GM/Y 5008-2024

基于可信执行环境的密码模块技术研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘要

可信执行环境（Trusted Execution Environment，TEE）被广泛应用于手机等移动终端设备和服务器等服务端设备中，为运行在其中的应用提供硬件隔离的防护能力。基于TEE的密码模块能够提供身份认证、数据保护、密码运算等安全功能和密码服务。密码模块的设计要遵循GM/T 0028中的安全要求，但这是普适性的通用安全要求，对基于可信执行环境的密码模块而言，如何确定划分密码模块边界的依据，如何划定密码模块边界，可以划分成哪几种密码模块，不同边界的密码模块在安全设计时有哪些要点和难点，这些方面尚未开展深入研究。

本课题结合当前智能手机等移动终端设备上的密码应用场景，调研基于可信执行环境的密码模块的发展现状以及相关课题和标准研究情况；研究基于可信执行环境的密码模块的技术架构、工作原理、安全性要求、国产密码算法应用和密码应用接口等内容，结合密码模块安全性评估，提出了基于可信执行环境的密码模块的技术架构、边界划分方法、密码模块分类依据、六类密码模块边界图以及安全性设计的要点和难点，旨在为我国可信执行环境密码应用领域的密码模块技术发展及标准研制规划提供参考与指导。

关键词 ：可信执行环境，可信应用，密码模块

目录

前言

可信执行环境（Trusted Execution Environment，TEE）被广泛应用于手机等移动终端设备和服务器等服务端设备中，为运行在其中的应用提供硬件隔离的防护能力。可信应用（Trusted Application，TA）是运行在可信执行环境中的应用程序。基于 TEE 的密码模块能够提供身份认证、数据保护、密码运算等安全功能和密码服务。可信应用密码模块是基于 TEE 的密码模块中的一种类型。

目前大多数基于可信执行环境技术的产品都遵循 GP（Global Platform）组织制定的标准规范。我国尚无针对基于可信执行环境的密码模块的安全技术要求与安全性评估等密码行业标准，其研制工作迫在眉睫。而且，当前基于可信执行环境的密码模块普遍存在如接口标准不统一、安全性要求参差不齐、未使用国产密码算法、无安全性评估依据等棘手问题，严重阻碍了可信执行环境技术的应用推广与移动智能终端安全等级的提升。

密码模块的设计要遵循 GM/T 0028 中的安全要求，但这是普适性的通用安全要求，对基于可信执行环境的密码模块而言，如何确定划分密码模块边界的依据，如何划定密码模块边界，可以划分成哪几种密码模块，不同边界的密码模块在安全设计时有哪些要点和难点，目前尚未开展深入研究，急需一个框架或指南用于指导基于可信执行环境的密码模块的安全设计以满足 GM/T 0028 的要求。

本课题调研基于可信执行环境的密码模块的发展现状以及相关课题和标准研究情况；研究基于可信执行环境的密码模块的技术架构、工作原理、安全性要求、国产密码算法应用和密码应用接口等内容，结合密码模块安全性评估，提出了基于可信执行环境的密码模块的技术架构、边界划分方法、密码模块分类依据、六类密码模块边界图以及安全性设计的要点和难点，旨在为我国可信执行环境密码应用领域的密码模块技术发展及标准研制规划提供参考与指导。

本研究报告是由密码行业标准化技术委员会根据国家密码管理局批准的《2020 年密码行业标准制/修订计划》下达的 2020 年密码行业标准研究编制工作任务。项目名称为《基于可信执行环境的密码模块技术研究》，项目类型为标准研究类项目，项目所属工作组为基础工作组。

本文件起草单位：北京握奇智能科技有限公司、华为技术有限公司、飞天诚信科技有份有限公司、北京信安世纪科技股份有限公司、格尔软件股份有限公司、北京数字认证股份有限公司。

本文件主要起草人：张渊、许东阳、朱鹏飞、汪宗斌、郑强、郭井龙、石玉平、李勃。

基于可信执行环境的密码模块研究

1. 概述

1.1 背景

可信执行环境（Trusted Execution Environment，TEE）是以构建隔离计算系统保障特定敏感软件代码运行环境的可信，以运行信任的角度实现可信计算的一个重要方向[1]。而在通用的 PC 平台、智能手机平台等构建的通用 TEE，扩展通用 CPU 的安全功能，在其特殊安全模式下增加内存隔离、数据代码加密及完整性保护等安全功能，典型代表有 Intel SGX，ARM Trust Zone 和 RISC-V Enclave。

随着技术发展，移动终端广泛使用，可信执行环境被广泛应用于手机等移动智能终端设备中，使用基于 TEE 的密码模块实现身份认证、数据保护、密码运算等安全功能。可信应用（Trusted Application，TA）是运行在可信执行环境中的应用程序。当前基于可信执行环境的密码模块普遍存在如接口标准不统一、安全性要求参差不齐、未使用国产密码算法、无安全性评估依据等棘手问题，严重阻碍了可信执行环境技术的应用推广与移动智能终端安全等级的提升。目前基于可信执行环境的密码模块的边界、接口以及相关标准规范尚未开展深入研究。

GP 国际标准化组织从 2011 年起开始起草制定可信执行环境相关的标准规范，目前已经形成了较成熟的标准系列。目前大多数基于可信执行环境技术的产品都遵循该组织制定的标准规范。

国内有关可信执行环境密码模块的标准制定工作也在开展中。北京移动金融产业联盟标准化委员会于 2017 年制定发布了 T/BMFIA 00001—2017《移动终端安全金融盾规范》，参与单位包括中国工商银行股份有限公司、华为技术有限公司、北京中金国盛认证有限公司等。中关村网络安全与信息化产业联盟于 2019 年制定发布了 T/ZISIA-EMCG 001—2019《移动智能终端密码模块技术框架》，参与单位包括北京握奇数据股份有限公司、鼎桥通信技术有限公司等。但是，目前基于可信执行环境的密码模块的边界、接口以及相关标准规范尚未开展深入研究。

1.2 研究目标

本课题调研基于可信执行环境的密码模块的发展现状以及相关课题和标准研究情况；研究基于可信执行环境的密码模块的技术架构、工作原理、安全性要求、国产密码算法应用和密码应用接口等内容，结合密码模块安全性评估，提出了基于可信执行环境的密码模块的技术架构、边界划分方法、密码模块分类依据、六类密码模块边界图以及安全性设计需求和安全性设计的要点、难点及实现建议，旨在为我国可信执行环境密码应用领域的密码模块技术发展及标准研制规划提供参考与指导。

2. 可信执行环境的发展现状

2.1 市场情况

GP 组织发布报告称，截止 2018 年底大约有 100 亿台设备使用了支持可信执行环境技术的芯片；预计到 2025 年，物联网设备数量将超过 754 亿。将基于可信执行环境的密码模块应用到现有密码应用场景中，可以为移动智能终端安全领域提供更高水平的密码安全保障。

国内市场，基于 TEE 的密码模块运行在移动智能终端中，被广泛应用于金融行业，实现便捷的移动金融支付。被广泛应用于移动政务、警务，实现安全便利的移动政务和警务。广泛应用于移动终端数字版权保护，隐私身份信息的安全比对，大规模数据跨机构联合建模分析的隐私求交和计算，数据资产的所有权保护，区块链上数据机密存储和计算等。而且基于 Arm TrustZone、Intel SGX 也被广泛应用到了服务器上，实现“软件定义密码模块、软件定义密码系统”的能力。

目前，基于 TEE 的密码模块在移动终端和服务器端都被都被广泛应用。移动智能终端设备实现移动端数据安全，认证安全。服务器端在云计算、大数据、机密计算等领域有着非常广阔的应用场景。

2.2 技术发展情况

可信计算定义为：一个实体是可信的，如果它的行为总是以预期的方式，朝着预期的目标进行。可以理解为以安全芯片为基础，依托安全硬件建立不受恶意代码攻击的可信执行环境，确保系统实体按照预期的行为进行。主要包括以固化信任根方式，TCM（TPM）为代表的可信计算和以运行信任方式，TEE 为代表的可信计算。

可信计算从运行信任的角度看发展脉络如下[1]：（1）专用可信系统。这类系统着眼于解决计算机安全启动、计算机隔离执行等安全问题。这类专用的可信系统的思路是隔离系统运行环境，将应用系统分割为两部分：一部分运行于不受保护的通用主机环境；另一部分运行于受保护的可信计算设备。（2）专用 TEE。采用与通用 X86 架构不兼容的增强改进型 CPU，按照程序分隔成独立的运行隔间，内存隔间中的代码和数据都是加密保护的，只有可信的 CPU 才拥有解密密钥。这些方案与专用可信系统相比具有更高的安全性，安全假设更强，其理论模型是假定应用程序不必信任操作系统和其他程序只需要信任 CPU。（3）通用 TEE。采用与专用 TEE 完全相同的安全模型和实施技术，针对通用的 PC 平台、智能手机平台等构建更为通用的 TEE，近年来通用 TEE 成为了可信计算领域一个重要发展方向。通用 TEE 扩展通用 CPU 的安全功能，在其特殊安全模式下增加内存隔离、数据代码加密及完整性保护等安全功能，典型代表有 Intel SGX,ARM Trust Zone 和 RISC-V Enclave。Intel SGX 的安全模型是不信任 Host 操作系统，TEE 只信任 Intel CPU，主要应用于云计算服务器的安全应用。Trust Zone 和 RISC-V Enclave 同样不信任 Host 操作系统，但除了信任 CPU 外，还需要信任 Secure OS，主要应用于移动嵌入式领域，保护移动终端中的用户指纹、支付数据等。

2.3 标准化现状

可信执行环境密码模块的相关标准如表 1 所示。

国外有关标准，GP 国际标准化组织从 2011 年起开始起草制定可信执行环境相关的标准规范，目前已经形成了较成熟的标准系列。包括系统架构标准《TEE System Architecture》；应用编程接口标准《TEE Client API Specification》用于实现 CA 应用时调用、《TEE Internal Core API Specification》用于实现 TA 应用时调用、《Trusted User Interface API》是可信的人机交互接口 TUI（Trusted User Interface，可信用户接口，在 TEE 内为 TA 与用户提供具有输入或输出安全交互能力的接口）、《TEE TUI Extension: Biometrics API》对于指纹等生物特征认证的扩展、《TEE Secure Element API》调用 SE 的接口；安全评估标准《TEE Protection Profile》TEE 的保护轮廓、《TEE Biometric System PP-Module》TEE 生物特征模块、《Secure Media Path PP-Module》、《Cryptographic Algorithm Recommendations》等 10 项标准。目前大多数基于可信执行环境技术的产品都遵循 GP 组织制定的标准规范。

国内有关可信执行环境密码模块的标准制定工作也在开展中。国家标准 GB/T 41388-2022《信息安全技术 可信执行环境 基本安全规范》确立了可信执行环境系统整体技术架构、硬件要求、安全启动过程基本要求、可信虚拟化、可信操作系统、可信应用与服务管理基本要求、可信服务基本功能及要求、跨平台应用中间件、可信应用架构及安全要求、测试评价方法的相关技术要求[2]。针对的是可信执行环境，其中整体架构中的模块一、二、三为本规范的密码模块边界划分和分类提供了基础。《信息安全技术 可信执行环境服务规范》，征求意见稿阶段，这个规范出了可信执行环境服务的整体技术框架及主要功能构成，并规定了相关安全技术要求及测试方法[3]。其第 14 章“通用安全要求”包括：事务防护、安全存储、访问控制、安全输入输出、第三方应用认证要求、通信要求等，但这些是站在功能的角度提的安全要求，并未以安全评估的角度，划分密码模块安全边界及分类分级的方式来提安全要求。

全国金融标准化技术委员会制定的 JR/T 0156—2017《移动终端支付可信环境技术规范》，这个标准规定了移动终端支付领域可信环境的整体框架、可信执行环境、通信安全、数据安全、客户端支付应用等主要内容[4]。其第 13 章“移动终端支付可信环境安全分级分类”中定义了 REE（Rich Execution Environment，运行通用操作系统的运行环境）、TEE 安全能力要求集合和一个安全能力级别模型。

北京移动金融产业联盟标准化委员会，2017 年制定发布了 T/BMFIA 00001—2017《移动终端安全金融盾规范》，参与单位包括中国工商银行股份有限公司、华为技术有限公司、北京中金国盛认证有限公司等。这个规范规定了移动终端安全金融盾的服务、终端生命周期管理、服务生命周期管理、密钥管理、安全要求、功能要求等[5]。其中第 8 章“安全及功能要求”提出了通用要求、TUI 要求、PIN 码要求、凭证要求、生物特征身份鉴别要求、SE 要求、TEE 要求、客户端要求、通信安全要求等，但是这些是站在功能的角度提的安全要求。该标准于 2020 年更新为 T/BFIA 00001—2020《移动终端安全金融盾规范》。

