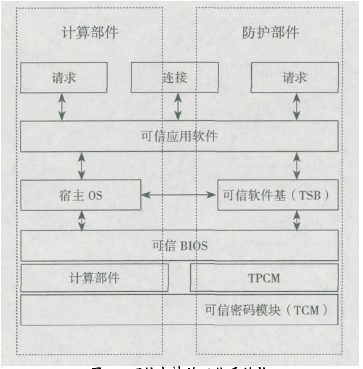
# 工业无线安全

## 安全需求和问题

可信计算是指计算运算的同时进行安全防护，计算全程可测可控，不被干扰，只有这样方能使计算结果总是与预期一样。改变只讲求计算效率，而不讲安全防护的片面计算模式。

在图１所示的双体系结构中，采用了一种运算和防护并存的主动免疫的新计算模式，以密码为基因实施身份识别、优态度量、保密存储等功能，及时识ｓｉ自己”和“非己”成分，从而破坏与排斥进入机体的有物质，相当于为计算机信息系统±咅育了免疫能力。



目前，可信计算已经成立国际组织TCG.

ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）将可信定义为：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．ＴＣＧ的可信计算技术思路是通过在硬件平台上引入可信平台模块ＴＰＭ（ｔｒｕｓｔｅｄ　ｐｌａｔｆｏｒｍ　ｍｏｄｕｌｅ）来提高计算机系统的安全性，这种技术思路目前得到了产业界的普遍认同．我们的思路与ＴＣＧ类似，认为可信是指以安全芯片为基础，建立可信的计算环境，确保系统实体按照预期的行为执行．

## 国内外研究进展

可信计算的基本思想是

1、首先计算机系统建立一个信任根，信任根的可信性由物理安全、技术安全、和管理安全共同确保。

2、再建立一条信任链，从根开始到硬件平台, 到操系,到软件系统，到应用体系，到可信网络，逐步建立信任级, 把信任扩展到整个计算机系统, 从而确保整个计算机系统的可信，信任链如图所示

