ICS 33.050
CCS M 30

团　体　标　准

T/TAF 224—2024

智能终端安全芯片通用技术要求

General technical requirements for smart terminal security chip

2024-03-26 发布　　2024-03-26 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：华为技术有限公司、中国信息通信研究院、郑州信大捷安信息技术股份有限公司、国民认证科技（重庆）有限公司、中移动金融科技有限公司、英飞凌科技（中国）有限公司、深圳市汇顶科技股份有限公司。

本文件主要起草人：李实、袁琦、衣强、张宏星、胡重阳、田琛、马四英、闫彦、宁丹、徐晓娜、刘献伦、李俊、董扬、果艳红、王昊、黄显明、孙金龙。

引　言

随着智能终端设备业务创新的持续演进，智能终端设备需要承载越来越多的敏感业务及隐私数据存储。相应地，智能终端设备作为整个社会基础设施的一部分，其攻击事件日益增长，攻击价值也日益增加。

安全芯片是密码技术的载体，也是重要数据的保险箱。从每个人的身份证、银行卡、手机电子钱包，到通信、金融、交通、安防、医疗等涉及安全的方方面面，都离不开安全芯片的保驾护航。在智能终端设备中部署安全芯片是提升智能终端设备安全竞争力的强有力构建途径，但在实际部署中，即使智能终端设备采用了安全芯片，其解决方案也呈现碎片化，无法在跨类型设备、跨操作系统平台直接部署。目前行业中需要对终端安全芯片的整体安全框架进行规范以及提出通用的安全技术要求，对安全芯片行业应用推广提供技术支撑。

智能终端安全芯片通用技术要求

1 范围

本文件规定了智能终端安全芯片整体架构设计、安全芯片需要支持的密钥管理服务、凭据管理服务、安全存储服务、防回退服务等安全技术要求。

本文件适用于智能终端安全芯片的设计与实现，其他安全芯片也可参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 18336 信息技术安全评估准则

GB/T 25069—2022 信息安全技术 术语

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GM/T 0008 安全芯片密码检测准则

ISO/IEC 15408（所有部分） 信息安全、网络安全及隐私保护 - IT安全评估准则（Information security, cybersecurity and privacy protection — Evaluation criteria for IT security）

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

终端安全芯片 terminal security chip

为终端提供加解密和安全认证服务，实现了密码算法功能，直接或间接地使用密码技术来处理密钥和敏感信息的集成电路芯片。终端安全芯片的实现形态包括集成在 SoC 内的安全计算单元，以及外置于 SoC 的安全芯片。

3.2

敏感个人信息 personal sensitive data

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

4 缩略语

下列缩略语适用于本文件。

API：应用编程接口（Application Programming Interface）

APDU：应用协议数据单元（Application Protocol Data Unit）

FW：固件（Firmware）

HW：硬件（Hardware）
REE：富执行环境（Rich Execution Environment）
SoC：片上系统（System on Chip）
SW：软件（Software）
TEE：可信执行环境（Trusted Execution Environment）
TRNG：真随机数发生器（True Random Number Generator）

5　安全芯片及管理架构

5.1　概述

智能终端中存在大量涉及敏感信息数据的处理和存储操作，如口令认证、密钥服务与设备可信证明、数据防回退、敏感数据存储（如系统关键密钥存储、个人敏感数据存储）等。终端安全芯片可以提供硬件级别的可信计算根与存储根，在TEE安全级别的基础上进一步强化系统安全能力，为终端的安全性提供保障。

安全芯片由提供安全服务和安全功能所需的硬件（HW）、固件（FW）和软件（SW）组成，其形态既可以是集成在SoC内的独立计算单元，如图1所示，也可以是外置于SoC的独立安全芯片，如图2所示。

