# STK模块基础知识总结

|  |  |  |
| --- | --- | --- |
| Date  日期 | Version  版本 | Comments  备注 |
| 2018-12-19 | 0.1 | First version |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Function  职位 | Name  姓名 | Date  日期 | Signature  签名 |
| Written by  拟定 | Software Engineer | 曾灿炫 | 2018/12/19 | 曾灿炫 |
| Verified by  审核 |  |  |  |  |
| Verified by  审核 |  |  |  |  |
| Approved by  批准 |  |  |  |  |

目录

[STK模块基础知识总结 1](#_Toc533239757)

[1. 概述 3](#_Toc533239758)

[**1.1.** **本文档的目的** 3](#_Toc533239759)

[**1.2.** **背景** 3](#_Toc533239760)

[**1.3.** **缩略语清单** 3](#_Toc533239761)

[**1.4.** **参考文献** 3](#_Toc533239762)

[2. 基本概念 4](#_Toc533239763)

[2.1. STK包含的机制 5](#_Toc533239764)

[2.2. 涉及的命令(ME->SIM) 5](#_Toc533239765)

[2.3. TERMINAL PROFILE 6](#_Toc533239766)

[2.4. Envelope 6](#_Toc533239767)

[2.5. Proactive Command(SIM->ME) 7](#_Toc533239768)

[2.6. Terminal Response 8](#_Toc533239769)

[3. 关键流程分析 8](#_Toc533239770)

[3.3. Profile download 8](#_Toc533239771)

[3.4. Proactive Command 9](#_Toc533239772)

[4. 总结 10](#_Toc533239773)

# 概述

* 1. **本文档的目的**

*本文档为学习输出文档，目的在于总结STK的基础概念，并记录主动式命令的运作流程。*

* 1. **背景**

*STK即SIM Tool Kit，它提供一系列用于移动设备与SIM卡间交互的机制。通过这些机制，支持STK的手机可以操作SIM卡里的应用。*

* 1. **缩略语清单**

| Term | Explanation |
| --- | --- |
| STK | SIM Tool Kit（SIM卡工具箱） |
| SAT | SIM Application Toolkit（同STK，SIM卡应用工具箱） |
| CAT | Card Application Toolkit（卡应用工具箱） |
| ME | Mobile Equipment（移动设备） |
| TP | Terminal Profile |
| TR | Terminal Response |
| SW1/SW2 | Status Word 1 / Status Word 2 |
| BER | Basic Encoding Rules of ASN.1 |
| TLV | Tag, Length, Value |
| SS | Supplementary Service（补充业务） |
| USSD | Unstructured Supplementary Service Data（非结构化补充数据业务） |
| 3GPP | 3rd Generation Partnership Project（第三代合作伙伴计划） |
| ETSI | European Telecommunication Standard Insitute（欧洲电信标准协会） |

* 1. **参考文献**

| Document | Explanation |
| --- | --- |
| 3GPP TS 11.14 | Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 1999) |
| 3GPP TS 11.11 | Specification of the Subscriber Identity Module -Mobile Equipment (SIM - ME) interface(Release 1999) |
| 3GPP TS 31.124 | Universal Subscriber Identity Module Application Toolkit (USAT) conformance test specification (Release 10) |
| STK模块知识总结 | 参考yangning.hong总结的《STK模块知识总结》 |
| Android STK模块学习总结  --基于Android 4.2 | 参考jianping.zhang总结的《Android STK模块学习总结--基于Android 4.2》 |

# 基本概念

ME和SIM的通信遵从ISO的T=0协议**（ISO 7816-3：异步半双工字符传输协议）**。在该协议中，命令都是由ME发给SIM卡的，没有SIM卡发起与ME通信的机制。这样看来，如果SIM卡需要主动请求ME的支持是不可能的。

