ICS 35.040
CCS L 80

T

团　　体　　标　　准

T/ZTCIA 005—2025

基于BMC的TPCM技术规范

Technical Specification for TPCM Based on BMC

2025 - 04 - 01 发布　　2025 - 07 - 01 实施

中关村可信计算产业联盟　发布

目　　次

目　次

前　言

本文件按照GB/T 1.1-2020给出的规则起草。

本文件由中关村可信计算产业联盟提出并归口。

本文件起草单位：北京工业大学、中关村可信计算产业联盟、华为技术有限公司、北京可信华泰信息技术有限公司、浪潮电子信息产业股份有限公司、飞腾信息技术有限公司、昆仑太科（北京）技术股份有限公司、江苏云涌电子科技股份有限公司、管芯微技术（上海）有限公司、浙江东安检测技术有限公司。

本文件主要起草人：张建标、刘燕辉、刘达、郑锟、于攀、王正鹏、段古纳、田健生、齐洪东、吴保锡、鲁彬、谭琳、孙亮、陈小春、王昱波、李小川、任彤、王亚洲、梁刚、黄坚会、刘金荣、刘明健、高渊、郭勇、张欢、沈汀、王一凡、姜凌艳。

基于BMC的TPCM技术规范

1 范围

本文件规定了基于BMC的TPCM可信计算产品技术规范要求。

本文件适用于基于BMC的可信计算产品的可信功能设计与研发。

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 29827-2013 信息安全技术 可信计算规范 可信平台主板功能接口

GB/T 29829-2022 信息安全技术 可信计算密码支撑平台功能与接口规范

GB/T 37935-2019 信息安全技术 可信计算规范 可信软件基

GB/T 40650-2021 信息安全技术 可信计算规范 可信平台控制模块

GM/T 0012-2020 可信计算可信密码模块接口规范

T/ZTCIA 001-2023 可信计算产品规范

3 术语和定义

GM/T 0012-2020、GB/T 40650-2021和GB/T 37935-2019界定的以及下列术语和定义适用于本文件。

3.1

可信平台控制模块 trusted platform control module

集成在可信计算节点中的防护部件组件，有硬件、软件及固件组成，与计算部件的硬件、软件及固件并行连接，是用于建立和保障信任源点的一种基础核心模块，为可信计算节点提供主动度量、主动控制、可信验证、加密保护、可信报告、密码调用等功能。

[来源：GB/T 40650-2021，定义3.3]

3.2

可信密码模块 trusted cryptography module

可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

[来源：GM/T 0012-2020，定义3.7]

3.3

基板管理控制器 baseboard management controller

部署于服务器上的具有独立供电、独立处理器、独立I/0接口的控制单元，用于监控服务器主板各功能部件的状态。

3.4

可信软件基 trusted software base

为可信计算平台的可信性提供支持的软件元素的集合。

[来源：GB/T 37935-2019，定义3.3]

3.5

可信根 root of trust

可信根是可信计算平台的信任源点，由TPCM、TCM和TSB构成。TPCM是可信平台控制模块，负责发起可信验证、获取可信验证数据、执行可信验证中运算（非密码相关）、存储相关策略信息、执行可信控制等。TCM是可信密码模块，为可信验证操作提供密码服务支撑。可信根是用于支撑可信计算平台信任链建立和传递的可对外提供完整性度量、安全存储、密码运算等服务的功能模块。

[来源：T/ZTCIA 001-2023，定义3.3]

3.6

可信管理中心 trusted management center

对可信计算节点的防护策略和基准值进行制定、下发、维护、存储等操作的集中管理平台。

[来源：GB/T 40650-2021，定义3.9]

3.7

可信验证 trusted verification

依据防护策略和基准值对防护对象进行主动度量和对度量结果判定的过程。

[来源：GB/T 40650-2021，定义3.11]

3.8

动态度量 dynamic measurement

在系统运行过程中，对系统完整性和行为安全性进行测量和评估的可信度量方法。

[来源：GB/T 37935-2019，定义3.9]