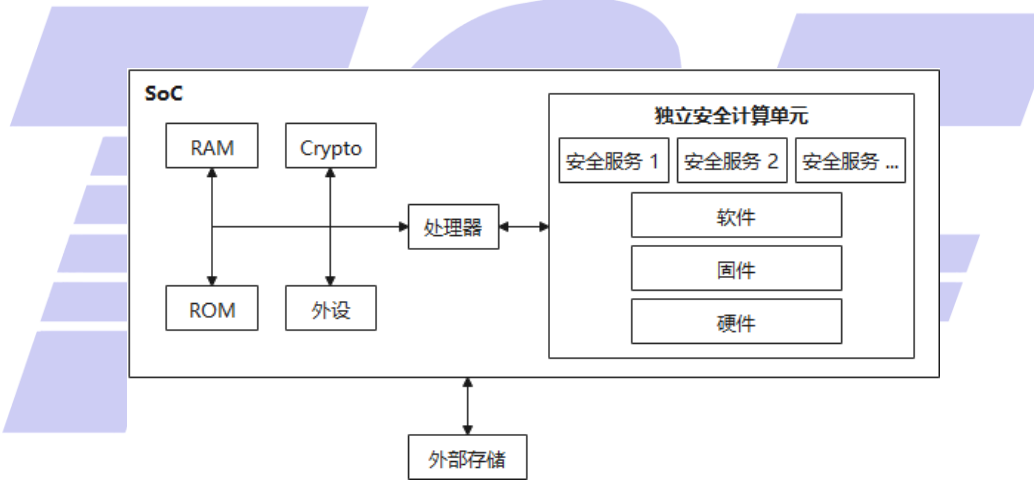

图1　集成在SoC内的独立安全计算单元

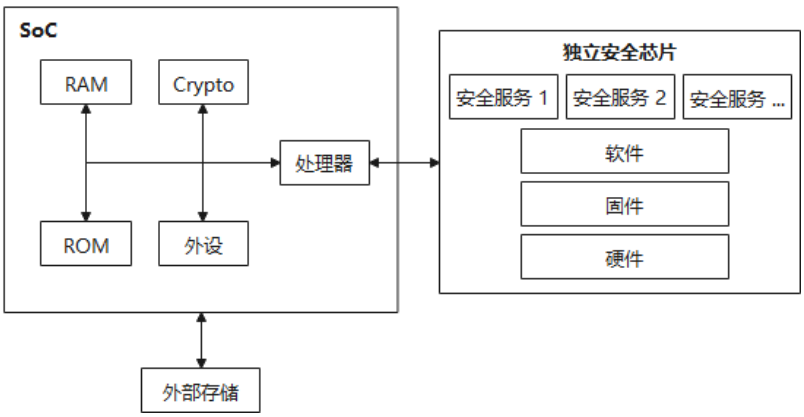

图2　外置于SoC的独立安全芯片

安全芯片及管理架构主要包括：应用层、服务管理层、硬件驱动层、硬件层四部分，如图 3 所示。

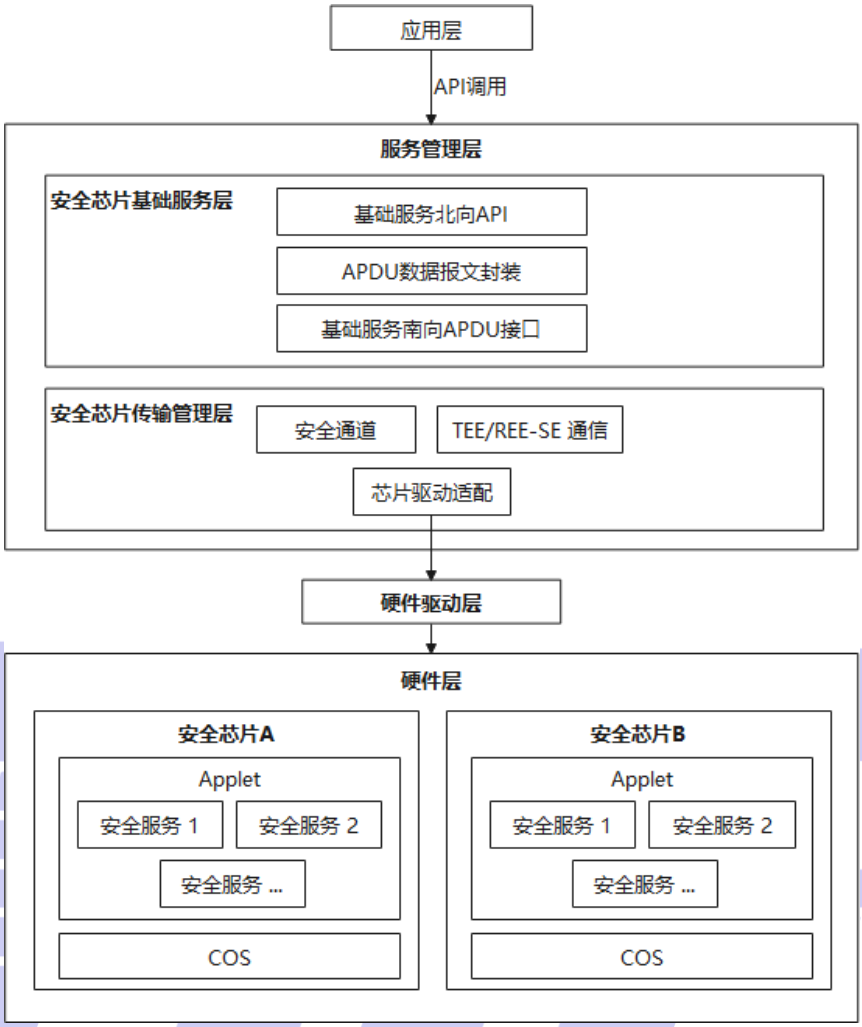

图 3　安全芯片及管理架构

5.2　架构组成

5.2.1　应用层

安全芯片服务的应用与智能终端设备的安全能力相关。安全芯片的应用包括但不限于以下几种：

a)　高安全等级应用可基于安全芯片部署的智能终端设备的核心安全能力；

b)　对业务核心资产的安全性要求较高的应用，如金融支付行业、政企行业等，其核心业务基于安全芯片部署；

c)　在涉及敏感应用的处理或与其他高安全等级智能终端设备进行连接交互时，智能终端设备使用安全芯片以保证安全性。

5.2.2　服务管理层

安全芯片管理框架主要包含安全芯片基础服务层、安全芯片传输管理层。安全芯片基础服务层主要负责系统安全类服务的实现和 APDU 封装以及安全芯片管理相关功能，对上层业务提供各系统安全类服务的 API 以及实现对南向安全芯片厂商提供的 APDU 数据报文格式。安全芯片传输管理层主要负责与安全芯片通信的标准协议以及安全通道协议的实现，同时对安全芯片厂商提供南向驱动注册接口，供安全

芯片厂商适配。

安全芯片管理框架的服务支持裁剪、扩展，智能终端设备中基于安全芯片的业务统一通过安全芯片基础服务层提供的 API 访问该管理框架及下层安全芯片的安全服务能力。安全芯片管理框架可部署在多种基础运行环境和设备中，如：TEE OS、REE OS（如：Linux）、轻量级设备中的轻量化 OS 等。