中关村网络安全与信息化产业联盟，2019 年制定发布了 T/ZISIA-EMCG 001—2019《移动智能终端密码模块技术框架》，参与单位包括北京握奇数据股份有限公司、鼎桥通信技术有限公司等。标准的第五部分《基于安全芯片的技术架构》中，针对移动智能终端使用基于可信执行环境和安全芯片的密码模块技术架构，给出了安全原理和保障措施，描述了技术架构组成、主要工作流程示例，以及 GM/T 0028—2014 中规定的 11 个安全域的适用情况[6]。

密码行业标准化技术委员会，《可信运行环境安全管理框架与接口规范》的研究报告，给出了系统总结了可信技术方案，包括 TPM 可信技术方案、TCM 可信技术方案和 GP TEE 可信技术方案，重点分析了可信运行环境系统及其密码框架，给出了可信安全管理

密码应用接口建议，给出了终端可信运行环境密码应用接口建议。在此基础上，提出了标准规划建议[7]：《基于 TEE 的安全管理框架与密码接口规范》、《可信运行环境密码框架与接口规范》，这些研究成果为我们进行基于可信执行环境的密码模块的边界划分、分类分级、不同类别密码模块的技术架构、安全性设计要求和实现建议奠定了基础。

表 1　TEE 相关标准

规范发布方	规范名称
Global Platform	**系统架构** TEE System Architecture **应用编程接口** TEE Client API Specification TEE Internal Core API Specification Trusted User Interface API TEE TUI Extension: Biometrics API TEE Secure Element API **安全评估** TEE Protection Profile TEE Biometric System PP-Module Secure Media Path PP-Module Cryptographic Algorithm Recommendations
全国信息安全标准化技术委员会（TC 260）	GB/T 41388-2022 信息安全技术 可信执行环境 基本安全规范 information security technology—Trusted execution environment basic security specification 信息安全技术 可信执行环境服务规范 Information security technology—Trusted execution environment service specification
全国金融标准化技术委员会（TC 180）	JR/T 0156—2017 移动终端支付可信环境技术规范 Mobile terminal payment trusted environment specification
北京金融科技产业联盟	T/BFIA 00001—2020 移动终端安全金融盾规范
中关村网络安全与信息化产业联盟	T/ZISIA-EMCG 001—2019 移动智能终端密码模块技术框架
密码行业标准化技术委员会	可信运行环境安全管理框架与接口规范

由此可知，和 TEE 相关的国内外相关标准和研究报告的成果：国外是以 GP 为代表的标准，主要集中在架构和功能接口，也涉及到了安全评估。国内主要集中在 TEE 环境的功能基本服务，也有基本安全规范，但是站在 TEE 自身功能或基于 TEE 开发的功能服务的角度，而不是以安全评估，分类分级划分安全边界的密码模块角度。

3. 基于可信执行环境的密码模块应用场景及需求分析

3.1 基于可信执行环境的密码模块应用场景

3.1.1 移动金融支付

随着 5G 网络和智能终端(如手机、智能电视等)的高速发展以及消费电子产品越来越智能化，移动应用的种类和数量越来越多。当前的移动应用已经不再局限于对智能终端基本功能及娱乐功能方面的扩展，它所涉及的领域逐渐扩大到各行各业之中，如金融支付行业、内容版权保护行业等。这些行业的应用需要更高的安全级别。

但就现在的智能终端安全而言，难以很好的满足上述要求，主要在于：

操作系统安全性不足，由于当前智能终端操作系统本身并非从安全性角度设计，再加上系统的庞大复杂性以及经常性的升级更新，导致目前的安全解决方案(如防火墙、杀病毒软件等)无法杜绝病毒、木马等恶意程序的侵入，使得移动终端的安全性始终无法得到根本性的全面保证。

操作系统恶意攻击次数增长迅速，随着应用数量的增加，恶意软件、病毒的攻击次数和种类就更是呈几何数增长，这些恶意软件的迅速增加对于移动支付的安全而言就是一大挑战。

因此，对于移动支付，防御恶意软件/病毒、保障智能终端的安全是重中之重，而就智能终端的安全而言，也不能再单纯依靠基于应用软件层面的解决方案来提供保护，而需要更进一步地提供基于终端硬件层面的安全解决方案来加强防护。

传统的高安全等级的移动金融安全解决方案主要依赖于安全芯片，然而常受限于芯片性能、交互及用户体验等问题。可信执行环境为设备安全提供了框架，在富操作系统（Rich OS，通用操作系统及运行在其中的应用程序具有不可信的特点）和安全芯片之间提供了一个安全层，借助可信执行环境，移动终端金融盾实现了在高安全性、易用性与用户体验之间的权衡。T/BFIA 001—2020 附录 B 中给出了移动终端金融盾在商业银行中的参考实现。

借助移动智能终端上的可信执行环境，移动终端金融盾不但能实现硬件保护用户证书私钥的高安全性，还能提供可信 UI 服务保护用户 PIN 码安全、交易信息真实与交易确认可信；在高安全性、易用性与用户体验等方面都达到了较高水平。

根据移动终端支付可信环境不同能力级别（分类分级参见 JR/T 0156—2017），可分为：TEE+SE 方式和 TEE 方式两种金融盾实现方式。商业银行在本行和跨行转账、单笔和批量转账、对私和对公转账、投资理财、生活服务、跨境汇款等业务场景中，可以金融盾 TEE 实现或 TEE+SE 实现方式作为账户风险分级管控的主要因素，辅以其他风险管控手段，提高商业银行账户管理风险管控能力，也从源头上遏制更多违法犯罪行为的发生，为银行资金和客户资金提供更有效的保障。

2017 年 10 月,中国建设银行联手华为率先推出首个基于 TEE+SE 实现方式的移动支付安全解决方案。截至 2021 年底，中国工商银行、中国农业银行、民生银行、南京银行、徽商银行、晋城银行、晋商银行、兰州银行、江苏银行、渤海银行等众多银行都已推出了 TEE 实现方式或 TEE+SE 实现方式的移动安全支付产品。

3.1.2 移动政务

党务信息化、政务信息化，在信息安全的重要性上升到国家层面的大背景下，相关

终端也需要硬件层面的安全解决方案来加强防护。

“互联网+政务服务”，采用基于可信执行环境的密码模块和数字证书服务提供的密钥保护、在线发证、签名验签、数据保护等密码服务，实现用户身份认证、业务预约申报签名、敏感信息加密、数据保护、操作留痕等功能，确保用户身份可信、敏感信息不泄露、业务申报不可抵赖。

更广泛的移动政务，有更好的用户体验，同时以基于可信执行环境的密码模块保证了数据的安全，便利和安全的平衡，是最大的优势。

3.1.3 移动警务

警务通是为公安民警进行移动警务时所需的信息管理系统。又称移动警务系统。为紧急和突发事件的处理提供了信息依据，可避免重特大案件的发生，为突发案件的迅速侦破创造信息条件。移动警务系统中移动警务终端作为系统的关键一环，采用国家密码管理局批准的国产自主安全芯片，能对终端数据进行硬件加密，支持如加密网络电话、加密信息、加密邮件、安全支付等各类敏感业务的应用。

传统的移动警务终端采用的是市场上独立模块的安全产品进行加密，存在耗电大、加密形式单一、管控力度差、用户体验不好等问题。2017 年开始，公安部在全国推动部署“新一代移动警务建设”、推广“新一代移动警务终端”。基于手机内置的可信执行环境和安全芯片来实现密码模块的功能，支持警务数字证书的安全发行、安全存储与安全使用。

据全国公安移动警务总体方案的规定，使用移动终端开展移动警务业务时，需要实现身份认证和通信加密等功能，其中涉及到多张证书的发放、存储、使用和对称加解密功能。在数据的加密存储和加密传输方面，对使用的密码算法也做了要求：数据机密性保护采用 SM1/SM4 算法，数据完整性保护采用 SM3 算法，抗抵赖保护采用 SM2 算法。

结合运用可信执行环境和安全芯片的优势，新型移动警务终端能够实现身份认证和签名验签等非对称密码运算及数据加密和通信加密等对称密码运算，安全等级高、密码处理能力强，可以满足增强受控型警务终端对密码模块的相关要求，兼具高安全性、高性能、便携易用和优秀的用户体验。

3.1.4 数字版权保护

基于 TEE 可信执行环境的 DRM 解决方案，可以满足全球主要内容提供商对于高品质内容的保护需要，TEE 可以为内容保护许可管理提供可信的执行环境。

可信执行环境技术因其较强的算法通用性和较小的性能损失，在许多涉及到隐私数据计算的场景中都得到了广泛应用，并且尤其适用于具备以下特征的应用场景：

——计算逻辑相对复杂，算法难以通过同态加密等技术进行改造，或者改造过后效率下降过多数据量大，数据传输和加解密的成本较高;

——性能要求较高，要求在较短时间内完成运算并返回结果;

——需要可信第三方参与的隐私计算场景，且数据（部分或间接）可被可信第三方获取或反推;

——数据的传输与使用环境与互联网直接接触，需要防范来自外部的攻击;

——数据协作的各方不完全互信，存在参与各方恶意攻击的可能。

其中最常见的具体应用场景包括：隐私身份信息的认证比对、大规模数据的跨机构联合建模分析、数据资产所有权保护、链上数据机密计算、智能合约的隐私保护等。

3.1.5 隐私身份信息的认证比对

身份信息的认证比对是许多数字化应用需要具备的基础功能之一，通过对使用者的指纹、脸部图像、声音等数据进行比对，验证使用者的真实身份以确保安全性。在一些场景中，监管部门还会要求应用对使用者的实名信息进行匹配，以便满足社会安全管理的相关需求。

在身份信息认证比对的过程中，用户的个人信息需要被设备采集上传，并存储在服务端的数据库当中。无论是网络传输、持久化存储还是验证过程中的数据调用，都有可能因外部攻击或应用本身的恶意行为而导致的用户隐私泄露，从而危害到用户的财产甚至人身安全。

为了降低身份信息认证比对过程中的隐私泄露风险，TEE 技术被应用于包括移动端、PC 端和各类终端设备中。由摄像头、指纹识别器等 IO 设备采集到的个人身份数据，经过加密后传输到基于 TEE 技术生成的隐私计算环境中，数据在 TEE 内进行解密、特征提取、相似性比对等一系列操作，并将最终结果和再次加密的数据，通过安全的传输通道上传至服务器端。

在整个过程中服务器仅能获得最终的比对结果和加密的原始数据，明文数据的计算完全在由用户掌握的终端设备的 TEE 中完成，既能够保障用户隐私信息的安全性，又可以防止终端设备上其它应用通过对校验过程进行干扰而发生作弊行为。

3.1.6 大规模数据的跨机构联合建模分析

在数字化社会的发展过程中，基于大数据技术和数据智能衍生出的各类产品和服务已经广泛地影响到商业和生活，包括但不限于基于大数据制定商业策略、预测市场趋势、评估用户购买意愿、控制金融和社会风险等。随着这些场景中各类算法的迭代发展，对于数据维度和数据量的要求也在日益增加，单个机构仅仅使用自身业务产生的数据已经不足以支撑这些场景的需求，因此联合多方数据进行联合分析建模已经成为一个重要趋势。

由于大数据分析难以避免会涉及到企业的用户数据和经营数据，在多方数据联合和协作的过程中，各方都希望输入的原始数据中的这些隐私信息能够得到充分保护，而最终输出的结果仅包括通过算法计算得到的不包含具体数据的分析结果或模型，即实现数据的“可用而不可见”。

在这类型的场景中，可以通过分布式部署在多个机构间的 TEE 节点网络，实现数据的隐私求交集和计算。各方通过部署在本地的 TEE 节点从数据库中获取数据，并通过一个基于 TEE 可信根生成的加密密钥对数据进行加密，该密钥通过多个 TEE 节点协商产生，仅在各节点的 TEE 安全区域内部可见。加密后的数据在 TEE 节点网络间传输，并最终在一个同样由 TEE 节点组成的计算资源池中，然后在 TEE 中进行数据的解密、求交集和运算。在运算完成后，TEE 节点仅对外部输出结算结果，而原始数据和计算过程数据均在 TEE 内部就地销毁。

通过 TEE 技术实现的多方数据联合建模，既能够满足多方数据协作的业务需求，也能够充分保护各方之间原始数据可用不可见。并且相比其它的分布式计算或纯密态计算的方案，基于 TEE 的方案具备更强大的性能和算法通用性，能够在涉及到大规模数据或对性能有一定要求的场景中达到更好地效果。