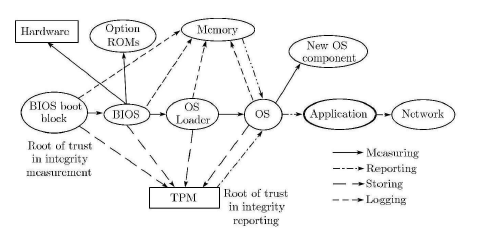


Figure 信任链

### 可信根和可信链

可信根是可信计算的基础，为保证可信，必须先建立一个最初的可信根。

可信根应该满足几个要求：

1. 可信根应该具有密码服务功能。
2. 可信根具备对系统启动过程的度量能力。
3. 可信根具备对系统启动过程的控制能力
4. 可信根优先于其他部分启动。

可信2.0框架由可信平台模块（TPM）以及度量代码段（CRTM）组成。其结构如图所示。

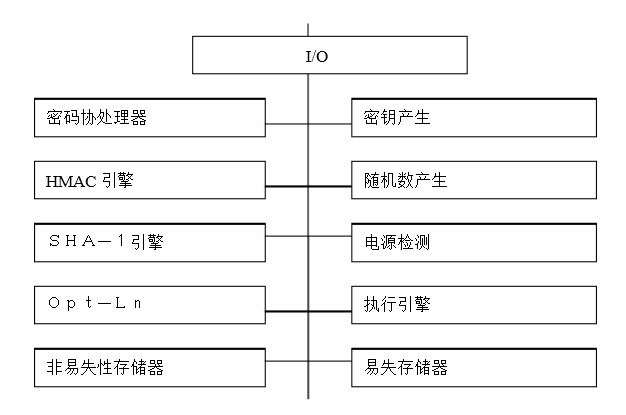


Figure TPM结构

可信3.0提出以可信平台控制模块(TPCM)作为系统可信根。由可信密码模块（TCM）和平台控制机制组成。

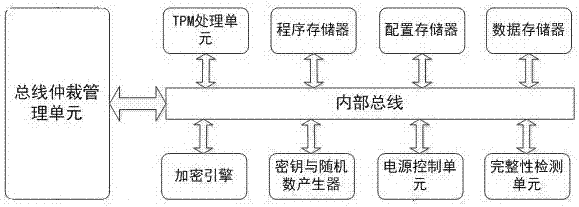


Figure 可信平台控制模块（TPCM）示意图

TPMCM先于 CPU启动，通过平台控制功能获取系统的控制权，并对系统进行可信度量，只有度量通过后，将控制权开发给系统。

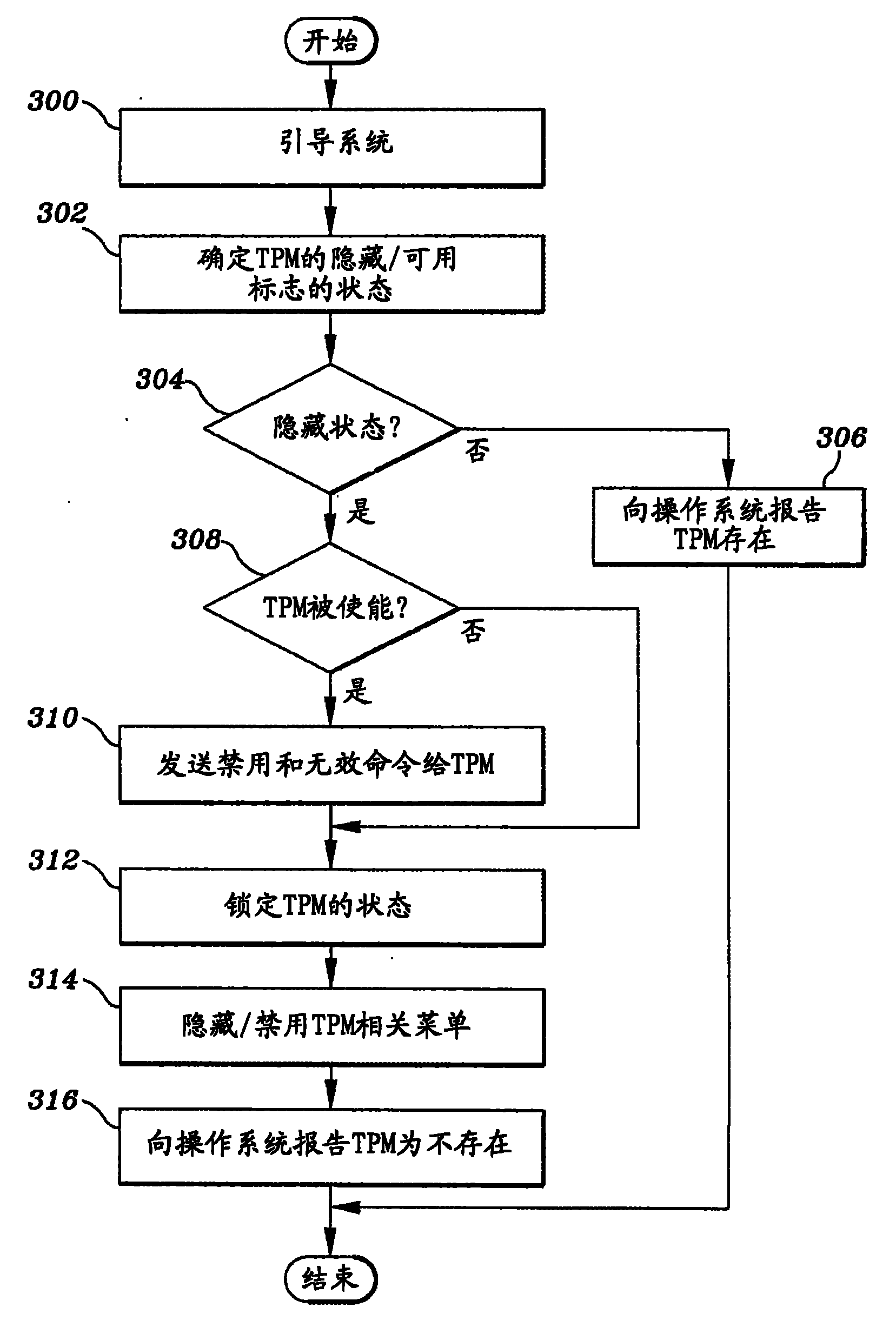


Figure 可信计算系统启动示意图

### 可信存储

TCG于2007年5月推出了TCG的存储体系结构核心规范。技术来源于细节DriveTrust技术。

DriveTrust 技术利用硬盘的封闭计算环境，定义基于硬件安全功能的硬盘级平台。该技术认为虽然操作系统专门设计用来支持各种应用程序，但硬盘是运行专用代码(固件)管理硬盘功能的封闭存储环境。因为其内部操作与计算系统的其他组件相隔离，故硬盘是实现数据安全功能的理想位置。该技术认为DriveTrust 平台不仅仅能够保护磁盘上存储的数据，该平台还在主机与硬盘之间建立对所发送数据的信任，并使硬盘能够对应用程序进行验证、分配安全存储分区、处理数字签名并提供多种其他安全功能

