PHYTIUM 飞腾

PSPA1.0白皮书

PHYTIUM SECURITY PLATFORM ARCHITECTURE 1.0
White Paper

2019/12 V1.0

飞腾信息技术有限公司
www.phytium.com.cn

目录

术语与缩略语

缩写	全称	描述
PSPA	Phytium Security Platform Architecture	飞腾安全平台架构
TEE	Trusted Execution Environment	可信执行环境
REE	Rich Execution Environment	丰富执行环境
API	Application Programming Interface	应用编程接口
PBF	Phytium Base Firmware	飞腾基础固件
PBR	Phytium Boot ROM	飞腾启动 ROM
OTP	One Time Programmable	一次可编程器件

01 前言

安全可信始终是信息系统最基础、最核心的目标，随着国产信息系统建设不断深入，实现系统的安全可信已经成为迫切的现实需求。其中，基础处理器芯片的安全属性和功能对系统安全性起到至关重要的决定性作用。飞腾致力于自主处理器的研发和推广，以打造高性能国产安全处理器为重要目标，为固件、整机、操作系统、应用等软硬件厂商提供安全的基础处理器产品，并助力安全可信应用的落地实现和推广。

安全可信处理器是一个完整的安全体系，需要从体系架构和软硬件总体上去定义和设计。为了安全可信应用的真正落地，必须联合生态圈内相关企业，基于稳定清晰统一的处理器安全平台架构规范进行研发、适配和推广。通过遵循统一的安全规范，可以充分发挥生态圈上下游厂家的合力。

为了统一飞腾安全可信处理器的属性和功能，规范软硬件厂商的接口，我们推出了飞腾安全处理器平台架构规范（Phytium Security Platform Architecture）。PSPA 定义了芯片安全相关的软硬件规范，目前推出的是 1.0 版本。PSPA 1.0 从十个方面定义了安全处理器中涉及的软硬件功能和属性。通过遵循该规范，既可以使飞腾安全处理器的定义和实现有规可循，避免安全短板，支撑全方位的系统安全；又可以给生态圈中各厂商提供清晰规范的软硬件接口定义，助力生态圈中各企业安全产品的实现和推广。

本白皮书的目的是对 PSPA 1.0 及其涉及的十个方面的安全内涵进行概要介绍。具体的规范定义请参见 PSPA 1.0 规范详细文本。

02 总体框架

处理器安全存在木桶效应，需要全方位考虑各类软硬件安全措施，防止出现系统短板，才能有效保障处理器硬件安全，进而构建安全可信的信息系统。PSPA 1.0 主要包含十个方面内涵，即：密码加速引擎、密钥管理、可信启动、可信执行环境、安全存储、固件管理、量产注入、生命周期管理、抗物理攻击及硬件漏洞免疫。具体如图 1 PSPA 总体框架所示。

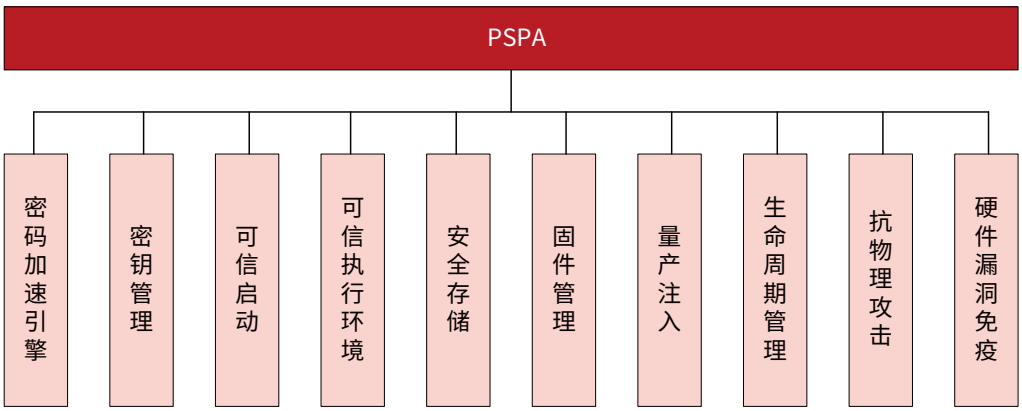

图 1 PSPA 总体框架

PSPA1.0 包括密码密钥相关的内容，即密码加速引擎、密钥管理；包括可信相关的内容，即可信启动、可信执行环境；包括敏感信息和固件保护的相关内容，即安全存储、固件管理；包括芯片生产及全寿命周期管理的相关内容，即量产注入、生命周期管理；包括抗物理攻击及硬件漏洞免疫相关内容。PSPA 1.0 是一个比较完备的系统安全架构规范。遵循该规范，可以防止出现安全短板，有效提升处理器的安全特性。