主动式SIM卡，顾名思义，SIM卡掌握了主动权。**通过proactive命令，主动式SIM卡可以要求ME进行相应的操作**，感觉像是SIM卡“控制”了ME。

ME和SIM卡需要知道对方是否支持proactive SIM。如果SIM卡是主动式SIM卡，应该在SIM卡的业务表中的相应业务进行标识(Service n°29—11.11 EF**SST**)，而如果ME支持主动式SIM卡，在确定是Proactive SIM的情况下，通过profile download命令通知SIM卡。这样，通信双方之间就有了共识：在之后的通信过程中，proactive SIM不会向不支持proactive SIM的ME发送任何命令请求；支持proactive SIM的ME也不会向未激活proactive SIM的SIM发送与proactive SIM有关的命令。

主动式SIM卡仍然使用T=0协议，通过增加一个新的状态响应字SW1来实现SIM卡的主动权。列示了与proactive command有关的新的返回报告内容

|  |  |  |
| --- | --- | --- |
| SW1 | SW2 | 解释 |
| 90 | 00 | 正常的成功报告，SIM卡无其他SAT命令 |
| 91 | xx | 命令成功执行，有一个长为xx的proactive command |
| 93 | 00 | SIM卡正忙于执行前一个proactive command |
| 9E | xx | SIM数据下载时出错，有一个长为xx的回应 |

’90 00’表示命令正常结束。’91 XX’除了像’90 00’一样通知ME SIM卡成功执行完前一个命令，还包含了一个SIM卡的命令，告诉ME还需要执行一个动作。然后ME使用fetch命令来取得这个数据，XX表示相应数据的长度。

### STK包含的机制

1. Profile Download，Proactive SIM，Data download to SIM，Menu selection，Call control by SIM，MO Short Message control by SIM，Event download，security，Multiple card，Timer Expiration，Bearer Independent Protocol

其中， **Profile Download**用于通知SIM卡ME的功能。ME通过SIM 服务表和EFPHASE了解SIM卡的功能，在SIM的初始化过程，ME会通过TERMINAL PROFILE命令发送一个配置文件，告诉SIM卡它所能支持的与SIM卡相关的功能。具体的命令编码请查看3GPP TS 11.14。

**Proactive SIM**则用来让SIM卡可以控制ME执行某些行为，如显示保存于SIM卡的文本发短信息，拨打保存于SIM卡的号码，发送SS，USSD等。基本是于涉及到用户的行为都可使用该机制。

### 2.2. 涉及的命令(ME->SIM)

**- TERMINAL PROFILE**

This function is used by the ME to transmit to the SIM its capabilities concerning the SIM Application Toolkit functionality.

该命令是ME用来告诉SIM卡它所支持的功能。

Input:

terminal profile.

Output:

none.

* **ENVELOPE**

该命令用来传输命令相关的数据给位于SIM卡里的应用。

Input:

data string.

Output:

- The structure of the data is defined in TS 11.14 [27].

* **FETCH**

该命令用来获取一个主动式命令。

Input:

none.

Output:

data string containing an SIM Application Toolkit command for the ME.

* **TERMINAL RESPONSE**

该命令发送上一个主动式命令的结果给SIM卡

Input:

data string containing the response.

Output:

none.

### TERMINAL PROFILE

Terminal Profile的结构和编码组成，请查看3GPP TS 11.14 5.2节Structure and coding of TERMINAL PROFILE。

### Envelope

- **SMS-PP DOWNLOAD**，当ME收到一条短信，协议标识符=SIM卡数据下载，数据编码方案=第二级消息时，ME将通过使用Envelope（SMS-PP DOWNLOAD）透明地将消息传递到SIM。移动将不会显示这条短信，也不会提示用户。

- **CELL BROADCAST DOWNLOAD**，当ME接收新SMSCB，如果该CB的CBMI在EF\_CBMID被找到，则ME将使用Envelope（CELL BROADCAST DOWNLOAD）通过CB页传递到SIM卡。ME将不会显示该CB给用户。

