ICS 35.020
CCS L60

团　　体　　标　　准

T/CIITA 101—2021
代替 T/CIITA 101—2020

PKS 体系　参考架构

PKS system—Reference architecture

2021-12-20 发布　　2022-02-01 实施

中 国 信 息 产 业 商 会　　发布

目　次

前　言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 3
5 参考架构 4

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。

本文件代替T/CIITA 101-2020《中央处理器/操作系统体系（PK体系） 参考架构》，与T/CIITA 101-2020相比，除结构调整和编辑性改动外，主要技术变化如下：

a） 更改了标准名称为“PKS 体系 参考架构”；

b） 增加了规范性引用文件“GB/T 35295-2017 信息技术 大数据 术语”、“T/CIITA 100-2021 PKS 体系 术语”、“T/CIITA 105-2021 PKS 体系 UEFI 固件内置可信启动技术要求”、“T/CIITA 107-2021 PKS 体系 可信网络架构要求”、“T/CIITA 104-2021 PKS 体系 操作系统安全可信技术要求”、“T/CIITA 110-2021 PKS 体系 生态软件可信安全认证分发流程”（见第 2 章）；

c） 增加了术语和定义“大数据”、“安全内存模组”（见 3.11 和 3.12）；

d） 删除了术语和定义“标准体系”、“标准体系表”（见第 3 章）；

e） 增加了缩略语 “SDN”、“AI”、“IoT”、“PSPA”、“JEDEC”、“UEFI”“CA”、“LSM”、“eBPF”（见第 4 章）；

f） 更改了“PKS 体系参考架构”图及概述（见 5.1）；

g） 增加了领域开发框架，包括对大数据、人工智能、物联网和移动网络等开发的支持（见 5.4）；

h） 增加了应用层的描述（见 5.5）；

i） 修改了对 PKS 体系中安全体系组成和内容的描述（见 5.6）。

本文件由中国信息产业商会团体标准委员会提出并归口。

本文件起草单位：中电（海南）联合创新研究院有限公司、中软信息系统工程有限公司、中国电子信息产业集团有限公司。

本文件主要起草人：王定健、陈锡明、孙迎新、符兴斌、黄明、胡春玲、张衷阁、赵丽爽、邓子畏、李景龙、焦峰、郑新华、李锁在、鲁振、郑世普、王昊。

本文件及其所代替文件历次版本发布情况为：

——2020年首次发布为T/CIITA 101-2020；

——本次为第一次修订。

PKS 体系　参考架构

1　范围

本文件确立了PKS体系参考架构的构成，规定了基本功能。

本文件适用于PKS体系的研发、制造和应用。

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 35295-2017　信息技术 大数据 术语

T/CIITA 100-2021　PKS体系　术语

T/CIITA 113-2021　PKS体系　操作系统安全可信技术要求

T/CIITA 114-2021　PKS体系　UEFI固件内置可信启动技术要求

T/CIITA 115-2021　PKS体系　可信网络架构要求

T/CIITA 118-2021　PKS体系　生态软件可信安全认证分发流程

3　术语和定义

T/CIITA 100-2021界定的以及下列术语和定义适用于本文件。

3.1

PK 体系　Phytium/Kylin system

PK system

以飞腾（Phytium）中央处理器（CPU）和麒麟（Kylin）操作系统（OS）为基础的产品、技术、管理、服务、生态、方案和应用的集成系统。

[来源：T/CIITA 100-2021，3.1.1]

3.2

PKS 架构　Phytium/Kylin/security architecture

PKS architecture

基于飞腾（Phytium）中央处理器（CPU）和麒麟（Kylin）操作系统（OS），具有双体系防护结构，具备内生内置安全能力的自主安全体系架构。

[来源：T/CIITA 100-2021，3.1.2]

3.3

PKS 体系　Phytium/Kylin/security system

PKS system

基于PKS架构（3.2　）的PK体系（3.1　）。

[来源：T/CIITA 100-2021，3.1.3]