3.1.7 数据资产所有权保护

随着国家宏观数据政策对于数据生产要素市场化的要求越来越明确，数据作为一种资产在企业间共享、交易和流通已经是大势所趋。然而数据作为一种数字化资产，具备

可复制、易传播的特性，如何在数据资产共享和交易过程中保护数据资产的所有权，成为了推动数据生产要素市场化需要解决的首要问题之一。

通过 TEE 技术与区块链技术的有机结合，可以在企业间进行数据共享和交易时有效确保数据所有权和数据使用权的分离和保护。所有数据资产通过数据指纹在区块链中存证，通过区块链的交易记录来追溯和监管数据所有权的变更。当数据使用权和所有权发生分离时，所有数据的使用过程必须在 TEE 内部发生，通过对运行在 TEE 中的程序可信度量值的存证，数据的所有者可以确定数据使用者仅在双方约定的范围和方式内使用数据，当计算过程完成后，原始数据将在 TEE 内部销毁，保障数据所有权不会因使用者对原始数据的沉淀而丢失。

在 TEE 和区块链技术的结合下，数据交易过程的安全、可信和公平可以得到更好的保障，数据权属的划分可以更加明确，从而让数据生产要素成为一种真正可流通的资产，促进数字化社会对于数据生产要素潜能的充分激活。

3.1.8 链上数据机密存储和计算

面对日益增长的电子数据存证需求，传统的存证方式因成本高、效率低、采信困难等不足，而逐步被区块链电子存证取代，利用区块链的可追溯、不可篡改和安全透明的特性去保证数据“存储、提取、出示、比对”等环节都在链上公示，如何保证链上公示数据的安全性，成为推动区块链电子存证发展的需要首要解决的问题之一。

在这类场景中，可以通过 TEE 节点，实现链上数据的机密存储和计算。链上的各方通过一个加密密钥对数据进行加密存储，该密钥通过链上的 TEE 节点协商产生，仅在各节点的 TEE 安全区域内部可见。当需要对链上数据进行验证时，加密后的数据在 TEE 节点网络间传输，然后在 TEE 中进行数据的解密，并与链上存储的经过区块链全网共识的数据指纹进行对比，确认数据未被恶意篡改后，再进行后续的运算。在运算完成后，TEE 节点仅对外部输出运算结果，而原始数据和计算过程数据均在 TEE 内部就地销毁，从而实现链上数据的机密存储和计算。

在 TEE 技术的加成下，链上数据以及使用流程的隐私性也可以得到更好的保证，从而让区块链具备安全、可信和公平的存证的能力，让区块链存证也可以更好的落地并服务于各行各业的用户，做到真正的为民所用。

3.1.9 服务器密码应用

华为、飞腾等厂商近年来均推出了国产 Arm 服务器，均支持 Arm TrustZone 体系架构，因此基于服务器 TEE 环境构建密码模块，使得通用服务器无需额外安装硬件密码模块即可提供合规的密码服务，这一应用模式除了能够有效降低密码硬件成本，在外部管理系统支撑下，还能够实现“软件定义密码模块、软件定义密码系统”的能力，在云计算、大数据、机密计算等领域有着非常广阔的应用场景。

3.1.10 实践案例

基于可信执行环境 TEE 的数据隐私计算服务通过 TEE 技术实现的多方数据协作运算，既能够满足数据协作的业务需求，也能够充分保护各方之间原始数据可用不可见。并且相比其它的分布式计算或纯密态计算的方案，基于 TEE 的方案具备更强大的性能和算法通用性，目前已在运营商、政务、金融、互联网和医疗行业不断落地，以下根据网上公开信息收集整理。

中国电信围绕电信集团内部和政企客户之间的数据流通场景展开，基于中国电信自主研发的区块链底层技术，在隐私计算方向的技术融合解决数据流通的可信、隐私、安

全、公平、可追溯等问题，提供链上数据智能合约化定价与流通的新范式。

浦发银行通过可信计算+区块链的能力，构建一个多方联合数据隐私计算的平台，让各参与方在不暴露原数据的情况下，在隐私安全、公平可追溯的前提条件下进行一些数据的联合计算，有助于打破数据孤岛，发挥出数据的价值。

蚂蚁推出的可信计算服务产品可信计算服务，打通了链上数据与链下数据源，支持多方数据融合和治理，为用户提供了通用的、可验证的隐私数据计算服务，当前该服务已在某数据物理平台落地，通过网络货运平台运单上链，将物流运输关键信息进行交叉核验，以真实运输背景为出发点，连接金融机构，为物流平台提供普惠金融服务，同时拥抱监管，确保各项业务真实合规。

国外的 Fortanix 是一家专注可信计算的公司，为企业提供数据隐私保护服务，该服务支持多家企业数据在可信环境中汇聚并进行数据分析任务，并在 PayPal、Standard Chartered Bank 等多家金融机构合作的项目中，完成了落地，通过多家金融机构的数据协作，极大的提升了金融机构反洗钱风控的准确性。

3.2 安全需求分析

通过以上应用场景的分析可知，从应用的行业来讲有：金融、政务、警务、版权保护、隐私信息比对等，这些行业应用各有特色，所以需要基于可信执行环境的密码模块的安全需求也各不同。例如：移动金融支付，是高安全，运算量相对较少，而且要具备可信人机交互（TUI），因此这类密码模块就需要具备这些典型特点，其分类分级、密码模块边界划分就尤其重要：SE 做主要密码服务，TEE 做人机交互的划分会比较合适。移动政务和移动警务应用，高安全，密码运算量大（保密通话），因此这类密码模块需要高性能，在密码模块边界上：TEE 下的可信应用做主要的密码服务，SE 做少量密码服务会比较合适，等等。

从密码模块应用的环境来讲，有客户端的各种移动终端设备，有 PC 端设备（链上数据机密存储），也有服务器端密码模块（服务器密码应用），所以基于可信执行环境的密码模块的使用环境差异很大。

从密码服务功能角度来看，一类是传统的加解密、签名验签密码运算；另一类是隐私身份等敏感信息要在可信的环境内保护；第三类是隐私计算，基于可信执行环境的密码模块实现大数据联合建模分析等这些新应用。

由此可知，对基于可信执行环境的密码模块，从行业应用特点、密码模块使用环境、密码功能服务有数据保护和隐私计算等这些角度来看，密码模块的分类分级、密码模块边界划分，以及不同边界类型密码模块的安全要求和设计要点的研究就尤为重要，能够更清晰的指导基于可信执行环境的密码模块在面临：行业应用需求、不同 TEE 实现技术、数据保护和隐私计算等需求时，能更快、更好的设计出满足功能且符合安全要求的密码模块。

4. 可信执行环境的系统框架

4.1 GP TEE 的架构

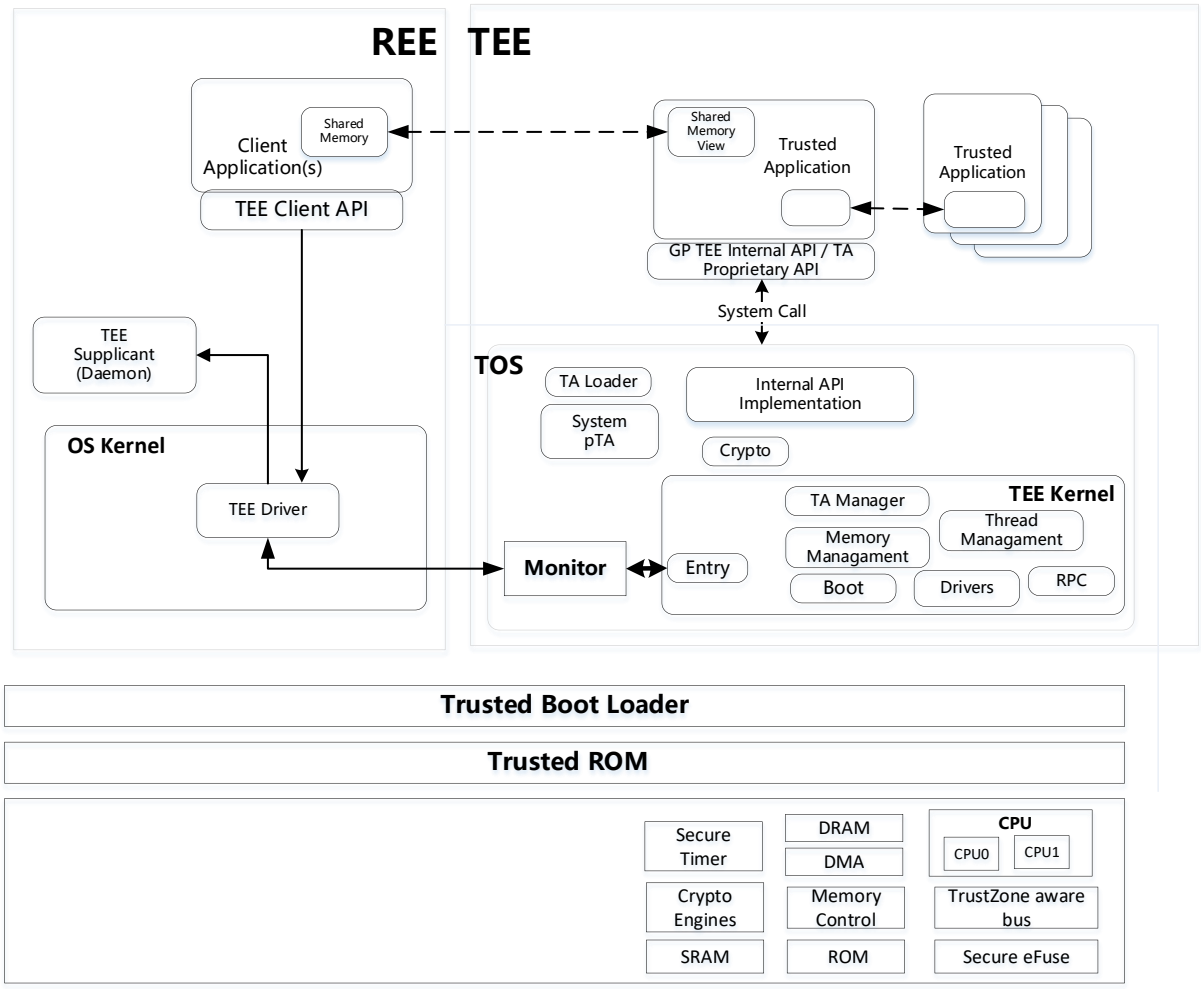

图 1 GP TEE 典型实现架构

如图 1 所示，TEE 正常功能需要 REE 提供 TEE 驱动和 TEE 服务 Daemon。可信应用（Trusted Application）一般保存在 REE 的文件系统，TOS（Trusted OS，可信操作系统）需要验证 TA 的签名后才能可动态加载到 TEE 执行，因此 TEE 是受限制的运行环境。尽管 REE 侧的 TEE 驱动和 TEE 服务 Daemon 不受 TEE 控制，这两个部件不影响 TEE 提供的安全功能，这里需要在划分密码模块边界时说明清楚。

可信应用的运行环境是TEE,TEE正常功能需要REE提供TEE驱动和TEE服务Daemon，这个问题，需要根据划分的密码模块边界来处理。

运行在 REE 侧的客户应用通过调用 TEE 客户应用 API（TEE Client API），可以请求指定的可信应用提供的安全服务。

可信应用运行在用户态，TEE 操作系统内核收到客户应用的请求后，创建可信应用进程（或线程）加载指定的可信应用的镜像，回调可信应用的回调接口；客户应用（Client Application）和可信应用通过客户应用侧分配的共享内存传输数据，需要根据密码模

块划分的边界，看是在密码模块规格，还是密码模块接口这个安全域来描述。

TA 运行在用户态，TOS 运行在内核态，提供密码运算和存储的 API 供可信应用调用，TOS 提供 TA 之间以及 TA 和 TOS 间的安全隔离；TEE 基于 SoC 硬件机制实现 TEE 和 REE 的隔离。基于 TA 实现的密码模块的敏感安全参数的保护严重依赖与 TOS 提供的安全机制。内核实现的密码模块的敏感安全参数的保护依赖与 SoC 提供的硬件安全机制以及 TOS 软件实现机制。