- **MENU SELECTION**，当ME从SIM卡发送的“SETUP MENU”命令定义的一个菜单项目中收到菜单选择时，或者用户需要对某一菜单项得到帮助信息时，ME会通过Envelope(MENU\_SELECTION)将所选菜单项的标识符传给SIM卡。

- **CALL CONTROL**，呼叫控制，SIM卡可以使用这个命令来决定是否要将一个播出的电话（SATK播出或MMI播出），一个SS服务（无论是Send SS或MMI SS），USSD的初始化（无论是Send USSD或MMI USSD）修改成同一类型的服务，但是不同的参数，或者可以将它们修改成与前一个不同新类型的服务。

- **MO SHORT MESSAGE CONTROL**，对于所有MO短消息尝试，ME用ENVELOPE (MO message control)命令，首先把业务中心地址-RP\_destination\_addres及收件人地址-TP\_destination\_adderss传递给SIM卡。ME还应使用ENVELOPE(MO message control)命令将当前服务小区的信息传递给SIM卡。

-  **TIMER EXPIRATION**，当一个由TIMER MANAGEMENT的主动式命令去启动的定时器超时，ME应该使用ENVELOPE (TIMER EXPIRATION)去传递这个定时器的标识符和值给SIM。

- **EVENT DOWNLOAD**，SIM卡用SETUP EVENT LIST命令为ME提供一套监控事件。如SIM卡已发出此命令，并且列表中的事件发生，ME会使用和此事件相关的过程通知SIM卡。

### Proactive Command(SIM->ME)

- **CLOSE CHANNEL**, 要求ME关闭指定的数据通道.

- **DISPLAY** **TEXT**, 在屏幕显示文本或者图表，高优先级的可覆盖其他内容.

- **GET CHANNEL STATUS**,要求ME返回所有可用数据通道的当前信息.

- **GET INKEY**, 在屏幕显示文本或图表，获取用户输入的字符并将字符传输给SIM卡。

- **GET INPUT**, 在屏幕显示文本或图表，获取用户的任何响应并将其传输给SIM卡。

- **GET READER STATUS**, 提供读卡器和插入卡的其他信息 (Card x state, e.g. powered on or not, Card x Presence), if class "a" is supported.

- **LANGUAGE NOTIFICATION**, 通知ME当前STK在文本字符串里使用的语言.

- **LAUNCH BROWSER**, 请求启动浏览器使ME能解析URL.

- **MORE TIME**, 用于请求更多处理时间，ME只需要返回一个正常的TR。

- **OPEN CHANNEL**,要求ME打开一个有参数显示的通道。(if class "e" is supported.)

- **PERFORM CARD APDU**, 它要求ME发送APDU命令到其他卡。这个命令与ME和其他卡之间的任何协议兼容。(if class "a" is supported)

- **PLAY TONE**, 它请求ME通过耳机、听筒或其他设备发出声音。.

- **POLL INTERVAL**, 协商在空闲模式期间ME向SIM卡发送STATUS命令的的频率、轮询操作可以由POLLING OFF命令禁止。

- **POWER OFF CARD**, 它会关闭与其他卡的会话。（如果支持Class A）

- **POWER ON CARD**, 它会发起与其他卡的会话，并且返回所有的ATR字节。（如果支持Class A）

- **PROVIDE LOCAL INFORMATION**, 要求ME将本地信息传给SIM卡，例如移动国家号码及用户注册的移动网络号码（MCC+MNC）。

- **RECEIVE DATA**, 它要求ME返回在指定通道上接收到的SIM卡数据。（如果支持Class E，BIP）

- **REFRESH**, 要求ME开始SIM卡的初始化，和/或提示SIM卡上的EF的内容或结构已经改变。这个命令可以使ME复位SIM卡而重新开始一个SIM卡的会话。

