可信计算技术原理与应用

服务计算技术与系统教育部重点实验室　　集群与网格计算湖北省重点实验室

标准化组织

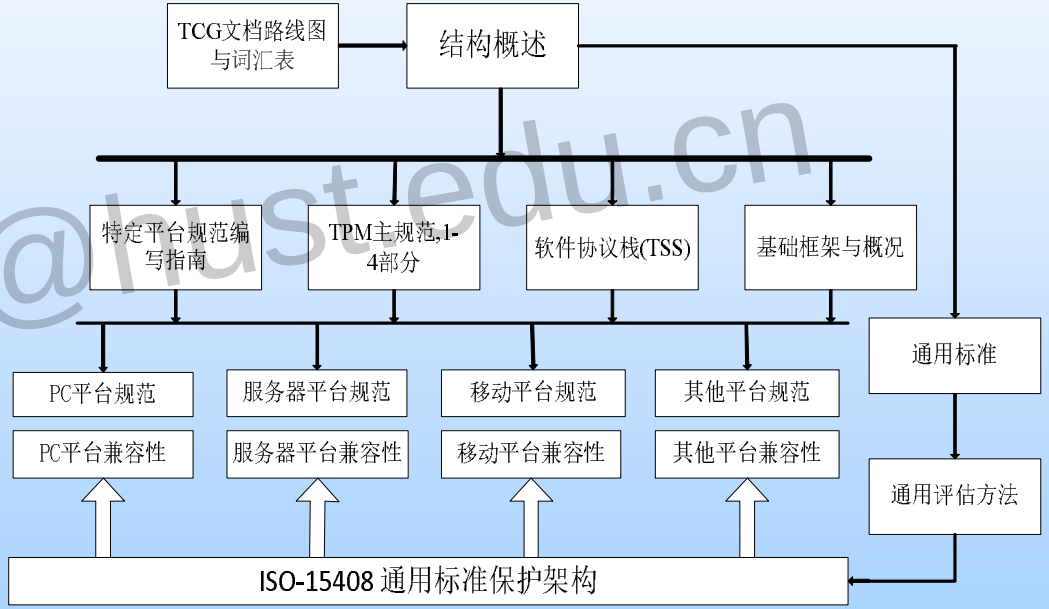
- 国际标准化组织
  - **ISO**：国际标准化组织
  - **IEC**：国际电工委员会
  - **ITU**：国际电信联盟标准
  - **IEEE**：美国电气与电子工程师协会标准
  - **… …**
- 中国标准化组织
  - 国家标准化管理委员会（隶属国家质检总局）
  - 农业部市场与经济信息司（农业）
  - 国家林业局科技司
  - 国家药品监督管理局医药司、医疗器械司
  - 民政部人事教育司
  - 教育部语言文字信息管理司（语言）
  - 国家烟草专卖局科教司
  - 中国机械工业联合会
  - 中国汽车工业协会
  - 中华人民共和国国家知识产权局

第3章 可信计算规范

- 3.1 TCG规范架构
- 3.2 TCG核心规范
- 3.3 特定平台规范
- 3.4 可信存储规范
- 3.5 可信网络连接规范
- 3.6 中国可信计算联盟规范

3.1 TCG规范架构

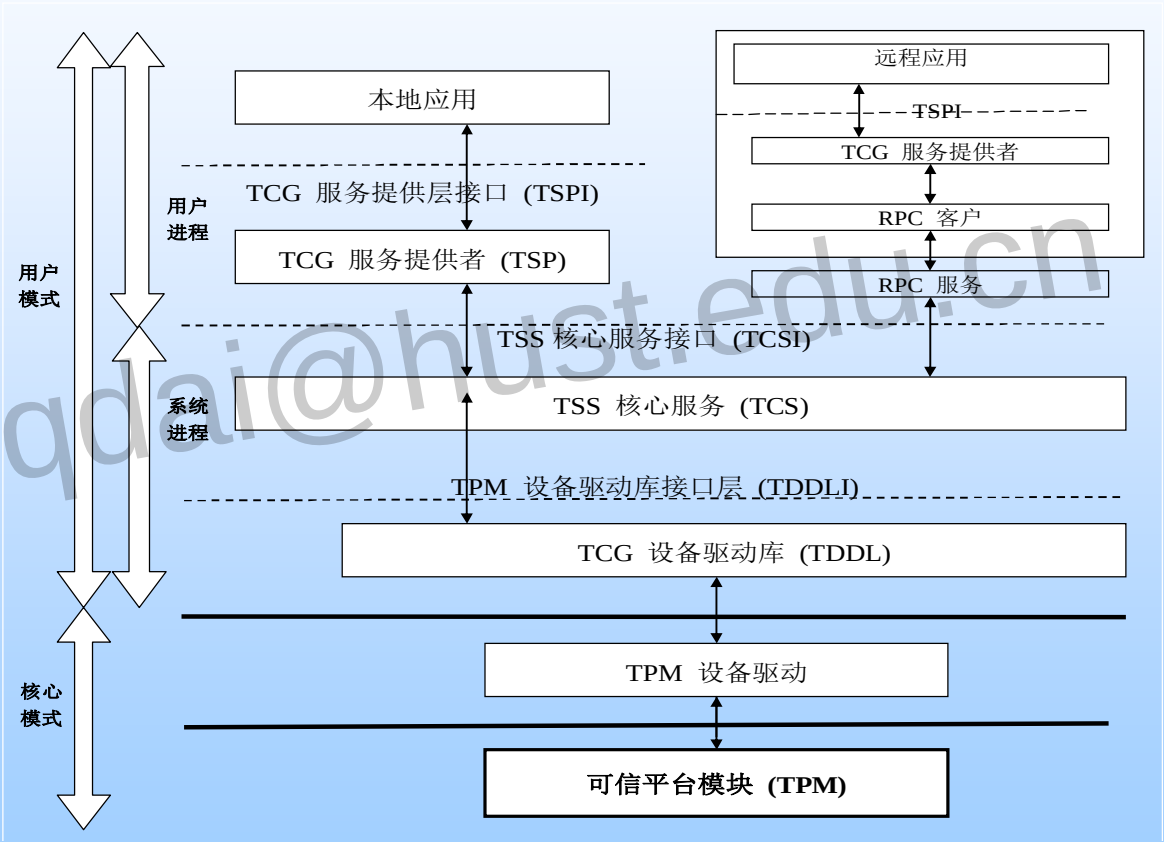
- 整个TCG规范是一个整体：
  - 包括从硬件安全芯片到可信软件栈
  - 从安全PC客户端和服务器到可信网络连接及可信存储
  - 从总体的体系结构到具体的操作接口



3.2 TCG核心规范

- TCG整个体系主要可以分为三层：TPM、TSS（TCG Software Stack ）和应用软件
- TSS处在TPM之上，应用软件之下，称作可信软件栈，它提供了应用程序访问TPM的接口，同时对TPM的管理
- TSS从上往下分为四层：
  - 服务提供层TSP（Trusted Service Provider）
  - 核心服务层TCS（TSS Core Services）
  - 设备驱动库层TDDL（TPM Device Driver Library）
  - 设备驱动层TDD（TPM Device Driver）

3.2 TCG核心规范



3.2 TCG核心规范

- 服务提供层TSP
  - TSP提供了应用程序访问TPM的C＋＋编程接口
  - 授权协议在这一层通过一个用户接口，或是TCS层的回调机制（如果调用者是远程的话）来实现
  - TSP提供两种服务: 上下文管理和密码操作

