团　　体　　标　　准

T/EMCG 001.1-2019

移动智能终端密码模块技术框架
第 1 部分：总则

Technical framework of cryptographic module in mobile smart terminal

Part 1: General

EMCG

2019－07－05 发布　　2019－07－05 实施

中关村网络安全与信息化产业联盟　发布

目 次

EMCG

前　言

T/EMCG 001-2019《移动智能终端密码模块技术框架》分为5个部分：

第1部分：总则

第2部分：密钥加密本地保护技术架构

第3部分：密钥加密服务端保护技术架构

第4部分：密钥多端协同计算保护技术架构

第5部分：基于安全芯片的技术架构

本部分为T/EMCG 001-2019《移动智能终端密码模块技术框架》的第1部分，是其他4部分的背景、原理概述。其他4个部分为4种满足GM/T 0028-2014要求的移动智能终端密码模块实现方案，用于指导厂家设计、实现移动智能终端密码模块。

本部分由中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）提出。

本部分由参与T/EMCG 001-2019《移动智能终端密码模块技术框架》标准制定的单位投票表决通过。

本部分主要起草单位：中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）、中国科学院信息工程研究所、奇安信科技集团股份有限公司、江苏通付盾科技有限公司、北京江南天安科技有限公司、北京握奇数据股份有限公司、鼎桥通信技术有限公司等。

本部分主要起草人：王克、刘宗斌、张凡、傅文斌、张晶、李勃、鲁洪成、李向荣、李强等。

EMCG

引　言

在移动互联技术应用中，使用密码技术以防止数据泄露和篡改，实现实体鉴别及行为抗抵赖。但密码技术使用不当，会使其安全作用失效，影响应用系统安全。密码技术使用的安全性取决于算法正确实现及密码模块敏感安全参数保护。在开放移动网络和便携移动终端系统环境中，如何设计、实现和使用密码模块，如何保护敏感安全参数成为移动智能终端密码模块设计和实现的核心问题。

T/EMCG 001-2019《移动智能终端密码模块技术框架》规范了移动智能终端（mobile smart terminal MST）使用的几种密码模块技术架构。

EMCG

移动智能终端密码模块技术框架 第1部分：总则

1. 范围

T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分界定了移动智能终端（MST）和移动智能终端密码模块(CMMST)的范围；列出了MST密码应用场景、CMMST安全威胁，明确了CMMST设计和实现须达到的安全目标；给出了CMMST安全模型以及安全保障。

本部分是T/EMCG 001-2019其他部分的背景及原理概述，适用于指导T/EMCG 001-2019其他部分的编写。

2. 规范性引用文件

下列文件中的条款通过T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分的引用而成为本部分的条款。

GM/T 0028-2014 密码模块安全技术要求

GM/T 0008-2012 安全芯片密码检测准则

3. 术语和定义

下列术语和定义适用于T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分。

3.1

核准的安全功能 approved security function

GM/T 0028-2014附录C中给出的安全功能。如密码算法。

3.2

关键安全参数 critical security parameter

与安全相关的秘密信息，这些信息被泄露或被修改后会危及密码模块的安全性。

[GM/T 0028-2014，定义3.15]

3.3

密码边界 cryptographic boundary

明确定义的连续边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有硬件、软件、和/或固件部件。

[GM/T 0028-2014，定义3.17]

3.4

密码组件 cryptographic component；CC

是密码模块的一部分，包括实现了安全功能的硬件、软件和/或固件。

3.5

密码模块 cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

[GM/T 0028-2014，定义3.18]

注：本标准中的密码模块均指GM/T 0028-2014所规范的密码模块。

3.6

移动应用 mobile application

可在移动智能终端操作系统中进行安装使用运行的应用软件。本标准所述的移动应用是指调用密码模块服务的应用软件。

3.7

个人身份识别码 personal identification number；PIN

用于鉴别身份的一串数字和字符。

3.8

用户私钥 user private key

在某一移动智能终端使用者的非对称密钥对中，只应由该用户掌握和使用的密钥。正常情况下，私钥不应泄露。

3.9

公开安全参数 public security parameter；PSP

与安全相关的公开信息，一旦被修改会威胁到密码模块安全。

[GM/T 0028-2014，定义3.73]

3.10

安全芯片 security chip

含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片。

[GM/T 0008-2012，定义3.1.3]

3.11

安全功能 security function

密码算法及其工作模式，包括：分组密码、流密码、对称或非对称算法、消息鉴别码、杂凑函数、或其他安全函数，随机比特生成器，实体鉴别和敏感安全参数生成和建立等。

[GM/T 0028-2014，定义3.78]

3.12

服务端 server side; SS

本标准T/EMCG 001-2019密码模块所包含的远程服务器。

3.13

敏感安全参数 sensitive security parameter; SSP

包括关键安全参数和公开安全参数。

[GM/T 0028-2014，定义3.82]

