# 鲲鹏 BoostKit 机密计算 TrustZone 套件

# 技术白皮书

文档版本 01

发布日期 2022-01-18

华为技术有限公司

## 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 目 录



# 1 产品简介



## 1.1 机密计算定义

在国际机密计算联盟 CCC 中，定义为 ： 机密计算是通过在基于硬件的可信执行环境中执行计算来保护使用中的数据的一种技术 。将机密计算与可信计算作为两类技术。

国内金融行业，各大行发布的技术白皮书中，则将所有保证数据机密性的可能的技术都归为“隐私计算”的范畴。

## 1.2 鲲鹏机密计算套件概述

鲲鹏机密计算TrustZone套件是基于ARM TrustZone的技术，结合华为鲲鹏芯片产品定位，通过适配、扩充TrustZone必要功能，提供的适用于数据中心服务器产品的机密计算解决方案。

TrustZone是ARM针对嵌入式设备设计的一种硬件架构，在概念上将芯片的硬件和软件资源划分为安全（Secure World）和非安全（Normal World）两个世界，应用根据需要可以将处理机密数据的业务逻辑部署在安全世界执行。

本套件目标是给行业客户提供一个安全的，应用开发和部署都便利的机密计算应用执行平台。因此，本产品并不是具体的业务。理论上，根据此产品的使用规则，任何需要保护应用计算过程或数据的场景都可以适用。

技术上可使用的场景包括不限于：

1. 金融大数据数据挖掘，保证数据处理过程中的机密性。
2. 一体化大数据中心数据可信交易。
3. 行业隐私计算，认证计算过程中避免泄漏个人隐私信息。

# 2 系统架构

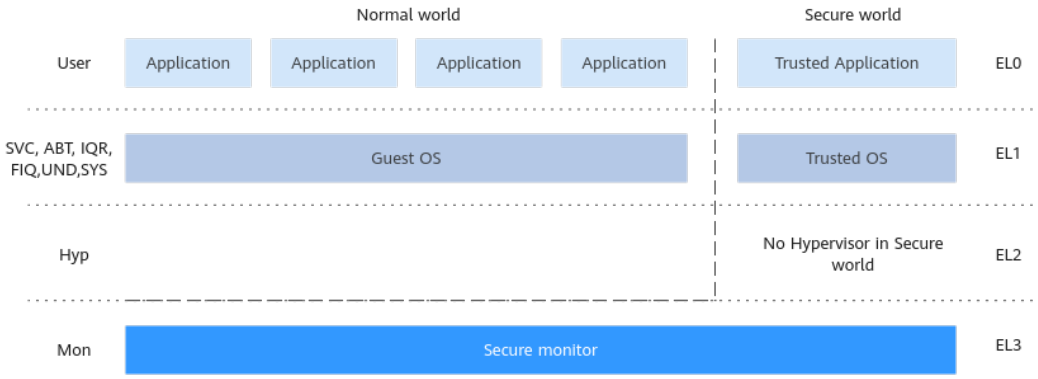


## 2.1 机密计算 TrustZone 技术原理

如前文所述，鲲鹏机密计算采用的是鲲鹏TrustZone技术。通过分时复用技术，区分CPU的运行状态，在同一套硬件系统上划分了两个独立的环境：

- Normal world：常规环境，即REE（Rich Execution Environment）
- Secure world：安全环境，即TEE（Trusted Execution Environment）

**图 2-1** 实现原理




这两个世界各自拥有自己的资源，包括内存和Cache，根据CPU的设计不同，硬件设备也可被设计为TEE专用或在需要时可动态切换。只有CPU处于TEE安全态时，才可以访问安全侧的资源和硬件。