3.2 TCG核心规范

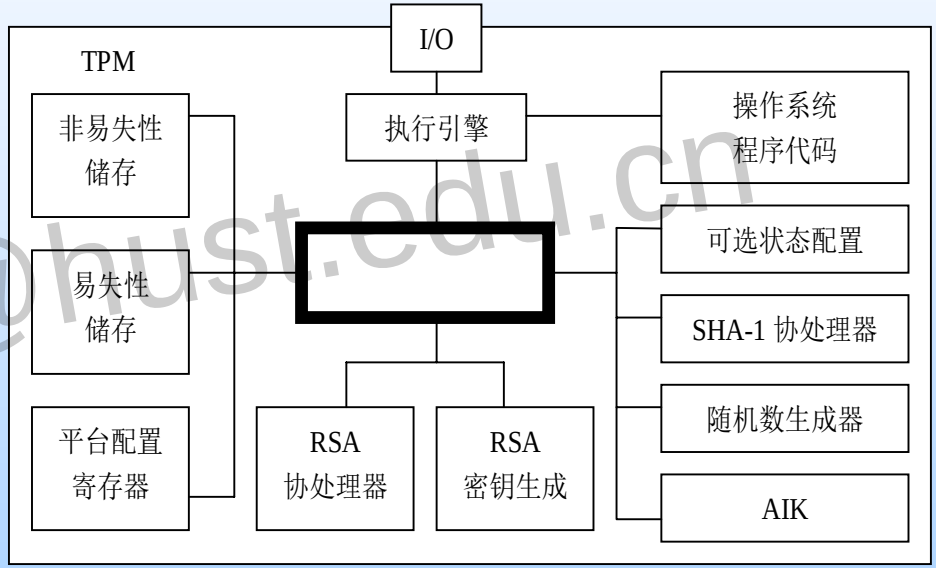
- 核心服务层TCS：TCS提供一组标准平台服务的API接口。一个TCS可以提供服务给多个TSP
- TCS提供了4个核心服务：
  - 上下文管理 — 实现到TPM的线程访问；
  - 证书和密钥的管理 — 存储与平台相关的证书和密钥；
  - 度量事件管理 — 管理事件日志的写入和相应PCR寄存器（Platform Configuration Registers）的访问；
  - 参数块的产生 — 负责对TPM命令序列化、同步和处理。

3.2 TCG核心规范

- 设备驱动库层TDDL
- TDDL是用户态和内核态的过渡，仅仅是一个接口而已
- 它不对上层线程与TPM的交互进行管理，也不对TPM命令进行序列化（serialization）。这些是在高层的软件堆完成
- 由于TPM不是多线程的，一个平台只有一个TDDL 实例，从而只允许单线程访问TPM
- TDDL提供开放接口，使不同厂商可以自由实现各自的TDD和TPM。

3.2 TCG核心规范

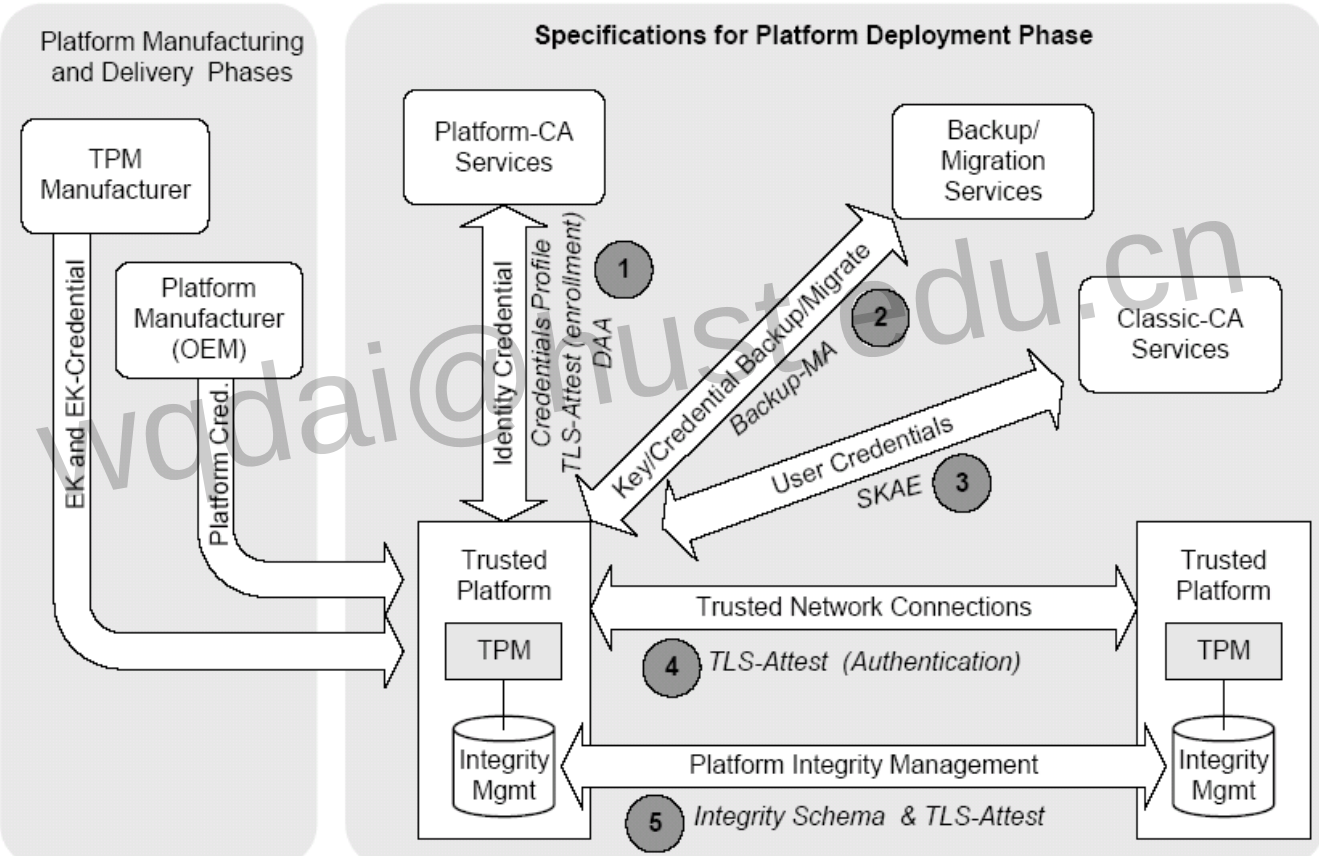
TPM至少需要具备四个主要功能：对称/非对称加密、安全存储、完整性度量和签名认证。数据的非对称加密和签名认证是通过RSA算法来实现的，而完整性度量则是通过高效的SHA-1散列算法来完成，对称加密可以使用任意算法，既可以使用专用协处理器也可以使用软件来完成。