Drive Trust 技术包含四个元素：

（1）增强型固件和硬件：固件是在硬盘内部计算机中运行的软件；通常，固件用于管理极为复杂的硬盘功能，如移动读取/写入磁头、跟踪磁盘上的坏扇区以及存储数据位置的位图。DriveTrust 技术添加优化硬盘存储资源的其他安全代码，扩展了硬盘的功能。DriveTrust 技术在硬盘中实现加密服务，它提供加密、散列、安全存储、解密、数字签名和随机数字生成等功能。

（2）可信发送/接收命令集：可信存储需要安全的通信基础架构。Drive Trust通信通过可信发送/接收（出/入）命令集发送。该命令集用于协调定义 ATA 和SCSI 接口的标准组织。ATA 和 SCSI 接口协议中包括安全消息传递的内容，以支持包括 DriveTrust 技术在内的安全技术支持。

（3）安全分区：200GB 的硬盘保留约 200MB 不可寻址空间，用于内部系统内存。Drive Trust 技术使用此空间创建安全分区，该分区在逻辑上和物理上均与硬盘存储的其余部分相独立，使用有效的条件访问控制，所以该安全分区也是存储加密密钥的最佳位置。如果硬盘采用 DriveTrust 技术，则只有提供正确凭证的应用程序能够访问上述安全分区，并在其中存储应用程序代码、其他内容或数据。ISV（Independent Software Vendors 的英文缩写，意为“独立软件开发商）可利用该功能构建具有其他功能的应用程序，如增强的身份验证、时间戳、对比日志记录或事务数据。

（4）隔离协议：软件应用程序、基本输入/输出系统和其他程序均可通过严格控制的通信渠道与应用 DriveTrust 技术的硬盘互操作。ISV 和其他开发商可以编写应用程序，并通过隔离协议将它们分配给硬盘中的安全分区。如果应用程序尝试访问这些安全分区，则必须向硬盘的管理员功能模块提供根据管理协议分配的凭证。管理员功能模块对应用程序进行验证，激活相应的安全分区，从而允许该应用程序通过可信发送/接收命令集与安全分区交互。

