RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

面向中国生态系统的可信计算池

Yan Li， 云解决方案首席架构师

DCSG 技术营销

Xin Liu， Nationz， 产品经理

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012

议程

- 安全趋势和问题
- 最安全处理的基础
- 应对安全挑战：
- 解决难题所采用的技术和使用模型

  虚拟化技术加强工作负载隔离

  可信执行技术提供可见性和执行点
- 中国新一代 TPM 标准
- 中国生态系统实现可信云
- 总结

企业的安全趋势

数据中心和云的安全问题日益增加

趋势：
攻击类型发生转变

不止软件，平台亦成为了攻击目标

隐蔽和控制成为攻击目的

趋势：
法规遵从性问题和成本增加

英国数据保护法案、FedRAMP、支付卡行业 (PCI) 等纷纷要求实施安全保护，并提出审核需求

趋势：
体系结构的变化要求

虚拟化和多租户

第三方依赖性

边界模糊不清

服务器安全技术

安全问题限制了云的采用

更高的安全性对于云增长至关重要

RSA CONFERENCE CHINA 2012

IT Pro 主要安全问题调查：

57%
避免将具有法规遵从性要求的工作负载放入云中[1]

61%
声称由于缺乏可见性而限制了私有云的采用[1]

55%
无法控制公共云[1]

intel

nationz

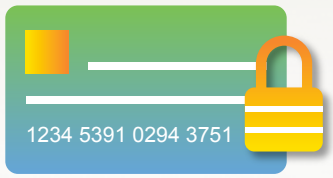
RSA信息安全大会2012

[1] McCann 2012 全球云安全现状调查，2012 年 2 月

服务器安全技术

焦点：植入安全性和可信性

强化了计算基础



保护身份安全和防欺诈

检测和阻挡
恶意软件

保护数据
和资产安全

恢复和加强修补

服务器安全技术

第一大难题：隔离

在共享基础架构上隔离工作负载至关重要

共享基础架构的主要问题

无法提供传统的物理分隔保证

多个工作负载可能会相互篡改或进行交互

国土安全小组委员会听证：
云计算：存在哪些安全隐患？[1]

多租户解决方案：
优点、疑问和集成问题[2]

云计算重点关注领域的相关安全指导[3]

*其他名称及品牌为其各自所有者的资产

http://www.outlookseries.com/A0995/Security/3817_Homeland_Security_Hearing_Cloud_Computing_Implications.htm

http://www.itbusinessedge.com/cm/blogs/lawson/multi-tenant-solutions-the-pros-the-questions-and-integration-concerns/?cs=45181&page=2

https://cloudsecurityalliance.org/csaguide.pdf

第二大难题：执行

需要采取新的控制措施以便对基础架构实施保护

新攻击类型的运行前

虚拟化和云弱化了保护力度

低层攻击难以检测，难以恢复

WEBROOT®

Mebromi：首例来路不明的 BIOS Rootkit[1]

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST 指导准则力求将 BIOS 攻击的风险降到最低[2]

Science & Technology Security & Trust

美国国土安全部网络安全研发跨机构公告 (BAA)：BAA 11-02[3]