4.2 国内提出的可信执行环境系统框架

国内研究报告[7]中抽象定义了如图 2 的可信执行环境系统框架。

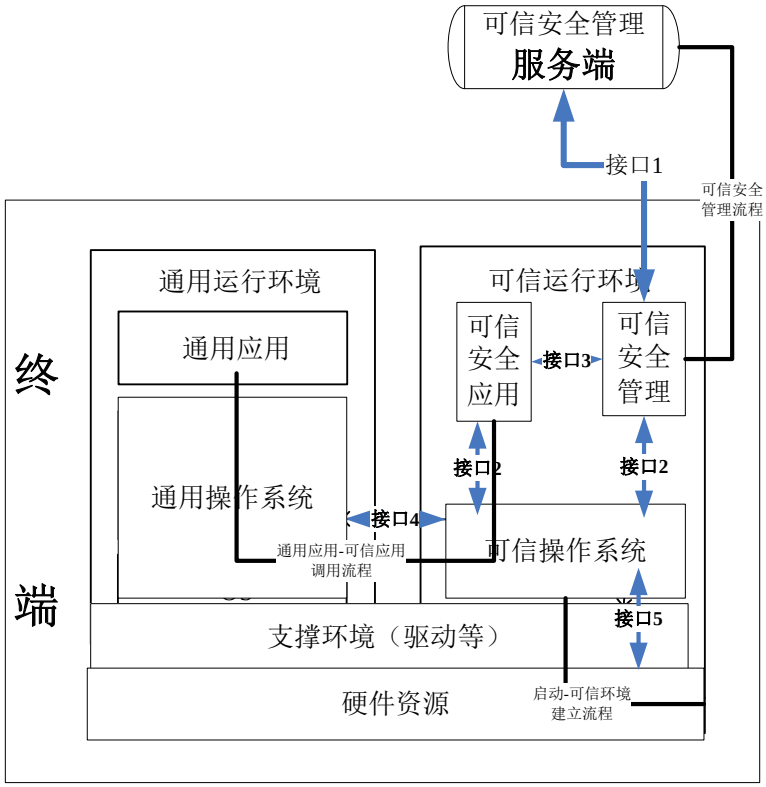

图 2 可信运行环境系统框架[7]

在这个框架中，终端侧至少包括一个可信运行环境，此环境是一个受控安全环境[7]（受控的、可信任的运行环境），可提供密码安全服务。终端侧的可信运行环境和通用运行环境共用硬件资源和支撑环境，因此这里的隔离机制则非常重要。

可信运行环境由可信操作系统、可信安全管理模块、可信安全应用构成，而这些也是本文档所述“基于可信执行环境的密码模块”的研究对象。根据划分密码边界的划分规则，将这些对象划分不同的边界，则可组成不同边界类型的密码模块。

可信操作系统：通过接口 5 统一管理底层系统资源，通过接口 2 为上层可信应用提供统一的接口，通过接口 4 为通用运行环境提供统一的交互接口。

4.3 TEE 的安全功能

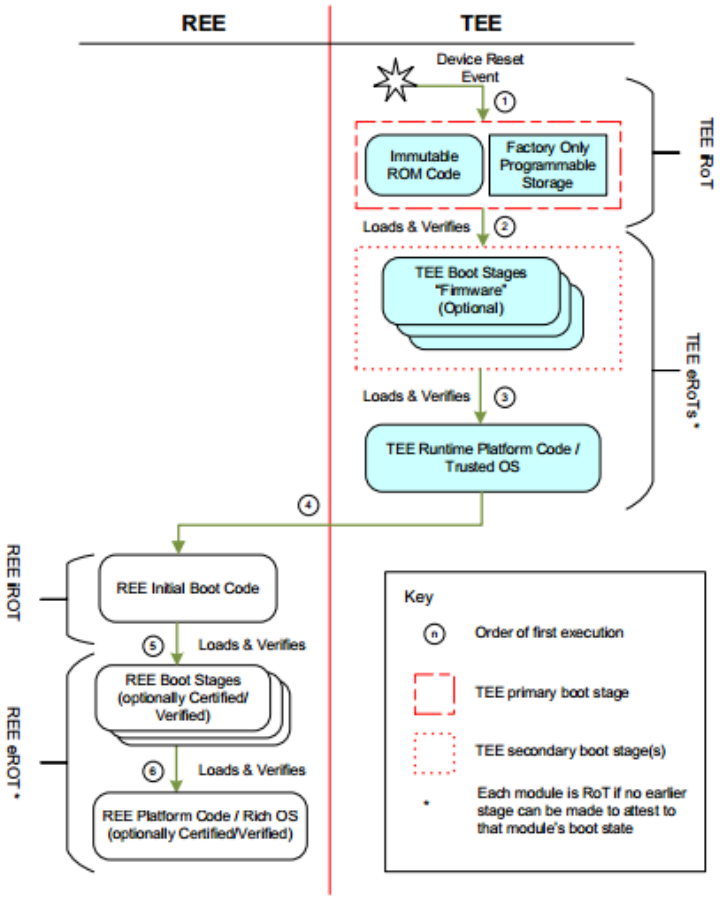

图 3 GP TEE 的启动序列框架[7]

GP TEE 可信技术的核心是安全分离隔离，强调启动序列上要保证可信环境要有限域通用环境启动，并不强调逐级度量机制，用户可以使用任何安全机制来保护 TEE 的启动安全性[7]。GP TEE 的启动序列框架如上图 3 所示。

4.3.1 启动安全

安全引导过程是可信执行环境安全的关键，安全启动过程必须验证可信执行环境镜像的完整性和真实性，安全启动依赖于信任链的原理，信任链以系统中不可更改软件组件 ROM 开始，包含了用于验证信任链中的下一个链所必需的信息，这些信息包括验证签名的公钥或者公钥的摘要，通过信任关系传递，可以确保所启动的系统是可信的。可信操作系统的签名和加密算法必须是核准的密码算法，终端厂商必须保证可信操作系统签名私钥的安全性，推荐使用 HSM 安全存储签名密钥对，支持可信操作系统镜像的 OTA 更新，需要具有防回滚机制。

4.3.2 通用操作系统与可信执行环境之间的隔离

需要通过防火墙机制实现可信执行环境和通用操作系统间的物理内存的隔离，只能通过安全监控器进行通用操作系统和可信执行环境间的切换。通用操作系统和可信执行环境间只能通过具有明确功能定义的通信协议进行通信。

可信执行环境和通用操作系统共享的内存区应满足如下访问要求：

a) 可信执行环境不能将任何敏感信息写入到可信执行环境和通用操作系统共享的内存区；
b) 对于客户应用传入的输入敏感数据，可信执行环境只能读取一次；
c) 对于客户应用传入的输入数据不能拥有执行权限。

中断处理应满足如下要求：

a) 中断区分安全中断和非安全中断；
b) 安全中断只能由可信操作系统进行处理，如果通用操作系统运行时触发安全中断，应通过安全监控器转发到可信操作系统进行处理；
c) 若可信操作系统运行时触发非安全中断，可信操作系统实现应通过监控器转发通用操作系统进行处理后再返回可信操作系统继续执行。

4.3.3 最小化可信计算基

a) 安全复用 REE 驱动设备代码；
b) 非安全敏感功能复用 REE 系统完成；
c) 非安全关键逻辑由用户态管理。

4.3.4 减少攻击面

a) 沿用现代操作系统安全隔离机制：地址空间隔离、ASLR、NX。

4.3.5 动静态保护

a) SecureBoot 完整信任链；
b) TA 签名验证与保护；
c) TA 中不同域与库间互相隔离；
d) 安全敏感数据明文仅在 SoC 内部。

4.3.6 On-chip TEE

a) 整个 OS 运行在 SoC 内部，外部内存中只保存密文数据；
b) 支持后向兼容，保持对现有 TA 的透明。

4.3.7 可信应用生命周期管理

可信应用程序通过可信操作系统组件提供的应用编程接口与系统的其余部分进行通信，可信执行环境的应用编程接口定义了可信执行环境的基本软件功能。当客户端应用程序创建与可信应用程序的会话时，它将连接到该可信应用程序的一个实例。可信应用程序实例具有与所有其他可信应用程序实例的物理内存地址空间分开的物理内存地址空间。会话用于逻辑连接可信应用程序中调用的多个命令，每个会话都有自己的状态，该状态通常包含会话上下文和执行该会话的任务的上下文。

由可信应用程序定义有效执行的命令及其参数的组合。可信应用仅在响应外部命令时才能开始执行，它们自行决定何时从该命令返回；典型的可信应用遵循较短的命令响应生命周期，但是复杂的可信应用可能会在处理输入和输出事件（例如可信用户接口）时进行长时间的重复。

可信应用安装和更新方式：

a) 可信应用可以选择集成到可信执行环境镜像内部；
b) 可信应用可以预安装也可以终端发行后 OTA 可信应用方式安装；

c）独立可信应用可以支持安全的 OTA 更新。

可信应用镜像的安全要求：

a）可信应用镜像必须经过签名，确保可信应用镜像的完整性和真实性；

b）可信应用镜像可选加密，保证可信应用镜像的保密性；

c）可信应用的生命周期管理，TA 安装元数据的安全存储；

d）可信应用的签名和加密算法必须符合密码算法要求的章节的规定；

e）终端或者可信执行环境厂商必须保证可信应用签名的私钥的安全性。

TOS 提供 TA 之间以及 TA 和 TOS 间的安全隔离；TEE 基于 SoC 硬件机制实现 TEE 和 REE 的隔离。基于 TA 实现的密码模块的敏感安全参数的保护严重依赖与 TOS 提供的安全机制。内核实现的密码模块的敏感安全参数的保护依赖与 SoC 提供的硬件安全机制以及 TOS 软件实现机制。

TEE OS 只可以加载可信应用，可信应用的代码可以通过鉴别且满足所有的适用要求，因此，本文档认为可信执行环境为受限的可信执行环境。

4.4 TEE 密码模块的参与方

由上述图 2 可知，可信执行环境包括：可信安全应用（TA）、可信安全管理、可信操作系统，以及可信操作系统中的：TUI、密码服务接口等。不同的参与方会用不同的组合方式来划分密码模块边界。

开放操作系统终端（共享）的参与方

——TEE 环境下密码模块的提供方；

——OEM 厂商提供密码模块的实现，可提供库、系统可信应用、内核集成的密码模块组件等方式；

——第三方提供密码模块，只是以可信应用方式提供，能实现的安全功能依赖 TEE 的诸多限制。

封闭操作系统终端的参与方

——TEE 环境下密码模块的提供方，将整个 TEE 作为密码模块；

——OEM 厂商提供密码模块的实现，可提供库、可信应用、内核集成的密码模块组件等方式。

5. TEE 的安全评估及密码模块安全评估

5.1 TEE 安全评估

GP 组织可以提供 TEE 的安全评估，采用基于 GP 提供的 PP（Protection Profile，保护轮廓）文档按照 CC（Common Criteria，通用准则）方式进行评估，包含了密码模块功能相关的评估测试，对密钥生命周期安全、访问控制等均有具体要求。国内的工信部下的泰尔实验室、独立评估机构 DPLS 等都是 GP 的授权评估实验室，可以开展 TEE 的安全评估。

TEE 的评估需要芯片生产商、设备生产商以及 TEE 提供商三方同时提供相应的安全相关的技术文档，才能进行评估，而且每次评估的结果只对特定的终端有效，考虑评估的费用、周期等因素，导致实际评估产品非常少。

目前为止通过 GP TEE 安全评估的国内公司的产品如表 2 所示。

表 2 GP TEE 安全评估通过的产品

公司名称	产品	通过时间
Watchdata	WatchTrust 2.1.1	2018/01
Alibaba	Alibaba Cloud Link TEE v1.1.3	2019/01
Huawei	Huawei iTrustTEE v3.0	2020/02

5.2 密码模块评估

密码行业标准中，已发布两项与密码模块相关的标准，即 GM/T 0028—2014《密码模块安全技术要求》和 GM/T 0039—2015《密码模块安全检测要求》，分别针对密码模块安全技术和安全检测提出了具体要求。

GM/T 0028—2014《密码模块安全技术要求》

该标准适用于密码模块的设计、生产、使用和检测，密码模块厂商可参照本产品执行设计，以确保产品满足该标准指定等级的安全要求；商用密码检测机构依据该标准执行检测，以确认送检产品是否达到了声称的安全等级。此外，该标准也适用于密码和信息相关的方案咨询、标准编制活动，当其中涉及对密码模块的安全要求时，可引用该标准的相应等级。

GM/T 0039—2015《密码模块安全检测要求》

该标准旨在描述可供检测机构检测密码模块是否符合 GM/T 0028—2014《密码模块安全技术要求》的一系列方法。这些方法是为了保证在检测过程中高度的客观性，并确保各检测机构测试结果的一致性。该标准还给出了送检单位提供给检测机构材料的要求。在将密码模块提交给检测机构之前，送检单位可将该标准作为指导来判断该密码模块是否符合 GM/T 0028—2014《密码模块安全技术要求》所提出的要求。

5.3 TEE 安全评估和密码模块安全评估的关系

国际组织 GP 提出了 TEE（Trusted Execution Environment，可信执行环境）的概念，指在移动终端主处理器上的一个安全区域，提供一个隔离的可信执行环境，保证加载到该环境内部的各种敏感数据的安全性、机密性和完整性。TEE 是与 REE（Rich Execution Environment，富执行环境）相对应的一个逻辑概念，也是一个与普通操作系统（TEE 规范中称为 Rich OS）平行的运行环境，可以基于不同的技术实现，提供安全加解密、安全存储、可信用户接口、可信身份认证等各种系统服务。GP TEE PP 在 CC3.1 框架下给出了 TEE 的安全功能组件集合。根据 GP TEE PP 的描述，TEE 可以对多种移动应用场景进行安全保护，包括企业办公、内容管理、个人信息保护、连接保护、移动金融服务等等。