可信存储的可信源头来源于可信根中的存储根密钥（SRK）。它存放于内部，永远不对外暴露。

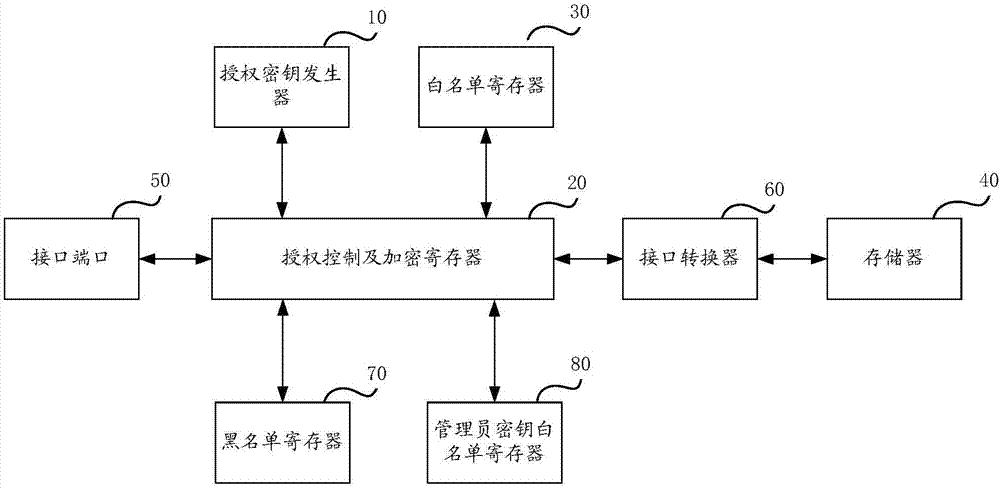


Figure 密钥可信存储示意图

### 可信度量

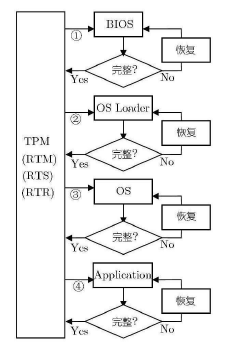


Figure 简单的度量模型

信任链的起点是信任根，信任链的传递则是依靠可信度量技术来实现。在信任链的理论中，无论是最底层的 BIOS 启动模块还是到最上层的应用，在得到信任以运行之前，都需要经过度量，即一个测量者认证的过程。数据完整性度量技术通过消息认证码 MAC（Message uthentication Code）的一致性校验来实现度量的功能。这是现在主的度量技术方法。对于 MAC 的产生，可以利用强的分组密码或者利 ASH 函数来实现。TPM 中提供了满足单向性、抗碰撞性的安全 HASH 数 SHA-1 引擎，可以为度量的实现提供保证。 同时 TPM 还提供安存储以及内部的平台配置寄存器 PCR（Platform Configuration egister），样配合 TPM 的内部接口函数就可以把信任链传递下去。可信度量的新以及实际应用都是以平台配置寄存器 PCR 作为载体的。

一个平台中可能会有大量的完整性度量，一个特殊的完整性度量需要实时地存储更新的值。一个完整性度量的新值不允许简单地覆盖现存的值。因为这样难以鉴别完整性度量的度量来源，而且攻击者可能擦除或者替换一个正确值。如果完整性度量值个别地存储，更新值也要个别地存储，那么就难以定位存储空间的大小。作为可信度量存储载体的 PCR 就是在寄存器中支持无限的度量数量。它通过使用密码学的哈希算法对更新的 PCR 做哈希（消息摘要）。伪代码如下：

PCRi New = HASH ( PCRi Old value || value to add)

新的 PCR 值产生过程中对两部分进行了哈希，一是旧的 PCR 值，一是所增加的新数据。这样更新 PCR 的顺序是不可交换的，例如度量从 A 到 B，并不等于从 B 到 A 的度量。哈希值的另外一个特性是单向的。这意味着对于攻击者要确定输入给 PCR 的值在计算上不可行。此后更新 PCR 若没有前一个 PCR 值作为基础将不能进行。或者在重启之后，如果所有提供给 PCR 寄存器的信息缺失，后续的更新 PCR 也不能进行。 另外，在使用一个 PCR 过程中，对于 TCG 平台规范明确规定忽略的事件，度量值便不用更新。如果 PCR 已经度量过最少一个某种类型的事件，那么该类事件也可以忽略。这样就可以避免频繁记录某些重复的状态（如睡眠状态），以便延长 TPM 的使用寿命。软件数据完整性是信息安全的重要部分，但是，软件数据完整性还不能保证动态的安全性。所以上层应用软件的度量除了完整性检测度量之外，还需要借鉴其他一些度量方法。

随着现代软件的功能越来越完善，软件代码的规模也越来越庞大，度量的数据量也超乎寻常，需要对软件程序有所选取地进行度量。通过层次分析法，尽可能多地列举多种可能的度量方面，并计算出每个方面的权重值，以确定最重要的度量点。 其次对应用软件进行可信级划分，对于基本不可信以及可信程度低的软件，则不能通过度量。外因为软件的模糊性，需要引入专家评估系统，对应用软件的等级进认定。只有通过完整性检验并且等级被认定为可信的软件才能得到操作系统的授权运行。