5.2.3 硬件驱动层

安全芯片硬件驱动由各芯片厂商提供，通过适配南向注册接口对接安全芯片管理框架，从而打通主 SoC 芯片与安全芯片之间的物理链路。

5.2.4 硬件层

安全芯片硬件层的具体规格由芯片厂商决定，但要满足安全芯片要求才能接入管理框架。安全芯片中所提供的安全服务包括：基础的密钥管理服务、安全存储服务、凭据管理服务、防回退服务等，安全应用根据实际需要调用安全芯片中的安全服务。

6 安全芯片通用要求

安全芯片的通用要求如下：

a） 安全芯片中应使用安全密码算法和真随机数发生器 TRNG，避免使用不安全的密码算法或不安全随机数。密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，产生的随机数应满足 GB/T 32915-2016 的随机性检测规范要求；

b） 安全芯片应具有防侧信道攻击、防物理攻击、防故障注入攻击等基础物理防护能力；

c） 安全芯片应支持基于物理或逻辑隔离机制，提供与其他 SoC 组件隔离的安全功能和安全服务；

d） 应确保存储在安全芯片内数据的机密性和完整性；

e） 如果安全芯片中不包含内置的安全存储模块，则安全芯片应连接到外部的安全存储模块，并应确保连接通道的安全性，和存储在外部安全存储模块内的数据应保证其机密性和完整性，并禁止数据回退；

f） 安全芯片应具备安全通道建立机制，以保证业务侧与安全芯片之间数据传输的机密性和完整性；

g） 安全芯片的安全能力应至少符合 GM/T 0008 安全等级二级、GB/T 18336 的 EAL4+要求、ISO/IEC 15408 的 EAL4+要求之一。