3.4

安全内存模组　security memory module

具有数据保护功能的内存模组。

3.5

参考板　reference board

某类芯片或某种硬件解决方案的参考设计板卡，用于指导开发人员开展相关的硬件设计及固件与软件的适配工作。

[来源：T/CIITA 100-2021，3.1.4]

3.6

操作系统　operating system

用于管理硬件资源、控制程序运行、提供人机界面，并为应用软件提供支持的一种系统软件产品。

[来源：T/CIITA 100-2021，3.2.2]

3.7

大数据　big data

具有体量巨大、来源多样、生成极快、且多变的等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[来源：GB/T 35295-2017,2.1]

3.8

开发运行框架　developing and running framework

在CPU和操作系统之上，为各种开发语言开发的应用程序提供开发调试的包、库、头文件、驱动、接口的集合。

3.9

容器　container

一种内核轻量级的操作系统层虚拟化技术。

3.10

生态服务平台　ecological service platform

为PKS体系生态软件提供包格式、接口和管理等运行环境支撑及共性服务的系统。

3.11

微服务　microservice

一种如下软件组织方式：应用程序被构建为多个不同的小型服务的集合，可以同时运行多个独立的应用程序，每个程序可以使用不同的编码或不同的编程语言创建。

[来源：T/CIITA 100-2021，3.2.14]

3.12

虚拟机 virtual machine

VM

一种虚拟的如下计算机系统：看起来是在某个特定用户的独占使用下，但其功能是通过共享真实计算机系统的各种资源得以实现的。

[来源：T/CIITA 100-2021，3.2.14]

3.13

云计算平台 cloud computer platform

云服务商提供的云计算基础设施及其上的服务软件的集合。

[来源：T/CIITA 100-2021，3.2.18]

3.14

中央处理器 central processing unit

CPU

由运算器、控制器、寄存器和实现它们之间联系的各类总线，以及包含在同一产品内的其他功能模块组成的集成电路。

[来源：T/CIITA 100-2021，3.1.23]

3.15

PK 体系 Phytium/Kylin system

PK system

以飞腾（Phytium）中央处理器（CPU）和麒麟（Kylin）操作系统（OS）为基础的产品、技术、管理、服务、生态、方案和应用的集成系统。

[来源：T/CIITA 100-2021，3.1.1]

4 缩略语

下列缩略语适用于本文件。

AI 人工智能（artificial intelligence）

B/S 浏览器/服务器（browser/server）

CA 证书认证机构（certification authority）

C/S 客户端/服务器（client/server）

CPU 中央处理器（central processing unit）

eBPF 扩展伯克利包过滤器（extended berkeley packet filter）

IoT 物联网（Internet of things）

JEDEC 联合电子设备工程委员会(joint electron device engineering council)

LSM Linux安全模块（Linux security modules）

OS 操作系统（operation system）

PSPA 飞腾安全平台架构（Phytium security platform architecture）

SDN 软件定义网络（software defined nerwork）

UEFI 统一可扩展固件接口（unified extensible firmware interface）

5 参考架构

5.1 概述

PKS体系参考架构面向办公及事务处理、复杂信息系统、数字化应用及AI应用，适合B/S和C/S等应用模式，由六部分组成：基础硬件层、基础运行层、开发框架层、应用层及安全体系和工程服务体系组成。基础硬件层是PKS体系的硬件基础，包括计算参考板和交换参考板；基础运行层提供PKS体系的基础开发运行环境和工具；开发框架层包括云平台、开发运行框架、外设接入、生态服务平台和领域开发框架，为PKS体系的应用开发运行提供平台支撑；安全体系对应基础硬件层、基础运行层和开发运行框架层分别提供安全可信基础、安全可信服务和安全管理与开发框架支撑，为PKS体系从内至外提供内生安全保障。工程服务体系主要为提供工程服务支撑。参考架构见图1。