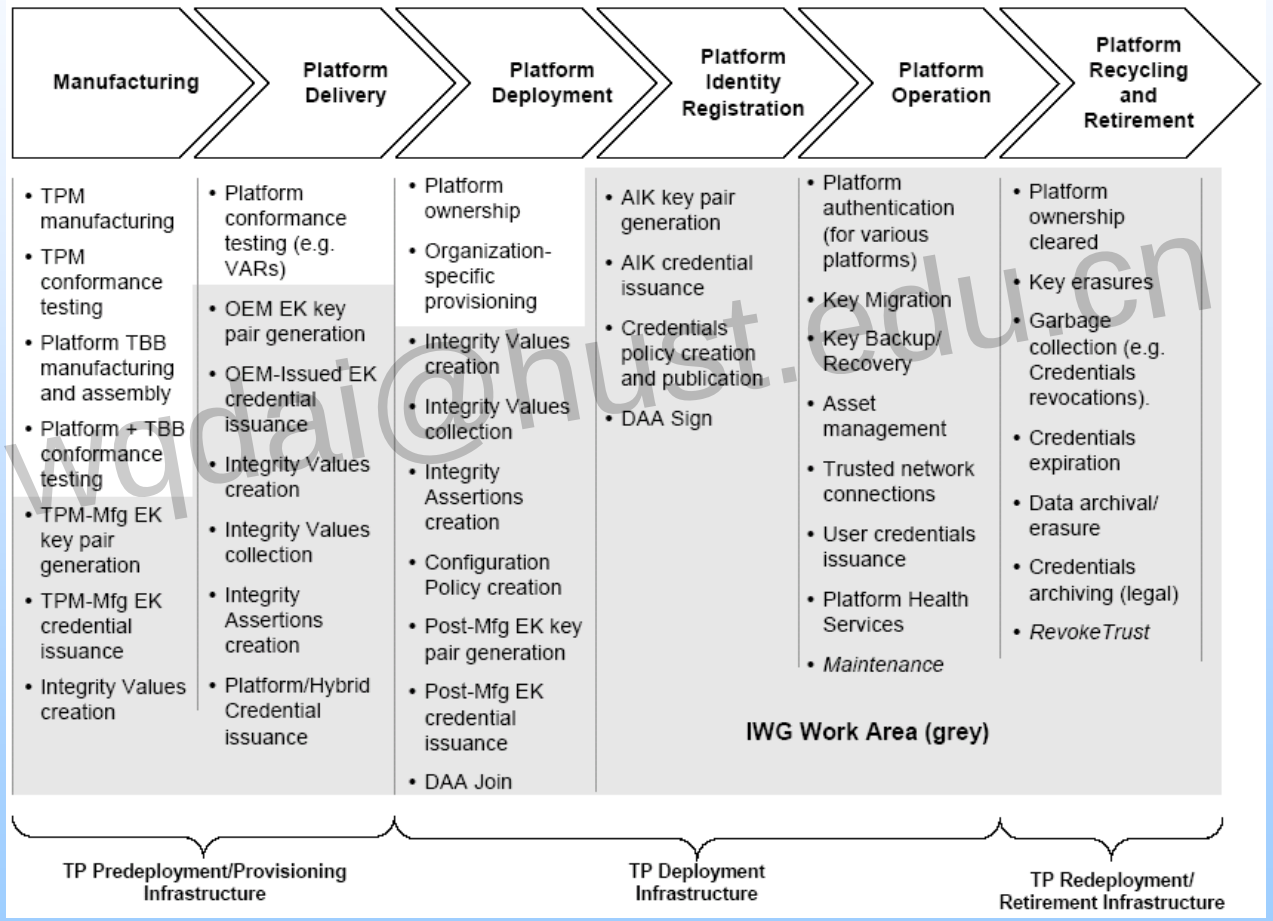
基础框架规范

- 互操作规范
  - 定义了不同实体，包括不同类型提供者和不同消费者之间的交互，以及不同阶段的交互
- 完整性管理架构规范
  - 为定义，收集，报告与软件完整性和系统配置相关的信息提供通用框架
  - 平台可信服务度量代理接口规范
    - 定义了执行、收集、度量和报告平台完整性信息的度量代理的应用程序编程接口
  - 基于通用XML的系统完整性信息获取和报告数据格式规范集和证书格式规范
    - 定义了收集和报告完整性信息的格式，参照度量值的表示格式，从评估报告验证度量结果的格式
  - 这些规范定义了与可信平台完整性相关的标准，侧重于可信平台完整性状态的度量、验证、报告等方面。