7 安全芯片的安全服务与要求

7.1 密钥管理服务

在安全芯片内部部署密钥管理服务，通过物理隔离提供硬件级安全的密钥全生命周期管理能力。基于安全芯片构建的密钥服务应满足以下功能及安全要求：

a） 应提供主流密码算法的硬件实现；

b） 应具备密钥生成功能，如在安全芯片中生成根密钥或业务密钥等；

c） 应具备密钥明文和密钥密文的导入功能，如向安全芯片内导入业务密钥等，并确保密钥导入的安全性；

d） 应具备密钥的访问控制功能。在密钥生成或导入时，密钥使用方应为密钥指定其被授权使用的方式或目的，包括但不限于加密、解密、签名、身份验证等。在密钥使用时，由安全芯片执行授权校验，以避免密钥被以未经授权的方式使用；

e） 应支持非对称密码算法的公钥及证书从安全芯片中导出的功能，确保其他类密钥的明文不出安

全芯片；不应支持在安全芯片内使用的私钥被导出；

f） 应具备密钥派生功能，可基于业务提供的派生根密钥和派生因子在安全芯片内部进行密钥安全派生；

g） 应具备密钥协商功能，如业务与安全芯片协商用于数据加密传输的业务密钥；

h） 应具备数据加/解密功能，并支持根据不同配置选择不同加密算法的能力；

i） 应具备数字签名及验签功能，并支持根据不同配置选择不同数字签名算法的能力；

j） 应具备 MAC（消息认证码）计算及校验功能，并支持根据不同配置选择不同 MAC 算法的能力；

k） 应具备证书导入功能，如向安全芯片导入并存储设备证书链、设备私钥及设备硬件标识符等，并保证其机密性和完整性；

l） 应具备设备身份认证功能，如通过安全芯片内部的设备证书私钥对业务密钥及业务信息进行签名生成业务证书，供云端或应用进行验证。

7.2 口令认证服务

口令作为用户身份认证的重要依据，被多种业务及场景使用，口令安全直接影响用户数据的安全性。为确保用户口令的安全性，基于安全芯片构建的口令认证服务应满足以下功能及安全要求：

a） 应具备口令写入与口令存储功能；

b） 用户口令应被安全的存储在安全芯片中，并提供口令防泄露机制；

c） 口令的注册与校验过程应在安全芯片内部进行，确保注册与校验过程的安全性，并提供防暴力破解机制，包括但不限于设置错误验证次数阈值、基于时间惩罚的验证锁定等；

d） 宜提供达到错误验证次数阈值后的口令删除功能，以防止恶意攻击。

7.3 安全存储服务

基于安全芯片的安全存储是将设备内的某些关键敏感数据存储到安全芯片内部，以提高防篡改、防泄漏能力。基于安全芯片构建的安全存储服务应满足以下功能及安全要求：

a） 应对外提供芯片内安全存储分区的读、写、空间申请、释放等功能；

b） 在进行安全芯片的数据读取和写入时，应建立安全通道和数据保护机制，确保数据的机密性和完整性；

c） 应在读、写、释放安全存储分区数据前进行鉴别和授权；

d） 在工厂模式下调用数据擦除功能时，应进行鉴别和授权；

e） 应提供数据隔离访问机制，通过安全芯片内的鉴别和授权机制对各用户数据进行隔离访问。

7.4 防回退服务

安全芯片中的防回退服务主要针对数据防回退保护，应满足以下功能及安全要求：

a） 应确保存储和读取的数据是当前最新数据，禁止回退到旧的数据；

b） 应在安全芯片内部实现一个或多个防回退计数器，并确保计数器只能单向递增（或递减）；

c） 应在安全芯片内部实现计数器的访问控制机制，并对访问计数器的业务进行鉴别和授权，防止拒绝服务攻击；

d） 应支持计数器初始值随机化，避免计数器值被仿冒。

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范
[2] GB/T 37092—2018 信息安全技术 密码模块安全要求
[3] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

电信终端产业协会团体标准

智能终端安全芯片通用技术要求

T/TAF 224—2024

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn