CBWIPS

宽带无线IP标准工作组标准化指导性技术文件

CBWIPS/Z ××××.××—××××

WAPI 私钥/证书
本地存储及使用技术规范

WAPI Private Key / Certificate
Secure Access Control and Application Protocol

（第二次征求意见稿）

（本稿完成日期：2010 年 12 月）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

工业和信息化部宽带无线 IP 标准工作组　发 布

目　　次

前　言

本指导性技术文件由工业和信息化部宽带无线IP标准工作组和WAPI产业联盟（中国计算机行业协会无线网络和网络安全接入技术专业委员会）共同提出，由工业和信息化部宽带无线IP标准工作组归口。

本指导性技术文件主要起草单位：工业和信息化部宽带无线 IP 标准工作组“WAPI 私钥/证书本地存储及使用技术规范标准项目组” 暨 WAPI 产业联盟“WAPI 私钥/证书本地存储及使用技术规范产品方案组”（北京中电华大电子设计有限责任公司、北京创原天地科技有限公司、北京登合科技有限公司、宇龙计算机通信科技（深圳）有限公司、西安西电捷通无线网络通信股份有限公司、广州杰赛科技股份有限公司、xxx 待补充）。

本指导性技术文件主要起草人：兰天、崔炳荣、奚红梅、单丹、童伟刚、张永强、张伟、xxx待补充。

WAPI 私钥/证书本地存储及使用技术规范

1 范围

WAPI私钥/证书的存储介质包括独立安全介质和开放介质两大类。本规范只定义独立安全介质的安全存取、安全分发和安全使用相关内容：

——私钥/证书的安全存取技术，包括文件格式、存取控制条件、存取操作命令。

——私钥/证书的安全分发技术，包括私钥/证书文件的申请、生成、更新、吊销流程中，独立安全介质和证书颁发设备的交互接口。

——私钥/证书的安全应用技术，包括 WAI 功能在独立安全介质和终端之间的划分，WAI 执行过程中，终端和独立安全介质的交互接口。

2 规范性引用文件

下列文件中的条款通过标准的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

ISO7816-1： 识别卡 带触点的集成电路卡 第 1 部分：物理特性

ISO7816-2： 识别卡 带触点的集成电路卡 第 2 部分：尺寸和触点的位置

ISO7816-3： 识别卡 带触点的集成电路卡 第 3 部分：电信号和传输协议

GSM 11.11： SIM 卡和移动设备接口规范

GSM03.40： 点对点短消息技术实现

GSM03.48： SIM卡应用的安全机制

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1 独立安全介质

与终端独立的、具备安全管理功能、访问受控的存储介质，如 SIM 卡/USB-KEY 等。

3.1.2 开放介质

集成在终端中、或者独立于终端的，不具备安全管理功能、可以完全访问的存储介质。

3.1.3 初始化阶段

在介质正式使用前，对介质进行预处理的阶段。

3.1.4 生命周期阶段

介质初始化完成后，从介质开始正式使用，直到介质终止使用的阶段。

3.2 缩略语

下列缩略语适用于本文件。

WAI 无线局域网鉴别基础结构
WPI 无线局域网保密基础结构
WAPI 无线局域网鉴权和保密基础结构
AE 鉴别器实体
AP 接入点
ASE 鉴别服务实体
ASU 鉴别服务单元
ASUE 鉴别请求者实体
BK 基密钥
BKID 基密钥标识
ECDH 椭圆曲线密码体制的 Diffie-Hellman 交换
MAK WAPI 消息鉴别密钥
ME 移动终端
SIM 用户身份识别模块
MF 主目录文件
DF 目录文件
EF 基本文件
OTA 空中下载
SMS 短消息

4 SMS 短消息综述

WAPI应用于终端时，安全的存储和使用用户私钥及其终端证书，是保证整个体系安全的起点和核心。

WAPI私钥/证书目前的存放载体主要有两种：一是存放在终端自带的开放介质中，如对于笔记本电脑就是存放在硬盘中，对于手机终端就是手机内存或MMC/SD等存储卡中；二是存放在可以与终端分离的独立安全介质中，对于笔记本电脑就是存放在USB Key中，对于手机终端就是存放在SIM卡中。本规范描述范围只包括独立安全介质，包括USB-Key和SIM卡，但不限于这两者。

本规范定义了在独立安全介质上，WAPI 私钥/证书的安全存取技术，包括文件格式、存取控制条件、存取操作命令。

本规范定义了在独立安全介质上， WAPI 私钥/证书的安全分发技术，包括申请、生成、更新、吊销流程中，独立安全介质和证书颁发设备的交互接口。

在WAPI私钥和证书使用中，要求所有加密运算均在独立安全介质上进行，不提供密钥输出，只向终端提供最终结果。本规范定义了私钥/证书的安全应用技术，包括WAI功能在独立安全介质和终端之间的划分，WAI执行过程中，终端和独立安全介质的交互接口。

本规范所述独立安全介质，除了可提供WAPI接入的相关功能外，也可以提供PKI扩展应用的相关功能。本规范定义了支持PKI扩展应用的交互接口。

5 WAPI 私钥/证书文件安全存取技术

5.1 独立安全介质上的目录结构和文件格式

独立安全介质上的目录结构遵循GSM11.11的规定，使用嵌套文件的组织方式，在独立安全介质MF主文件下的任意一级或二级目录下,增加一个目录文件:DF_WAPI,以及两个EF文件:EF_PK_List、EF_CMD。其中DF_WAPI下面又包含若干EF文件，文件目录结构见图1，目录和文件的详细定义见5.2。

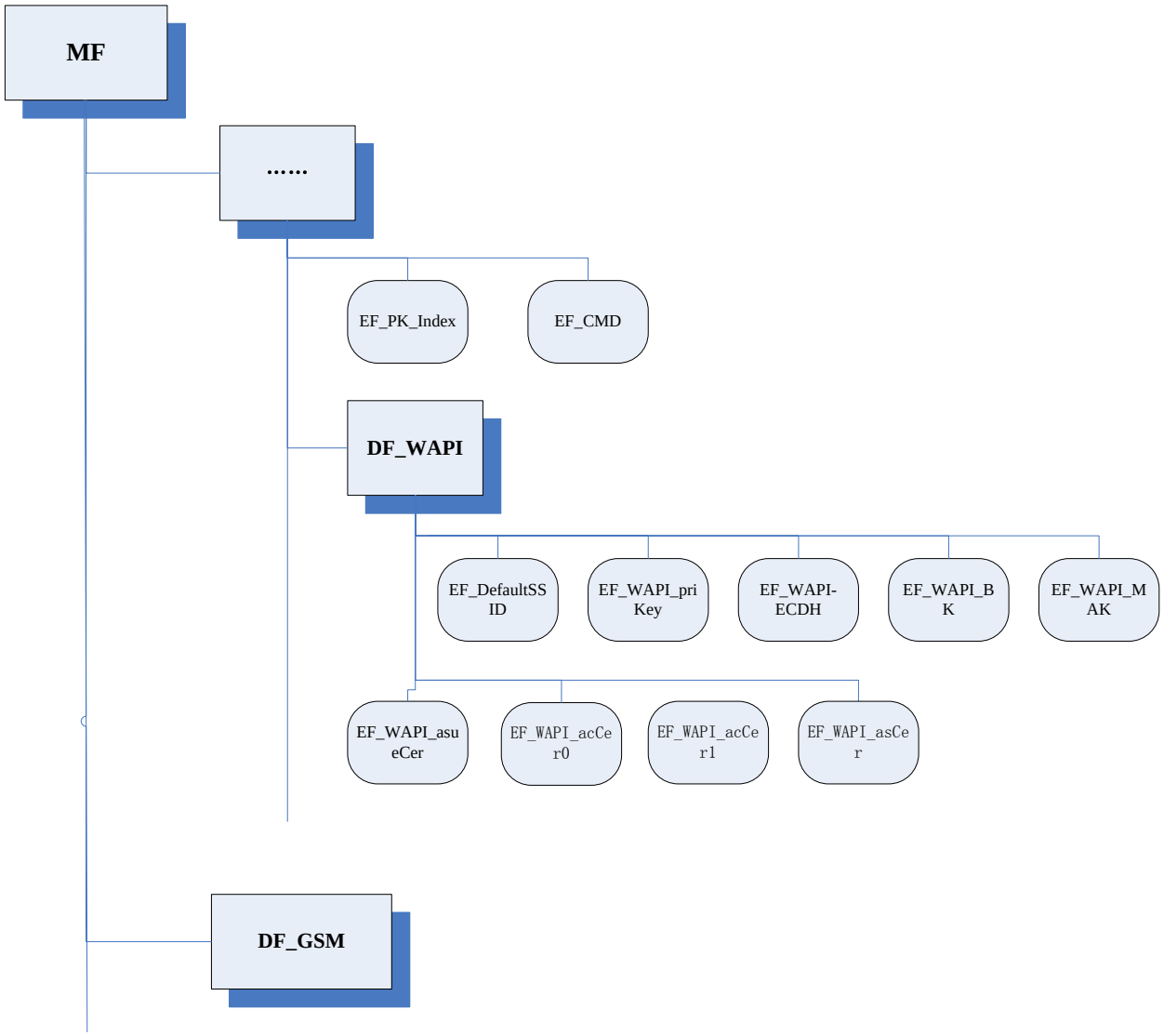


图1　独立安全介质上 WAPI 相关目录结构

WAPI私钥/证书的文件格式使用GSM11.11中定义的透明文件、线性定长两种文件格式。

5.2　独立安全介质上 WAPI 私钥和证书文件

5.2.1　概述

独立安全介质上，EF_PK_List、EF_CMD、DF_WAPI 及其包含的各个 EF 文件列表见表 1，由于独立安全介质的容量限制，处理能力有限，本规范中规定下列文件在独立安全介质初始化阶段生成，在运行过程中只能修改；本规范也定义了下列文件的最大长度。但本规范并不限定在安全介质的运行期间创建和删除非本规范定义的文件。