在此被严格隔离的资源之上，TEE和REE侧分别拥有自己的操作系统，用来执行用户的可信应用。

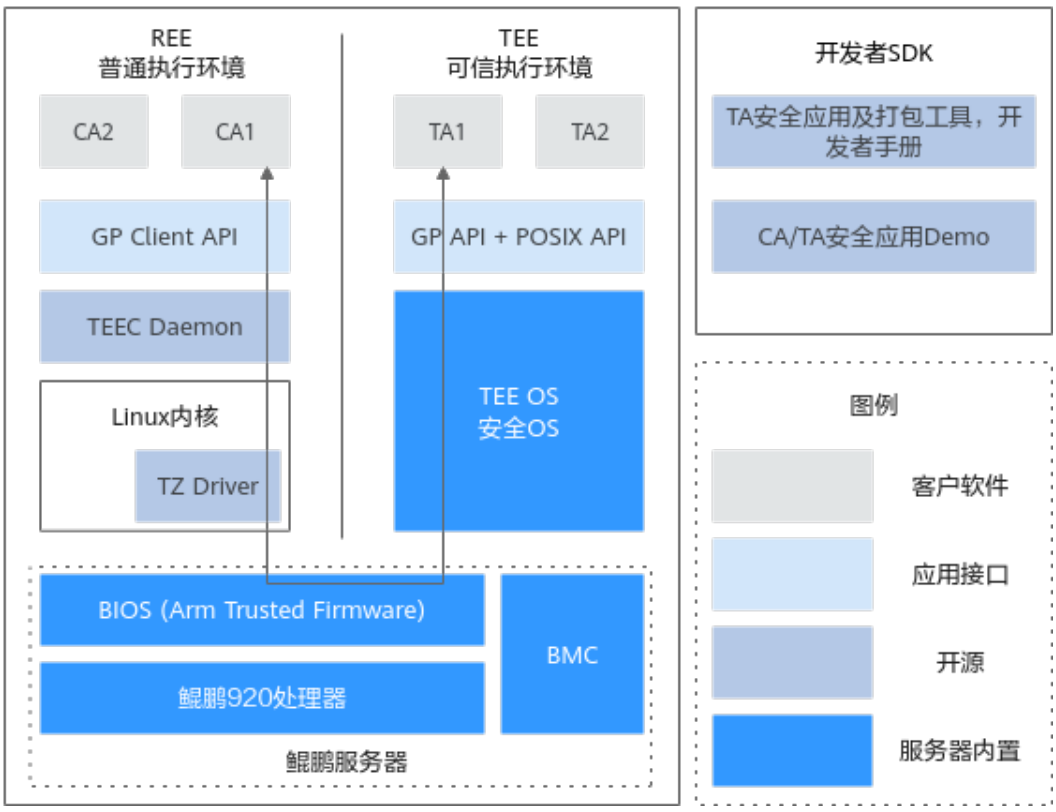
## 2.2 鲲鹏机密计算 TrustZone 套件

## 2.2.1 系统架构

鲲鹏机密计算TrustZone套件以ARM TrustZone为技术实现基础，并不针对特定业务的业务功能，而是一个由硬件（包括BIOS、BMC）、机密计算运行环境，以及配套的patch、应用开发指导和应用打包工具等组成的端到端的解决方案。

本文不会针对具体某一个组件展开说明，而是面向行业开发者，以解决方案角度展开对涉及的组件说明，旨在指导开发者可以快速的了解鲲鹏机密计算TrustZone套件所涉及的软硬件实体，以便快速部署和使用自己的开发环境。

**图 2-2** 鲲鹏机密计算 TrustZone 套件组成




通过此套件，华为旨在提供一个安全的，方便客户开发者部署自有应用（包括CA和TA）的平台。涉及方包括华为以及客户，表2-1分别以华为和客户责任方来描述套件中所涉及的组件和功能。