*其他名称及品牌为其各自所有者的资产

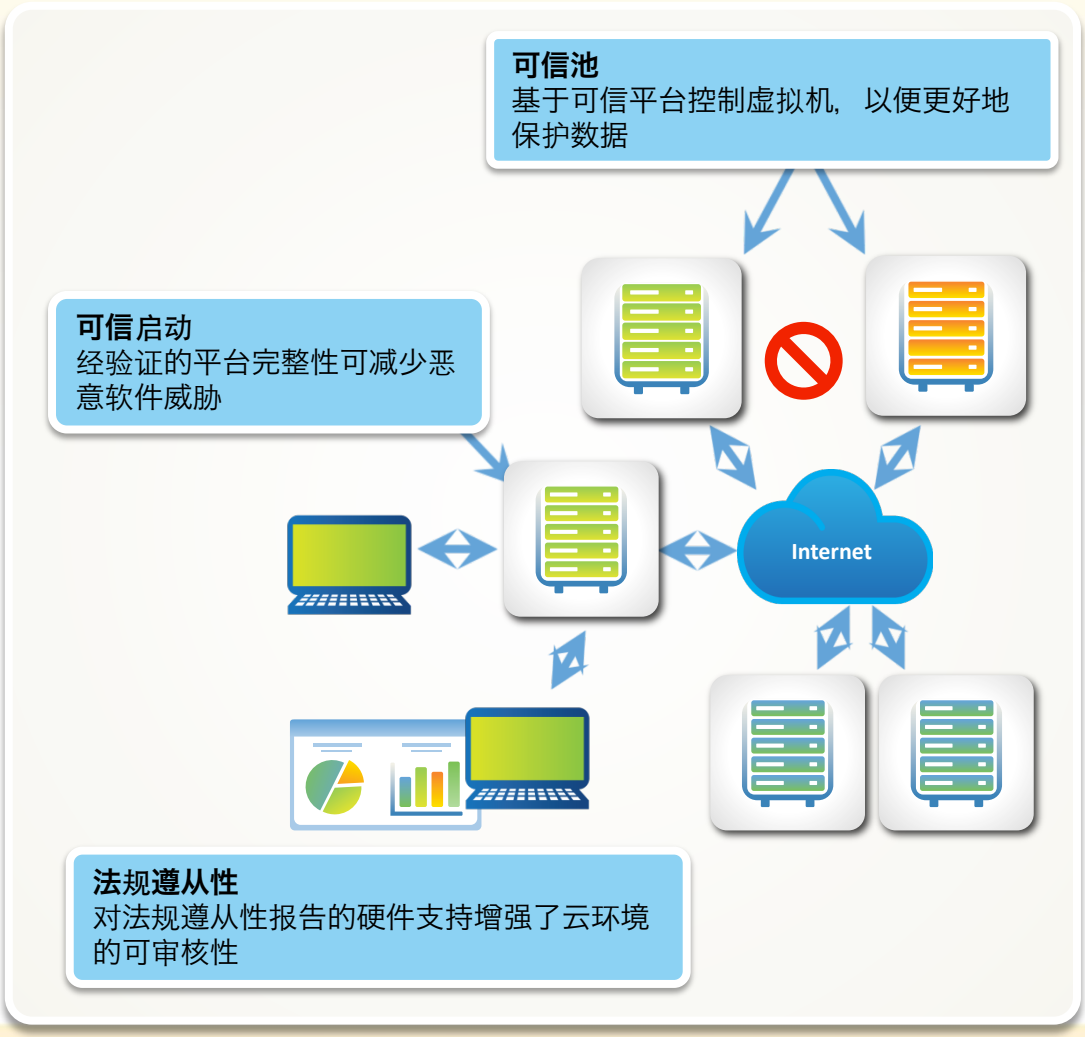
http://www.outlookseries.com/A0995/Security/3817_Homeland_Security_Hearing_Cloud_Computing_Implications.htm
http://www.itbusinessedge.com/cm/blogs/lawson/multi-tenant-solutions-the-pros-the-questions-and-integration-concerns/?cs=45181&page=2
https://cloudsecurityalliance.org/csaguide.pdf