03 安全内涵

3.1 密码加速引擎

密码加速引擎是指通过硬件方式实现密码运算功能，提升密码运算的速度，降低功耗。PSPA 1.0 要求处理器芯片具备专用的硬件密码加速引擎或加速指令，并且具备专用的物理随机源以生产符合国家相关标准的随机数。

PSPA 1.0 对处理器芯片密码加速引擎的要求包括以下几个方面：

- 至少支持对称算法、非对称算法、哈希算法三类算法加速。
- 必须支持 SM2、SM3、SM4 三种商密算法加速。
- 支持专用指令或者 API（Application Programming Interface）的方式调用密码加速引擎，以实现密码计算加速。
- 片内至少集成两个独立的物理随机源，产生的随机数满足《GM/T 0005-2012 随机性检测规范》规定的随机数检测要求。

3.2 密钥管理

密钥管理是指对芯片内部密码运算所使用的各种密钥的管理，包括密钥的生成、存储、访问、使用等。安全处理器中密钥定义为三类：芯片厂商密钥（飞腾密钥）、整机厂商密钥和用户密钥。其中芯片厂商密钥由芯片厂商注入并可以被芯片厂商、整机厂商及用户使用，但不可被整机厂商及用户读写，整机厂家密钥由整机厂商注入并使用，但不可被芯片厂商及用户访问和使用，用户密钥由用户注入并使用。

PSPA 1.0 对密钥管理的要求包括以下几个方面：

- 密钥生成：芯片厂商密钥在芯片的生产过程中由芯片厂商通过可靠手段注入；整机厂商密钥由整机厂商在整机生产环境注入；用户密钥由用户自行注入。
- 密钥存储：芯片厂商密钥和整机厂商密钥存储在片内非易失性存储器件中，且不能出芯片，用户密钥可以存储在片内非易失性存储器件中，也可以由用户程序决定存储在其它位置。
- 密钥访问：不同种类的密钥在不同生命周期状态下，具有不同的访问权限，只有特定的生命周期状态下，才能读写特定的密钥。
- 密钥使用：芯片厂商密钥和整机厂商密钥在特定生命周期状态下，不能由软件读写，但是仍然可以由密码加速引擎使用该密钥，且只可应用于相关计算，不能存储或转发。用户密钥的

使用方式由用户定义。

3.3 可信启动

可信启动，是指安全处理器启动过程中，所有被执行的代码、引入的数据都是通过度量认证的。可信启动原理是在启动过程中建立一条基于逐级验签认证的信任传递链，其前提是存在一个无需验证、确保可信的基础启动模块，称为可信根。PSPA 1.0 要求可信根存储在片内不可篡改的存储介质中，由可信根对下一步启动流程引入的代码、数据进行验签。被可信根验签过的代码执行时，会对由其引入的代码和数据进行验签。以此类推，在整个启动过程中，各个模块对必须对由其引入的代码和数据进行验签，实现信任链的传递，保证启动过程执行的所有代码都是可信的。

飞腾平台的固件架构分为三个层次：芯片内置的飞腾启动 ROM（Phytium Boot ROM，PBR）、飞腾基础固件（Phytium Base Firmware，PBF）和第三方固件。PBR 保存在飞腾安全处理器芯片内，无法被篡改。系统加电后，执行 PBR，其主要的功能是验签位于片外非易失存储介质上的 PBF，如果验签通过则加载 PBF。PBF 的主要功能是完成处理器的基本硬件初始化，然后验签、加载第三方固件。验签通过后，即跳转到第三方固件执行。第三方固件按照逐级验签的模式，依次加载、验签、执行后续模块，进而引导操作系统。具体的可信启动流程如图 2 可信启动流程所示。

图 2 可信启动流程

PSPA 1.0 对可信启动的要求包括以下几个方面：

- PBR 必须位于片内不可篡改的存储空间。
- PBR 对片外 PBF 进行验签，再由 PBF 对第三方固件进行验签，以此逐级扩展、建立信任链。
- 启动过程中任何软件代码和数据在加载使用前，必须经过前一级软件的验签并通过。
- 对于关键的固件或数据，可以采用加密的方式存储在片外，在可信启动过程中需要对其进行解密后再验签。

3.4 可信执行环境

可信执行环境（Trusted Execution Environment，TEE）是指在处理器内部通过硬件资源隔离方式建立一个独立的安全区域。与 TEE 对应的为丰富执行环境 REE（Rich Execution Environment），REE 与 TEE 在硬件上完全隔离。但是 TEE 具有更高的安全级别，REE 不能访问 TEE 的相关资源，以此保护 TEE 内部代码和敏感信息的安全性。TEE 与 REE 之间有相应的通信机制，REE 可以请求 TEE 为其提供安全服务。同时 TEE 所有出片数据都必须经过加密，不得明文出片。