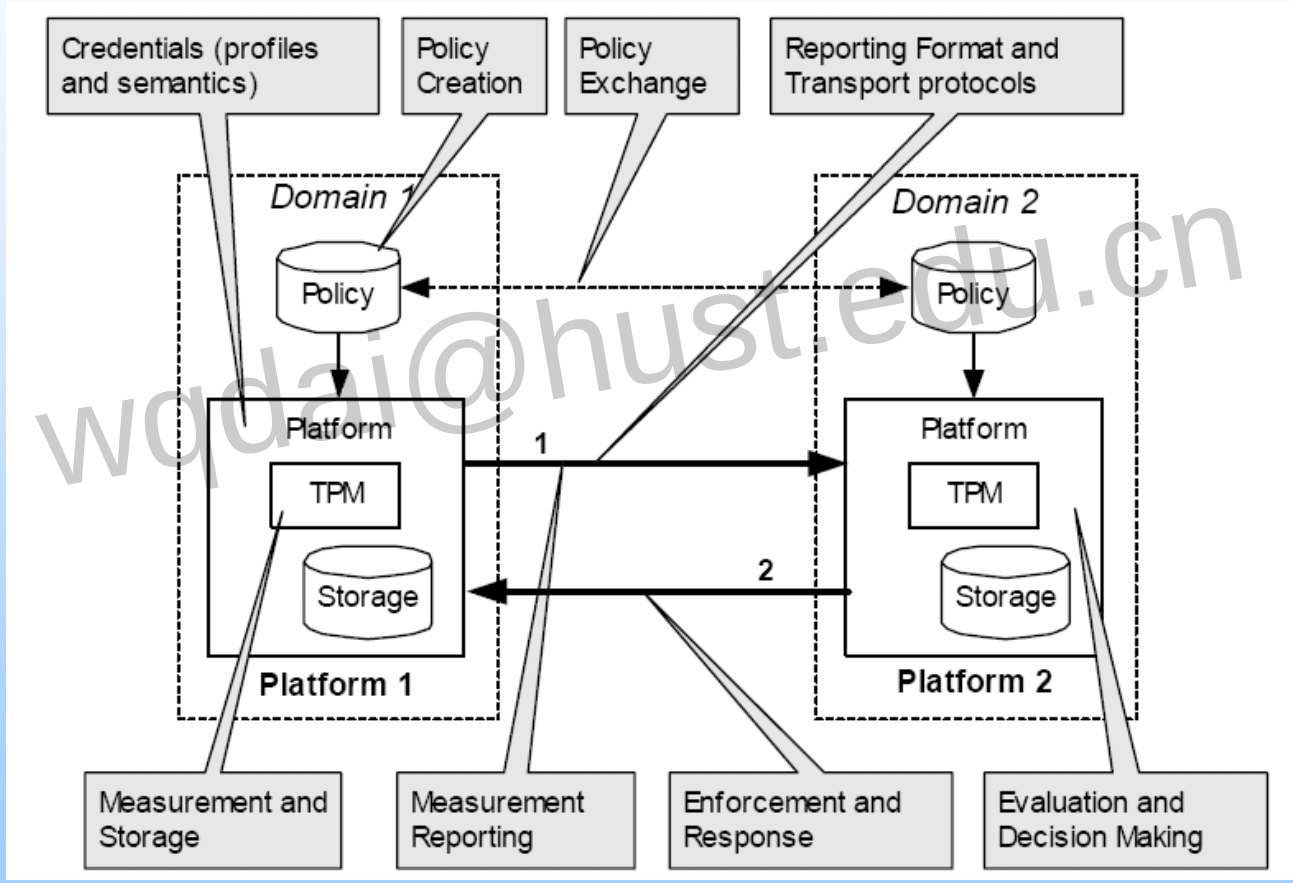
基础框架规范
——互操作规范



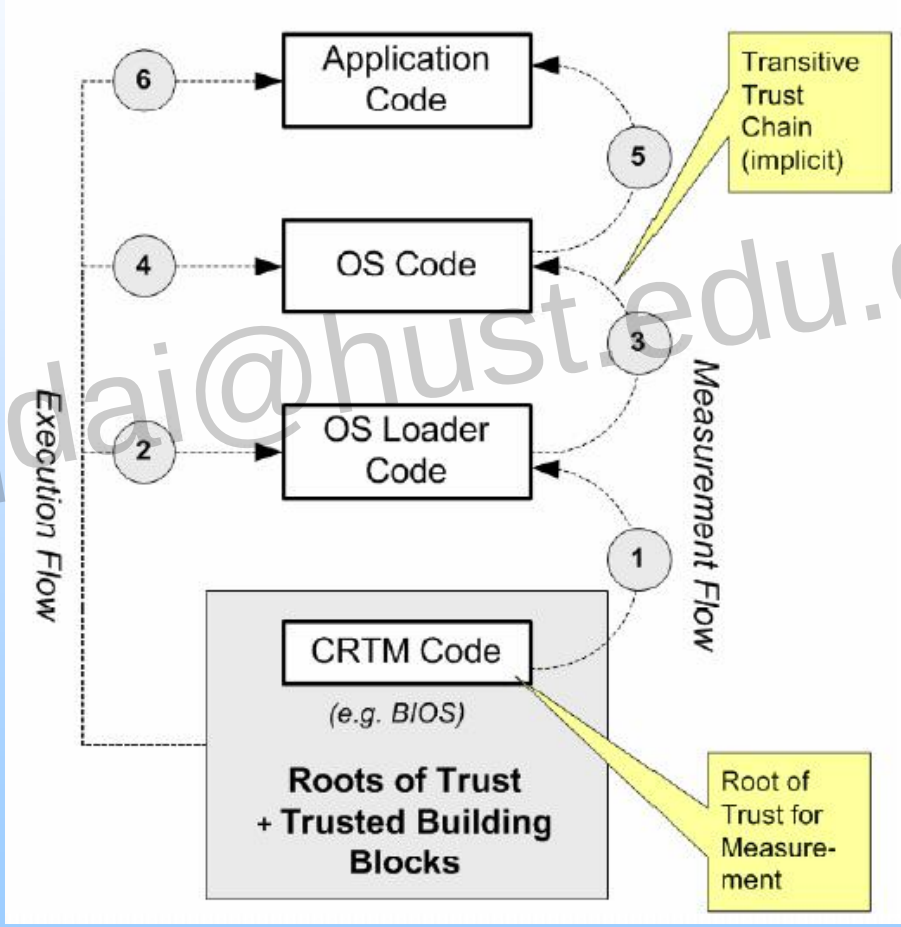
基础框架规范
——互操作规范



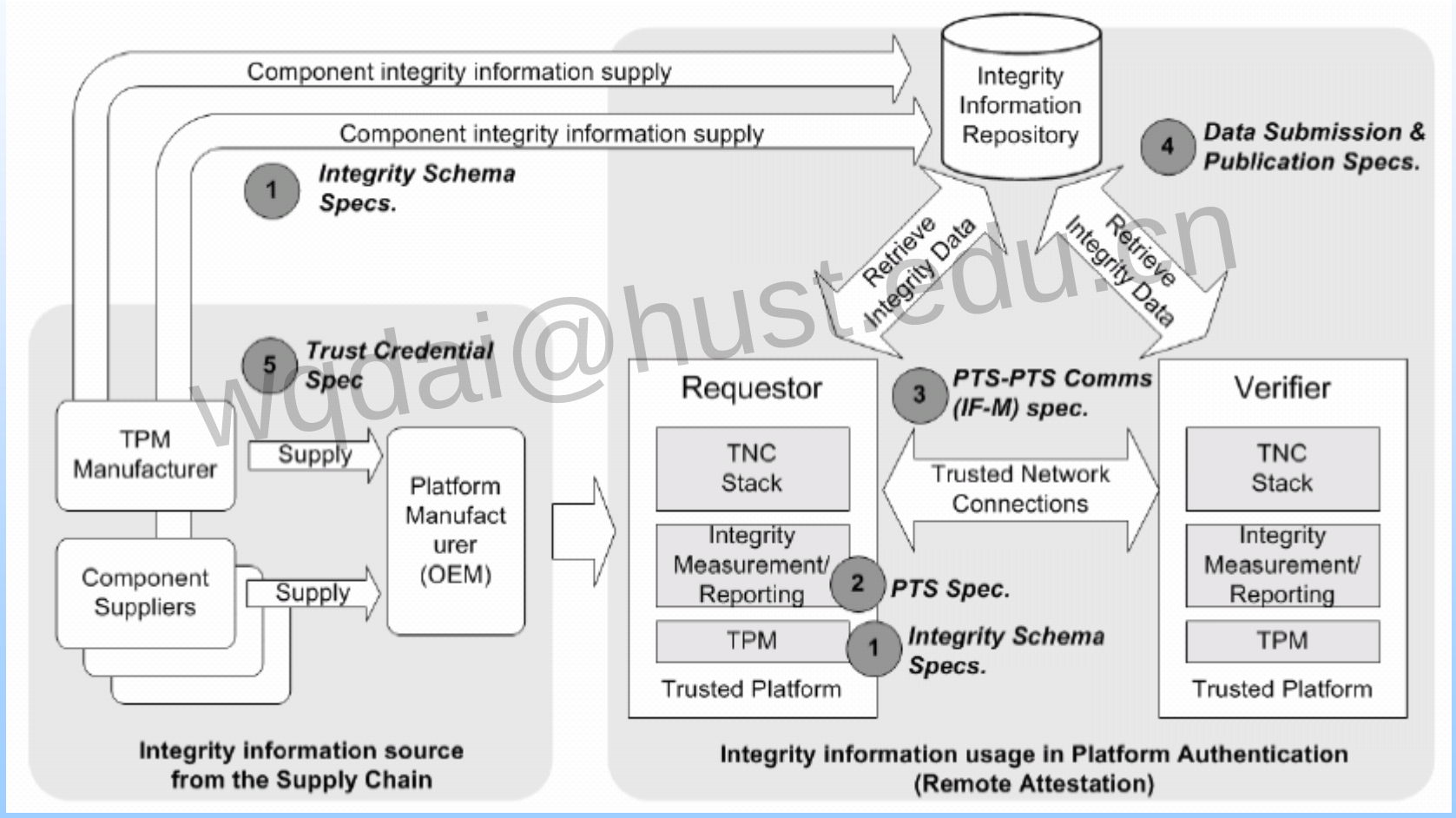
基础框架规范
——互操作规范



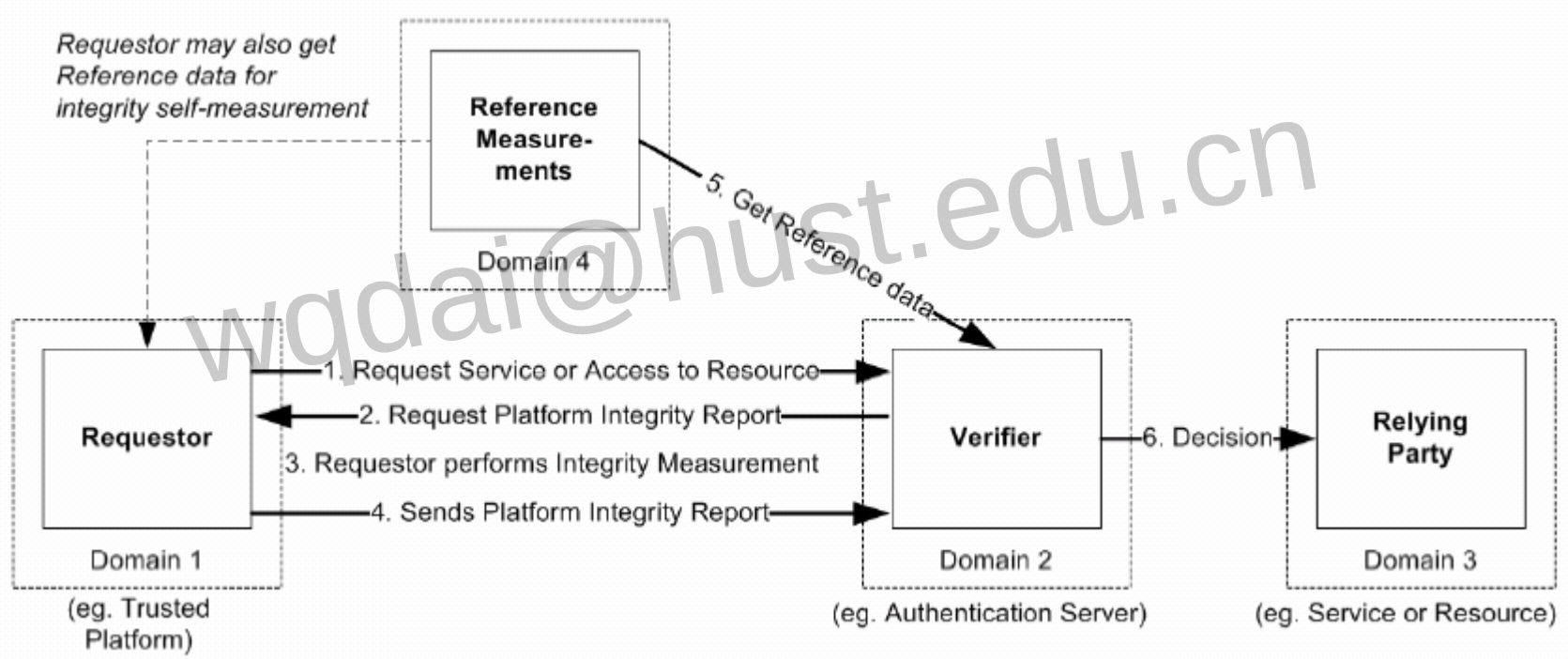
基础框架规范
——完整性管理规范



基础框架规范
——完整性管理规范



基础框架规范
——完整性管理规范



可信平台模块规范

- 详细阐述了TPM的体系结构，各个部件的功能，设计规范，TPM内部通信的数据结构，TPM底层执行的命令规范
- 包括三个规范
  - TPM 主规范（TPM Main Specification）部分1设计原理（Part 1 Design Principles Specification）
  - TPM 主规范（TPM Main Specification）部分2 TPM架构规范（ Part 2 TPM Structures Specification ）
  - TPM 主规范（TPM Main Specification）部分3 命令规范（Part 3 Commands Specification）