**表 2-1** 基于鲲鹏机密计算 TrustZone 套件完整组成说明

| 类别 | 子类 | 说明 |
| --- | --- | --- |
| 行业客户 | 业务应用 | 根据TrustZone的软件开发模型，某一个具体的业务应用分别被拆分为TA和CA。<br>• TA（Trusted Application），运行在安全世界TEE的应用服务。<br>• CA（Client Application），运行在Host OS非安全世界REE的应用。 |

| 类别 | 子类 | 说明 |
| --- | --- | --- |
| | Linux OS | 客户自行选择并部署的Linux操作系统。TEE执行环境与用户操作系统没有耦合关系，但是CA和TA的通信会依赖于REE侧的通信框架，华为以REE Patch的方式提供。为了确保与操作系统兼容，华为已将REE Patch在openEuler社区开源，开发者可以根据自己的需要，在选定的OS上自行编译。 |
| 华为交付件 | 安全OS | 华为TEE侧OS，提供在TEE内的应用执行环境。它适配了鲲鹏平台的多CPU多核，以及鲲鹏平台特有硬件。正常情况下，客户如果购买了支持TrustZone功能的鲲鹏服务器，TEE OS会内置于硬件平台内，后续可以通过升级更新版本。 |
| | 硬件Firmware | 为支持TrustZone特性，硬件Firmware版本也进行了相关的适配：<br>● BIOS：支持对TEE OS的解密、安全启动，以及对TEE OS涉及功能的配置。<br>● BMC：支持对TEE OS的升级维护。<br>● 支持TrustZone功能的硬件Firmware随同硬件在产线预装，客户需要通过硬件的Firmware版本获取途径获得更新。 |
| | REE侧Patch | 为了让客户的业务应用CA与部署在TEE内的TA通信，需要在客户的操作系统中部署Patch，该Patch包括用户态的API库、守护进程以及内核驱动。<br>为应对客户不同的操作系统的诉求，华为已将源码开源。 |
| | 应用开发SDK | 包括应用开发接口说明、应用打包工具、头文件以及Demo代码等。目前SDK已开源发布。 |

## 2.2.2 关键组件获取

**表 2-2** 关键组件获取

| 组件 | 开放方式 | 获取说明 |
| --- | --- | --- |
| 安全OS | 闭源，二进制 | 通过华为Support获取。 |
| 硬件Firmware（BIOS、BMC） | 闭源，二进制 | 通过华为Support获取：<br>**https://support.huawei.com/enterprise/zh/kunpeng-computing/ts200-2280-pid-250697162/software/**<br>**须知**<br>鲲鹏第三方服务器厂商自行发行的版本信息不在此文档范围内。 |

| 组件 | 开放方式 | 获取说明 |
| --- | --- | --- |
| REE侧Patch | 社区开源 | 代码已在openEuler社区开源，获取地址：<br>**https://gitee.com/openeuler/itrustee_tzdriver**<br>**https://gitee.com/openeuler/itrustee_client** |
| 应用开发SDK | 社区开源 | **https://gitee.com/openeuler/itrustee_sdk**<br>**说明**<br>由于延时，可能存在社区版本可能没有及时更新的情况。必要的情况下可与项目接口人确认版本。 |

# 3 关键功能



## 3.1 TrustZone 功能开关

TrustZone采用硬件隔离资源的方式来确保TEE环境的安全。在功能使能的情况下，TEE环境资源在系统启动时即刻被通过安全的方法设定，并且这部分资源将在服务器上电生命周期内一直为TEE环境独占，对REE不可见也不可访问。

鲲鹏机密计算TrustZone套件是面向有机密数据保护需求场景而提供的特性，即只有特定需求的用户才需要。如果默认开启功能，这意味着有部分资源被保留而浪费。因此BIOS提供了TrustZone的功能开关，由管理员根据实际需求情况决定是否使用该功能。

需要注意的是，关闭此功能并不意味着旁路或绕过某些安全机制，它只是TrustZone的功能开关，关闭之后TrustZone功能将不再生效，部署在平台之上的相关组件也都将不可用，但不会导致系统不可用，或削弱即有的安全机制。