- **RUN AT COMMAND**, 它将传达一个AT命令到ME，并且将AT命令的响应结果返回到SIM卡。

-SELECT ITEM, SIM卡提供一张项目列表供用户选择。

- **SEND DATA**, 它要求ME向SIM卡提供的指定通道发送数据。（如果支持Class E，BIP）

- **SEND DTMF**, 它要求ME在建立呼叫期间发送DTMF音频。

- **SEND SHORT MESSAGE**, 此命令向网络发送短信息或SMS-COMMAND。

- **SEND SS**, 此命令向网络发送SS请求。

- **SEND USSD**, 此命令是向网络发送USSD。

- **SET UP CALL**, 有三种类型：

在没有其它呼叫时，建立呼叫。

保持所有其它的呼叫（如果有），建立呼叫。

切断所有其它的呼叫（如果有），建立呼叫。

- **SET UP EVENT LIST** 用此命令提供一套事件集，ME应该将此事件集去作为当前的事件列表去监视。

- **SET UP IDLE MODE TEXT**, 提供一个字符串给ME用于待机模式文本。

- **SET UP MENU**, SIM卡提供一个项目列表供用户选择后合并到ME的菜单中。（SET\_UP\_MENU是建立STK的主菜单，也是第一个主动式命令）

- **TIMER MANAGEMENT**, w它要求ME以下命令方式（开始，停用，获取当前值）去管理一个定时器。并且在启动定时器的情况下，在命令中指示持续的时间。

### Terminal Response

Terminal Response，简称TR。ME执行完proactive command后，用Terminal Response告诉SIM卡命令的执行结果，以便SIM卡判断接下来的动作：如是否重复这个命令，还是不再尝试。对于每一个proactive command，必须发送一个且仅一个Terminal Response告诉SIM卡命令执行的结果。SIM卡在接收到前一个proactive command的Terminal Response之前不会执行下一个命令。Terminal Response分为三种主要类型：

——命令执行成功

——执行命令时遇到暂时问题。一般来说，此类问题意味着SIM卡稍后可以再试一次

——执行命令时遇到永久问题，一般来说，此结果表明若在同一个GSM会话期间重复执行相同的命令会有同样的结果，所以SIM卡不再需要再次尝试

这三种主要类型的具体定义可见3GPP TS 11.14(6.7)

# 关键流程分析

### Profile download



见2.1. STK包含的机制

Phase文件指的是SIM卡所支持的GSM标准的级数，值为3则指SIM卡支持**GSM phase 2和profile download(3GPP 11.11)**。

这个过程很重要，可以让SIM卡知道ME支持的功能，从而控制自己的指令范围。在SIM卡初始化过程中，如果ME未向SIM卡发送此命令，SIM卡认为ME不支持SAT。

### Proactive Command

sw=91 xx

Fetch

proactive command

terminal response

sw=90 00

command

SIM

ME

sw=90 00

Step1

Step2

Step3

Step4

Step5

Step6

Step7

sw1 sw2 for command

sw1 sw2 for fetch

sw1 sw2for TR

step1-7称为一个sat session.

1．ME总是命令的发起者，首先ME发送SAT命令给SIM卡

2． SIM卡执行完命令后，返回Status Words（91XX），告诉ME有一个proactive command需要执行

3．ME用fetch命令取得proactive command

4．SIM将proactive command数据传送给ME

5．SW1 SW2 for Fetch

6．ME发送 Terminal Response给SIM卡

7．SW1 SW2 for Terminal Response

Step4-6是ME执行proactive command的时间：如显示数据，让用户输入，播放声音，发送短信等等。

# 总结

STK的基本概念并不复杂，但是大多数内容是与协议强相关的。如主动式命令的运作流程很好理解，实际解决问题时更多的是要依靠查阅相关的协议。

下一步需要深入了解该模块的整体框架，并掌握相关协议的内容。同时了解各种类型的测试case。避免出现解决实际问题时因不了解case导致的效率低下。(XR7101933)