可信平台模块规范
——part 1

可信平台模块规范
——part 1

可信平台模块规范
——part 2

可信平台模块规范
——part 3

可信平台模块规范
——part 3

课题问题？

- 1. TPM密钥有哪几种参数，共有多种不同类型？并简要描述使用一个子密钥的过程？
- 2. 为什么说虚拟机回滚和可信计算是矛盾的？
- 3. 虚拟机回滚会产生何种攻击？
- 4. 为什么单纯回滚tpm无法解决问题？还存在何种攻击？
- 5. 如何解决回滚问题？
- 6. 描述静态可信度量根的几个问题？易用性、可扩展性、度量时机、包容性。
- 7. 德国研究者发现TPM1.0的3个缺陷？

课题问题？

- 8. 动态可信度量根如何消除缺陷1和缺陷2？
- 9. 动态可信度量根如何消除缺陷3？
- 10. TPM1.2 有多少个Locality？作用是什么？
- 11. AC Module如何验证？ 简单描述Intel的TXT如何构建动态信任链的？

TPM软件栈规范

- TPM的软件服务层的结构，TCG软件开发接口，中间服务接口。TSS直接和应用挂钩，提供应用程序开发接口，规范了各个角色对于TSS的操作权限
- 提供了各种接口函数（本书TSS内容来自该规范）

个人计算机客户端规范

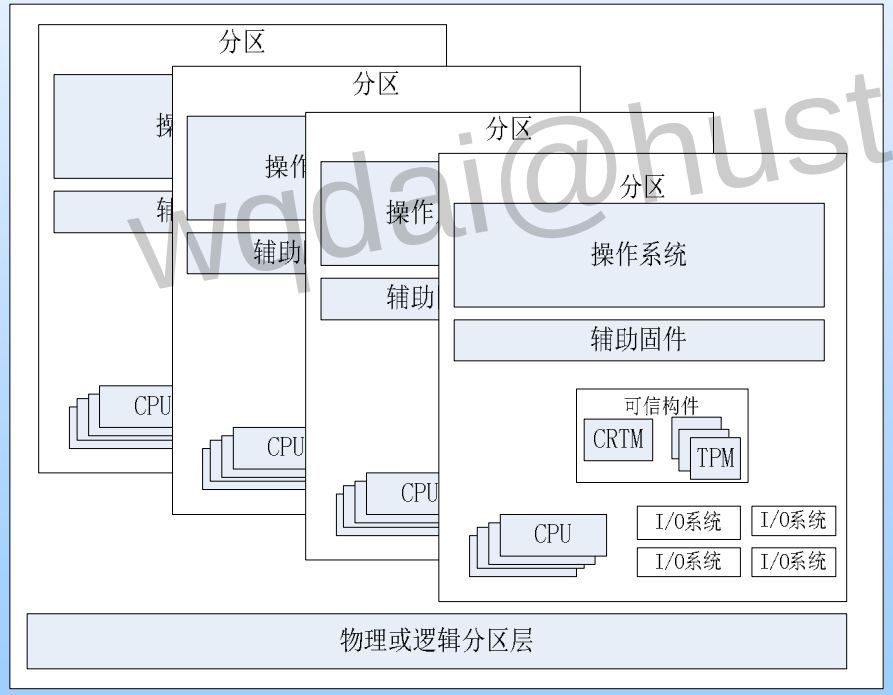
- 个人计算机具体实现规范（**PC Client Work Group PC Specific Implementation Specification, Version 1.1**）
- 个人计算机客户端**TPM**详细接口规范（**PC Client Work Group PC Client Specific TPM Interface Specification (TIS), Version 1.2**）
- 通用**BIOS**规范（**PC Client Work Group Specific Implementation Specification for Conventional Bios Specification, Version 1.2**）
- 重置攻击防御规范（**PC Client Work Group Platform Reset Attack Mitigation Specification, Version 1.0**）等

服务器规范

- 定义可信服务器的架构和如何创建、管理和维护这些服务器
  - 通用服务规范 **Version 1.0 （Server Work Group Generic Server Specification, Version 1.0）**
  - 服务器强制和可选**TPM**命令规范（**Server Work Group Mandatory and Optional TPM Commands for Servers Specification, Version 1.0**）
  - 基于安腾架构的服务器规范（**Server Work Group Itanium Architecture Based Server Specification, Version 1.0**）
  - 高级电源管理通用协议（**Server Work Group ACPI General Specification, Version 1.0**）等

可信服务器规范

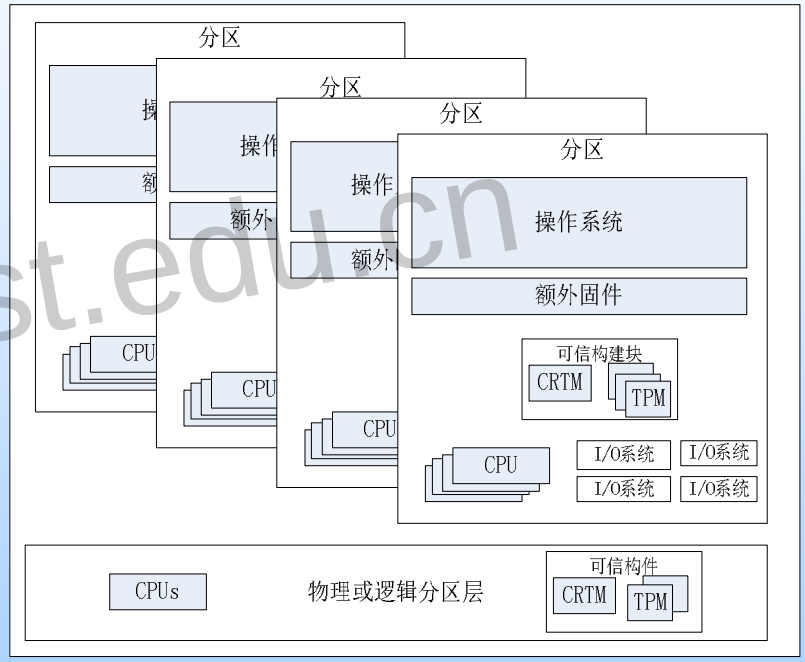
- 可信服务器规范给出了服务器中可信构件（**Trusted Building Block，TBB**）的基本要求



可信构件由每个分区管理

可信服务器规范

- “分区层”（**partitioning layer**）可以被实现为一个单独的计算引擎并维护着自己的**TPM**；
- 分区层相当于一个物理或逻辑的独立机器。因此，分区层是一个独立于分区的执行环境；
- 分区由分区层创建，分区的信任链中需要包含该分区层



可信服务器规范

- 分区
  - 分区：包括硬件和固件环境，可以提供隔离的可信执行环境从而允许单一操作系统映像的运行。
  - 分区层：将服务器资源划分成相互隔离的分区所需的硬件，固件和（或）软件。
  - 平台：制造商服务器产品的一套物理硬件和固件，可以被配置为一个或多个分区。
  - 在非分区环境下，存在特定目的的单一分区。在这种情况下，分区=服务器=平台
  - 在分区环境中可能存在多个分区，在这种情况下，一个TPM只能被绑定到一个分区。但是单个分区可以绑定多个TPM。

可信服务器规范

- **CRTM：可信度量根**
  - 由服务器制造商唯一控制，非TPM制造商
  - 是一种先验可信的代码，是开机后或服务和硬件重置后应执行的第一段代码
  - 服务器是否可信取决于CRTM和平台证书
  - 所有测量组件是否可信取决于其完整性以及可信度量根能否在该时刻取得对服务器环境的完整控制权