具体设置方法可参考BIOS操作手册，或《**TrustZone 部署指南**》。

## 3.2 安全内存配置

数据中心场景中的应用可能是面向海量数据处理的，应用程序也是相对复杂和庞大的，同时用户根据业务需求选择的内存配置也不再是固定的，传统的终端上的解决方案如固定TEE内存大小、小容量的安全内存如128MB等，不再能够满足业务需求。

为适应数据中心的场景，本方案支持管理员设置TEE安全内存的大小，当前最大可持到128GB的安全内存的设置。

具体设置方法以及限制可参考BIOS操作手册，或《**TrustZone 部署指南**》。

# 3.3 多核并发

由于应用场景不同，早期的方案中，TEE侧的应用并不需要非常强的运算能力，因此一般TA仅能固定使用某一个核。

本方案并不会限定TEE侧应用的运算能力，如果需要，TA可以使用足够多的CPU资源，以应对服务器数据中心TEE内高算力的应用场景。性能上可以达成REE则和TEE侧运算基本无差异。

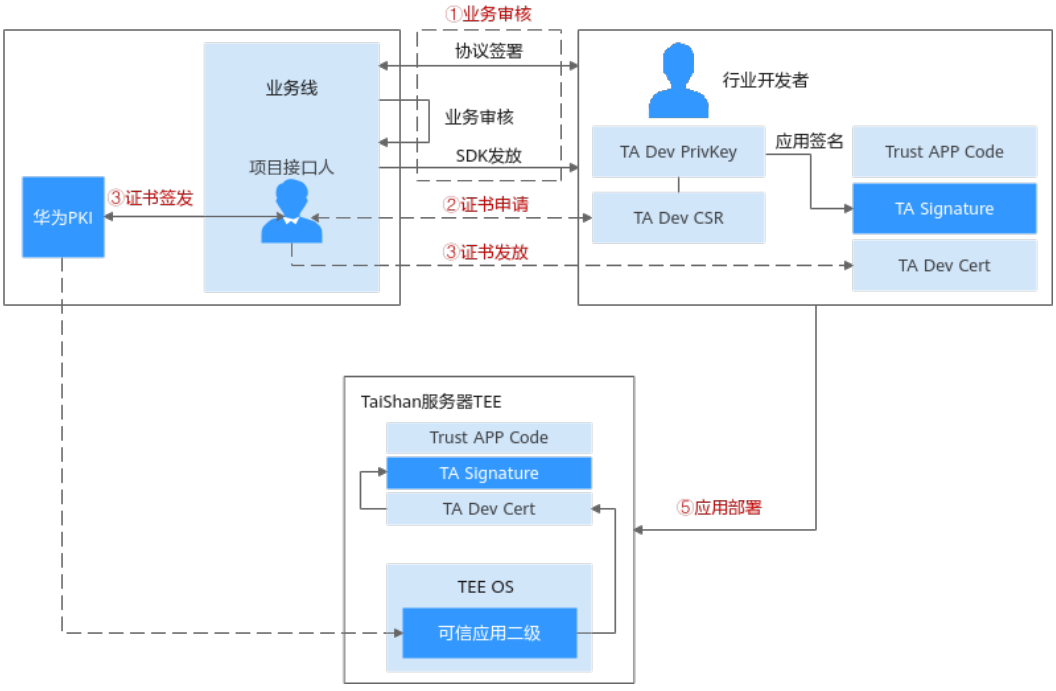
如何提高多核的使用率，可参考产品提供的Demo代码（后续会开源），或在开发过程中咨询项目接口人。