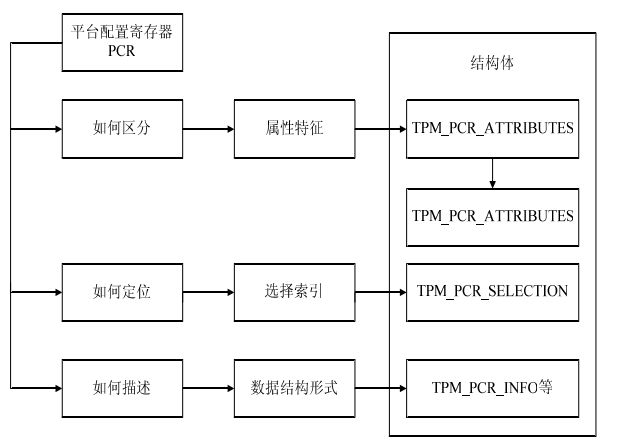


Figure 可信度量存储体系

### 可信软件

TCG组织提出的可信软件栈TSS(TCG Software Stack)是与TPM进行交互的核心软件部件，其作用主要是为操作系统和应用程序提供使用TPM的接口，并提供增强TPM功能的函数，是TPM与上层应用之间的桥梁。

TSS的主要功能如下：

1）为应用程序提供到TPM功能服务的单入口点。

2）按标准构建字节流隐藏应用程序锁构建的复杂命令流格式。

3）提供对TPM的同步访问控制。

4）对TPM的资源进行管理。

TSS由四个层次组成，由上向下分别为：TSS服务提供者TSP(TCG Service Provider)，TSS核心服务TCS(TCG Core Services)，TCG设备驱动库TDDL(TCG Device Driver Library)，以及TPM设备驱动TDD(TPM Device Driver)。TSP为应用程序直接提供接口函数，TCS向上为TSP提供通用服务，TDDL提供TSS用户模式与内核模式的接口函数，TDD直接驱动TPM芯片。

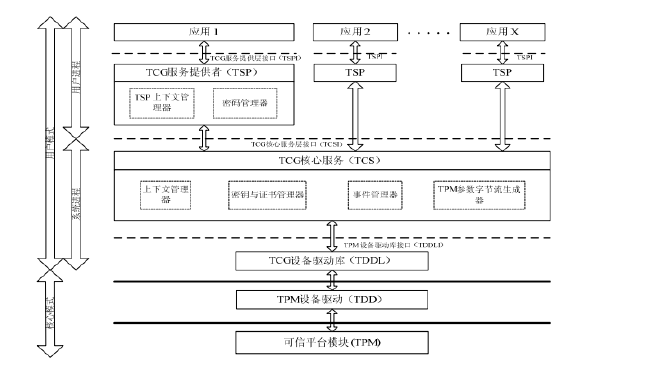
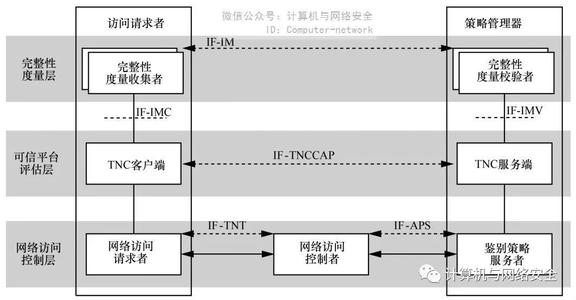


Figure TCG可信计算结构框架

### 可信网路连接

可信网络连接（Ｔｒｕｓｔｅｄｎｅｔｗｏｒｋｃｏｎｎｅｃｔｉｏｎ，ＴＮＣ）是通过对信任链的建立，然后将可信计算平台的可信性延伸到网络环境来实现整个网络可信的网络连接。可信网络连接的核心思想是：通过对请求连接的终端平台的可信性进行验证，根据其可信性对终端的接入进行控制，来确保网络连接环境的可信。可信网络连接的基础架构如图３．５所示，架构对网络终端接入的过程、连接的方式、通讯协议等进行了整合，同时与传统的信息安全防御设备、网络行为控制等设施进行了交互。在可信网络连接架构下，终端可信平台不再是孤立可信任点，相应的网络控制设施的加入更是对可信网络信任链的建立提供了有力的保障，使整个信任链处在安全的环境中