表1　独立安全介质上 WAPI 相关文件说明

DF 目录文件	EF 文件	文件 ID	描述	备注
	EF_PK_List	0xF100	公钥证书列表索引文件	线性定长记录文件，每条记录 24 字节，共支持 16 条
	EF_CMD	0xF101	用于写入请求类型的操作命令；以及可读出的操作结果	2K 字节
DF_WAPI		0xF102	WAPI 目录文件，包含以下对应的节点文件	
	EF_Default_SSID	0xF103	WAPI 缺省的 SSID	32 字节
	EF_WAPI_ECDH	0xF104	WAPI ECDH 临时密钥文件	72 字节
	EF_WAPI_BK	0xF105	WAPI 基密钥文件	线性定长记录文件，每条记录 64 字节；共支持 4 条
	EF_WAPI_MAK	0xF106	WAPI 的消息鉴别密钥文件	64 字节
		0xF107-0xF10F	文件 ID 保留	
	EF_WAPI_asueCer	0xF110	用户证书文件	2K 字节
	EF_WAPI_acCer	0xF111	颁发者根证书文件	2K 字节
	EF_WAPI_asCer	0xF112	注册地认证服务器证书文件	2K 字节
		0xF113-0xF11F	文件 ID 保留	
	EF_WAPI_priKey	0xF120	用户的私钥文件	256 字节
		0xF121-0xF12F	文件 ID 保留	

5.2.2　EF_PK_List、EF_CMD 和 DF_WAPI 及其包含的各个 EF 文件详细定义

(1) EF_PK_List

Identfier:0xF100		Structure: linear fixed		Mandatory	
FileSize:24*16			Update activity:low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM					
Byte	Description			M/O	Length

1	参数	M	1
2-9	公钥/证书 ID	M	8
10	公钥/证书文件类型	M	1
11-12	公钥/证书文件的文件标识	M	2
13-14	公钥/证书在文件中的起始偏移	M	2
15-16	公钥/证书长度	M	2
17	私钥文件长度	M	1
18-19	私钥文件的文件标识	M	2
20-24	保留	0	5

其中参数部分定义如下：

Bit	Value	Description
1	1	本文件为证书文件
	0	本文件为公钥文件
2	1	如果 bit1=1,该位有效，标识证书文件对应的私钥文件有效，私钥文件 ID 由后面字段标识
	0	保留
其他	保留	

其中标识部分定义如下：

BYTE	Value	Description
1	1	缺省值为 1
	其他	保留

其中证书文件类型部分定义如下：

BYTE	Value	Description
1	0	WTLS 证书文件
	1	X.509 证书文件
	2	X9.68 证书文件
	其他	保留

在 EF_PK_List 文件中，每一条有效的记录都通过“公钥/证书文件的文件标识”字段，对应了一个公钥/证书文件，如果该公钥/证书文件同时有一个私钥，那么通过“私钥文件的文件标识”对应该私钥文件。当得到一个有效的公钥/证书文件时，同时也应该在本文件中建立一条对应的有效记录；当公钥/证书文件无效时，同时也应该删除对应的记录。

(2) EF_CMD

Identfier:0xF101	Structure: transparent	Mandatory
FileSize:4K	Update activity:low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Byte	Description	M/O	Length
1	命令权限类别	M	1
2-9	命令的权限值	M	8
10-2057	请求命令	M	2048
2058-4105	响应命令	M	2048

其中命令的权限类别定义如下：

类别编码	描述
0x00	NULL
0x01	CHV1
0x02	CHV2
0x03	ADM
其他	保留

(3) DF_WAPI 目录文件：

Identfier:0xF102	Structure:transparent	Mandatory
FileSize:0	Update activity:low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE CHV1 REHABILITATE CHV1		

Byte	Description	M/O	Length
0	目录文件，包含一系列 EF 文件	0	0

(4) EF_Default_SSID 文件：

Identfier:0xF103	Structure:transparent	Mandatory
FileSize:32	Update activity:low	
Access Conditions: READ CHV1 UPDATE ADM		

INVALIDATE ADM REHABILITATE ADM			
Byte	Description	M/O	Length
1-32	证书颁发者对应的 SSID	O	32

(5) EF_WAPI_ECDH

Identfier:0xF104	Structure:transparent	Mandatory	
FileSize:72	Update activity:low		
Access Conditions: READ NEVER UPDATE NEVER INVALIDATE NEVER REHABILITATE NEVER			
Byte	Description	M/O	Length
1-24	ECDH 生成的临时私钥	M	24
25-72	ECDH 生成的临时公钥	M	48

(6) EF_WAPI_BK

Identfier:0xF105	Structure:linear fixed	Mandatory	
FileSize:256	Update activity:low		
Access Conditions: READ NEVER UPDATE NEVER INVALIDATE NEVER REHABILITATE NEVER			
Byte	Description	M/O	Length
1-64	BK 记录 1	M	64
65-128	BK 记录 1	M	64
129-192	BK 记录 1	M	64
193-256	BK 记录 1	M	64

BK 记录定义如下：

字段	长度	描述
BK	16	WAPI 基密钥
BKID	16	基密钥对应的 ID
保留	32	保留

(7) EF_WAPI_MAK

Identfier:0xF106	Structure:transparent	Mandatory	
FileSize:16	Update activity:low		
Access Conditions: READ NEVER UPDATE NEVER INVALIDATE NEVER REHABILITATE NEVER			
Byte	Description	M/O	Length
1-16	消息鉴别密钥 MAK	M	16

(8) EF_WAPI_asueCer

Identfier:0xF110	Structure:transparent	Mandatory	
FileSize:2048	Update activity:low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Byte	Description	M/O	Length
1-X（x<2048）	用户个人证书	M	X

(9) EF_WAPI_acCer

Identfier:0xF111	Structure:transparent	Mandatory	
FileSize:2048	Update activity:low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Byte	Description	M/O	Length
1-X(x<2048)	颁发者根证书	M	X

(10) EF_WAPI_asCer

Identfier:0xF112	Structure:transparent	Mandatory
FileSize:2048	Update activity:low	
Access Conditions: READ CHV1		

UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Byte	Description	M/O	Length
1-X(x<2048)	用户注册地认证服务器证书	M	X

(11) EF_WAPI_priKey

Identfier:0xF120	Structure:transparent	Mandatory	
FileSize:256	Update activity:low		
Access Conditions: READ NEVER UPDATE NEVER INVALIDATE NEVER REHABILITATE NEVER			
Byte	Description	M/O	Length
1-24	私钥	M	24
25-256	保留	M	232

5.3 WAPI 私钥/证书文件存取控制

本规范中，存取控制出现在独立安全介质初始化和独立安全介质生命周期两个阶段，涉及的文件操作包括创建(CREATE)、读取(READ)、更新(UPDATE)、使无效(INVALIDATE)、使有效(REHABILITATE)四类。

本规范中，存取控制只针对5.1节中所列文件，除了上述文件外，其他文件不在本规范定义的范围内。

5.3.1 独立安全介质初始化阶段存取控制

在独立安全介质的初始化阶段，需要且必须创建EF_PK_List、EF_CMD、DF_WAPI目录文件及其下属所有EF文件，初始化阶段完成后，在介质的生命周期中不允许重新创建文件和删除本规范所列文件，只允许对本规范所列EF文件进行更新。

在独立安全介质的初始化阶段，DF_WAPI目录下的EF_Default_SSID、EF_WAPI_acCer需要且必须被初始化为有效内容，同时EF_PK_List中应该包含一条指向EF_WAPI_acCer的有效记录。EF_WAPI_priKey、EF_WAPI_asueCer、EF_WAPI_asCer三个文件可以被初始化为有效内容，也可以置空；除上述提到文件外的其他文件内容置空。

初始化阶段的安全管理，根据各初始化主体企业的规定来执行，在本规范范围内不做定义。

5.3.2 独立安全介质生命周期阶段存取控制

在独立安全介质在生命周期阶段，外部应用可以对本规范定义的部分EF文件进行读写、更新、使有效和使无效操作。但是外部应用对文件的每个操作必须满足特定的受控条件。本规范中所定义的受控条件和GSM11.11中的规定保持一致，该受控条件应该在外部应用执行文件操作之前得到。

