST互斥。FILTER包含如下几个子元素： TERMIDRANGE：终端设备序列号的起始号段，包含开始和终止号码两个子元素；	String	不定长

	MODEL：终端设备型号编码； PRODUCTOR：终端设备厂家代码； REGISTDATE：终端设备上线注册的日期范围； AREA：安装终端设备的地区。采用电话区号。		
CONFIG	应用向终端设备设置的配置数据（参见附录A：（1）配置参数相关内容），可重复使用	String	4 VALUE长度与配置数据TAG有关

终端设备参数设置响应(T_CONFIG_SET_Resp)

参数标识	TConfigSetRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TConfigSetRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TConfigSetRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</ RESULTCODE > </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	返回结果代码。 0——M2M 平台接受请求 1——M2M 平台拒绝请求 2——该应用未登录 其他：失败，原因待定。	String	2

w) 终端设备参数设置结果

终端设备响应M2M应用下发的参数配置指令后，M2M平台通过本接口向M2M应用转发终端设备的响应结果。

T_CONFIG_SET_RESULT包头中的消息序号SID应与对应的T_CONFIG_SET包头中的SID一致。

调用名称：TConfigSetResult

终端设备参数设置结果请求(T_CONFIG_SET_RESULT_Req)

参数标识	TConfigSetResultReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TConfigSetResultReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TConfigSetResultReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为 YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端设备序列号</TERMID> <RESULTCODE>返回结果代码</ RESULTCODE > <CONFIG> <TAG id=终端设备不支持的配置项TAG/> …… </CONFIG> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端设备序列号	String	16
RESULTCODE	响应结果代码 0——接收成功 1——数据无效 其他：失败，原因待定。	String	2
CONFIG	终端设备不支持的配置项TAG，为4位16进制字符串（参见附录A：（1）配置参数相关内容），可重复使用	String	4

终端设备参数设置结果响应(T_CONFIG_SET_RESULT_Resp)

参数标识	**TConfigSetResultRsp**
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TConfigSetResultRsp> <HEAD> <SID>消息流水号</SID>

	<TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </TConfigSetResultRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
TConfigSetResultRsp包是对TConfigSetResultReq包请求的确认，无消息体			

x) 终端设备请求参数配置

M2M平台通过本接口向M2M应用请求终端设备的配置信息。

调用名称：TConfigReq

终端设备请求参数配置请求(T_CONFIG_REQ_Req)

参数标识	TConfigReqReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TConfigReqReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> <TERMID>终端设备序列号</TERMID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TConfigReqReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
TERMID	终端设备序列号	String	16
未加密的消息体格式			
消息体格式	<BODY> <CONFIG>配置项TAG</CONFIG> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
CONFIG	终端设备请求的配置参数TAG（参见附录A：（1）配置参数相关内容），可重复使用	String	4

终端设备请求配置响应(T_CONFIG_REQ_Resp)

参数标识	TConfigReqRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TConfigReqRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TConfigReqRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</ RESULTCODE > <CONFIG> <TAG id=配置项TAG/> …… </CONFIG> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	响应结果代码 0——接收成功 1——数据无效 其他：失败，原因待定。	String	2
CONFIG	无效的配置项 TAG，为 4 位 16 进制字符串（参见附录 A：（1）配置参数相关内容），可重复使用	String	4

y) 终端设备上报信息

M2M终端设备向M2M平台上报信息，包括告警信息、统计信息、配置信息。M2M平台通过本接口向终端设备订购的M2M应用转发上报的信息。一个T_TERMINFO_REPORT包体中可以同时包含告警、统计或者是配置信息。同时也可以包含0x3006、0x3007、0x3003等终端设备相关属性信息。具体告警信息、统计信息、配置信息参见“附A TLV说明”部分。

调用名称：TTermInfoReport

终端设备上报信息请求(T_TERMINFO_REPORT_Req)

参数标识	TTermInfoReportReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermInfoReportReq>