3.14

可信信道 trusted channel

在密码模块和发送者或接收者之间建立的安全可信的通信链接，用以安全传输未受保护的关键安全参数、密钥分量和鉴别数据。

[GM/T 0028-2014，定义3.99]

4. 符号和缩略语

下列符号和缩略语适用于T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分。

CC 密码组件（cryptography component）

CMMST 移动智能终端密码模块（cryptographic module of mobile smart terminal）

SS-CC 服务端密码组件（server side cryptography component）

MST 移动智能终端（mobile smart terminal）

MST-CC 移动智能终端密码组件（mobile smart terminal cryptography component）

PIN 个人身份标识码（personal identification number）

5. 移动智能终端（MST）

T/EMCG 001-2019《移动智能终端密码模块技术框架》规范了移动智能终端（mobile smart terminal MST）使用的各种密码模块技术架构。

T/EMCG 001-2019中所有部分内容中的MST是指能够接入移动通信网，具有提供应用软件开发接口的开放操作系统，并能够安装和运行第三方移动应用软件的移动设备。包括手机、Pad。这些MST可以是市场通用型的，也可以是机构专用型的。

6. 移动智能终端密码组件（MST-CC）

T/EMCG 001-2019中所有部分内容中的移动智能终端密码组件（mobile smart terminal cryptography component；MST-CC）是指部署在移动智能终端中的密码组件，或独立构成，或与服务端密码组件（SS-CC）一起构成移动智能终端密码模块。

7. 服务端密码组件（SS-CC）

T/EMCG 001-2019 中所有部分内容中的服务端密码组件（server side cryptography component；SS-CC）是指部署在服务端中的密码组件，与移动智能终端密码组件（MST-CC）一起构成移动智能终端密码模块。

8. 移动智能终端密码模块（CMMST）

在T/EMCG 001-2019中所指的移动智能终端密码模块（cryptographic module in mobile smart terminal；CMMST）是为MST使用的，实现核准安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。这些硬件、软件可以包含在一个MST中，如手机中的安全芯片、密码应用SDK；也可以存在于MST以外的环境中，如服务端的密码组件，或独立Ukey等。

9. 移动智能终端密码技术应用场景

在保护网络安全中，密码技术主要应用在两方面：信息加密和信息签名。信息加密包括通信信息加密和存储信息加密，以防止信息被非法泄露。信息签名包括用户对数据进行签名以及实体（如计算机、路由器）对数据进行签名，以保证交换数据的真实性和不可抵赖性。信息加密一般使用对称密码算法（如SM4）；信息签名一般使用非对称密码（如SM2）算法；对通信信息实施加密时可使用非对称密码算法进行通信密钥协商。

密码技术在移动互联系统中的应用包括但不限于以下场景：

（1）移动终端及操作系统使用密码技术。如，

a) 移动终端开机启动对操作系统进行完整性校验（可信计算技术），保证移动终端操作系统的完整性；

b) 操作系统对移动应用代码签名进行验证，验证移动应用的合法性和完整性；

c) 操作系统对文件（或存储介质）进行加密，保证移动终端失控时存储的数据不被泄露；

d) 移动终端无线局域网接入安全认证。如WAPI安全协议密码应用，防止非法移动终端接入企业网络；

（2）移动应用系统使用密码技术。如，

e) 在公共网络上建立企业虚拟专用网络（VPN），保证企业信息在移动互联网络上传输的信息不被泄露；

f) 移动通信语音加密（如VoIP），防止移动电话通信内容被监听；

g) 移动终端电子邮件加密，防止电子邮件被非授权阅读；

h) 移动用户上网登录身份认证（如FIDO协议），防止非法用户登录网络应用系统；

i) 企业移动终端信息文件加密存储，防止非法用户或程序读取企业信息造成信息泄露；

j) 企业信息移动终端文件电子签名，保证企业用户对移动办公文件签名的真实性和不可抵赖性；

k) 移动金融业务保护，使用密码技术保证移动支付、转账操作的合法性、不可抵赖性。

10. CMMST 安全威胁

T/EMCG 001-2019所针对安全威胁是指可使移动智能终端密码模块安全功能失效的威胁。在移动互联网环境中，攻击者可以利用网络监听、网络攻击、移动终端物理介入、恶意应用软件等手段对CMMST进行攻击，加上CMMST设计和实现不当都可能对密码应用构成威胁。包括:

（1）影响密码算法实现和使用的有效性。如，密码算法实现问题导致加密结果安全性降低，密码模块在使用中密码算法程序被修改等。

（2）影响密钥生成的有效性。如，随机数发生器质量不合格。

（3）影响敏感安全参数存储和使用的安全性。如，私钥生成、存储和使用不当导致私钥泄露，密钥被非授权从CMMST导出，密码模块的PIN码构成和保护不当导致CMMST非法使用，以及对密码安全芯片进行访问、能量、电磁分析非法获取敏感安全参数等。