# 3.4 TA 证书管理

为确认TA应用的来源可信，方案采用证书校验的方式确认TA的合法身份。

客户/TA开发者需要先与华为行业接口人签署相关的协议，之后获得业务审批之后才被视为合法的TA开发者。

**图 3-1** 鲲鹏机密计算 TrustZone TA 证书管理




- TA Dev Cert

  TA开发者证书，与TA的标识绑定，代表着某一个TA的身份。

- TA Dev Cert申请流程

  a. 业务审核

     i. 一线生态接口与开发者签署免责协议。

     ii. 业务线内部启动业务审核，审批通过，启动项目，提供SDK、工具和文档。

b. TA证书申请

   i. 开发者通过获得的指导，在本地为TA生成公私密钥对以及证书请求文件（CSR），私钥由开发者自行保管。之后通过PGP邮件方式将请求发送给项目接口人。

   ii. 项目接口人将与开发者沟通协商，包括组织技术评审等。

c. 由业务线项目接口操作申请证书。

d. 确认业务审批已完成，技术评审完成之后，通过华为PKI申请证书，之后再将证书通过PGP邮件方式发送给客户。

# 4 技术规格



## 4.1 概述

鲲鹏机密计算TrustZone套件以ARM TrustZone为技术实现基础，但并不是TrustZone就代表了全部，本套件针对服务器数据中心的应用场景进行了比较系统的适配，例如安全OS是华为自研的TEE OS，它适配了鲲鹏服务器平台上多CPU多核的并发能力。我们也扩展支持了服务器场景中必要的功能，例如可以支持用户在菜单选择内存大小的配置等。

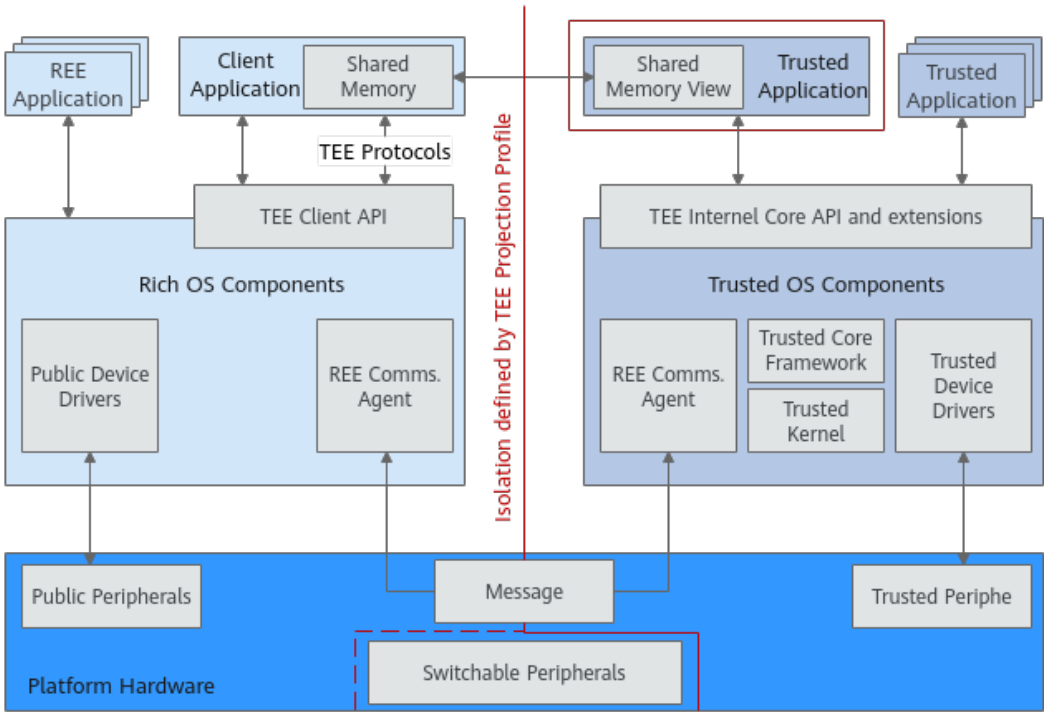
我们设计了TA应用的管控和证明的方案，并向开发者提供SDK、打包签名工具和示例代码，形成了一个面向生态的应用解决方案。