GSM11.11中定义访问条件的级别编码见表2：

表2　访问条件级别编码

级别	受控条件
0	ALW
1	CHV1
2	CHV2
3	保留
4-14	ADM
15	NEV

在 2 表受控条件解释如下:

a)　ALW：无条件执行；

b)　CHV1:（持有者认证 1)：能够满足下列 3 种条件之一者，可执行动作：
在当前对话期间，一个正确的 CHV1 值已经提供给独立安全介质；
CHV1 使能/不使能指示器已处于“不使能”状态；
当前对话期间已经成功的执行了 UNBLOCK CHV1。

c)　CHV2:（持有者认证 2）能满足下列两条件之一者，能够执行动作：
在当前对话期间，一个正确的 CHV2 值已经提供给独立安全介质；
当前对话期间已经成功的执行了 UNBLOCK CHV2；

d)　ADM：要求具有管理员权限；

e)　NEV：在独立安全介质向终端的外接口上，不能执行动作。但在介质内部可执行操作。

在本规范中，外部应用对WAPI相关文件的操作受控条件见表3。

表3　WAPI 相关文件的操作受控条件

安全介质生命周期阶段								
WAPI 相关文件	创建/删除文件 (CREATE/DELETE)		读取文件 (READ)		更新文件 （UPDATE）		使能文件 (INVALIDATE/ REHABILITATE	
	是否允许	受控条件	是否允许	受控条件	是否允许	受控条件	是否允许	受控条件
EF_PK_List	不允许		允许	CHV1	允许	ADM	允许	ADM
EF_Default_SSID	不允许		允许	ALW	允许	ADM	允许	ADM
EF_CMD	不允许		允许	CHV1	允许	ADM	允许	ADM
EF_WAPI_ECDH	不允许		不允许		不允许		不允许	
EF_WAPI_BK	不允许		不允许		不允许		不允许	
EF_WAPI_MAK	不允许		不允许		不允许		不允许	
EF_WAPI_asueCer	不允许		允许	CHV1	允许	ADM	允许	ADM
EF_WAPI_acCer	不允许		允许	CHV1	允许	ADM	允许	ADM
EF_WAPI_asCer	不允许		允许	CHV1	允许	ADM	允许	ADM

EF_WAPI_priKey	不允许		不允许		不允许		不允许	

5.4 独立安全介质的文件安全操作流程

在本规范中，外部应用对文件的操作过程包括读取(READ)、更新(UPDATE)、使无效(INVALIDATE)、使有效(REHABILITATE)四类，具体的操作流程可以使用GSM11.11规范中定义的流程，也可以使用本规范的自定义流程。

本规范自定义流程见图2。

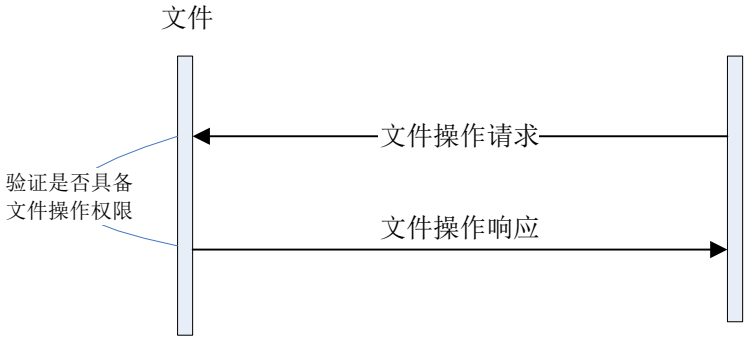


图2 本规范自定义的文件安全操作流程

本规范自定义流程描述如下：

a) 向独立安全介质发出文件操作请求命令，该命令中包含了操作权限；

b) 独立安全介质首先验证请求命令中的操作权限，如果不符合，停止文件操作并返回错误；否则操作文件，并返回操作结果。

GSM11.11规范中定义的文件操作命令包括SELECT（选择文件）、VERIFY CHV(ADM)（验证操作权限）、STATUS（查询文件状态）、READ BINARY(读文件)、UPDATE BINARY（更新文件）、INVALIDATE/ FEHABILITATE（设置文件有效/失效）。

GSM11.11中定义文件安全操作基本流程见图3。

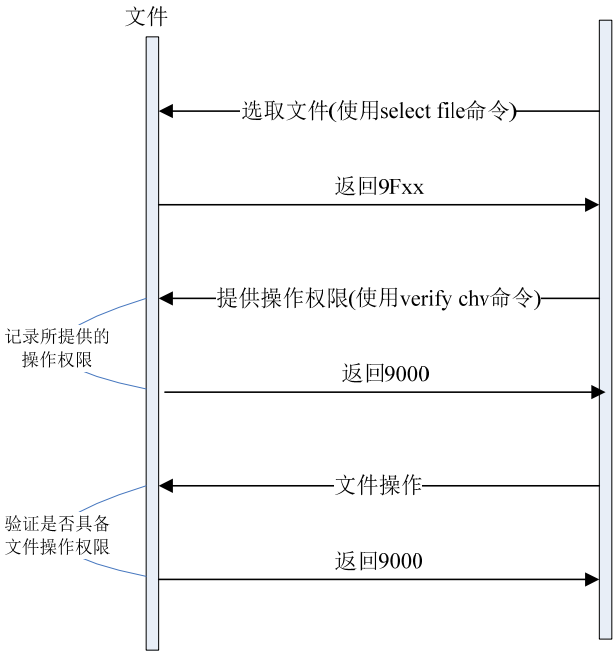


图3　GSM11.11 中文件安全操作基本流程

GSM11.11中定义文件安全操作基本流程描述如下：

a)　执行文件操作前，首先需要选取文件(使用 select 命令)，如果介质有该文件，返回 0x9Fxx，否则返回错误代码，然后终止文件操作；

c)　向文件系统提供操作权限，文件系统记录该权限；

d)　发出执行文件操作命令，文件系统收到该操作命令后，验证上一步所提供的权限是否满足，如果满足则执行，否则终止操作。

下面以电子证书文件的读取为例，见图 4，说明受控条件下的读取过程描述如下：

a)　通过 SELECT FILE 指令选择电子证书文件；

b)　通过验证指令 VERIFY CHV/ADM 认证电子证书文件读取权限。

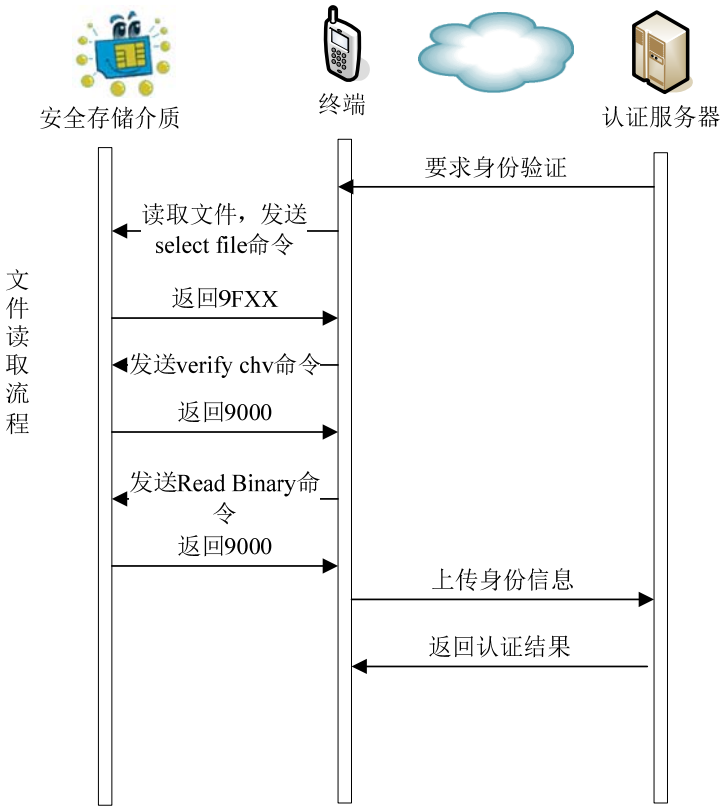


图4　证书文件读取过程

5.5　WAPI 私钥/证书文件安全操作指令

5.5.1　操作命令列表

本规范中自定义的文件操作命令，当前版本仅规定读取(READ)一项，其他命令保留，见表 4。

表4　WAPI 私钥/证书文件安全分发操作命令列表

消息	操作命令	命令功能描述	备注
文件读取请求命令	fileReadReq	STA→独立安全介质 通知独立安全介质读指定文件	见 5.5.3(1)
文件读取响应命令	fileReadRsp	独立安全介质→STA 独立安全介质完成读取操作，返回结果	见 5.5.3(2)
其他	保留		

5.5.2　操作命令编码规则

使用GSM11.11规范定义的文件安全操作指令编码遵循GSM11.11规则。

本规范自定义操作命令使用如下编码规则，见图5。

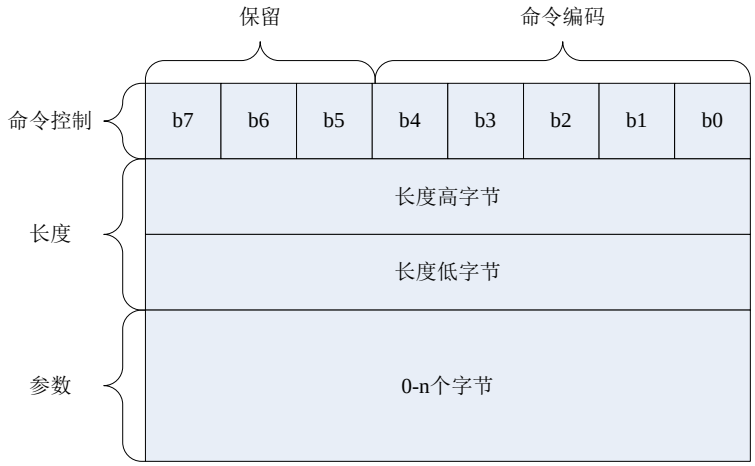


图5　操作命令编码规则

命令帧使用大端格式，由三部分构成：
——命令控制部分为一个字节，b4-b0 为命令编码，剩下保留；
——长度部分为由两个字节构成，按大端存放，指示了参数部分的总长度；
——参数部分由 0-N 个字节构成，不同的命令携带不同的参数，具体定义下文。