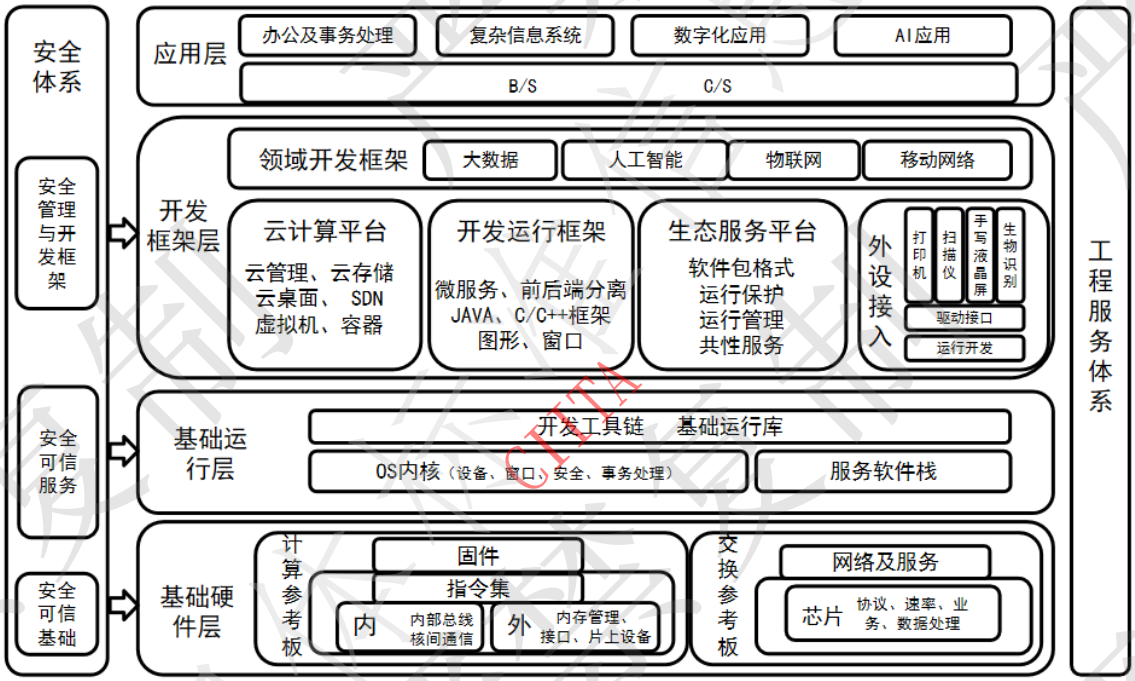

图 1 PKS 体系参考架构

5.2 基础硬件层

基础硬件层应包括如下部分：

a) 以CPU为核心的计算参考板，具有4个子部分：
   1） CPU内部基本技术架构，具备内部总线、核间通信等基本功能性能及主要技术特征；
   2） CPU外部基本技术架构，包括片上设备、内存管理、接口等计算参考板卡架构的主要技术特征，能够展现如何设计参考板和参考板架构；
   3） 指令集,该部分是软硬件接口的基本技术特征，是PK技术体系的生态原点；
   4） 固件，该部分是整机硬件与软件接口的基本技术特征，体现PK计算整机的设备组成、技术路线、软件引导配置以及与操作系统OS对接等整体硬件特征；
b) 以网络交换芯片为核心的交换参考板具有2个子部分：
   1） 网络芯片基本技术架构，包括对网络数据层面的处理功能、业务、速率、协议等，体现网络芯片基本功能性能定位及主要技术特征；
   2） 网络及服务，该部分应能体现参考板整体技术特征，体现交换设备主要网络指标、网络协议及服务。