密码行业标准 GM/T 0082—2020《可信密码模块保护轮廓》以基本等效于 CC3.1 的 GB/T 18336—2015《信息技术安全性评估准则》（ISO/IEC 15408:2008,IDT）为基础，构建可信密码模块的保护轮廓，对符合评估保障级第 3 级的 TOE 的定义、安全环境、安全目的、安全要求等进行了详细说明，并给出相应的基本原理说明。

将 TEE PP 和 GM/T 0082—2020 的安全功能要求分别与密码模块安全要求相对照，

如表 3 所示。

表 3　密码模块安全要求对照

GP TEE PP	GM/T 0082—2020	简介（GB/T 18336—2015）	密码模块安全域
FAU_ARP.1		安全审计自动响应：安全告警	运行环境
FAU_SAR.1		安全审计查阅：审计查阅	运行环境
FAU_STG.1		安全审计时间存储：受保护的审计迹存储	运行环境
—	FCO_NRO.2	通信：强制性原发证明	密码模块接口
—	FCS_CKM.1	密码运算：密钥生成	密码模块规格
—	FCS_CKM.4	密码运算：密钥销毁	密码模块规格
FCS_COP.1	FCS_COP.1	密码运算	密码模块规格
FCS_RNG.1*	FCS_RNG.1*	密码运算：随机数生成	密码模块规格
FDP_ACC.1	FDP_ACC.1	用户数据保护：子集访问控制	敏感安全参数管理
FDP_ACF.1	FDP_ACF.1	用户数据保护：基于安全属性的访问控制	敏感安全参数管理
—	FDP_ETC.2	用户数据保护：有安全属性的用户数据输出	敏感安全参数管理
FDP_IFC.2		用户数据保护：子集信息流控制	敏感安全参数管理
FDP_IFF.1		用户数据保护：简单安全属性	敏感安全参数管理
—	FDP_ITC.2	用户数据保护：有安全属性的用户数据输入	敏感安全参数管理
FDP_ITT.1		用户数据保护：基本内部传送保护	敏感安全参数管理
FDP_RIP.1		用户数据保护：子集残余信息保护	敏感安全参数管理
—	FDP_RIP.2	用户数据保护：完全残余信息保护	敏感安全参数管理
FDP_ROL.1		用户数据保护：基本回退	敏感安全参数管理
FDP_SDI.2		用户数据保护：存储数据完整性监视和行动	敏感安全参数管理
FIA_ATD.1	FIA_ATD.1	标识和鉴别：用户属性定义	角色、服务与鉴别
—	FIA_UAU.1	标识和鉴别：鉴别的时机	角色、服务与鉴别
—	FIA_UAU.4	标识和鉴别：一次性鉴别机制	角色、服务与鉴别
—	FIA_UAU.6	标识和鉴别：重鉴别（重新鉴别）	角色、服务与鉴别
—	FIA_UID.1	标识和鉴别：标识的时机	角色、服务与鉴别
FIA_UID.2		标识和鉴别：任何动作前的用户标识	角色、服务与鉴别
FIA_USB.1		标识和鉴别：用户-主体绑定	角色、服务与鉴别
—	FMT_MOF.1	安全管理：安全功能行为的管理	敏感安全参数管理
FMT_MSA.1	FMT_MSA.1	安全管理：安全属性的管理	敏感安全参数管理
—	FMT_MSA.2	安全管理：安全的安全属性	敏感安全参数管理
—	FMT_MSA.3	安全管理：静态属性初始化	敏感安全参数管理

表 3　密码模块安全要求对照（续）

—	FMT_MTD.1	安全管理：TSF 数据的管理	敏感安全参数管理
FMT_SMR.1		安全管理：安全角色	敏感安全参数管理
—	FMT_SMR.2	安全管理：安全角色限制	敏感安全参数管理
—	FMT_AMT.1	TSF 保护：抽象机测试	自测试
FPT_FLS.1	FPT_FLS.1	TSF 保护：失效即保持安全状态	有限状态模型
FPT_INI.1*		TSF 保护：TSF 初始化	有限状态模型
FPT_ITT.1		TSF 保护：内部 TSF 数据传送的基本保护	敏感安全参数管理
—	FPT_PHP.1	TSF 保护：物理攻击的被动检测	物理安全
—	FPT_RCV.4	TSF 保护：功能恢复	敏感安全参数管理
—	FPT_RPL.1	TSF 保护：重放检测	敏感安全参数管理
—	FPT_RVM.1*	TSF 保护：TSP 的不可旁路性	敏感安全参数管理
—	FPT_SEP.1*	TSF 保护：TSF 域分离	敏感安全参数管理
FPT_STM.1		TSF 保护：可靠的时间戳	敏感安全参数管理
—	FPT_TDC.1	TSF 保护：TSF 间基本的 TSF 数据一致性	敏感安全参数管理
FPT_TEE.1		TSF 保护：外部实体的测试	自测试
—	FPT_TRP.1*	TSF 保护：可信路径	密码模块接口
—	FPT_TST.1	TSF 保护：TSF 测试	自测试

截止到 2023 年 6 月，基于可信执行环境的密码模块相关的安全评估及测评情况如下：TEE 的安全评估大多是在 GP 组织，采用基于 GP 提供的 PP（Protection Profile，保护轮廓）文档按照 CC 方式进行评估，目前安全评估通过的 GP TEE 产品见表 2。国内的泰尔终端实验室、北京智慧云测设备技术有限公司可以做 GP TEE 的安全评估。

北京国家金融科技认证中心（NFTC）开展的涉及可信执行环境的认证业务包括：

——金融科技产品认证-移动终端可信执行环境（TEE）

依据 JR/T 0156—2017《移动终端支付可信环境技术规范》，对移动终端可信执行环境（TEE）的功能性、安全性、场所的安全保证能力、质量保证能力及产品一致性等方面进行审查，客观、公正地评价是否符合金融行业对移动终端可信执行环境（TEE）的技术标准符合性和安全性要求。已获证机构包括：沈阳谦川科技有限公司、阿里云计算有限公司。

——金融科技产品认证-可信应用程序（TA）

依据 JR/T 0156—2017《移动终端支付可信环境技术规范》，对可信应用程序（TA）的 TA 安全、场所的安全保证能力、质量保证能力及产品一致性等方面进行审查，客观、公正地评价是否符合金融行业对可信应用程序（TA）的技术标准符合性和安全性要求。已获证机构包括：国民认证科技（北京）有限公司。

——移动终端安全金融盾认证

依据 T/BMFIA 00001—2020《移动终端安全金融盾规范》、Q/CFNR 160001—2017《移动终端安全金融盾检测规范》，对商业银行、支付机构、终端厂商、电子认证服务商等在移动终端上开展基于电子签名认证的金融盾服务应用进行认证。通过推动移动终端安全金融盾规范落地增强支付产品的安全性，提高产品质量，为供需双方建立信任、降低成本，促进产业发展。已获证机构包括：北京握奇智能科技有限公司、中国银联股份有限公司、恒宝股份有限公司。

商用密码检测中心可以依据GM/T 0028—2014《密码模块安全技术要求》和GM/T 0039—2015《密码模块安全检测要求》对基于可信执行环境的密码模块进行检测，但由于这类密码模块组成的复杂性，其重要组成部分之一的TEE检测未建立国内的检测体系，以及TEE检测认证和密码模块检测之间的协调等问题，导致目前还没有对此类密码模块进行检测认证。

6. 基于可信执行环境的密码模块分类

6.1 密码模块边界划分

密码模块的密码边界应由定义明确的边线(如硬件、软件或固件部件的集合)组成，该边线建立了密码模块所有部件的边界。密码边界应当至少包含密码模块内所有安全相关的算法、安全功能、进程和部件。非安全相关的算法、安全功能、进程和部件也可以包含在密码边界内，但其实现应不干扰或破坏密码模块的安全运行。

依据密码边界内包含的所有部件的情况，GM/T 0028中定义了五种不同的密码模块类型，具体包括：硬件密码模块、软件密码模块、固件密码模块、混合软件密码模块和混合固件密码模块。

根据不同的模块类型，为达到目标安全等级，需要设计和实现相应的物理/逻辑边界隔离机制，以及确定在物理/逻辑边界上对外服务的物理端口或逻辑接口。

6.2 基于可信执行环境的密码模块特征

TEE一般包括可信操作系统以及运行在操作系统内的可信应用，可信操作系统提供应用编程接口供可信应用访问操作系统提供的各种服务，可信操作系统接收REE请求实现可信应用的加载、运行以及卸载等管理任务，可信操作系统一般不直接提供传统密码模块的安全功能给密码模块用户使用，因此不宜将整个TEE的操作系统当作密码模块。

可信应用可以提供接口供客户应用访问，也为密码模块的安全功能提供了多种灵活的实现方式，是实现密码模块的可行方式；对于资源较受限的物联网设备通常采用安全库方式实现TEE功能，此类设备通过库方式实现密码模块的安全功能比较方便。因此基于TEE的密码模块分类依据及规则，需要按照密码模块的定义以及TEE软硬件环境考虑以下各种因素进行分类。

基于可信执行环境的密码模块典型特征：

——可信操作系统、富操作系统，两者之间通过物理隔离以及系统级的逻辑隔离；

——对HSM/安全元件的使用一般只有可信操作系统可以访问，富操作系统不能直接访问；

——可信应用实现加解密、签名验签等密码功能；

——可信应用的密码功能和 HSM/安全元件的密码功能需要根据业务需求和安全需求进行合理划分；

——可信应用会调用可信操作系统的一些密码功能、安全存储功能来实现密码功能。

可信操作系统目前业界只有CC这样的评估，而没有密码模块检测相关的标准、规范、检测平台。

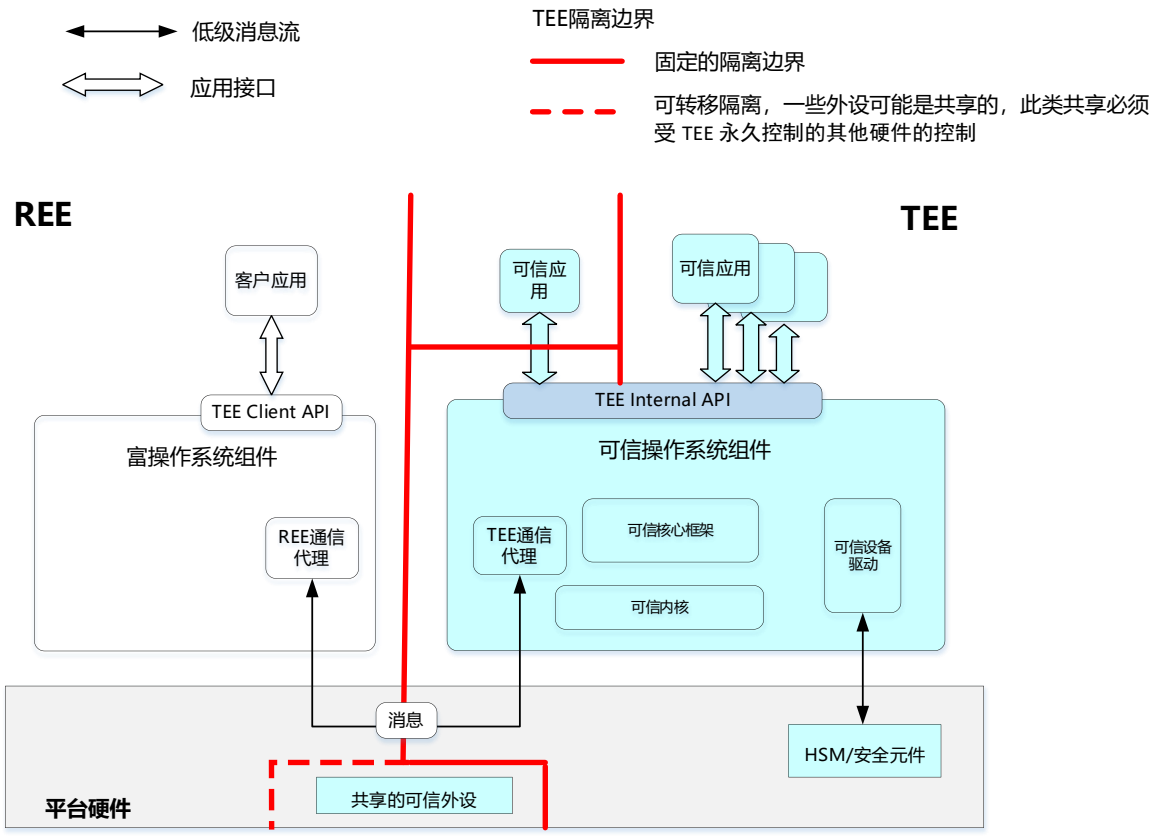

图 4　可信执行环境软件架构图

TEE 的典型实现方式有：
——库方式，提供应用编程接口供客户应用使用；
——操作系统方式，操作系统通常采用微内核和应用组件方式；

可信应用的类型：
——可信应用，运行在用户态，通过调用 TOS 提供的应用编程接口，访问操作系统提供的服务；
——伪可信应用，伪可信应用（Pseudo Trusted Applications，非 TA 形态、在 TOS 内部实现的并向外部提供接口的功能模块）和操作系统组件运行在内核态，不能直接调用 TOS 提供的应用编程接口，提供可信应用接口供客户应用以及可信应用访问。