PSPA 1.0 对可信执行环境的要求包括以下几个方面：

- 硬件支持资源隔离，将系统划分为 TEE 和 REE，TEE 的安全级别更高，REE 无法访问 TEE 内部资源。
- 支持安全监控固件、安全操作系统内核（TEE-OS）、可信应用（TA）及 REE 侧的接口库等软件架构。
- TEE 与 REE 之间支持安全通信机制。
- 支持对 TEE 所使用的安全内存空间实时加解密，即对写入安全内存空间的数据进行实时加密，读出时再实时解密。

3.5 安全存储

安全存储是指提供一个安全的存储环境，用来保护口令、密钥、证书、会话标识、隐私数据等信息。非易失性存储系统作为数据的保存空间，容易受到攻击。一旦受到攻击，可能导致其中的敏感信息被窃取、篡改或破坏。因此，安全存储非常重要，而安全存储的核心技术是数据加密技术。

PSPA 1.0 对安全存储的要求包括以下几个方面：

- TEE 所有需要存入片外非易失存储器的敏感数据，都支持加密存储。
- 安全存储的加解密过程都在 TEE 内完成，且加解密的密钥只能在 TEE 内生成、存储、使用。

3.6 固件管理

固件存在版本更新的需求。固件管理就是指在固件的版本更新过程中，对固件内容、固件版本、固件备份等进行管理。

飞腾平台固件包括飞腾启动 ROM PBR、飞腾基础固件 PBF 和第三方固件。其中，PBR 固件在芯片出厂时固定，无法更新；PBF 固件由飞腾负责维护；第三方固件由整机或固件厂商维护。

PBF 和第三方固件更新时，必须对固件内容进行检查，保证固件来源的合法性。为了防止固件回退至不安全的版本，PBF 和第三方固件还必须具备版本防回滚机制。固件更新可能失败，需要引入相应的容错机制，对固件加以备份。

PSPA 1.0 对固件管理的要求包括以下几个方面：

- 固件更新前必须进行内容合规检查。
- 固件更新必须具有版本防回滚机制。
- 支持具有固件备份机制，防止更新失败。

3.7 量产注入

量产注入是指飞腾安全处理器在量产过程中，在测试产线上通过一定的安全手段进行最初始的密钥灌注的过程。由于测试产线环境本身的安全性难以得到保证，因此必须通过一定的技术手段，防止安全芯片中最重要的初始密钥在产线灌注过程中被泄露。要求在测试机台旁边放置受控的密钥灌注控制终端，该终端通过安全链接与远程服务器进行通信，远程服务器下发密钥并进行登记，当芯片在测试机台上测试通过以后，由灌注控制终端控制测试机台进行初始密钥的灌注。具体的结构如图 3 量产注入所示。

PSPA 1.0 对量产注入的要求包括以下几个方面：

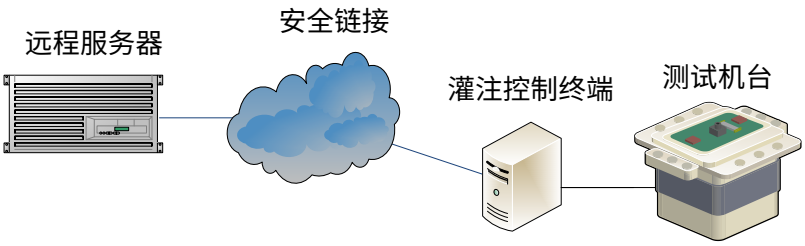

图 3 量产注入

- 远程服务器与灌注控制终端之间采用安全链接，两者之间的所有通信是安全、可靠的。
- 远程服务器需要对灌注控制终端进行身份鉴别。
- 灌注控制终端通过安全、可靠的接口将初始密钥灌注到机台测试通过的芯片中。

3.8 生命周期管理

生命周期管理是指对芯片全生命周期中被使用和流转过程的管理，覆盖从芯片生产到交付整机厂商，再由整机厂商将其作为整机的一部分交付最终客户的全生命周期过程。在生命周期的不同阶段，控制不同的密钥及调测试接口具有不同的访问使用权限，以此保证芯片属于不同所有者时，具有不同所有者相对应的安全特性和权限。