5.5.3　操作命令编码

使用GSM11.11规范定义的文件安全操作指令编码使用GSM11.11定义。
本规范自定义操作命令编码如下。

(1) readFileReq

命令编码：01101b	保留：0
长度：0x0016	
参数：	

字节	描述
1-8	相对 MF 的绝对文件目录路径，两个字节为一级，最大支持 4 级
9-10	文件 ID
19-20	文件读起始偏移
21-22	文件读取长度

(2) readFileRsp

命令编码：01110b	保留：0
长度：3+X(x<2045)	
参数：	

字节	描述
1-2	返回的文件长度信息
3	文件读取结果
4-X(x<2048)	读取内容

其中文件读取结果定义如下：

类别编码	描述
0x00	成功
0x01	无对应文件
0x02	权限验证失败
0x03	其他失败
其他	保留

6 WAPI 私钥/证书安全分发技术

6.1 WAPI 私钥和证书的的安全分发流程

6.1.1 概述

本规范中，WAPI 私钥/证书安全分发涉及到独立安全介质的初始化阶段和生命周期阶段。

在初始化阶段，WAPI 私钥/证书安全分发主要是初始化下列文件：

——EF_Default_SSID、EF_WAPI_acCer 需要且必须被初始化为有效内容；EF_PK_List 文件中同时应该建立一条指向 EF_WAPI_acCer 的有效记录；

——EF_WAPI_priKey、EF_WAPI_asueCer、EF_WAPI_asCer 四个文件可以被初始化为有效内容，也可以置空。

在独立安全介质的生命周期阶段,本规范主要定义 WAPI 私钥/证书安全分发(包括证书文件的申请、更新和吊销）过程中，独立安全介质和证书颁发设备的交互接口，包括：

——如果用户注册开通 WLAN 服务，则需要进行私钥/证书的生成过程；

——在完成密钥生成和证书发放后，在需要时可以对证书进行更新，或者吊销。

6.1.2 WAPI 私钥和证书的生成流程

当独立安全介质已经初始化并且发放给用户，用户已经拿到该安全介质后，在下述情况下执行本过程：

a）用户首次申请开通WLAN业务时，执行本过程；

b）用户原来申请开通过WLAN业务，后期注销该业务，重新申请开通时，执行本过程；

c）用户使用WLAN业务，但是证书已经过期，执行本过程。

WAPI私钥/证书的生成流程见图6。

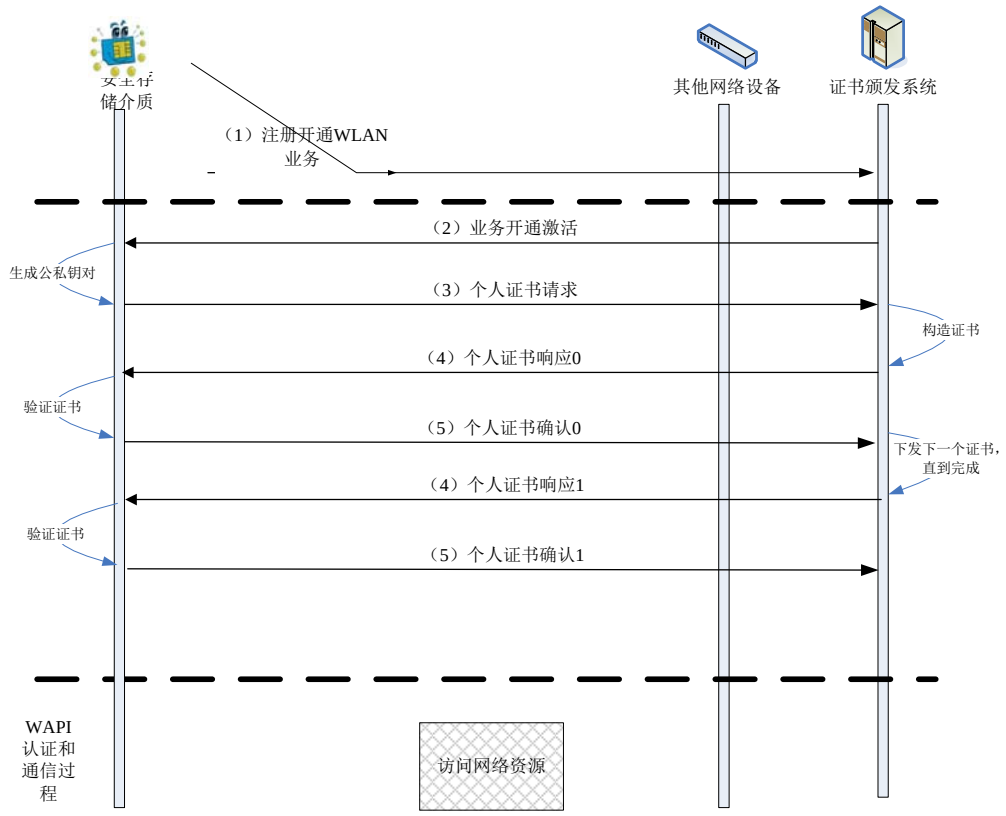


图6　WAPI 私钥/证书生成流程

WAPI 私钥/证书的生成流程描述如下：

a) 用户通过网络、短信等方式发起 WLAN 业务的开通；或者当用户证书已经过期，用户使用 WLAN 业务时；后台业务系统收到请求后，发出“业务开通激活”消息，该消息中类别字段置 0，并使用 HMAC-SHA256 计算哈希值，然后使用证书颁发系统的私钥对该哈希值进行签名；

b) 独立安全介质收到该消息后，验证证书颁发系统的签名。如果验证通过，在介质内部生成一对公私钥，并用公钥和用户 ID 构造“个人证书请求”消息，然后发送给证书颁发系统；

c) 证书颁发系统收到“个人证书请求”后，用消息中的公钥对消息的签名进行验证。验证通过后，提取消息中的用户 ID，根据该 ID 绑定用户的其他注册信息，然后为用户生成个人证书，注册地认证服务器证书等证书文件。构造“个人证书响应”消息，该消息每次只能携带一个证书，然后发给独立安全介质；

d) 独立安全介质收到“个人证书响应”消息，对该消息的签名进行验证。验证通过后，存储该证书，并向证书颁发系统发送“个人证书确认”消息。如果业务开通激活消息中类别字段为 0，那么在 EF_PK_List 中建立一个记录，并指向公钥证书文件和 EF_WAPI_priKey，如果业务开通激活消息中类别字段为 1，那么更新公私钥文件，EF_PK_List 中记录保持不变；

e) 证书颁发系统收到“个人证书确认”消息后，如果还有证书未发送，那么继续构造“个人证书响应”消息，携带需要下送的证书，然后发送给独立安全介质。然后转到 d)操作。如此直到所有证书下送完成。

6.1.3　WAPI 私钥和证书的更新流程

当用户已经完成 WAPI 私钥和证书的生成流程后，在独立安全介质联网中，如果后台系统检测到介质所存储的任何证书到达有效期时，证书颁发系统发起更新过程，如下：

(1) 如果是用户个人证书到达有效期，证书颁发系统直接发出“业务开通激活”消息，将类别字段置1，后续流程遵循密钥和证书的生成过程；

(2) 如果是其他证书到达有效期，证书颁发系统发出“证书更新请求”消息，标识需要更新的证书类别，独立安全介质收到该消息后，执行图7描述的证书更新流程。

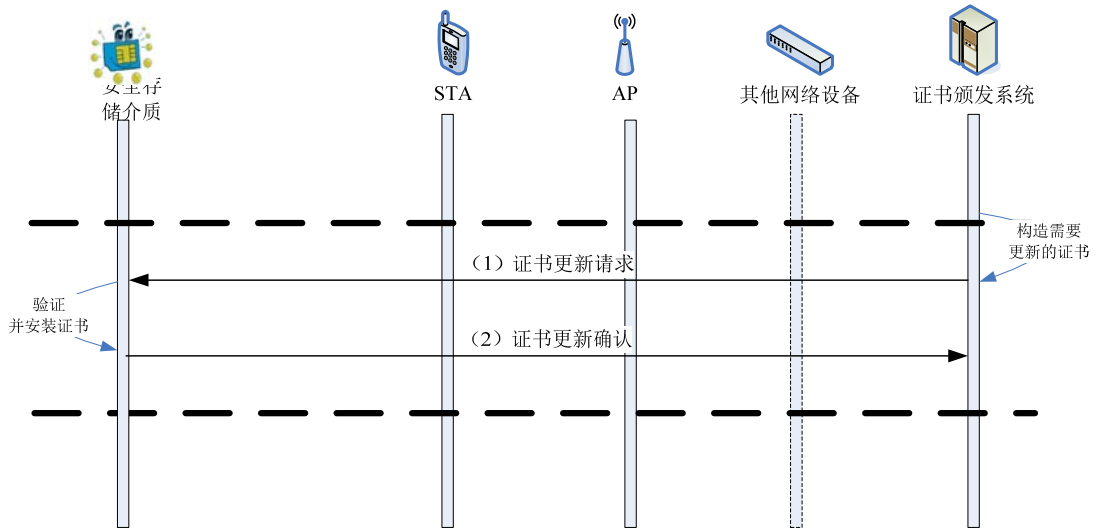


图7　WAPI 私钥和证书的更新流程

图 7 所述过程描述如下：

a) 当证书颁发系统需要将独立安全介质中的证书进行更新时，从证书库中提取需要更新的证书，构造“证书更新请求”消息，该消息每次只能携带一个证书，该消息使用HMAC-SHA256计算哈希值，然后使用证书颁发系统的私钥对该哈希值进行签名，然发送给独立安全介质，然后等待“证书更新确认”消息；