可信服务器规范

- 可信块（TBB）
  - 由可信度量根CRTM、可信平台模块TPM，及它们与平台的连接部分构成
  - CRTM到TPM的可信连接取决于CRTM和TPM到系统的可信连接
  - 由于TPM的功能可能分布在平台不同部件中，因为TBB包含了可信度量根（无论是静态的还是动态的）、TPM以及它们之间的连接

可信服务器规范

- 服务器绑定
  - 标识TPM身份的背书密钥（Endorsement Key, EK）和分区之间的绑定
  - 一个背书密钥将会和整个硬件环境相关联并被该环境中的所有分区所使用
    - 每个分区中TPM其他的功能特性必须是唯一的，包括平台配置寄存器PCR和计数器，而不变计数基可以被所有分区共享

可信服务器规范

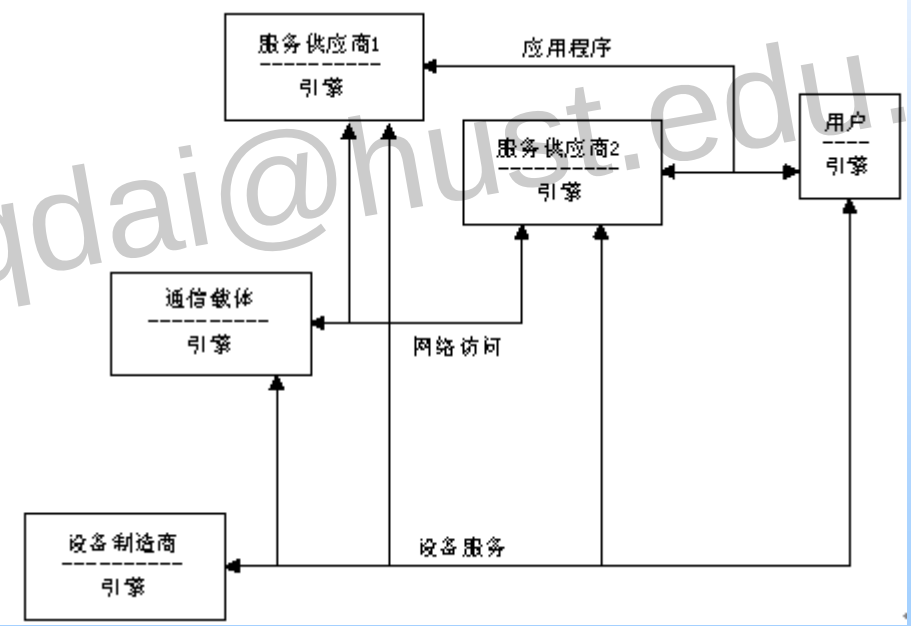
- 平台状态
  - 在支持静态CRTM的TCG服务器中，由固件或操作系统控制和维护每个PCR
  - 固件的PCR值和日志对操作系统是只读的

移动平台规范

- 提供一套用于构建TCG安全装置的硬件和软件在移动平台的核心架构，命令和控制规范
  - 移动平台参照架构（**Mobile Phone Work Group Mobile Reference Architecture**）
  - 移动可信模块规范（**Mobile Phone Work Group Mobile Trusted Module Specification, Version 1.0**）
  - 精选用例分析（**Mobile Phone Work Group Selected Use Case Analysis Specification, Version 1.0**）

移动平台规范

- 可信移动平台包含多个引擎，不同的引擎为不同的利益实体**(stakeholder)**服务，每个利益实体都有自己的引擎

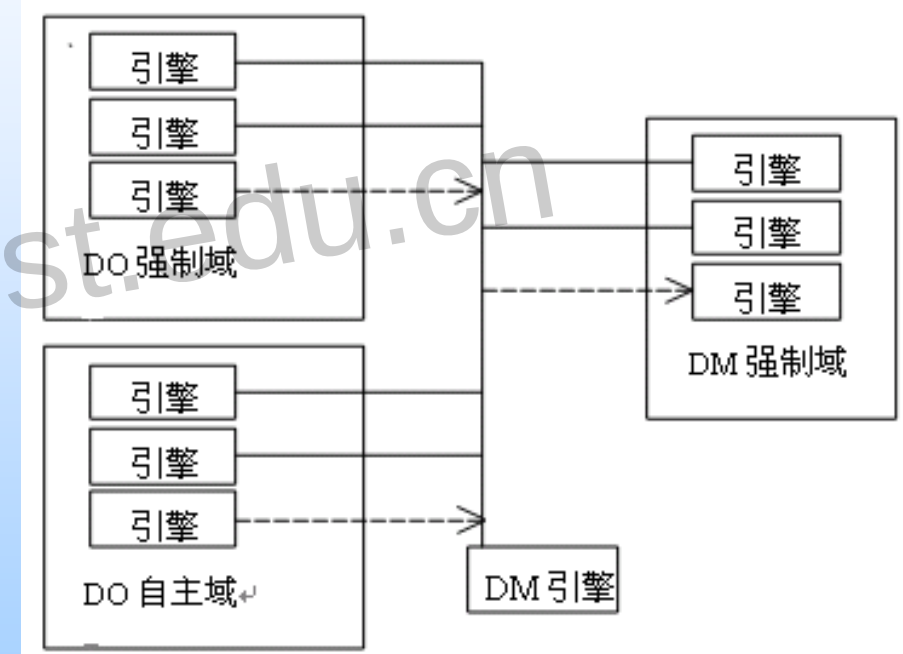


移动平台规范

- 可信移动平台引擎
  - 可信移动平台内的每个引擎需要相应配套的资源来完成它的工作，接受设定的服务并输出设定的服务
- 引擎功能
  - 报告引擎信任证书或证明；
  - 报告引擎当前状态证明；
  - 获取和使用身份证明密钥（**Attestation Identity Key，AIK**）；
  - 为其它引擎提供受保护的存储；
  - 其它**TCG**可信平台可能会使用的功能（如时间戳、分发等等）。
- 引擎保证它提供和使用的服务都是可信的，引擎分为强制和自主两种类型
  - 强制性引擎常驻于一个平台之中，之所以被称为强制性引擎，是因为它们提供强制（关键、必不可少的）服务，需要“移动远程属主可信模块”**(Mobile Remote owner Trusted Module, MRTM**）的支持（安全引导），禁止本地移除
  - 自主性引擎提供的服务必须是可以不依赖外部服务供应商的授权来自行添加、移除、启用和禁用的，需要“移动本地属主可信模块”**(Mobile Local-owner Trusted Module, MLTM**）的支持，设备所有者应保证所有的自主性引擎和它们的利益实体服从其隐私规则

移动平台规范

- 可信移动平台的域
  - 强制域和自主域
  - 设备制造商（**Device Manufacturer, DM**）控制一些在强制域内的引擎的行为
  - **TCG**规范也定义了一个设备所有者（**Device Owner, DO**）角色，它控制强制域内部分引擎以及自主域内所有引擎的行为
  - 引擎提供的服务决定了它被列于强制性表还是自主性表：若它提供的服务是平台必需的，则该引擎应被列于强制性表；否则，它应被列于自主性表

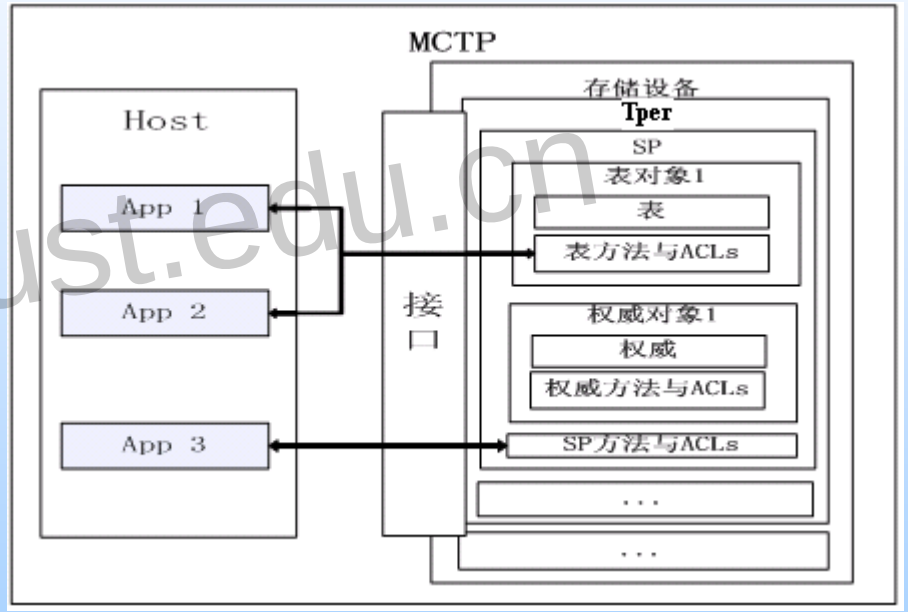


TCG的可信存储规范

- 针对用于所有类型存储设备和密钥管理规划的全盘加密，包括三项规范：
  - 存储界面交互--这项规定详细规定了所有TCG规范是如何与存储互连与接口规范(包括ATA、ATAPI、SCSI、光纤通道等)进行交互的
  - Opal--这项规范详细阐述了PC和笔记本电脑混合存储介质的相关要求
  - 企业级安全子系统等级--这项规范主要针对数据中心驱动器和高容量应用，往往这些方面的安全架构比较薄弱。