5.3 基础运行层

以OS为核心的基础运行层应具有3个子部分：

a） 内核基本技术架构，包括设备管理、内存管理、窗口管理、安全管理、事务处理等。

b） 服务软件栈，包括内核之外的常用软件、网络服务、窗口服务、邮件服务、安全服务等基本功能。

c） 开发工具链和基础运行库，包括基本开发规则、库管理、运行环境等，该部分应具有支持的语言、脚本、库的种类、工具等开发运行环境。

5.4 开发框架层

开发框架层为应用场景提供开发环境和框架支持，应具有5个子部分：

a） 云计算平台，包括云管理、云存储、SDN、云桌面、虚拟机、容器等，应支持云和容器管理框架OpenStack、Docker、云桌面等。

b） 开发运行框架，包括Java微服务SpringCloud、SpringBoot、C/C++框架、图形Mesa、OpenGL、QT窗口，支持面向办公和一般事务处理的应用场景以及B/S、C/S场景进行应用开发。

c） 外设接入，具有3个特征：

1） 外设类别，应给出PK支持的外设种类和数量，能够支持的功能效果；

2） 接入方式，应给出外设与主机的接入方式、协议、开发外设接口和数据传输格式；

3） 运行开发，包括驱动开发框架、库、对OS内核的适配等。

d） 生态服务平台系统，主要提供PKS体系生态软件的运行环境支撑和共性服务等，为PKS体系生态软件的运行提供统一的格式、接口和管理策略等。

e） 领域开发框架，包括对大数据、人工智能、物联网和移动网络等开发的支持：

1） 支持大数据，能够支撑常用的大数据分析、挖掘、计算和存储的常用框架、算法；

2） 支持人工智能，支持业界常用的AI框架、算法库、开发组件工具等，为AI应用的开发提供支撑；

3） 支持物联网应用中的基础服务框架、核心框架以及IoT管理协议栈；

4） 支持移动互联网的多种传输和服务协议。

5.5 应用层

PKS 体系面向政府、企业、商业等，可支持多种行业和领域的应用，包括办公与事务处理应用、复杂信息系统应用、智能应用和数字化应用等，支持 B/S 和 C/S 等不同架构模式。

a） 办公与事务处理应用可实现公文处理、即时通信、公文交换及移动应用等常用办公处理能力；

b） 复杂信息系统应用可支持规划、推演、决策和指挥、态势等应用实现；

c） 数字化应用主要包括数字城市、数字政务、数字工厂等方面的应用；

d） 智能应用主要包括语音识别、自然语言处理、机器人及智能预测等智能化应用。

5.6 安全体系

安全体系采用内生安全机制，通过安全可信基础、安全可信服务和安全管理与开发框架分别在基础硬件、基础运行、开发框架各层构建 PKS 体系的安全防护手段，形成安全的 PKS 体系。

a） 安全可信基础，包括飞腾处理器内部的PSPA 框架、密码引擎、可信执行环境以及安全内存模组、安全固件和安全网络架构：

1） 安全内存模组兼容业内JEDEC标准的通用内存条，提供软件定义区域的关键数据关键代码的读写权限管控功能；

2） 安全固件兼容业内通用UEFI字节码和相关技术，详细技术要求见T/CIITA 114-2021；

3） 安全网络架构由网络设备和SDN控制器组成，前者主要包括交换机和路由器，后者指软件

定义网络控制器，详细要求见T/CIITA 115-2021。

b） 安全可信服务应包括3个部分：

1） 密码服务，提供商密、国密等密码体系的挂接，密钥存储管理、CA认证体系，对称密钥、非对称密钥及算法、证书的服务等；

2） 白名单服务，提供文件白名单、程序和脚本、模组白名单、指令白名单的机制运行和管理；

3） 操作系统安全可信机制及服务，包括可信引导、内核安全可信和系统安全可信，具体要求见T/CIITA 113-2021。

c） 安全管理与开发框架，具有安全控制台、安全开发运行框架和生态软件可信安全认证分发，包括LSM、eBPF等linux安全机制，用于挂接具体安全工具模组和安全工具监控或拦截。PKS体系生态软件可信认证具体要求见T/CIITA 118-2021。

5.7 工程服务体系

在基于PKS体系的信息化系统集成项目实施过程中，由专门机构负责提供专业化和系统性的技术服务支持。除符合一般性要求外，还要在方案编制、工程实施、服务保障三方面符合特定要求。