b) 独立安全介质收到“证书更新请求”消息后，对该消息的签名进行验证。验证通过后，安装该证书，构造“证书更新确认”消息，设置状态码为成功，否则设置状态码为失败,并向证书颁发系统发送“证书更新确认”消息；

c) 证书颁发系统得到“证书更新确认”消息，并且状态码为成功，如果还有证书需要更新，那么继续构造 “证书更新请求”消息发送给独立安全介质；否则整个更新过程结束。

6.1.4　WAPI 私钥和证书的吊销流程

当用户已经完成WAPI私钥和证书的生成流程，证书颁发系统在系统侧吊销用户证书时，执行WAPI私钥和证书的吊销过程：

a) 证书颁发系统发出“证书吊销通知”消息，该消息是一个通知消息，不要求回复；

b) 独立安全介质收到该消息后，设置相关文件为无效状态，同时删除 EF_PK_List 文件中的对应记录。

6.2　WAPI 私钥/证书文件安全分发操作命令

本部分定义了WAPI私钥/证书文件分发过程中,独立安全介质和证书颁发设备之间的交互命令接口。

6.2.1　操作命令列表

WAPI私钥/证书文件安全分发操作命令列表见表5。

表5 WAPI 私钥/证书文件安全分发操作命令列表

消息	操作命令	命令功能描述	备注
业务开通激活	WAPI_businessAct	CA→独立安全介质 通知独立安全介质执行开通流程	见 6.5.3(1)
个人证书请求	WAPI_cerBuildReq	独立安全介质→CA 向证书颁发系统请求个人证书	见 6.5.3(2)
个人证书响应	WAPI_cerBuildRsp	CA→独立安全介质 证书颁发系统构造证书，并发送给独立安全介质	见 6.5.3(3)
个人证书确认	WAPI_cerBuildAck	独立安全介质→CA 独立安全介质收到证书后，发送确认消息	见 6.5.3(4)
证书更新请求	WAPI_cerUpdateReq	CA→独立安全介质 请求更新证书	见 6.5.3(5)
证书更新确认	WAPI_cerUpdateAck	独立安全介质→CA 安装证书后，通知证书颁发系统更新成功	见 6.5.3(6)
证书吊销通知	WAPI_cerRevokeNtf	CA→独立安全介质 证书颁发系统吊销证书，发送通知消息	见 6.5.3(7)

6.2.2 操作命令编码规则

操作命令编码规则见图8。

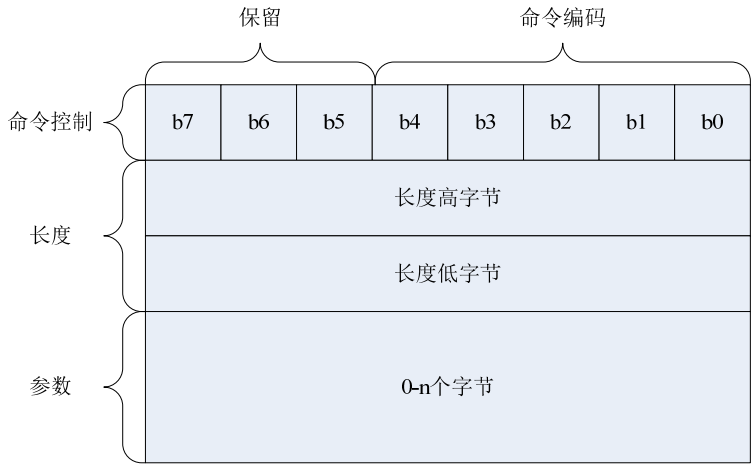


图8 操作命令编码规则

命令 PDU 使用大端格式，由三部分构成：

——命令控制部分为一个字节，b4-b0 为命令编码，剩下保留；

——长度部分为由两个字节构成，按大端存放，指示了参数部分的总长度；

——参数部分由 0-N 个字节构成，不同的命令携带不同的参数，具体定义下文。

6.2.3 操作命令编码

(1) WAPI_businessAct

命令编码：10001b	保留：0

长度：81		
参数：		
	字节	描述
	1	类别字段，0：表示初次业务开通；1：表示个人证书更新；其他保留
	2-33	本消息 HMAC-SHA256 哈希值
	34-81	CA 系统私钥对哈希值的 ECDSA-192 签名

(2) WAPI_cerBuildReq

命令编码：10010b	保留：0	
长度：X+25		
参数：		
	字节	描述
	1--X	用户 ID 字段
	X+1--X+23	独立安全介质生成的用户公钥

用户 ID 字段定义如下：

字节	描述
字节 1 高 4 位	用户 ID 类型
字节 1 低 4 位	用户 ID 长度
2--X	用户 ID 的内容

其中用户 ID 类型编码定义如下：

类型编码	描述
0001b	用户 IMESI 号码
其他	保留

(3) WAPI_cerBuildRsp

命令编码：10011b	保留：0	
长度：X+5		
参数：		
	字节	描述
	字节 1 高 4 位	本次交易总共需要下发的证书数量
	字节 1 低 4 位	本次下发的证书索引
	2	证书类别
	3--4	证书长度，记为 X

	5--5+X	证书内容	

其中证书类别编码定义如下：

类别编码	描述
0x01	用户个人证书
0x02	注册地认证服务器证书
0x03	保留
其他	保留

(4) WAPI_cerBuildAck

命令编码：10100b	保留：0
长度：1	
参数：	

字节	描述
1	处理状态码

其中处理状态编码定义如下：

类别编码		描述
高 4 位	0000b	证书安装失败
	0001b	证书安装成功
	0010b	保留
	0011b	保留
	其他	保留
低 4 位	0000b	保留
	0001b	保留
	0010b	保留
	0011b	保留
	其他	保留

(5) WAPI_cerUpdateReq

命令编码：10101b	保留：0
长度：X+85	
参数：	

字节	描述
字节 1 高 4 位	本次交易总共需要下发的证书数量
字节 1 低 4 位	本次下发的证书索引
2	证书类别
3-4	证书长度，记为 X
5-5+X	证书内容

	X+6-X+37	对上述消息内容的 HMAC-SHA256 哈希值	
	X+38-X+85	CA 对上面哈希值的签名	

证书类别字段的定义请参考上文。

(6) WAPI_cerUpdateAck

命令编码：10110b	保留：0
长度：1	
参数：	

字节	描述
1	处理状态码

其中处理状态编码定义如下：

类别编码		描述
高 4 位	0000b	证书更新失败
	0001b	证书更新成功
	其他	保留
低 4 位		保留

(7) WAPI_cerRevokeNtf

命令编码：10111b	保留：0
长度：81	
参数：	

字节	描述
1	原因状态码
2-33	对上述消息内容的 HMAC-SHA256 哈希值
34-81	CA 对上面哈希值的签名

其中原因状态编码定义如下：

类别编码		描述
高 4 位	0000b	后台强制吊销
	0001b	保留
	0010b	保留
	0011b	保留
	其他	保留
低 4 位	0000b	保留
	0001b	保留
	0010b	保留
	0011b	保留
	其他	保留

7 WAPI 私钥/证书安全使用技术

7.1 WAPI 私钥/证书安全使用操作流程

WAPI 标准流程见图 9。

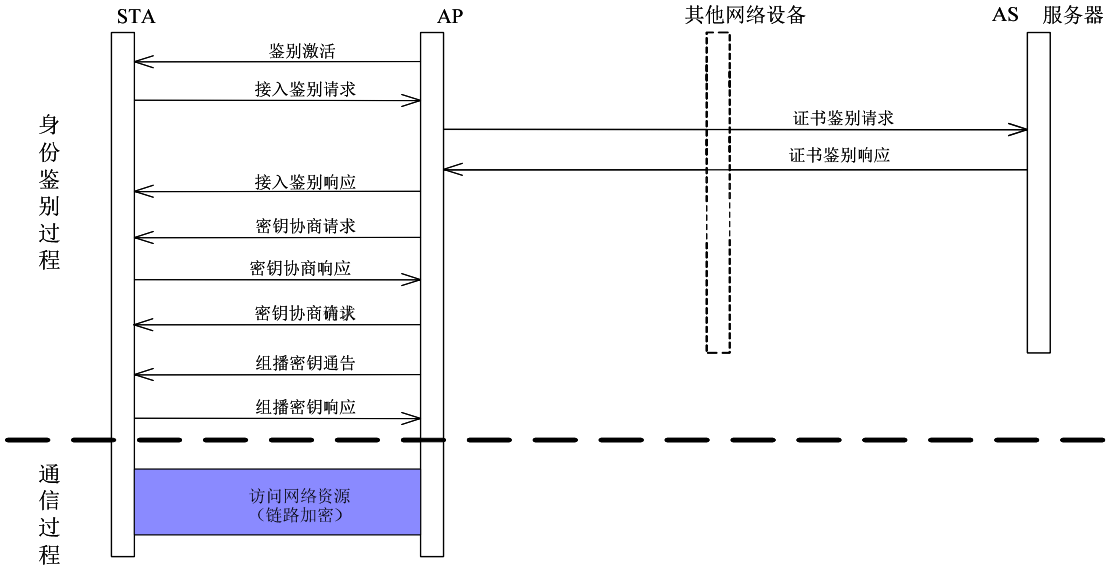


图9 WAPI 标准流程

根据上述流程，STA 中包含有终端私钥和证书，并在 STA 中完成身份鉴别密钥推导。当增加独立安全介质后，会将 STA 中所包含的私钥/证书存储功能、密钥推导和使用功能划分到独立安全介质中，基本流程见图 10。