可信应用链接库的方式：
——静态库，静态链接到可信应用镜像；
——动态（共享）库，运行时动态加载的动态链接库。

可信应用的部署实现方式：
——独立镜像，可以预安装或 OTA 方式安装；
——TA 镜像可以和操作系统镜像打包在一起部署，是操作系统镜像的一部分，TA 运行方式同独立镜像方式；
——伪可信应用集成到操作系统，是操作系统镜像的一部分。

密码模块的实现是否依赖硬件部件，TEE 实现的密码模块涉及的硬件部件有：

——HSM；
——SE，安全元件，支持 Applet 的动态下载；
——密码加速引擎，提供随机数发生器、大数运算等功能；
——RPMB，可为 TOS 提供较高安全等级的存储方式；
——屏幕、触屏、物理按键等，在具有 TUI 功能的密码模块中提供安全人机接口的硬件部件。

RPMB（Replay Protected Memory Block 重放保护内存块）是 eMMC 中的一个具有安全特性的分区，eMMC 在写入数据到 RPMB 时，会校验数据的合法性；RPMB 是 TEE 增强敏感安全参数安全存储常用机制,RPMB 密钥可由 TEE 初始化,但 TEE 一般不直接访问 RPMB，而是通过 REE 侧的 TEE 驱动、TEE 安全存储代理方式实现，如果 TOS 的安全存储使用了 RPMB,是否需要将 REE 侧的 TEE 驱动、TEE 安全存储代理划入密码模块的边界需要考虑，本报告作者考虑到 RPMB 密码由 TEE 控制，REE 侧这些组件只是传输通道，不影响存储数据的安全性，本报告为简化密码模块的实现，没有包括这些 REE 侧组件，密码模块的产品实现方可以确定是否加入。

TUI（Trusted User Interface）实现需要和 REE 共享显示和触摸屏，如果密码模块使用 TUI 功能需要将显示和触摸屏硬件部件加入密码模块边界内，密码模块类型为混合固件模块。

如果密码模块使用了应用处理器的密码加速引擎，需要将应用处理器硬件部件加入密码模块边界内，密码模块类型为混合固件模块。

6.3 基于可信执行环境的密码模块分类依据

划定密码模块边界时，应该考虑以下约束：
——需要提供明确的密码接口供客户应用或者可信应用使用；
——密码模块安全功能在独立进程内实现，以可信应用或者伪可信应用方式实现；
——密码模块要有独立的镜像，加载时可保证完整性。

在不同应用领域中、具有不同程度安全需求的基于 TEE 的密码模块，应根据具体的功能需求和安全需求，有针对性的划定密码边界，确定模块类型和目标安全等级。

要求运行环境在运行时，具备把密码模块的功能与该运行环境中的其他功能相互隔离的能力，使得那些被隔离的其他功能无法从密码模块获取与关键安全参数相关的信息，而且除了密码模块自身提供的接口方法以外，无法通过其他途径修改密码模块的关键安全参数，公开安全参数或执行流。

依据 GM/T 0028—2014 中 7.2.2 密码模块类型的定义，软件模块与固件模块的主要区别是：密码模块的运行环境所包含的计算平台和操作系统是否与模块明确绑定。据此，基于可信执行环境的密码模块中的软件/固件部件，当与其所处的计算平台和操作系统有明确绑定关系时，可看作固件；否则应看作软件。

考虑下列几种密码模块类型的典型实现：
——软件密码模块。密码模块由可信应用和/或可信执行环境组成，且不与所处的计算平台和操作系统绑定时，可作为软件密码模块。软件密码模块的密码边界内还可包含客户端应用。
——固件密码模块。密码模块由可信应用和/或可信执行环境组成，且与所处的计算平台和操作系统明确绑定时，可作为固件密码模块。
——混合软件密码模块。组成密码模块的软件部件为可信应用和/或可信执行环境（不与所处的计算平台和操作系统绑定），硬件部件为安全元件或其它安全硬

件。

——混合固件密码模块。组成密码模块的固件部件为可信应用和/或可信执行环境（与所处的计算平台和操作系统明确绑定），硬件部件为安全元件或其它安全硬件。

可信执行环境通常包含一些在 TEE OS 中与安全无关的功能和部件。将可信执行环境整体划入密码边界内部时，应列举其中所有排除在外的部件，并说明排除在外的原因，确保这些排除在外的功能和部件不干扰或破坏模块的安全运行。

为了优化可信执行环境的设计、实现和检测，可在 TEE OS 内部逻辑上划出若干与安全功能密切相关的部分组成一个部件，作为可信执行环境“安全核”。用“安全核”代替可信执行环境作为组成密码模块的软件/固件部件，即密码边界内不包含可信执行环境整体，只包含“安全核”。在“安全核”与可信执行环境中的其它部分之间，应建立有效的逻辑隔离边线。

后续章节列出了一些可能的密码模块实现方式，以及在不同实现方式下的目标安全等级。

6.4 基于可信执行环境的密码模块分类

本章根据基于可信执行环境的密码模块特征，分类依据，对常用的典型密码模块边界进行了划分。下面在描述不同方式的密码模块边界时，蓝色底色表示可信执行环境密码模块的相关组件，灰色底色表示富操作系统和可信操作系统共同的硬件平台，红色虚线框表示密码模块边界。

6.4.1 方式一——库形态的可信执行环境

嵌入式设备常见的 TEE 实现方式，适用于资源受限的处理器下实现可信执行环境。

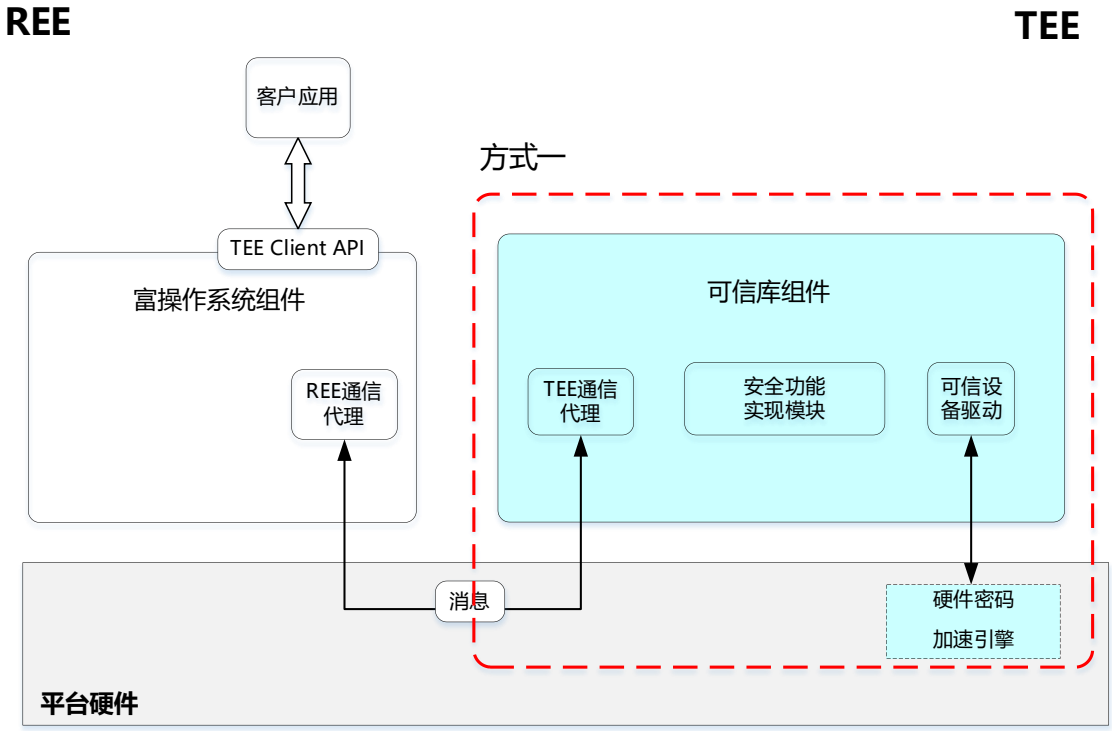

图 5 方式一的密码密模块边界

密码模块规格概述

——密码模块实现方式，以库方式实现的可信执行环境是基于可信执行环境的密码模块；

——密码模块类型，常见为固件密码模块或者混合固件密码模块；

——密码模块边界，包含 TEE 可信库镜像；

——目标安全等级，达到安全二级或安全三级。

6.4.2 方式二——可信应用

可信执行环境以操作系统方式实现，支持多个互相隔离的可信应用，可以预集成或者后安装到可信执行环境。常见 ARM 架构 Cortex-A 系列的处理器实现可信执行环境的典型方式。

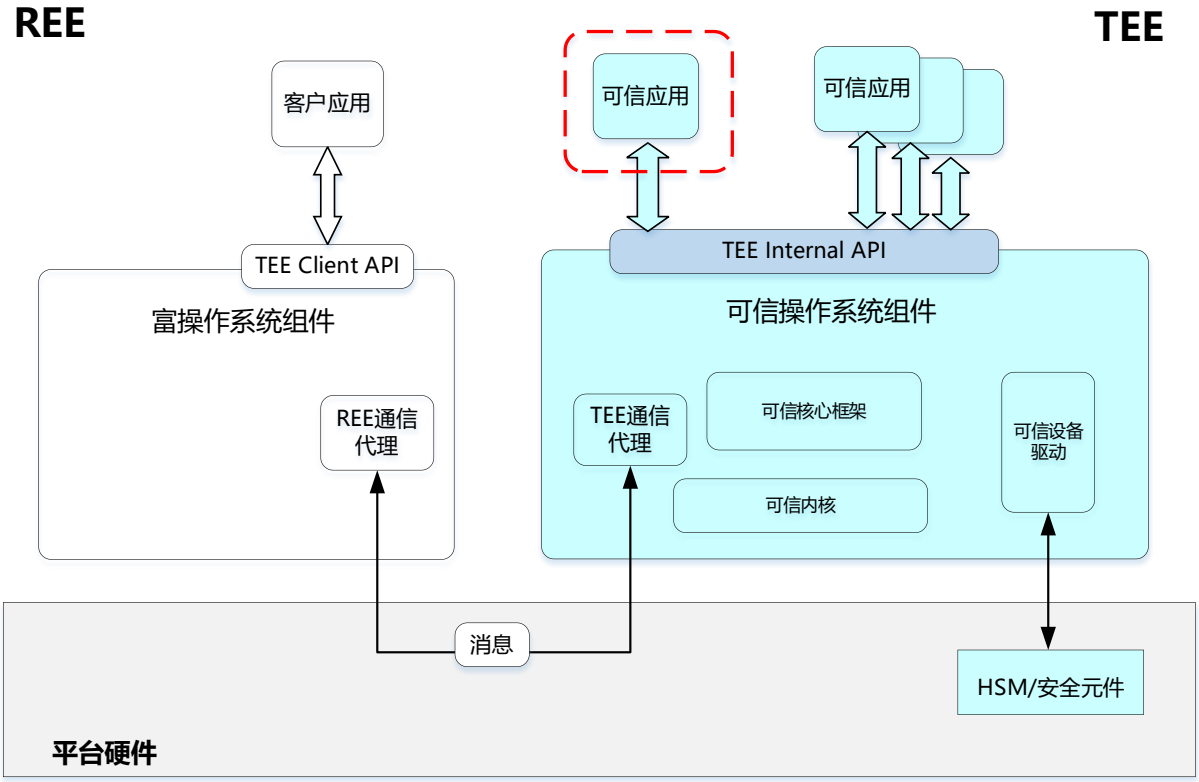

图 6 方式二的密码模块边界

密码模块规格概述

——密码模块实现方式，可信应用是基于可信执行环境的密码模块，核准的安全功能与对敏感安全参数的保护由可信应用独立实现，可信应用可以调用操作系统提供的 API 实现可信应用保护后的敏感安全参数的持久化存储功能；