4 缩略语

下列缩略语适用于本文件。

BIOS：基本输入输出系统（Basic Input Output System）

TPCM：可信平台控制模块（trusted platform control module）

TSB：可信软件基（trusted software base）

TCM：可信密码模块（trusted cryptography module）

BMC：基板管理控制器（baseboard management controller）

Grub：GUN项目的多操作系统启动程序（GRand Unified Bootloader）

IPMI：智能平台管理接口（Intelligent Platform Management ）

5 概述

可信计算产品由计算部件和防护部件组成，其启动过程可信引导应包含防护部件上电到计算部件系统加载。防护部件可以访问计算部件的所有资源，对计算部件的启动及运行过程进行度量。计算部件无法直接访问防护部件资源，双方资源隔离，只能通过安全信道通信。

针对可信服务器，BMC模块通常是服务器首先上电的模块，拥有独立的系统和硬件资源，能够实现对服务器硬件设备的主动监测和控制，因此可基于BMC模块构建TPCM方案。

基于BMC形态构建的TPCM可信计算框架，遵循GB/T 40650提出的“TPCM应是整个可信节点中第一个获得执行权的部件”的要求，通过在BMC模块构建TPCM模块，完成对服务器所有重要固件与软件的启动及运行过程进行度量。

基于BMC的TPCM在服务器中的位置及其与其他部件互动关系的示意图如图1所示。TPCM功能由BMC实现，与TSB、TCM、可信管理中心和计算部件交互，交互流程见GB/T 40650-2021 5.2章节。

在服务器启动与运行阶段，各模块主要完成以下功能：

可信管理中心负责全系统策略管理、基准管理及节点状态评估等，并为可信接入提供裁决能力。防护部件的可信组件包括TPCM模块，TSB模块以及底层支持的TCM模块等。计算部件的可信组件主要由计算部件固件层可信代理、引导层可信代理、系统层可信代理以及相关驱动等模块组成。在服务器启动过程中，TPCM支撑计算部件各级可信代理完成启动信任链的逐级度量加载，在系统运行过程中，TPCM支撑可信代理对关键文件的动态度量。计算部件各级可信代理完成要素信息收集与执行控制操作通知等。通过可信管理中心、防护部件、计算部件各模块之间的互相配合实现可信相关功能。

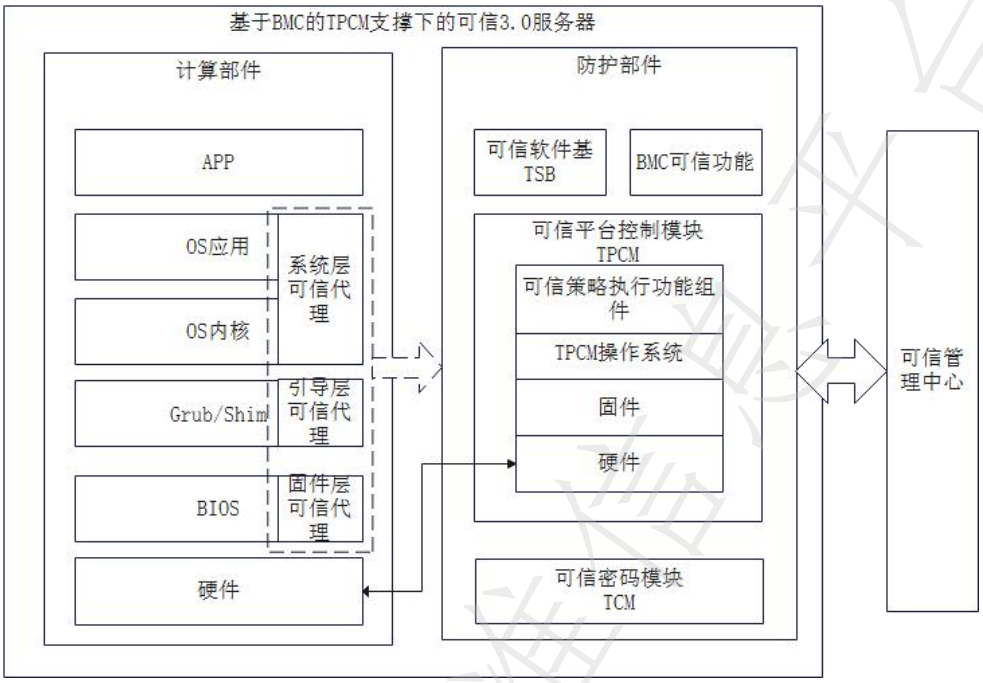

图1 基于BMC的TPCM支撑下的可信3.0服务器

6 技术要求

6.1 可信根要求

基于BMC的TPCM硬件可信根应满足如下要求：

a) 是服务器完整性度量的起点。
b) 应包含TPCM模块使用的处理器、安全存储及TCM模块等。
c) TPCM模块与TCM模块应以硬件形态实现，应具有独立的硬件资源。
d) TPCM功能应由BMC芯片处理器独立核实现。
e) 应符合相关技术规范要求，包含但不限于GB/T 29829-2022 第6.2.1章的要求。

