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

目 次

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

移动智能终端密码模块技术框架

第1部分：总则

1 范围

T/ZSA 67-2019《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/ZSA 67-2019其他部分的背景及原理概述， 适用于指导T/ZSA 67-2019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/ZSA 67-2019《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/ZSA 67-2019《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