PSPA 1.0 对芯片生命周期的要求包括以下几个方面：

- 至少实现芯片厂商所有、整机厂商所有、用户所有、返厂至整机厂商、返厂至芯片厂商五个生命周期状态。
- 通过片内一次可编程存储器（One Time Programmable，OTP）内存储的数据特征表征不同的生命周期状态，通过 OTP 烧写的不可逆性保证生命周期状态的变迁顺序的不可逆性。
- 不同的生命周期状态下，对不同的密钥具有不同的访问和使用权限。
- 不同的生命周期状态下，对调试、测试接口具有不同的使用权限。

3.9 抗物理攻击

物理攻击是指攻击者针对芯片实体所做的破坏或者非破坏性攻击。物理攻击方式主要包括错误注入攻击、侧信道攻击与侵入式攻击等几大类。错误注入攻击是指通过抖动电源与抖动时钟等手段，使电路产生错误操作，影响个别指令或某个电路的执行。侧信道攻击是指通过测量分析芯片的功耗、电磁等信息，获取芯片内部的敏感信息。侵入式攻击是指通过打开芯片的封装，使用探针检测或修改电路以获取芯片内部信息。

PSPA 1.0 要求芯片具有一定的抗物理防护功能，以支持芯片安全可靠运行。

PSPA 1.0 对抗物理攻击的要求包括以下几个方面：

- 必须具备电压、时钟、温度传感器，对相应的错误具备检测功能，并能够采取相应措施进行防护。
- 密码引擎计算时具备运行时间随机、功耗随机或功耗平滑等技术防范手段，防止功耗、电磁

- 等侧信道信息泄露。
  可选顶层金属覆盖、侵入检测电路等技术手段，提升侵入式攻击的难度。

3.10 硬件漏洞免疫

计算机系统由底层硬件、系统软件、应用软件组成，而底层硬件又包含处理器核、内存、外设等，是一个非常复杂的系统。正是由于计算机系统的复杂性，其面临的安全风险也是复杂多样的。处理器如果存在安全漏洞，将会产生严重后果，可以使攻击者能够在未授权的情况下访问或破坏系统。处理器漏洞往往与计算机系统结构或硬件具体实现有关。在进行计算机系统或安全芯片设计的时候，必须充分考虑处理器与系统软件存在漏洞的可能性，设计系统级防范措施。针对各种重要漏洞，计算机系统能够从硬件角度进行安全防护，我们称之为硬件漏洞免疫。目前最著名的硬件漏洞包括 Spectre（幽灵）、Meltdown（熔断）及其各种变种。

PSPA 1.0 要求芯片支持典型的硬件漏洞免疫机制，具有一定的硬件漏洞免疫能力。PSPA 1.0 对硬件漏洞免疫的要求包括以下几个方面：

- 支持分级访问控制，应用软件及系统软件具有不同的访问权限。
- 支持数据执行保护机制，非代码段的数据禁止运行。
- 支持内核保护机制，不允许内核直接执行用户态代码。
- 支持面向返回的编程（ROP，Return-Oriented Programming）攻击防护，可以通过软件或硬件的手段来防止栈溢出或阻止栈溢出执行。
- 对于内存中的数据，支持不允许 Load 指令前瞻执行；对于特殊功能寄存器 SPR，支持不允许 SPR 读指令前瞻执行。

04 结束语

为了应对目前信息系统面临的越来越严峻的安全形势，提升作为信息系统核心的处理器的自身硬件安全，并且为安全应用生态圈内上下游厂商提供一个清晰的安全架构规范，飞腾发布了 PSPA 1.0 规范定义。该架构定义涵盖了十个方面的安全内涵，并对其中的每个方面都提出了详细的定义。遵循该规范，可以有效防止处理器出现安全短板，提升处理器的安全性。

需要注意的是，安全的范畴和内涵是不断发展的。因此，PSPA 也将随之不断演进，未来将根据硬件安全的发展，不断推出更新的版本，力争探索出一条具有中国特色的安全架构规范之路。飞腾还将不断推出符合 PSPA 标准的安全处理器，并且和上下游厂商一道推动各安全应用在飞腾平台上的实现和推广，为我国的安全可信事业不断贡献新的力量。

PHYTIUM 飞腾

天津总部
地址：天津市滨海新区海缘中路
1号信安创业广场5号楼
邮编：300459
电话：(+86) 022 59080100

北京分公司
地址：北京市海淀区知春路
27号量子芯座8层
邮编：100191
电话：(+86) 010 62001812

长沙分公司
地址：湖南省长沙市开福区三一大道
526号旺德府凯悦国际大厦写字楼10楼
邮编：410100
电话：(+86) 0731 84930100

广州子公司
地址：广东省广州市番禺区大学城外环西路100号
广州国家集成电路基地（GZICC），3楼326室
邮编：510006
电话：(+86) 020 39337889