6.2 防护部件要求

6.2.1 防护部件组成

防护部件应包含：

a) BMC芯片及运行在BMC芯片的固件、引导程序、操作系统及相关软件等。
b) TSB模块。
c) TPCM模块、TCM模块等，TCM应符合GM/T 0012-2020的要求。

6.2.2 防护部件度量要求

防护部件度量过程应满足：

a) 防护部件度量应以硬件可信根为起点。
b) 防护部件BMC芯片内TPCM独立核固件应采用安全措施度量启动，可具有独立的保护机制，然后应依次完成BMC内引导程序及操作系统，TSB等组件度量启动。
c) 度量过程信任链建立流程应满足GB/T 29827-2013 第6.2章的规定。
d) 度量算法应使用符合国家密码管理部门规定的密码算法。

6.3 计算部件要求

6.3.1 计算部件组成结构

计算部件应包含：

a) 计算部件硬件、BIOS、Grub/Shim、OS内核、OS应用以及上层应用软件等。

b) 可信软件基代理：固件层可信代理、引导层可信代理、操作系统可信代理等。

6.3.2 计算部件度量要求

计算部件度量过程应满足：

a) 计算部件启动度量应在防护部件启动度量之后，由防护部件完成对计算部件的度量。

b) 防护部件应首先完成BIOS度量，然后计算部件代理协助防护部件依次完成Grub/Shim、OS内核、OS应用以及APP应用软件等组件度量启动，其中BIOS的度量应在计算部件启动运行之前由防护部件率先完成。

c) 计算部件各模块的关键度量数据由模块所对应的可信软件基代理获取，并发送至防护部件。各模块与可信软件基代理对应关系如图1所示。

d) 计算部件OS内核应支持被防护部件动态度量，应通过可信软件基代理的度量机制、支撑机制，向TSB提供度量数据，支撑对计算部件OS内核实现动态度量。

e) 度量过程信任链建立流程应满足GB/T 29827-2013 第6.2章的规定。

f) 度量算法应使用符合国家密码管理部门规定的密码算法。

6.4 可信软件基及代理要求

6.4.1 可信软件基要求

基于TPCM运行的TSB并行于计算部件代理，通过计算部件代理在操作系统内进行主动拦截，实现对应用程序及运行环境的可信验证。TSB应遵循GB/T 37935的规定。

6.4.2 可信软件基代理要求

可信软件基代理模块应满足以下要求：

a) BIOS应率先由防护部件协助TPCM完成可信启动。

b) 固件层可信代理集成在计算部件BIOS中，协助TPCM完成引导程序可信启动。

c) 引导层可信代理集成在计算部件操作系统引导程序（如Grub/Shim等）中，其中Grub 协助 TPCM 完成 OS Kernel 度量，完成操作系统的可信启动。如操作系统引导层含有Shim， 则Shim协助 TPCM 度量 Grub。

d) 系统层可信代理集成在计算部件操作系统中，由 TSB 通过度量确保可信代理安全。可信代理协助TSB完成对操作系统应用度量和控制。

6.5 服务器启动及复位要求

6.5.1 整机启动要求

整机启动场景下，服务器应按照本规范6.2.2章节防护部件启动度量要求，6.3.2章节计算部件启动度量要求依次完成度量启动。

6.5.2 服务器复位要求

服务器各部件服务应满足：

a) 防护部件单独复位，服务器应遵循本规范6.2.2章节防护部件度量要求对防护部件启动过程完成度量。

b) 计算部件单独复位，服务器应遵循本规范6.3.2章节计算部件度量要求对计算部件启动过程完成度量。

7. 可信平台控制模块的接口

7.1 计算部件接口要求

计算部件接口包含访问计算部件接口及计算部件与防护部件通信接口，应满足以下要求：

a) 访问计算部件接口主要为总线接口，与服务器各部件中不同类型的总线相连，用于访问计算部件内存、I/O、系统固件等系统资源。接口应满足GB/T 40650-2021 7.1章节的规定。