——密码模块类型，常见为固件密码模块，也可以为软件模块或混合软件模块；

——密码模块边界，包含可信应用的镜像和运行实例；

——目标安全等级，达到安全一级或安全二级。

6.4.3 方式三——供可信应用调用的库

将密码模块实现为供可信应用使用的动态链接库，称为可信应用库。

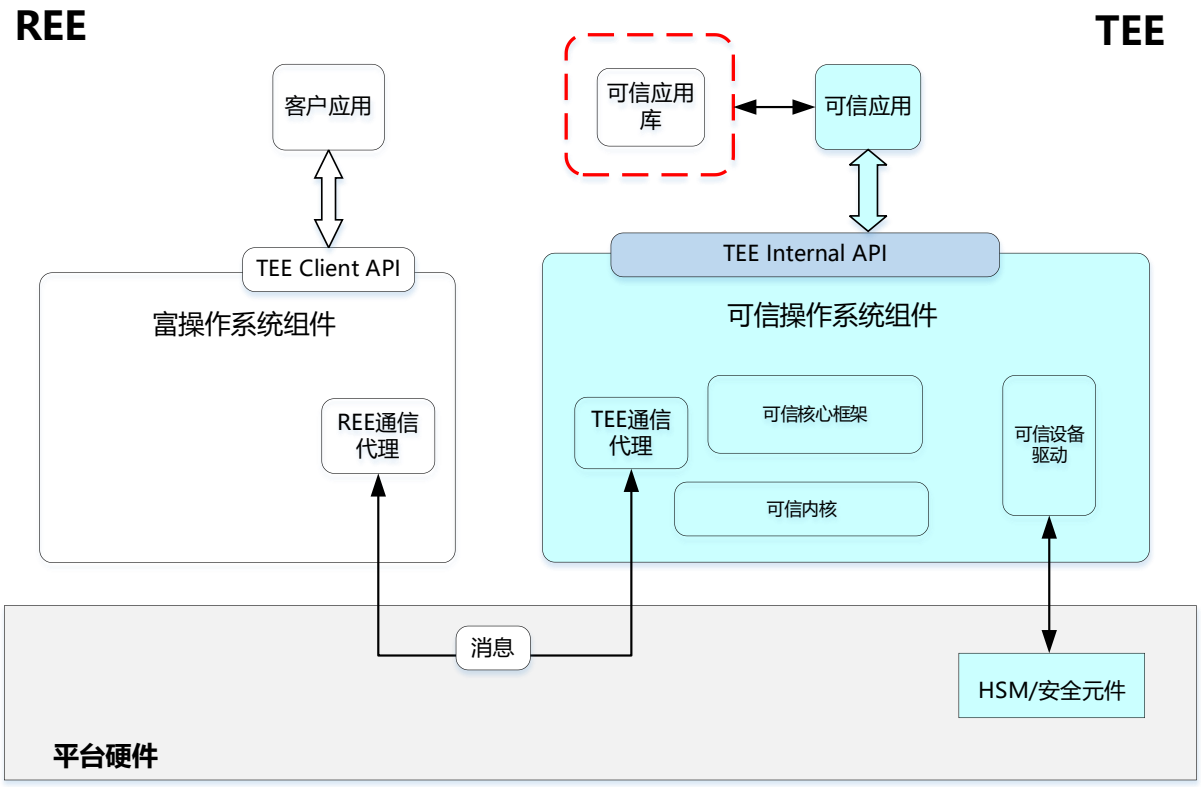

图 7　方式三的密码模块边界

密码模块规格概述

——密码模块实现方式，供可信应用使用的动态链接库是基于可信执行环境的密码模块，核准的安全功能与对敏感安全参数的保护由可信应用库实现，此类模块不提供敏感安全参数的持久化存储功能；

——密码模块类型，常见为固件密码模块；

——密码模块边界，包含可信应用库的镜像和运行实例；

——目标安全等级，达到安全一级或安全二级。

6.4.4　方式四——可信应用与可信执行环境

由可信操作系统和运行在其中的可信应用共同组成的密码模块。

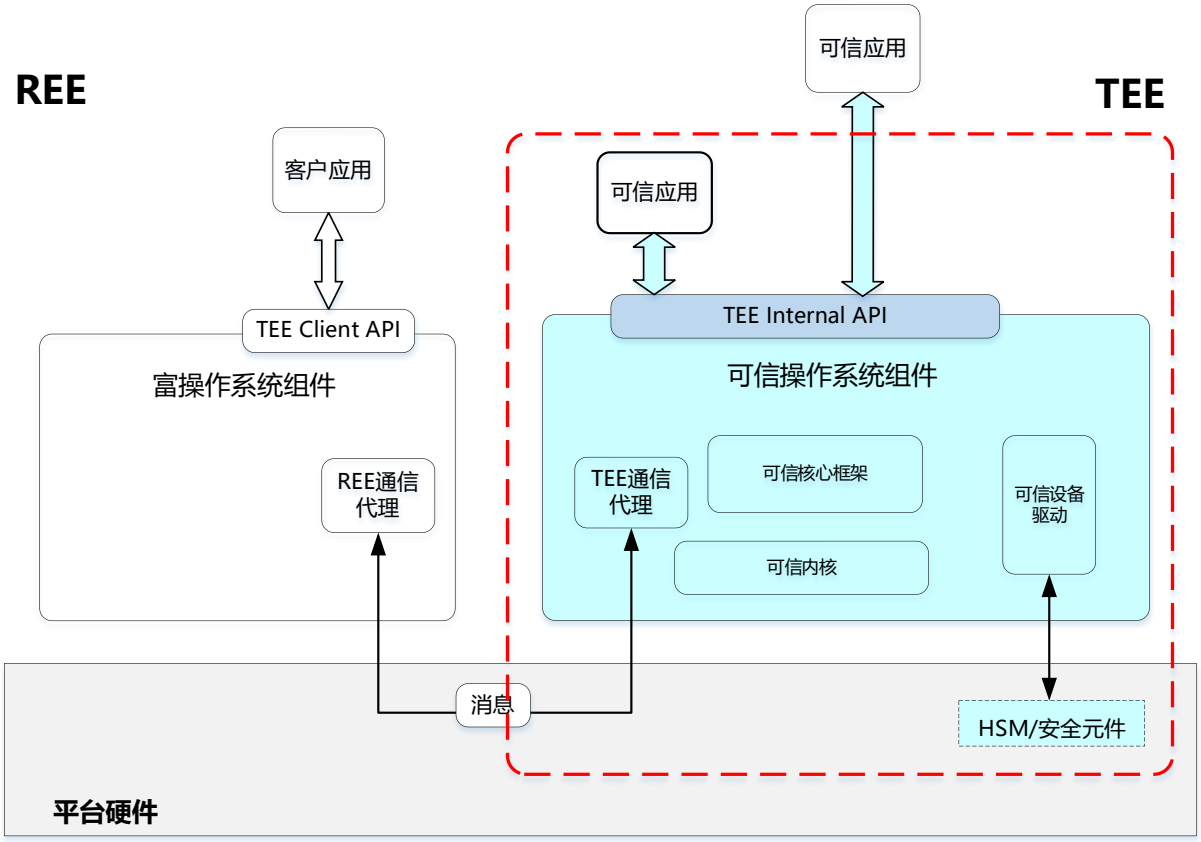

图 8　方式四的密码模块边界

密码模块规格概述

——密码模块实现方式，可信应用和可信操作系统是基于可信执行环境的密码模块，核准的安全功能与对敏感安全参数的保护由可信应用调用操作系统提供的 API 实现；

——密码模块类型，常见为固件或者混合固件密码模块；

——密码模块边界，包括将可信应用和 TEE OS 一同打包的镜像；

——目标安全等级，达到安全二级。

6.4.5　方式五——包含伪可信应用的可信执行环境

由包含伪可信应用的可信操作系统实现的密码模块。

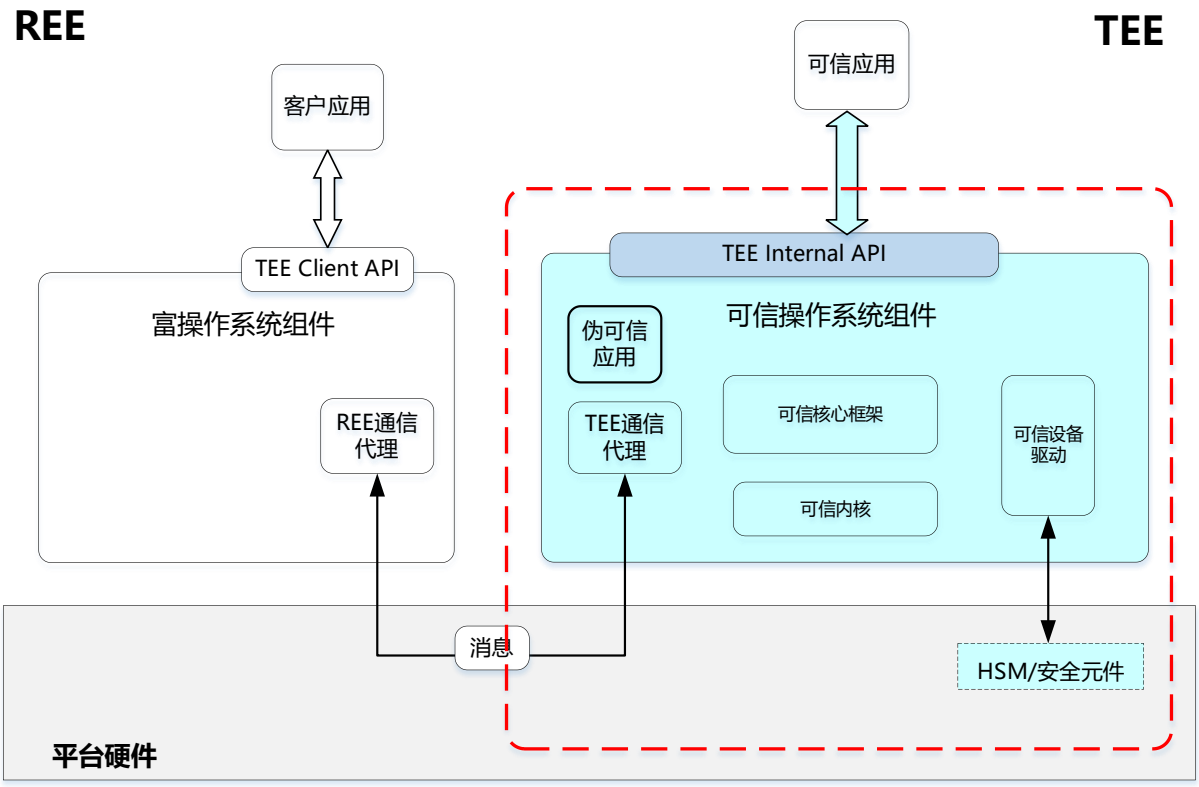

图 9　方式五的密码模块边界

密码模块规格概述

——密码模块实现方式，可信操作系统集成一个实现密码模块安全功能的伪可信应用，核准的安全功能与对敏感安全参数的保护由伪可信应用调用操作系统提供的 API 实现，可信操作系统是基于可信执行环境的密码模块；

——密码模块类型，常见为固件密码或者混合固件模块；

——密码模块边界，包含 TEEOS 的镜像和实例；

——目标安全等级，达到安全二级或安全三级。

6.4.6　方式六——伪可信应用

可信执行环境以微内核操作系统方式实现，密码模块是运行在其中的伪可信应用。

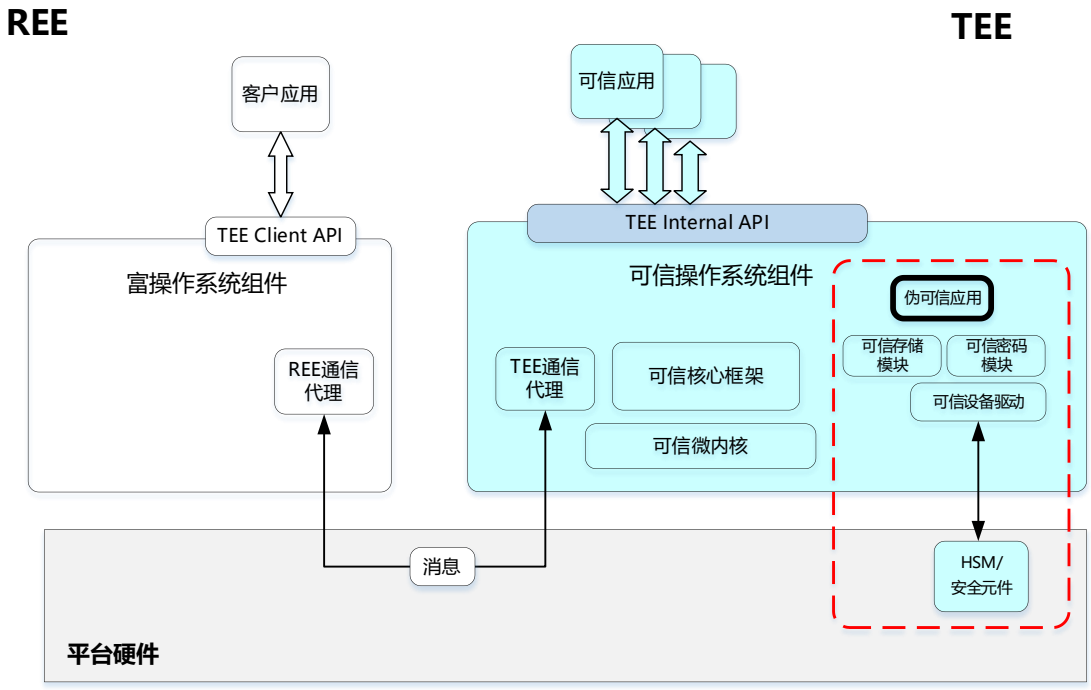

图 10　方式六的密码模块边界

密码模块规格概述

——密码模块实现方式，微内核方式实现可信操作系统，基于微内核实现密码模块安全功能的伪可信应用是基于可信执行环境的密码模块，伪可信应用运行在用户态，通过微内核系统调用接口和 REE 侧的客户应用通信；核准的安全功能与对敏感安全参数的保护由伪可信应用独立实现；伪可信应用也可以通过 IPC 访问实现可信存储、可信密码服务、可信设备驱动等各种所谓的服务器应用方式实现。