	<HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermInfoReportReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <TERMID>终端设备序列号</TERMID> <MONITOR> <TAG id=终端设备监控内容TAG>终端设备监控数据</TAG> …… </MONITOR> <ALARM> <CODE>故障代码1</CODE> <CODE>故障代码2</CODE> …… </ALARM> <RECOVERY> <CODE>已恢复的故障代码1</CODE> <CODE>已恢复的故障代码2</CODE> …… </RECOVERY > <CONFIG> <TAG id=配置项TAG>配置项的值</TAG> …… </CONFIG> <STATISTIC> <TAG id=统计项TAG>统计值</TAG> </STATISTIC> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
TERMID	终端设备序列号	String	16
MONITOR	终端设备返回的终端设备监控数据的TAG，包含一个VALUE子节点，为该TAG的值。（附录A（4）终端设备监控相关内容）。消息中可重复使用	String	4 VALUE长度与监控数据TAG有关

	MONITOR。		
ALARM	终端设备返回故障代码列表（参见附录A（4）终端设备监控相关内容，0x300D（报警代码））。	String	CODE值的长度为4
RECOVERY	终端设备返回已恢复的故障代码列表（参见附录A（4）终端设备监控相关内容，0x300D（报警代码））。	String	CODE值的长度为4
CONFIG	终端设备返回的配置数据（参见附录A:（1）配置参数相关内容），可重复使用	String	4 VALUE长度与配置数据TAG有关
STATISTIC	终端设备返回的统计数据（参见附录A:（3）终端设备统计相关内容），可重复使用	String	4 VALUE长度与配置数据TAG有关

终端设备上报信息响应(T_TERMINFO_REPORT_Resp)

参数标识	TTermInfoReportRsp		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <TTermInfoReportRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </TTermInfoReportRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <RESULTCODE>返回结果代码</RESULTCODE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
RESULTCODE	0：数据正确； 1：数据无效； 其他：失败，原因待定。	String	2

z) 基本密钥过期通知

当基本密钥超过有效期，管理员如果更新了M2M平台和M2M应用间的基本密钥，M2M平台通过本接口通知M2M应用基本密钥已过期。M2M应用的管理员应通过M2M平台的门户下载基本密钥或通过EMAIL信箱接收基本密钥。

调用名称：PKeyExpiration

基本密钥过期通知请求(P_KEY_EXPIRATION_Req)

参数标识	PKeyExpirationReq		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PKeyExpirationReq> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <BODY>加密后的消息体</BODY> <HASH>消息摘要</HASH> </PKeyExpirationReq>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳，格式为YYYYMMDDHHmmssnnnn	String	18
SERVICEID	业务应用标识	String	16
未加密的消息体格式			
消息体格式	<BODY> <DATE>密钥过期的日期</DATE> </BODY>		
名称	**说明**	**数据类型**	**长度（字节）**
DATE	密钥过期的日期	整形	2

基本密钥过期通知响应(P_KEY_EXPIRATION_Resp)

参数标识	**PKeyExpirationRsp**		
消息格式	<?xml version="1.0" encoding="UTF-8"?> <PKeyExpirationRsp> <HEAD> <SID>消息流水号</SID> <TIMESTAMP>时间戳</TIMESTAMP> <SERVICEID>业务应用标识</SERVICEID> </HEAD> <HASH>消息摘要</HASH> </PKeyExpirationRsp>		
名称	**说明**	**数据类型**	**长度（字节）**
SID	消息流水号	String	16
TIMESTAMP	系统时间戳,格式为YYYYMMDDHHmmssnnnn	String	18

SERVICEID	业务应用标识	String	16
本消息无消息体。			

附录 I
（资料性附录）
同步交互报文与异步交互报文

在协议中，应答报文往往是表示应答方对请求方所发报文的正确接收或理解，而无法确认应答方对请求方命令的执行结果。因此，往往需要再发起一次数据交互以确认请求方的请求是否被应答方正确执行。

根据一次报文交互能否完成一个完整的逻辑事件，可以将报文分为同步交互报文和异步交互报文。若一次报文交互即可完成某个完整的逻辑事件，则该次报文交互的请求和应答报文即为同步交互报文；若一次报文交互只完成某个完整的逻辑事件的某一部分，还需要其它报文交互的配合才能完成该逻辑事件，则用于完成该逻辑事件的报文交互的请求和应答报文即为异步交互报文。与之对应，只需要一次报文交互即可完成的逻辑事件，称为同步交互事件；反之，则称为异步交互事件。

在M2M终端设备和M2M平台的数据交互中，异步交互事件多为涉及M2M终端设备参数设置的操作。