TCG的可信存储规范

- 多部件的可信平台（MCTP）描述了有一个或多个主机、应用、外围部件参与的，处于可信状态的平台
- 可信外围部件（TPer）位于存储装置中，TPer管理可信存储的功能和数据结构
- 基于TPer特性的数据加密和访问控制
- TPer和主机之间的双向注册和连接
- 可以有一个或多个安全提供者（Security Provider，SP），一个安全提供者是一系列表和方法
  - 认证、安全属性值的存储、磁盘加密/解密、备份、时间戳和事件日志



TCG的可信存储规范

- 安全提供者
  - 表：字节表和对象表
  - 方法：增加删除表，表的可读访问控制和备份表
  - 权威：制定的密码和加密的凭证
  - 访问控制列表和访问控制元素

主机和TPer的通信

- 主机和TPer(SP)使用接口命令进行通信

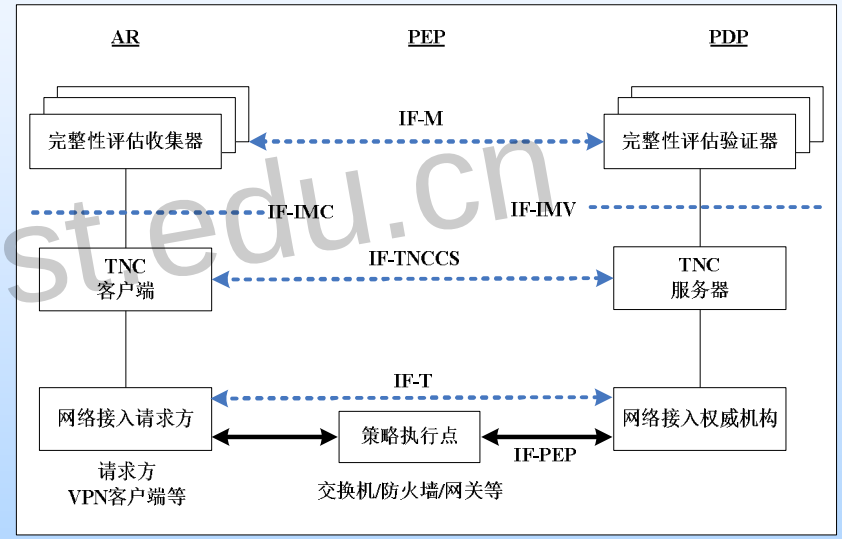
- SP发布和个性化定制
  - SP的创建需要结合多个模块，包括管理模块、时钟模块、加密模块、锁定模块、日志模块，模块定义了初始化的表和方法
  - 个性化是指SP初始化得定制过程，可持续整个生命周期

可信网络连接规范

- 设计了网络连接的抽象模型，定义了安全通讯的层次，规定TNC服务器，TNC客户端所必须遵循的操作接口
  - TNC架构规范主要定义网络连接的抽象模型和整体架构；
  - TNC IF-IMC和TNC IF-IMV规范定义了客户端和服务端用于实现TNC功能的插件标准API；
  - IF-TNCCS规范定义了TNC客户端(TNCC)和TNC 服务端(TNCS)的互操作标准；
  - IF-T 规范规定支持多种传输协议的标准；
  - IF-PEP 定义了如何使用RADIUS协议在网络访问权威（Network Access Authority，NAA）和策略实施点（PEP）之间通信。

可信网络连接规范

- TNC架构由三个主要功能实体组成
- AR（Access Requestor）
- PEP（Policy Enforcement Point）
- PDP（Policy Decision Point）



可信网络连接操作流程

- 1. 在进行网络连接和平台完整性验证之前，TNCC需要对每一个完整性评估收集器（IMC）进行初始化；TNCS对完整性评估验证器（IMV）进行初始化
- 2. 网络连接发生时，NAR向PEP发请求
- 3. PEP向网络接入权威机构（NAA ）转发网络访问决策请求
- 4. AR与NAA之间用户认证成功，则NAA通知TNCS有一个连接请求
- 5. TNCS与TNCC进行平台验证
- 6. 成功后，TNCS通知IMV有新请求，需要进行完整性验证；同时TNCC通知IMC新的请求已经发生，需要准备完整性信息。IMC通过IF-IMC向TNCC返回IF-M消息
- 7. TNCS将每个IMC消息发送给相应的IMV，IMV对IMC消息进行分析，如果需要更多完整性信息，它将通过IF-IMV接口向TNCS发送请求，如果做出判断，则返回结果给TNCS
- 8. TNCC和TNCS交换完整性验证的各种消息。这些消息被NAR、PEP和NAA转发，直到AR的完整性状态满足TNCS的要求
- 9. 当TNCS完成和TNCC的完整性检查握手之后，它发送TNCS推荐操作给NAA
- 10. NAA发送网络访问决策给PEP实施，NAA也必须向TNCS说明它最后的网络访问决定，这个决定也将发送给TNCC

可信网络连接支撑技术

- 802.1x：提供基于端口的访问控制
- VPN：使用IPSec或SSL建立安全连接
- PPP协议：两个网络节点间建立连接的数据链路协议
- 安全消息传输技术：可扩展认证协议EAP、HTTPS等等