## 4.2 接口规格

业务应用在开发时首先需要设计和规划，将应用划分为CA和TA，其中处理敏感数据的部分一般被部署到TEE内。

面向CA的接口，称为TEE Client API， 而面向TA的接口则称为TEE Internal Core API，同时会有一些TEE OS提供的扩展的可选接口。

**图 4-1** 鲲鹏机密计算 TrustZone 套件接口说明




鲲鹏机密计算TrustZone套件在REE侧通过REE Patch在操作系统中提供TEE Client API，在TEE侧由TEE OS提供TEE Internal Core API，并提供部分POSIX API。

接口兼容：

- Client_API_v1.0 GlobalPlatform Device Technology TEE Client API Specification Version 1.0
- GlobalPlatform Technology TEE Internal Core API Specification Version 1.1.1

具体GP接口差异或限制、POSIX支持列表，以“iTrustee SDK开发者手册”中的相关说明为准，该手册可通过接口人获取。

# 4.3 性能规格

## 4.3.1 REE 与 TEE 侧计算性能差异

鲲鹏TrustZone技术通过分时复用技术，区分CPU的运行状态，在同一套硬件系统上划分了REE和TEE两个独立的环境，从理论上讲，REE和TEE都执行在真实的CPU时间片内，因此性能并不会有显著的区别。

# 5 适用范围和约束



## 5.1 技术依赖

### 5.1.1 安全启动

鲲鹏机密计算TrustZone套件提供的是一个可信的执行环境，它的软件可信依赖于服务器整机系统的可信，因此服务器“安全启动”的使能是前提之一。

### 5.1.2 工厂流程（Provisioning）

鲲鹏机密计算TrustZone套件使用的TEE OS镜像，以及后续部署的TA都有机密性的诉求；同时在运行态时也有身份证明的需求。服务器要使能该特性，首先要在华为工厂完成必要的数据加载，工厂烧流程过程包括：

1. HUK烧写并锁定
2. 镜像加密密钥的烧写
3. 身份证书的申请并随同私钥烧写
4. 版本防回退

**须知**

由于机密性要求，TrustZone的机密和可信数据加载无法在线（如客户现场等非华为工厂环境外部）操作。

## 5.2 版本配套

- BIOS：机密计算TrustZone套件组件TEE OS的加载依赖于BIOS的解密和验签。BIOS 1.83版本以后（含）开始支持。

- BMC：机密计算TrustZone套件组件TEE OS为单独可升级模块，TEE OS作为Kunpeng BoostKit的组件发布，依赖BMC对TEE OS的升级。BMC 3.01.12.49版本以后（含）开始支持。

# 5.3 免责要求

鲲鹏机密计算TrustZone套件是华为在合理商业努力下，应客户的明确要求而向客户提供的功能特性。

您需要理解，任何产品或组件都不可能是绝对安全的。如客户意图将此特性部署在自己的商用环境中，应在客户下单前提醒并签署华为单方“特性使用免责协议”。相关协议请与对应的行业接口人联系获取。

# A 术语及缩略语

| | | |
|---|---|---|
| **C** | | |
| CA | Client Application | 客户端应用程序 |
| CSR | Certificate Signing Request | 签名证书请求 |
| **G** | | |
| GP | Global Platform | 国际标准化组织，TEE标准的制定者 |
| **P** | | |
| PKI | Public Key Infrastructure | 公共密钥基础设施 |
| **R** | | |
| REE | Rich Execution Environment | 业务执行环境 |
| **S** | | |
| SDK | Software Development Kit | 软件开发工具包 |
| SEC | Security Engine | 硬件算法加速引擎 |
| **T** | | |
| TA | Trusted Application | 可信应用程序 |
| TEE | Trusted Execution Environment | 可信执行环境 |

# B 修订记录

| 发布日期 | 修改说明 |
| --- | --- |
| 2022-01-18 | 第一次正式发布。 |