——密码模块类型，常见为固件密码或者混合固件模块；

——密码模块边界，包括伪可信应用的独立镜像；

——目标安全等级，达到安全二级或安全三级。

7. 基于可信执行环境的密码模块安全设计的要点和难点

基于可信执行环境的密码模块的安全设计也应该符合 GM/T 0028 中的安全要求。根据 GM/T 0028 的安全要求，基于可信执行环境的密码模块的 11 个安全域在安全设计时该如何考虑如何做，我们提出如下的建议方案。

7.1　密码模块规格

按不同方式实现的密码模块，在密码模块规格安全域中的设计要点，第 6 章已作过说明，详见 6.4 中按方式一至方式六实现的密码模块的“密码模块规格概述”。

7.2 密码模块接口

7.2.1 接口定义和类型

按不同方式实现的密码模块，在密码模块接口安全域中，关于接口定义和类型的设计要点见表 4。

表 4 接口定义和类型的设计要点

实现方式	设计要点
方式一	可信执行环境通信代理模块作为出入密码边界的逻辑接口，负责在富执行环境与可信执行环境之间交换承载控制输入/输出、数据输入/输出和状态输出所需的消息。
方式二	具有两类逻辑接口，分别为： ——用于对外提供服务的逻辑接口。可信应用需实现与可信执行环境操作系统约定的可信应用接口，由可信执行环境的操作系统调用，可信应用响应。可信执行环境的操作系统通过应用编程接口，向可信应用提供资源管理、时间服务、存储服务等功能。 ——用于支撑服务的逻辑接口。可信操作系统通过 TEE Core API 等接口方法，向可信应用提供资源管理、时间服务、存储服务等运行环境功能。可信应用调用这些接口（控制输出、数据输出），并接收接口的响应数据（数据输入），用于支撑实现其自身的安全功能和服务。
方式三	这种类型的密码模块，其密码边界上的接口是可信应用与密码模块之间约定的函数调用形式的逻辑接口。
方式四、 方式五	这两种类型的密码模块，具有三类逻辑接口，分别为： ——可信执行环境通信代理模块，作为出入密码边界的逻辑接口，负责在富执行环境与可信执行环境之间交换控制输入/输出、数据输入/输出和状态输出所需的消息。 ——用于支撑可信应用的逻辑接口。可信执行环境的操作系统通过应用编程接口，向可信应用提供资源管理、时间服务、存储服务、可信用户接口服务等功能。可信应用依赖这些接口支撑其自身的安全功能和服务。 ——用于可信应用管理的逻辑接口，实现可信应用的加载、执行以及卸载等功能。
方式六	这种类型的密码模块，其密码边界上的接口是伪可信应用与微内核之间约定的系统调用形式的逻辑接口。

由于不同的边界划分方式形成的不同密码模块类型而引起的这些差异，在安全设计时需要格外关注。不仅要实现 GM/T 0028 的物理通道中数据、控制、状态接口的隔离，而且还有逻辑通道中数据、控制、状态接口的隔离，并且将上述差异在选定类型的安全设计中明确说明。

7.2.2　可信信道

按不同方式实现的密码模块，在密码模块接口安全域中，关于可信信道的设计要点见表 5。

表 5　可信信道的设计要点

实现方式	设计要点
方式一、 方式二、 方式三	这三种类型的密码模块，在其密码边界内不足以支持 TUI 功能，因此可不设计可信信道。
方式四、 方式五、 方式六	这三种类型的密码模块，如果可信执行环境操作系统支持可信用户接口（TUI），可以使用可信用户接口技术可用于实现密码模块与使用者之间的可信信道。可信用户接口提供安全的输入输出环境，保护可信应用的显示输出信息和触摸屏等设备的输入信息不被泄露、劫持或篡改。 ——在初始化鉴别和后续的鉴别过程中，要求用户在可信用户接口环境中设置或输入口令、PIN 码等鉴别信息，是可信信道的数据输入； ——在可信用户接口环境中显示的秘密信息或需保护不被篡改的信息，是可信信道的数据输出； ——要求用户在可信用户接口环境中点击按钮以确认授权操作，是可信信道的控制输入。

7.3　角色、服务和鉴别

7.3.1　角色

按不同方式实现的密码模块，在角色、服务和鉴别安全域中，关于角色的设计要点见表 6。

表 6　角色的设计要点

实现方式	设计要点
方式一、 方式二	这两种类型的密码模块，其操作员可以是： ——运行在富操作系统中的客户端应用； ——通过客户端应用访问密码模块的用户。
方式三	这种类型的密码模块，其操作员可以是： ——运行在可信执行环境中（但在密码边界外部）的其他可信应用。
方式四、 方式五、 方式六	这三种类型的密码模块，其操作员可以是： ——运行在富操作系统中的客户应用； ——运行在可信执行环境中（但在密码边界外部）的可信应用； ——通过客户端应用或 TUI 功能访问密码模块的用户。

TEE 密码模块的主管角色可以执行 TEE 密码模块的各种初始化操作。

7.3.2　鉴别

当密码模块的安全等级达到安全二级及以上时，应实现对操作员的鉴别机制。

按方式四、方式五、方式六实现的密码模块，在鉴别机制中，如需要用户输入口令或 PIN，宜使用 TUI 功能保护用户鉴别数据。

7.3.3　软件/固件加载

按方式四和方式五实现的密码模块，具有加载外部软件或固件（可信应用或库、伪可信应用等）的能力，需要满足 GM/T 0028 中的相关要求。

7.4　软件/固件安全

软件/固件安全，主要包括安装前的防篡改校验、模块加载时的完整性校验、以及在服务运行过程中按需提供模块安全性校验功能。

由于实现方式的差异，基于可信执行环境的密码模块具有不同的密码模块规格和密码边界，但都应确保密码模块在安装前未被修改。如，针对可信应用的镜像或可信操作系统的镜像，应使用核准的完整性技术进行保护，安装前先验证镜像文件中的消息鉴别码或数字签名，验证失败时终止安装或加载。

7.5　运行环境

由于实现方式的差异，基于可信执行环境的密码模块具有不同的运行环境。需要先正确识别其运行环境的内涵与边界，再按照 GM/T 0028 对运行环境的安全要求进行设计。

按不同方式实现的密码模块，在运行环境安全域中的设计要点见表 7。

表 7　运行环境的设计要点

实现方式	设计要点
方式一、方式四、方式五	这三种类型的密码模块，其运行环境为可信执行环境操作系统绑定的硬件平台。
方式二、方式三	这两种类型的密码模块，其运行环境为可信执行环境操作系统和与其绑定的硬件平台。
方式六	这种类型的密码模块，其运行环境为可信执行环境操作系统的微内核以及绑定的硬件平台。

7.6　物理安全

由于实现方式的差异，基于可信执行环境的密码模块具有不同的密码模块类型。按方式一、方式四、方式五和方式六实现的密码模块，当实现为混合固件密码模块时，物理安全主要由其中的硬件部件负责设计实现。

7.7　非入侵式安全

基于可信执行环境的密码模块运行在硬件隔离的环境中，其所面临的非入侵式攻击有限，比较典型的如 RowHammer 硬件旁路攻击和 Cache 侧信道攻击。在此基础上，当实

现为混合固件密码模块时，其中的硬件部件应具备对典型错误注入攻击的防护能力，如电磁攻击、电压攻击等。

7.8 敏感安全参数管理

7.8.1 敏感安全参数的输入和输出

按方式四、方式五、方式六实现的密码模块，可使用 TUI 提供的可信信道传输明文密钥分量、鉴别数据以及其他关键安全参数输入或输出密码模块。

7.8.2 随机数生成器

密码模块中使用的随机数应来自核准的随机数生成器；混合固件密码模块可以使用核准的硬件随机数发生器，GM/T 0078—2020《密码随机数生成模块设计指南》可作为硬件随机数发生器的设计参考；固件密码模块可以在模块内部构建软件随机数发生器，GM/T 0105—2021《软件随机数发生器设计指南》可作为软件随机数发生器的设计参考。

按方式二、方式三实现的密码模块，可以绑定密码边界外的随机数生成器。

按方式一、方式四、方式五和方式六实现的密码模块，如果支持硬件部件，宜使用 SE 或密码加速引擎等硬件部件实现的随机数生成器。

7.8.3 敏感安全参数的存储

密码模块中的敏感安全参数应以加密形式存储，密码模块需要依赖 TEE OS 提供的 TEE API 实现数据的持久存储。对于安全一级，密码模块可以利用 TEE OS 提供的安全机制保护存储的敏感安全参数。对于安全二级及以上，密码模块应不依赖 TEE OS 的安全机制，独立设计和实现保护存储的敏感安全参数的安全机制。

按不同方式实现的密码模块，在敏感安全参数管理安全域中，关于敏感安全参数的存储的设计要点见表 8。

表 8 敏感安全参数的存储的设计要点

实现方式	设计要点
方式一	敏感安全参数应以加密形式存储。
方式二	可通过可信操作系统提供的可信存储 API 实现加密后的敏感安全参数的持久化存储功能。
方式三	可以返回保护后的敏感参数，但不应提供敏感安全参数的持久化存储功能。
方式四、方式五	可以采用 RPMB、SE 等硬件部件方式存储安全敏感参数。 这两种类型的密码模块，其密码边界包括了整个可信操作系统，可信操作系统既要和外部的富执行环境通信，也要为可信应用提供应用编程接口（系统调用），因此这类密码模块的实现尤其需要考虑通过这些接口攻击密码模块敏感安全参数的各种方式。
方式六	相比方式四和方式五的密码模块，排除了操作系统一些和实现密码模块功能关系不大的组件，可以简化密码模块的实现，便于实现较高安全等级（比如安全等级 3），有助于密码模块的安全评估。

7.9 自测试

按 GM/T 0028 的要求执行运行前自测试和条件自测试，确保密码模块没有故障。

7.9.1 运行前软件/固件测试

按方式四和方式五实现的密码模块，可信应用管理框架在加载密码模块可信应用前进行完整性测试。

7.9.2 运行前关键功能测试

实现密码模块的可信应用，可在会话入口点成功打开会话后，可选择执行关键功能测试。

7.9.3 条件自测试

按方式四和方式五实现的密码模块,可信应用管理框架在安装密码模块可信应用后，对支持的全部密码算法进行自测试。

7.10 生命周期保障

“生命周期保障”这个安全域在不同类型密码模块间未发现明显差异，按 GM/T 0028 的要求执行生命周期保障。

7.11 对其他攻击的缓解

按 GM/T 0028 的要求，根据密码模块的具体实现进行安全设计。

参考文献

[1] 冯登国，刘敬彬，秦宇，冯伟. 创新发展中的可信计算理论与技术[J]. 中国科学：信息科学，2020,50(08)：3-78.

[2] GB/T 41388—2022，信息安全技术 可信执行环境 基本安全规范[S].

[3] GB/T XXXXX—XXXX，信息安全技术 可信执行环境服务规范[S].

[4] JR/T 0156—2017，移动终端支付可信环境技术规范[S].

[5] T/BMFIA 00001—2017，移动终端安全金融盾规范[S].

[6] T/ZISIA-EMCG 001—2019 移动智能终端密码模块技术框架[S].

[7] 吴振，杜之波等. 可信运行环境系统密码框架与接口规范研究[R]. 成都：成都信息工程大学，2019.