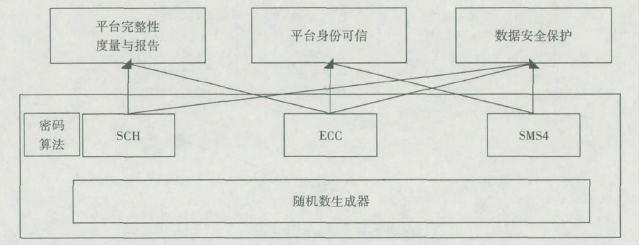
可信网络连接框架由５个实体、３层结构以及多个对象接口组成，５个实体分别是访问请求者ＡＲ、策略执行点ＰＥＰ、策略决定点ＰＤＰ、元数据存取点ＭＡＰ和网络行为控制和监控点。

ＴＮＣ接入策略为：访问请求者发出接入请求，报告其可信完整性给策略决定点，请求接入，策略决定点通过安全策略对访问请求者的接入访问进行判别，然后根据访问请求者的报告信息决定其接入控制，再由策略执行点对其接入进行决策。而元数据服务器作为可信网络连接的接入终端连接完整性、策略信息等存储中心，对申请接入的终端的连接信息进行储存；网络行为控制和监控点作为可信网络连接的控制终端，对可信网络接入点的完整性、接入策略等信息向元数据存取点进行报告，同时根据元数据存储点中存储的相关信息对接入终端的连接进行管理。

## 待解决的问题和后续研究

1 密码体制的局限性

ＴＣＧ原版本只采用了公钥密码算法ＲＳＡ，杂凑算法只支持ＳＨＡ１系列，回避了对称密码。由此导致密钥管理、密钥迁移和授权协议的设计复杂化（５类证书、７类密钥），也直接威胁着密码的安全。在未来，希望采用了我国对称非对称结合的密码体制，保证自主可控。

在密码算法上，全部采用国有自主设计的算法，定义可信计算密码模块（ＴＣＭ）；在密码机制上，对称密码与公钥密码相结合，提高了安全性和效率；在证书结构上，采用双证书结构，简化了证书管理，提高了可用性和可管性。

2体系结构的合理性

ＴＣＧ采用外挂式结构，未从计算机体系结构上作变更，把可信平台模块（ＴＰＭ）作为外部设备挂接在外总线上。软件上，可信软件栈（ＴＳＳ）是ＴＰＳ的子程序库，被动调用，无法动态主动度量。

3结合区块链技术的可信存储技术

TCG规范中，使用硬盘的封闭计算环境，定义基于硬件安全功能的硬盘级平台。通过增强型固件和硬件、可信发送/接收命令集、安全分区、隔离协议等技术进行可信存储，但是随着分布式技术和物联网的发展，分布式数据管理逐步成为数据系统中的重要手段，而原本的这种集中存储方式面临数据恶意篡改、单点故障攻击等风险。针对这些信息安全问题，利用区块链分布式存储技术的去中心化、防篡改、高度可拓展等特征为分布式的高效可信存储提供有效的解决方案



## 研究内容和技术路径

1. 自主可控的可信密码模块

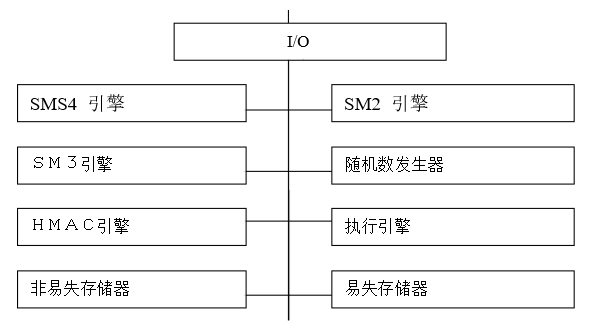


Figure 1自主可控的可信密码模块

TCM 定义了一个具有存储保护和执行保护的子系统，该子系统将为计算平台建立信任根基，并且其独立的计算资源将建立严格受限的安全保护机制。为防止TCM 成为计算平台的性能瓶颈，将子系统中需执行保护的函数与无需执行保护的函数分开，将无需执行保护的功能函数由计算平台主处理器执行，这些功能函数构成TSM。