图 10 所示流程各步骤描述如下：

(1) 参数读取：STA 读取 SSID，asue 证书、asu 证书等，为身份鉴别做准备。该操作属于文件操作，使用 5.3.3 所规定的操作指令,或者使用本规范自定义的“文件读取请求”、“文件读取响应”一对操作指令。参数读取操作只需要在身份鉴别开始之前完成即可，不限定具体操作时间。

(2) 临时密钥推导：该步骤包括“临时密钥推导请求”、“临时密钥推导响应”一对操作命令， STA 向独立安全介质发起“临时密钥推导请求”，独立安全介质收到请求后，推导出一对临时密钥，并将临时公钥通过“临时密钥推导响应”回传给 STA 。

(3) 私钥签名：该步骤包括“私钥签名请求”“私钥签名响应”一对操作命令，STA 发出签名请求后，独立安全介质使用自己存储的私钥对数据签名并返回响应。

(4) 基密钥推导：该步骤仅包括“基密钥推导请求”“基密钥推导响应”一对操作命令，STA 发出该请求，独立安全介质使用“EDCH 密钥推导”步骤中生成的基密钥及其其索引，将索引返回。

(5) 单播密钥推导：该步骤包括“单播密钥推导请求”“单播密钥推导响应”一对操作命令，STA 发出该请求，独立安全介质使用基密钥生成单播密钥、组播密钥，并返回给 STA。

(6) 消息鉴别：该步骤包括“消息鉴别请求”“消息鉴别响应”一对操作命令，STA 发出该请求，独立安全介质使用消息鉴别密钥对消息做散列运算生产消息鉴别码，返回给 STA。

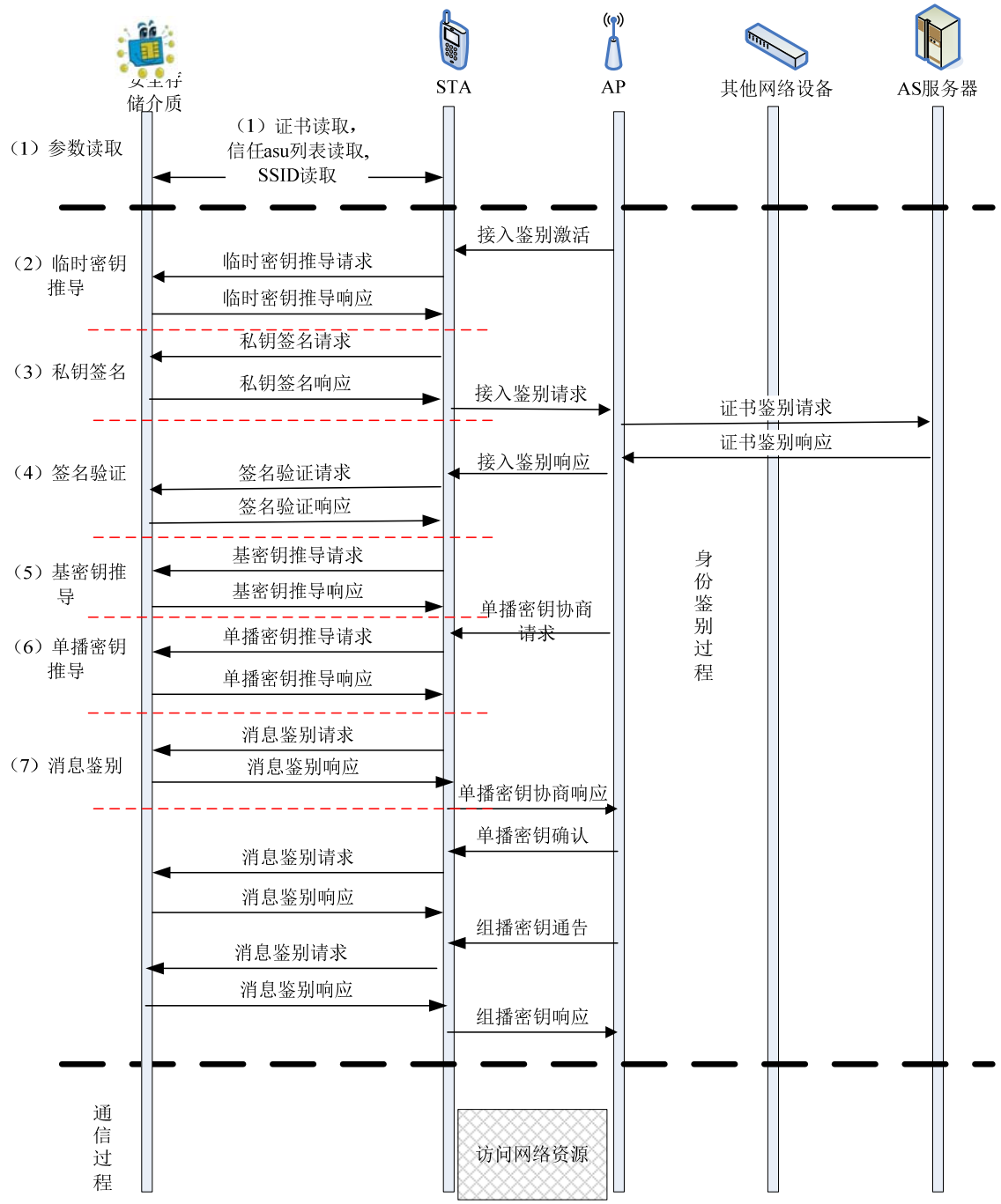


图10　增加独立安全介质后的 WAPI 操作流程

7.2　WAPI 私钥/证书安全使用的操作命令

7.2.1　操作命令列表

WAPI私钥/证书安全使用的操作命令见表6。

表6　操作命令列表

功能	操作命令	命令功能描述	备注
临时密钥推导	WAPI_mkTempKeyReq	临时密钥推导请求，STA 发给独立安全介质，要求独立安全介质产生用于 ECDH 算法用的临时密钥	见 7.2.3(1)
	WAPI_mkTempKeyRsp	临时密钥推导响应，独立安全介质发给 STA，返回 EDCH 算法用的临时密钥的公钥	见 7.2.3(2)
私钥签名	WAPI_mkSignReq	私钥签名请求，STA 发给独立安全介质，要求对数据使用私钥进行签名	见 7.2.3(3)
	WAPI_mkSignRsp	私钥签名响应，独立安全介质发给 STA，独立安全介质使用私钥对数据签名后，将签名返回给 STA	见 7.2.3(4)
签名验证	WAPI_verifySignReq	基密钥推导请求，STA 发给独立安全介质，要求生成基密钥	见 7.2.3(5)
	WAPI_verifySignRsp	基密钥推导响应，独立安全介质发给 STA，生成基密钥后，将索引返回给 STA	见 7.2.3(6)
基密钥推导	WAPI_mkBKReq	单播密钥推导请求，STA 发给独立安全介质，要求根据基密钥推导出单播密钥等一系列通信密钥	见 7.2.3(7)
	WAPI_mkBKRsp	单播密钥推导响应，独立安全介质发给 STA，独立安全介质生成通信密钥后，返回给 STA	见 7.2.3(8)
单播密钥推导	WAPI_mkUSKReq	消息鉴别请求，STA 发给独立安全介质，要求使用消息鉴别密钥对所携带数据生成消息鉴别码	见 7.2.3(9)
	WAPI_mkUSKRsp	消息鉴别响应，独立安全介质发给 STA，独立安全介质生成消息鉴别码后，返回给 STA	见 7.2.3(10)
消息鉴别	WAPI_mkMsgCodeReq	临时密钥推导请求，STA 发给独立安全介质，要求独立安全介质产生用于 ECDH 算法用的临时密钥	见 7.2.3(11)
	WAPI_mkMsgCodeRsp	临时密钥推导响应，独立安全介质发给 STA，返回 EDCH 算法用的临时密钥的公钥	见 7.2.3(12)