11. CMMST 设计和实现的安全目标

根据GM/T 0028-2014密码模块设计和实现的安全目标要求，T/EMCG 001-2019的CMMST设计和实现安全目标包括：

（1）使用并正确实现核准的安全功能。

（2）防止非授权操作、使用和查看CMMST。

（3）防止非授权泄露CMMST内容，如私钥和PIN码。

（4）防止对CMMST和密码算法进行非授权或检测不到的修改，包括非授权的修改、替换、插入和删除敏感安全参数。

（5）提供CMMST运行状态指示。

（6）保证CMMST在核准的工作模式下能够正确运行。

（7）检测出CMMST运行中的错误，防止这些错误非授权地公开、修改、替换或使用私钥或PIN码，或者非授权地修改或替换公开安全参数。

（8）保证正确地设计、分配和实现CMMST。

12. CMMST 安全模型

为保证CMMST设计和实现的安全目标,根据移动互联网应用的需求和特点，CMMST采取服务端安全模型和移动端安全模型实现对敏感参数保护。服务端安全模型适合软件密码模块，移动端安全模型适合硬件密码模块。

CMMST服务端安全模型（CMMST server security model；CMMST-SSM）如图1所示。MST密码组件（MST-CC）为移动应用提供核准的安全功能；服务端密码组件(SS-CC)实现关键安全参数保护，如PIN生成、私钥加密存储保护、私钥拆分生成及其分量保护；安全通信保证MST-CC与SS-CC安全交互。

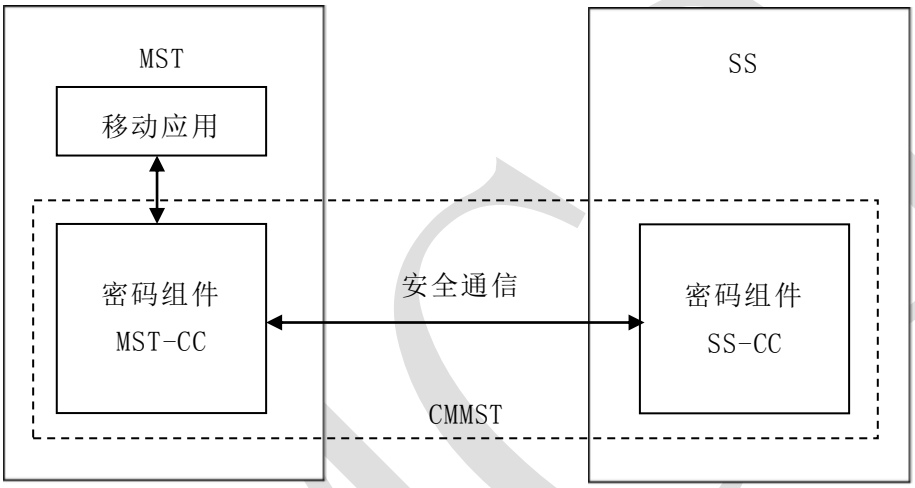

图1 CMMST服务端安全模型

CMMST移动端安全模型（CMMST mobile security model；CMMST-MSM）如图2所示。MST密码安全芯片为移动应用提供核准的安全功能，以及敏感安全参数存储保护；可信信道为CMMST提供关键安全参数通信，例如用户PIN的输入；物理安全组件为安全芯片（security chip）提供满足高级密码模块的物理安全要求，包括密码模块拆卸检测及响应、敏感安全参数清除等硬件电路。

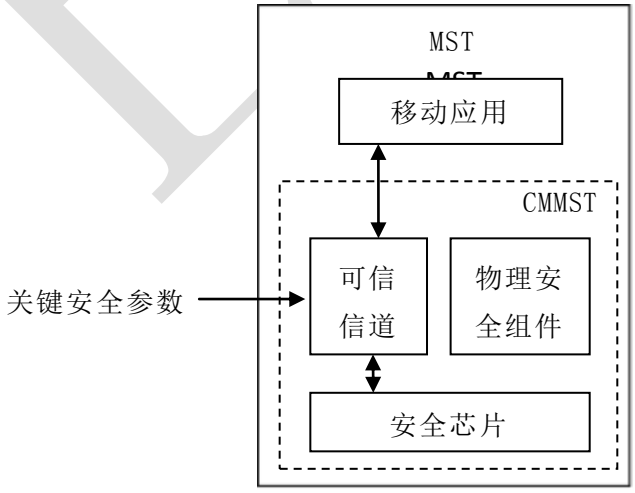

图2 CMMST移动端安全模型

13. CMMST 安全保障

（1） CMMST使用的安全芯片须满足GM/T 0008-2012《安全芯片密码检测准则》要求。

（2） CMMST服务端应采用独立服务器设备，并专用于CMMST。

（3） CMMST应实施配置管理，防止CMMST及文档被非授权修改。

（4） CMMST应有严格的开发过程管理。

（5） 应采取必要措施对移动端密码组件、服务端密码组件与非CMMST系统实施数据及代码隔离。

（6） 应对所有在开放环境里运行的CMMST软件进行软件实名签名，防止密码模块软件被篡改。

EMCG