可信网络连接局限性

- 缺乏理论支撑
- 局限在完整性
- 单向性的可信评估
- 各接口缺乏安全协议支持
- 缺乏接入后的安全保护
- 应用范围的局限性（仅企业内部网络）

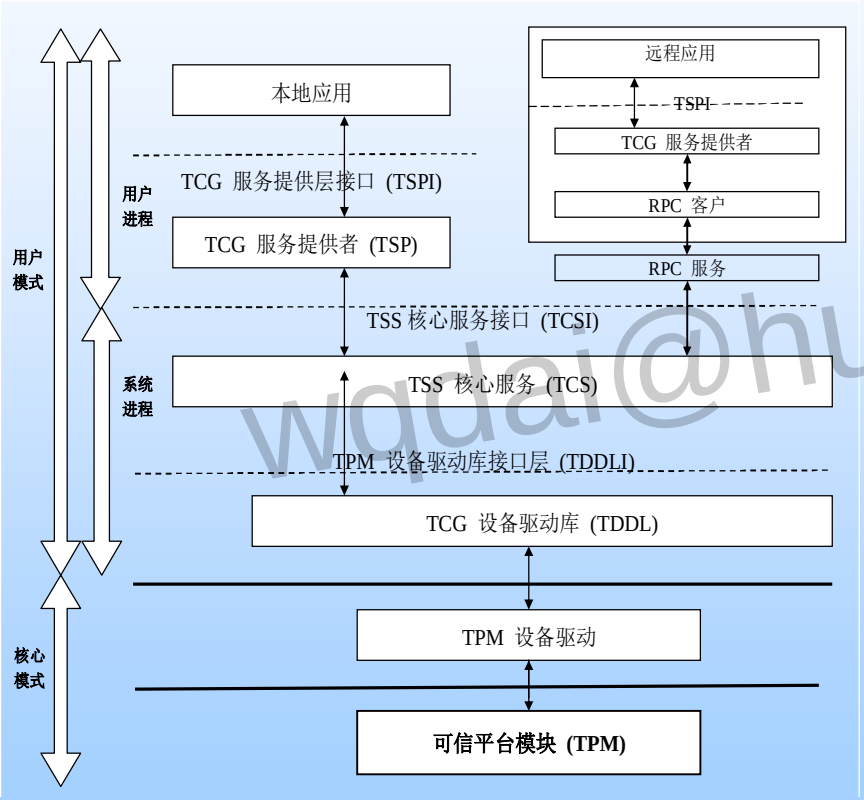
3.6 中国可信计算联盟规范

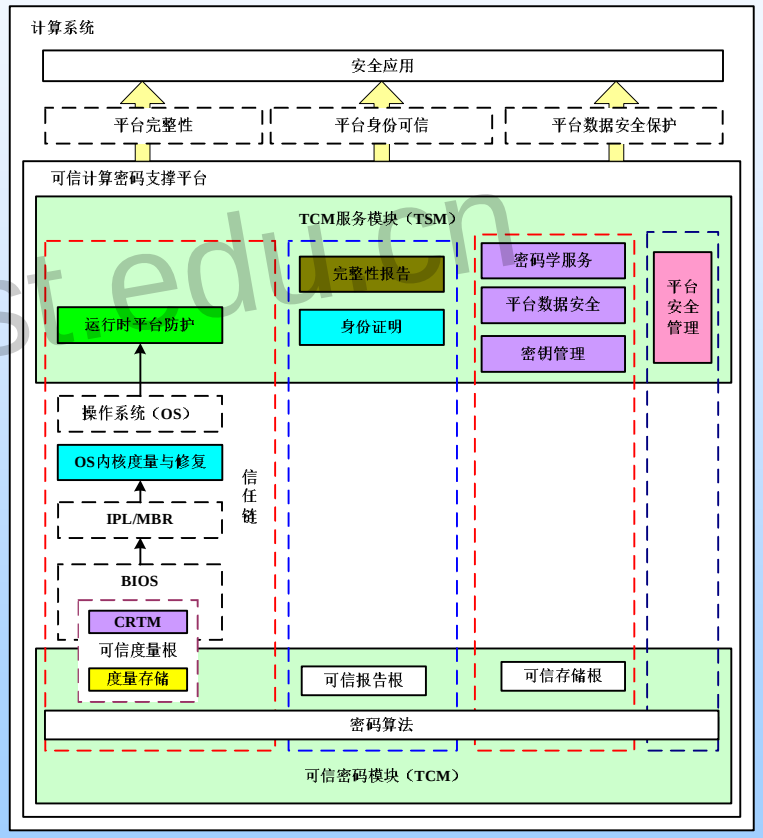
- 中国可信计算工作组是中国的可信计算标准的行业规范制订组织
  - 已发布《可信计算密码支撑平台功能与接口规范》
  - 其他规范草案，如：《可信计算平台密码规范》、《可信计算基础支撑软件》、《可信平台主机规范》、《可信网络连接规范》等草案尚未公布

可信计算密码支撑平台功能与接口规范

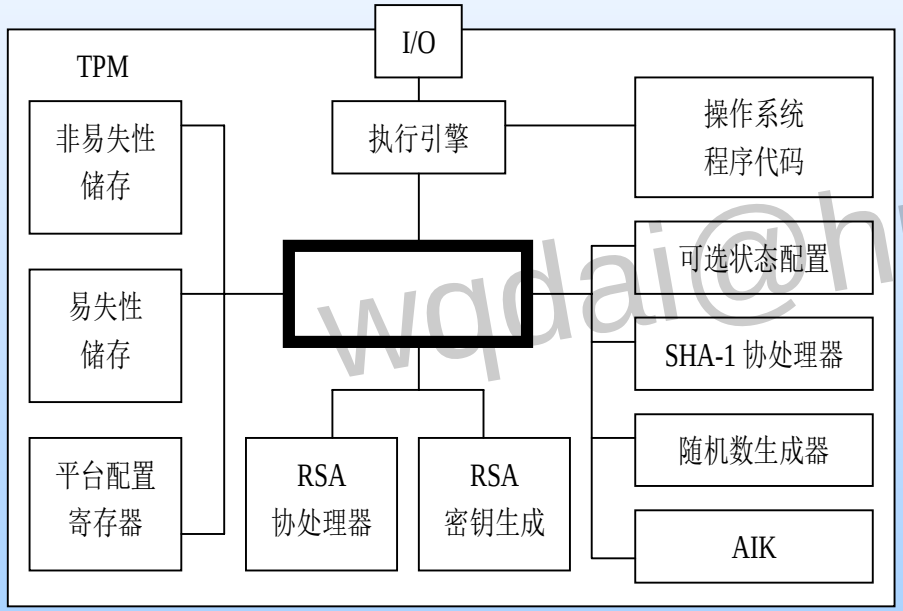
- 平台完整性
  - 利用密码机制，通过对系统平台组件的完整性度量，确保系统平台完整性，并向外部实体可信地报告平台完整性。
- 平台身份可信
  - 利用密码机制，标识系统平台身份，实现系统平台身份管理功能，并向外部实体提供系统平台身份证明。
- 平台数据安全保护
  - 利用密码机制，保护系统平台敏感数据。其中数据安全保护包括平台自身敏感数据的保护和用户敏感数据的保护。另外也可为用户数据保护提供服务接口。

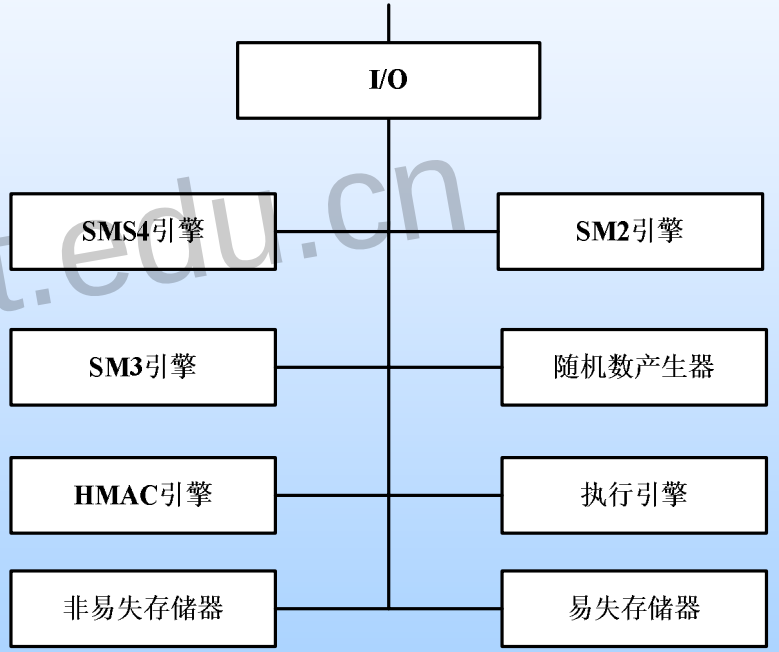
可信计算密码支撑平台功能与接口规范





可信密码模块结构





可信密码模块结构

- I/O：TCM的输入输出硬件接口；
- SMS4引擎：执行SMS4对称密码运算的单元；
- SM2引擎：产生SM2密钥对和执行SM2加/解密、签名运算的单元；
- SM3引擎：执行杂凑运算的单元；
- 随机数产生器：生成随机数的单元；
- HMAC引擎：基于SM3引擎的计算消息认证码单元；
- 执行引擎：TCM的运算执行单元；
- 非易失性存储器：存储永久数据的存储单元；
- 易失性存储器：TCM运行时临时数据的存储单元。

TCM服务模块

- 设计目标
  - 为应用程序调用TCM 安全保护功能提供一个入口点；
  - 提供对TCM 的同步访问；
  - 向应用程序隐藏TCM 所建立的功能命令；
  - 管理TCM 资源。
- 功能
  - 定义了一个具有存储保护和执行保护的子系统
  - 提供对TCM 基础资源的支持，由多个部分组成，每个部分间的接口定义应具有互操作性，TSM 应提供规范化的函数接口