7.2.2　操作命令编码规则

WAPI私钥/证书安全使用操作命令编码规则见图11。

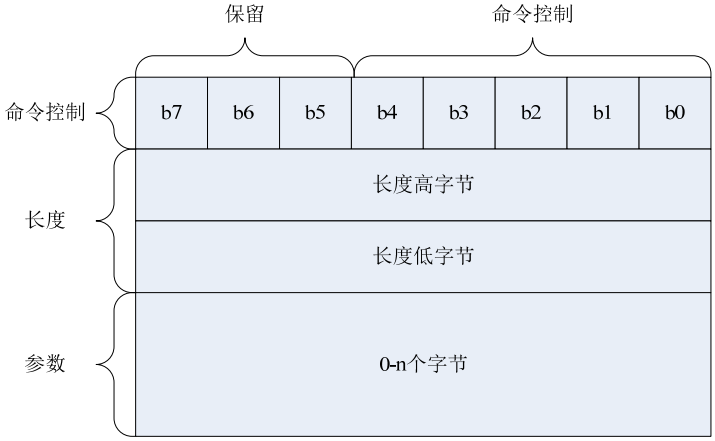


图11　WAPI 私钥/证书安全使用操作命令编码规则

命令 PDU 使用大端格式，由三部分构成：

——命令控制部分为一个字节，b4-b0 为命令编码，剩下保留；

——长度部分为由两个字节构成，按大端存放，指示了参数部分的总长度；

——参数部分由 0-N 个字节构成，不同的命令携带不同的参数，具体定义下文。

7.2.3 操作命令编码

(1) WAPI_mkTempKeyReq

命令编码：00001b	保留：0
长度：0x0000	
参数：无	

(2) WAPI_mmkTempKeyRsp

命令编码：00010b	保留：0
长度：0x0030	
参数：	

字节	描述
1-48	构造的临时公钥

(3) WAPI_mkSignReq

命令编码：00011b	保留：0
长度：32	
参数：	

字节	描述
1-32	要求签名的 WAPI 数据帧的 SHA-256 哈希值

(4) WAPI_mkSignRsp

命令编码：00100b	保留：0
长度：0x0030	
参数：	

字节	描述
1-48	私钥签名

(5) WAPI_mkBKReq

命令编码：00111b	保留：0
长度：0x007C	
参数：	

字节	描述
1-32	256 位 AE 挑战
33-64	256 位 ASUE 挑战
65-112	48 字节 AE 临时公钥

	113-125	96 位 ADDID

(6) WAPI_mkBKRsp

命令编码：01000b	保留：0
长度：0x0030	
参数：	

字节	描述
1-16	128 位 BKID
17-48	256 位下一次鉴别标识

(7) WAPI_mkUSKReq

命令编码：01001b	保留：0
长度：0x004C	
参数：	

字节	描述
1-12	96 位 ADDID
13-44	256 位 AE 挑战
45-76	256 位 ASUE 挑战

(8) WAPI_mkUSKRsp

命令编码：01010b	保留：0
长度：0x0050	
参数：	

字节	描述
1-16	128 位单播加密密钥
17-32	128 位单播完整性校验密钥
33-48	128 位组播密钥加密密钥
49-80	256 位下一次单播会话密钥协商过程的 AE 挑战

(9) WAPI_mkMsgCodeReq

命令编码：01011b	保留：0
长度：X(x<2048)	
参数：	

字节	描述
1-X	用于计算消息鉴别码的 WAPI 帧

(10) WAPI_mkMsgCodeRsp

命令编码：01100b	保留：0

<table>
<tr><td>长度：0x0014</td></tr>
<tr><td>参数：
<table>
<tr><td>字节</td><td>描述</td></tr>
<tr><td>1-20</td><td>160 位消息鉴别码</td></tr>
</table>
</td></tr>
</table>

附 录 A
（规范性附录）
在 SIM 卡上承载安全存储和使用规范

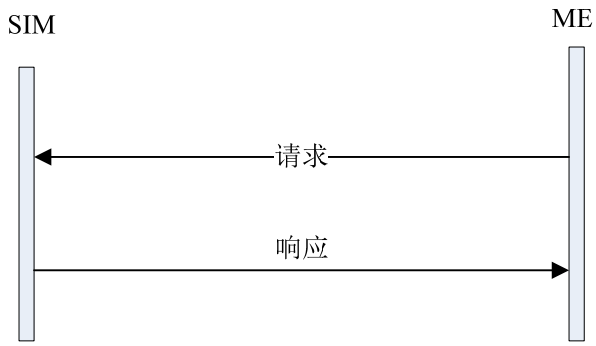
A.1 概述

私钥/证书安全存储和使用规范可以承载到 SIM 卡/USBKey 等独立安全介质。由于不同的承载介质有各自不同的协议定义，具体实现本规范时，需要根据承载介质的操作协议来进行封装，本部分描述了私钥/证书安全存储和使用规范在 SIM 卡上的具体封装方法。

A.2 WAPI私钥/证书安全存取和安全使用技术在SIM卡上的实现

在 SIM 卡作为安全介质的应用中，ME 和 SIM 卡之间的交互接口是 GSM 协议约定好的，对于不在该约定范围内的交互过程，需要将该交互过程封装到标准的 ME-SIM 接口中。

本部分中所有的自定义 WAPI 私钥/证书的安全存取交互和安全操作交互均使用一对“请求-响应”命令来完成，由 ME 向 SIM 发起请求命令，SIM 完成后，返回一个应答命令，如图 A.1 所示。



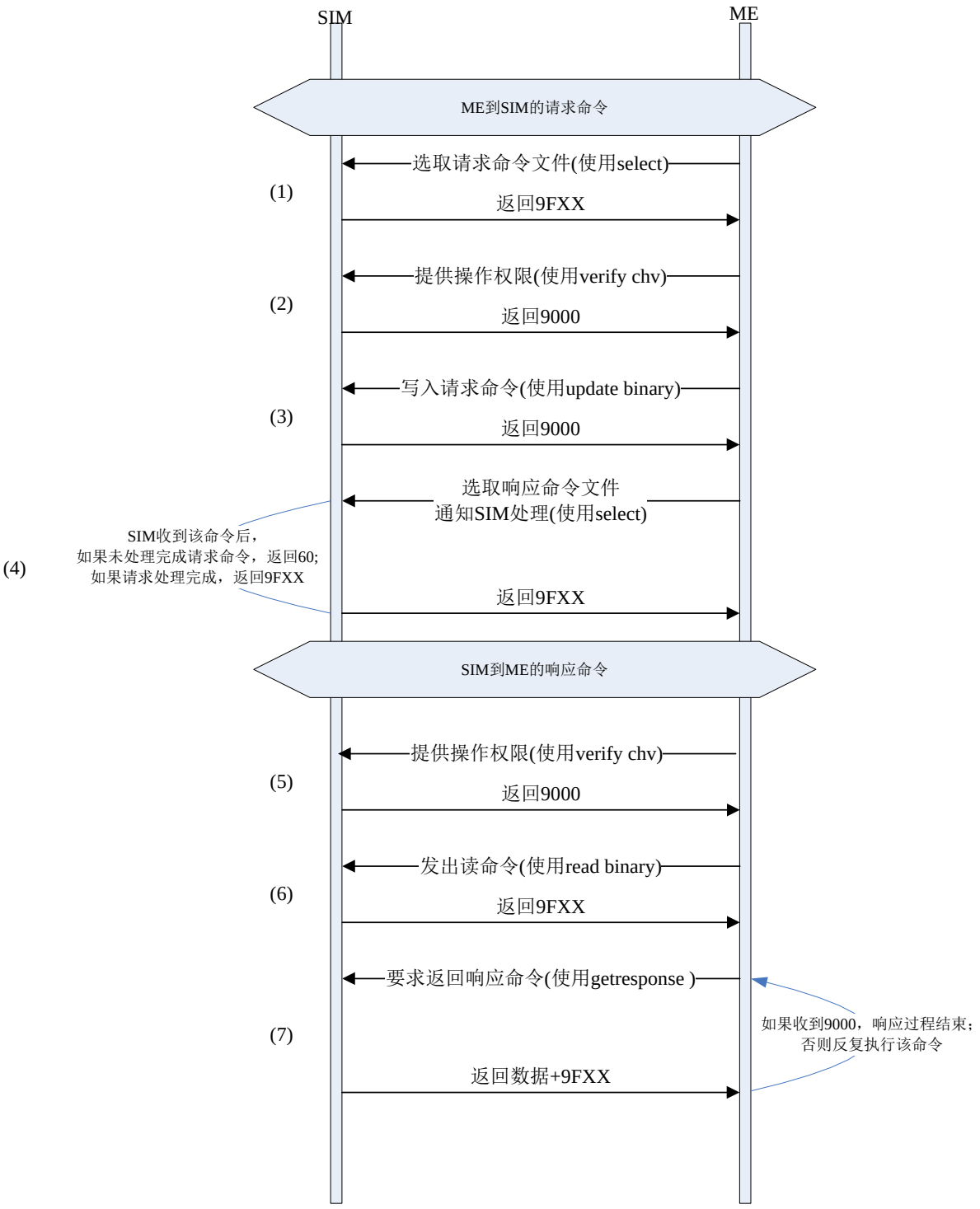
图A.1 WAPI 私钥/证书的安全操作交互流程

这样一对“请求-响应”命令使用如下的 ME-SIM 文件存取接口来承载，如图 A.2。

整个过程描述如下：

a) ME 需要执行安全使用操作时，首先使用 select 命令选取 EF_CMD 请求命令文件；
b) ME 使用 verify chv 命令提供 EF_CMD 文件的写操作权限；
c) ME 使用 update binary 命令向 EF_CMD 文件写入请求操作命令；
d) ME 完成命令写入后，通过 select 命令选取 EF_CMD 文件；该命令同时也起到通知 SIM 有请求命令需要处理的作用。SIM 收到该命令后，读取 EF_CMD 文件中的请求命令内容，执行处理过程，并将处理结果写入 EF_CMD 文件中的命令响应部分。SIM 如果处理未完成，向 ME 返回 0x60 等待消息；否则返回 0x9Fxx 消息。ME 应当在写完请求命令并发出 Select 命令后，等待直到收到 0x9Fxx 返回值，然后就可以对 EF_CMD 文件进行读取操作，得到命令响应；
e) ME 收到 0x9Fxx 消息后，表明 SIM 已经完成对请求命令的响应，ME 应当发出 Read binary 命令，SIM 收到后，返回 0x9FXX，提示有数据输出；

f） ME 发出 getresponse 命令，SIM 收到后，返回数据+0x9FXX，如果 SIM 的数据已经返回完毕，返回 0x9000；否则返回数据+0x9FXX。ME 根据返回消息，持续发出 getresponse 消息获取数据。



图A.2 “请求-响应”命令使用 ME-SIM 文件存取接口承载流程

在上述过程中，通过将本规范自定义的操作命令封装到 GSM11.11 规范定义的 ME-SIM 文件安全存取命令中，实现了 ME-SIM 的接口交互。本方法所使用机制是 GSM11.11 规范中定义的标准机制，可适用于