b) 计算部件与防护部件间通信接口用于度量数据传输与度量结果获取，接口原型可参考附录A设计，基于IPMI协议实现可参考附录B中实现。

7.2 可信软件基接口要求

TSB接口为软件接口，为TSB提供TPCM功能的调用。TSB接口应遵循GB/T 37935的规定。

7.3 管理接口要求

管理接口为物理接口，应为网络或总线接口模式，由可信管理中心访问。接口应满足GB/T 40650-2021 7.3章节的规定。

7.4 可信密码模块接口要求

可信密码模块接口提供TPCM对可信密码模块访问的I/O通道，接口应遵循GB/T 29829的规定。

附录A

（资料性）
计算部件通信接口

A.1 SHIM/GRUB/OS度量命令发送接口

计算部件请求度量接口用于将待度量数据传输到防护部件，并返回传输的状态信息，接口原型定义为：

```
struct {
   IN UINT8 firmware_type;
   IN UINT8 firmware_detail_type;
   IN UINT8 firware_hash_len;
   IN UINT8 *firmware_hash_content;
   IN UINT8 firmware_version_len;
   IN UINT8 *firmware_version;
   OUT UINT8 code
};
```

接口参数描述：

表 A-1 度量命令发送接口参数描述

数据	描述
firmware_type	固件类型，包含SHIM、GRUB、OS等
firmware_detail_type	根据固件类型划分子类型，例如OS包含kernel、initrd等
firware_hash_len	固件HASH长度
*firmware_hash_content	固件HASH值
firmware_version_len	固件版本长度
*firmware_version	固件版本
code	接口完成码，用于确认接口调用状态

A.2 SHIM/GRUB/OS获取控制结果接口

计算部件获取控制结果接口用于从防护部件获取度量结果，接口原型定义：

```
struct {
   IN UINT8 firmware_type;
   IN UINT8 firmware_detail_type;
   OUT UINT8 code;
   OUT UINT8 result;
};
```

接口参数描述：

表A-2 获取度量结果接口参数描述

数据	描述
firmware_type	固件类型，包含SHIM、GRUB、OS等
firmware_detail_type	根据固件类型划分子类型，例如OS包含kernel、initrd等
code	接口完成码，用于确认接口调用状态
result	度量结果

附录B

（资料性）

基于IPMI协议接口实现

B.1 请求度量接口实现

请求度量接口基于IPMI协议实现各参数定义参考如表B-1。

表B-1 请求度量接口实现

参数说明	字节顺序	域内容
IPMI厂商自定义字段	NetFn	厂商自定义请求值
	CMD	
	1:03	
	4	
固件类型	5	Firmware Type
		0: SHIM
		1: GRUB
		2：OS
固件子类型	6	Firmware Detail Type
		Firmware Type:0
		0: SHIM
		1: reserved1
		2: reserved2
		Firmware Type:1
		0: GRUB
		1: reserved1
		2: reserved2
		Firmware Type:2
		0: grub.cfg
		1: kernel
		2: initrd
固件HASH长度	7	Firmware Hash Len：M
固件HASH内容	8:7+M	Firmware Hash Content
固件版本长度	8+M	Firmware Version Len： N
固件版本内容	9+M:8+M+N	Firmware Version
接口响应值	1	Completion Code
厂商自定义字段	2:04	厂商自定义返回值

B.2 获取控制结果接口实现

获取控制结果接口基于IPMI协议实现各参数定义参考如表B-2。

表B-2 获取控制结果接口实现

参数说明	字节顺序	域内容
IPMI厂商自定义字段	NetFn	厂商自定义请求值
	CMD	
	1:03	
	4	
固件类型	5	Firmware Type
		0: SHIM

		1: GRUB
		2：OS
固件子类型	6	Firmware Detail Type
		Firmware Type:0
		0: SHIM
		1: reserved1
		2: reserved2
		Firmware Type:1
		0: GRUB
		1: reserved1
		2: reserved2
		Firmware Type:2
		0: grub.cfg
		1: kernel
		2: initrd
响应说明	字节顺序	域内容
接口返回值	1	Completion Code
厂商自定义字段	2:04	厂商自定义返回值
度量结果	5	Control Result
		0: success
		1: fail