TCM 结构如图所示，各部件功能如下：

I/O：TCM 的输入输出硬件接口；

SMS4 引擎：执行SMS4 对称密码运算；

SM2 引擎：产生SM2 密钥对，执行SM2 加/解密、签名

运算；

SM3 引擎：执行杂凑运算；

随机数产生器：生成随机数；

HMAC 引擎：基于SM3 引擎，计算消息认证码；

执行引擎：TCM 的运算执行部件；

非易失性存储器：存储永久数据的存储部件；

易失性存储器：TCM 运行时的临时数据存储部件。

可信计算密码支撑平台涉及密码算法包括：SM2 椭圆曲线密码算法、SMS4 对称密码算法、SM3 密码杂凑算法、HMAC 消息认证码算法、RNG（随机数发生器）。SM2 椭圆曲线密码算法，密钥长256 位，包括：系统参数、密钥对生成和三个子算法，三个子算法分别是：数字签名算法(SM2-1)、密钥交换协议(SM2-2)、加密算法(SM2-3)。SMS4 是对称密码算法，分组长度为128bit，密钥长度为12bit，加密算法和密钥扩展算法都采用32 轮非线性迭代结构，加、解密算法的结构相同，只是轮密钥的使用顺序相反。规范要求采用CBC 模式，Ⅳ由用户自定义，数据的最末分组(128bit/16byte)需填充，如果最末数据分组长度为16byte，则在其后填充16 个内容为16 的byte，否则按最末数据分组不足16byte 所缺少的字节个数d，填充d 个内容为d 的byte。

SM3 密码杂凑算法，对给定的长度为k(k<264)的消息，经填充、迭代压缩和选裁，生成杂凑值，迭代压缩时，输入为预处理的消息分组64byte，输出摘要为32byte。HMAC 消息认证码算法，利用密码杂凑算法SM3，对给定的消息和验证双方共享的密码信息产生长度为t(16≦t≦32)个字节的消息验证码，计算公式：HMAC＝SM3((K0⊕opad) || SM3((K0⊕ipad) || text))[2]，TCG 规范对TPM 要求

HMAC 消息认证码算法使用支持20byte 的SHA-1 算法[3,4]。RNG，规范不限定随机数生成的算法，算法由TCM 制造商设计实现，要求所生成的随机数必须为真随机数，并满足国家商用密码随机数检测要求。

1. 构建主动免疫体系

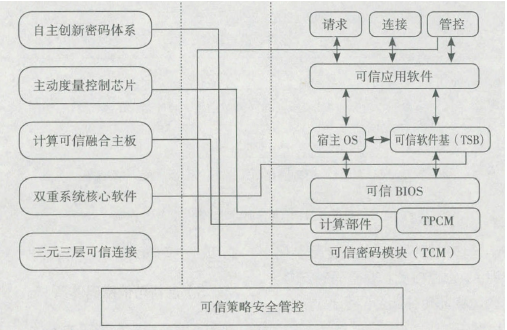
在双系统体系框架下，采用自主创新的对称非对称相结合的密码体制，作为免疫基因；通过主动度量控制芯片（ＴＰＣＭ）植入可信源根，在ＴＣＭ基础上加以信任根控制功能，实现密码与控制相结合，将可信平台控制模块设计为可信计算控制节点，实现了ＴＰＣＭ对整个平台的主动控制；在可信平台主板中增加了可信度量节点，实现了计算和可信双节点融合；软件基础层实现宿主操作系统和可信软件基的双重系统核心，通过在操作系统核心层并一个可信的控制软件接管系统调用，在不改变应用软件的前提下实施主动防御；网络层采用三元三层对等的可信连接架构，在访问请求者、访问控制者和策略仲裁者之间进行三重控制和鉴别，对访问请求者和访问控制者实现统一的策略管理，提高系统整体的可信性。

Figure 主动免疫体系结构