主要的 ME 环境。

但在具体应用中，由于各厂商对 GSM11.11 规范实现中存在差异，有些 ME 不支持对 SIM 卡中新扩展出的文件的读写操作，需要将 EF_CMD 文件中的内容装入到 SIM 卡中已有的文件，通过复用已有文件实现操作。下述一个例子是利用 EF_{AD}(文件 ID 6FAD)，将 EF_CMD 装到 EF_{AD}(文件 ID 6FAD)来实现对本规范所定义的操作。

EF_{AD} 文件定义如下：

Identfier:0x6FAD	Structure:transparent	Mandatory
FileSize:32+4096	Update activity:low	
Access Conditions: READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Byte	Description	M/O	Length
1	操作模式	M	1
2-3	附加信息	M	2
4-X	保留	M	29

本规范中对 EF_{ADw} 文件中的保留字段进行复用，将 EF_CMD 中的字段添加到 EF_{ADw} 文件中，扩展出如下定义：

33	命令权限类别	M	1
34-35	命令的权限值	M	8
36-2083	请求命令	M	2048
2084-4131	响应命令	M	2048

经过如上扩展后，可以通过 EF_{ADw} 文件来承载本规范所定义的操作。

A.3 WAPI私钥/证书安全分发技术在SIM卡上的实现

WAPI私钥/证书的安全分发主要包括文件生成、更新、吊销过程中，独立安全介质和证书系统的交互接口。在SIM卡上实现安全分发技术，可以使用OTA-SMS机制来承载，该过程见图A.3。

图A.3所示流程说明如下：

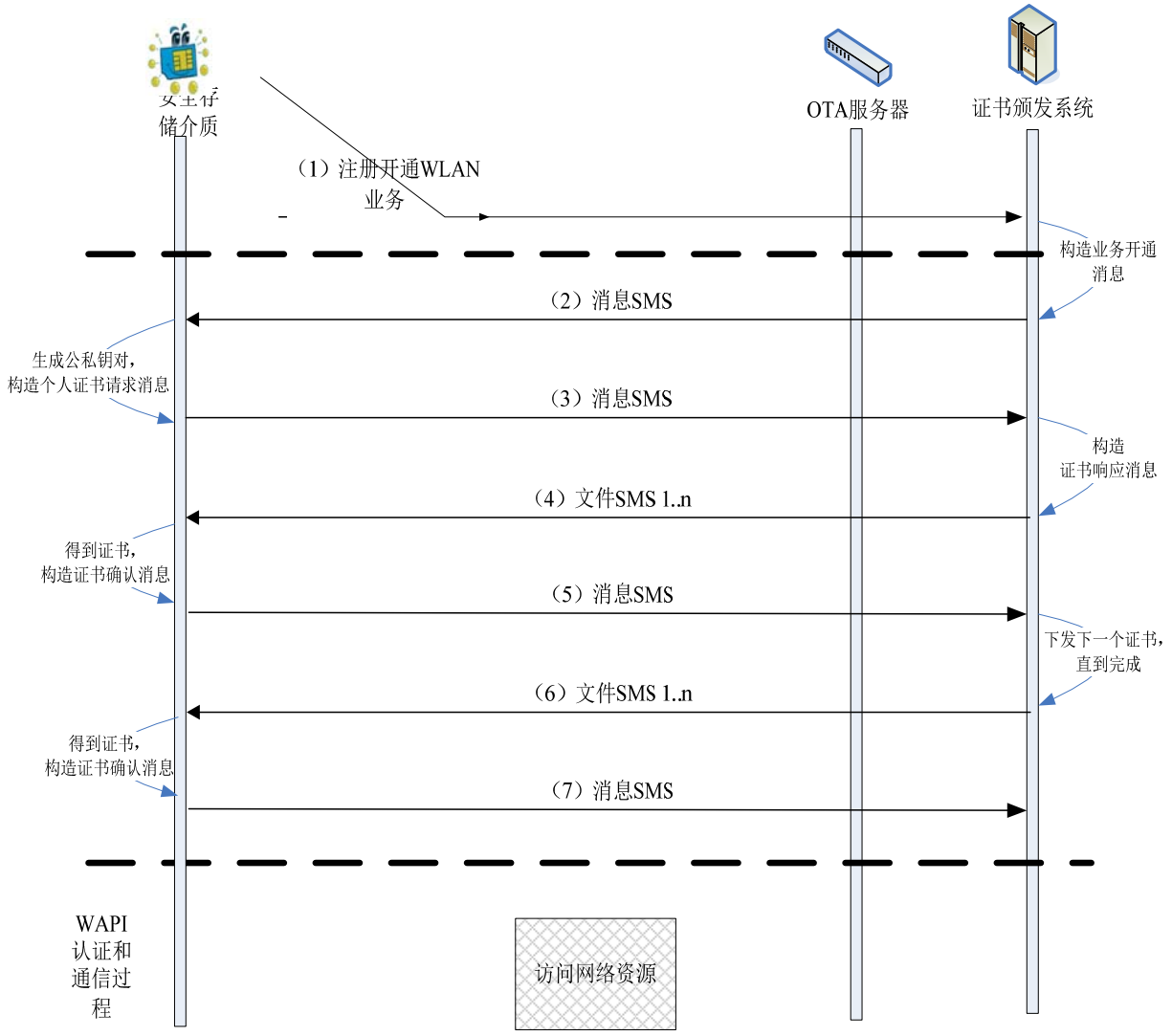
a）对于流程(2)(3)(5)(7)，安全分发消息能够封装在一条短信中，而且不涉及文件下载，所以使用“普通OTA-SMS”来承载；

b）对于流程(4)(6)，安全分发消息中携带有证书文件，而且涉及到文件下载，需要将该消息分解后装入到多条OTA短信中，逐条发送给SIM卡；SIM卡收到后，逐条取出其中包含的有效内容，组合后得到证书文件。所以该类消息使用“带有文件头的OTA-SMS”来承载。

安全分发技术涉及的相关消息分别使用“普通OTA-SMS”和“带有文件头的OTA-SMS”来承载，其对应列表见表A.1。

表A.2是运营商的“普通OTA-SMS”，格式定义如下，其中KLC字段要求设置为0（不使用加密）。

表A.3是运营商“带有文件头的OTA-SMS”的短消息，该短消息是在“普通OTA-SMS”的格式基础上，在命令参数部分增加了如下的协议头,本协议头是针对本规范定义的。



图A.3　WAPI 私钥/证书的安全分发操作流程

表A.1　安全分发中涉及的相关消息承载 OTA 短信类别

消息	操作命令	承载的 SMS
业务开通激活	WAPI_businessAct	普通 OTA-SMS
个人证书请求	WAPI_cerBuildReq	普通 OTA-SMS
个人证书响应	WAPI_cerBuildRsp	带有文件头的 OTA-SMS
个人证书确认	WAPI_cerBuildAck	普通 OTA-SMS
证书更新请求	WAPI_cerUpdateReq	带有文件头的 OTA-SMS
证书更新确认	WAPI_cerUpdateAck	普通 OTA-SMS
证书吊销通知	WAPI_cerRevokeNtf	普通 OTA-SMS

表A.2　普通 OTA-SMS 格式定义

标识		长度（字节）	值	说明
TPDU_Header		可变	短消息头	TP-UDHI 为 1
UDL		1		后续数据长度
安全应用数据	UDHL	1	0X02	信息标识长度
	IEIb	1	0X70	安全头标识
	IEIDLb	1	0X00	信息长度
	CPL	2		后续数据长度,从 CHL 到最后
	CHL	1	0X11	安全报文头长度，从 SPI 到 CC
	SPI	2	0X02	只使用第一字节 bit1,bit2。
			0X00	
	KLC	1	0X00	不使用加密。
	KID	1	0xx1	DES CBC,高 4 位为密钥编号
	TAR	3	B0 00 10	OTA 业务下载
	CNTR	5		参见 11 节，计数器的管理
	PCNTR	1	0x00	参见 GSM03.48 。
	CC	4		使用 MAC，参见 11 节，MAC 算法。
	随机数	4	HEX	密钥分散及密钥选择用,不能加密
	计数器类型标识	1	HEX	0 表示使用计数器 A 1 表示使用计数器 B 其他保留。
命令数据	命令类型	1	HEX	
	命令长度	1	HEX	本条短信中命令参数的长度。
	命令参数	X	HEX	

表A.3　带有文件头的 OTA-SMS 格式

项目	名称	长度（字节）	值	说明
命令类型	多证书下载	1	0x03	
	菜单索引	3	HEX	同上行申请或远程下载选择的菜单索引
	本批次证书 ID	2	HEX	一个批次理论上可以放置 4 个证书的内容（参见证书 ID 定义）
		1	HEX	高 4bit：为当前短信所属证书的 ID
				低 4bit：为当前短信在当前证书的短信索引

	下载任务批次	1	HEX	1-255,递增加 1，循环使用，一次完整应用下载为一个批次。
	短信总数	1	HEX	整个应用的短信总数
	短信索引	1	HEX	该短信在整个应用中的索引
	应用数据空间	2	HEX	为全部应用数据的总空间。 与应用数据组成定义中的应用数据空间相等
	当前短信下载证书总长度	2	HEX	
	应用数据地址偏移	2	HEX	应用数据地址偏移的计算见应用数据说明
	应用数据	X	HEX	详见菜单数据组成定义

附 录 B
（资料性附录）
在 USB KEY 上承载安全存储和使用规范

在 USB KEY 做为安全介质的应用中，USB KEY 和主机之间可以通过驱动直接承载安全操作命令，无需特别考虑。