可信执行技术

强化并帮助控制平台

TXT：

- 在启动过程中进行隔离和篡改检测
- 与运行时保护互补
- 基于硬件的可信性将提供验证，有助于遵从法规
- 安全和策略应用程序通过可信状态控制工作负载



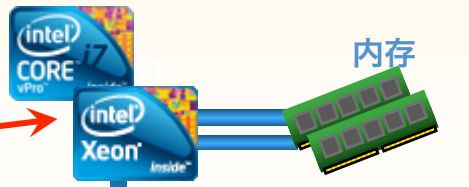
TXT 要素

可信执行技术为提供可度量的启动和内存保护 (SMX) 进行了扩展

处理器包含用于验证 AC Module 和执行度量的硬件

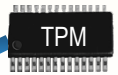
VT-d 芯片组功能可阻止设备 DMA 内存页面

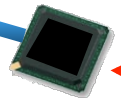
SINIT AC Module
BIOS AC Module



内存

第三方 TPM
存储和报告可信的环境度量值

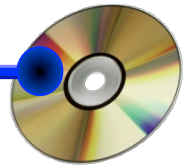




BIOS/闪存
BIOS AC Module 和平台初始化

Intel 经验证的软件

第三方软件
VMM/OS 利用 TXT 机制建立可度量的启动环境



议程

- 安全趋势和问题
- 最安全处理的基础
- 应对安全挑战：
- 解决难题所采用的技术和使用模型

虚拟化技术加强工作负载隔离

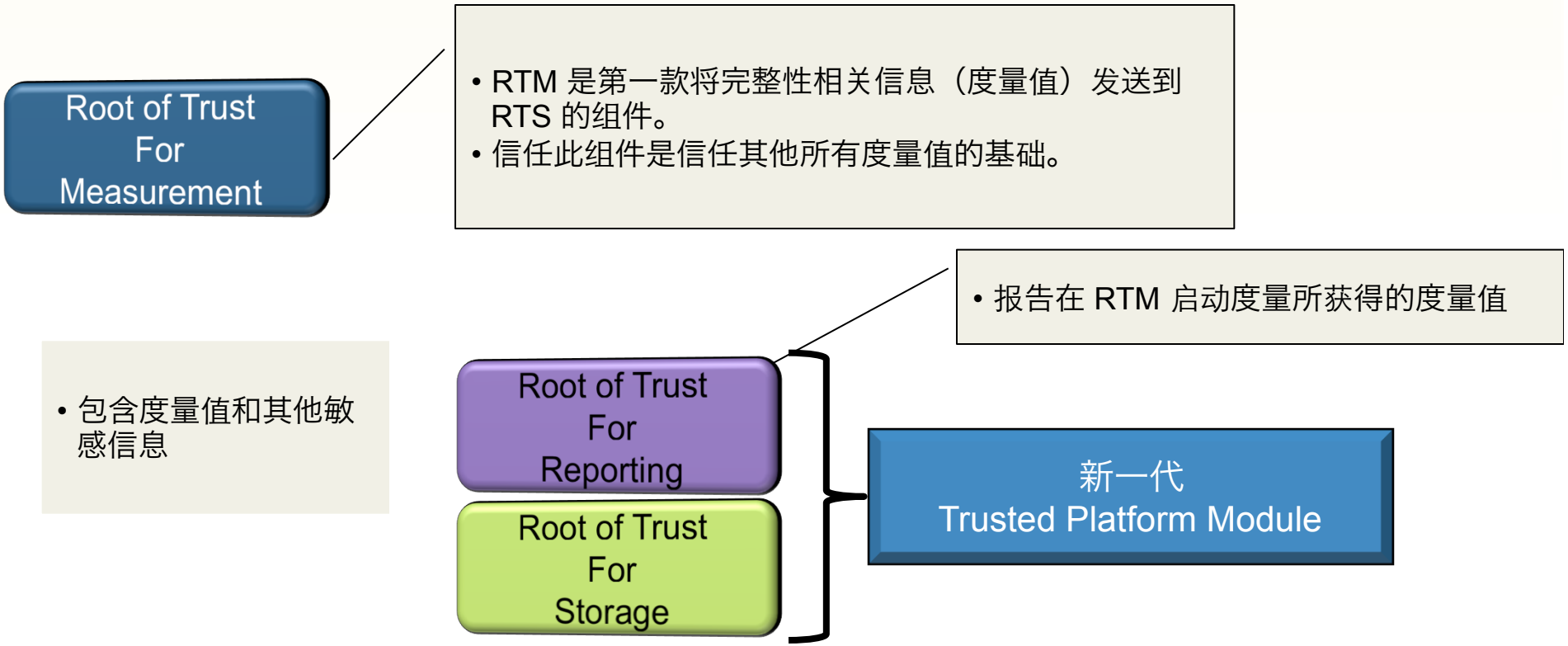
-

- 最安全处理的基础
- 应对安全挑战：

解决难题所采用的技术和使用模型

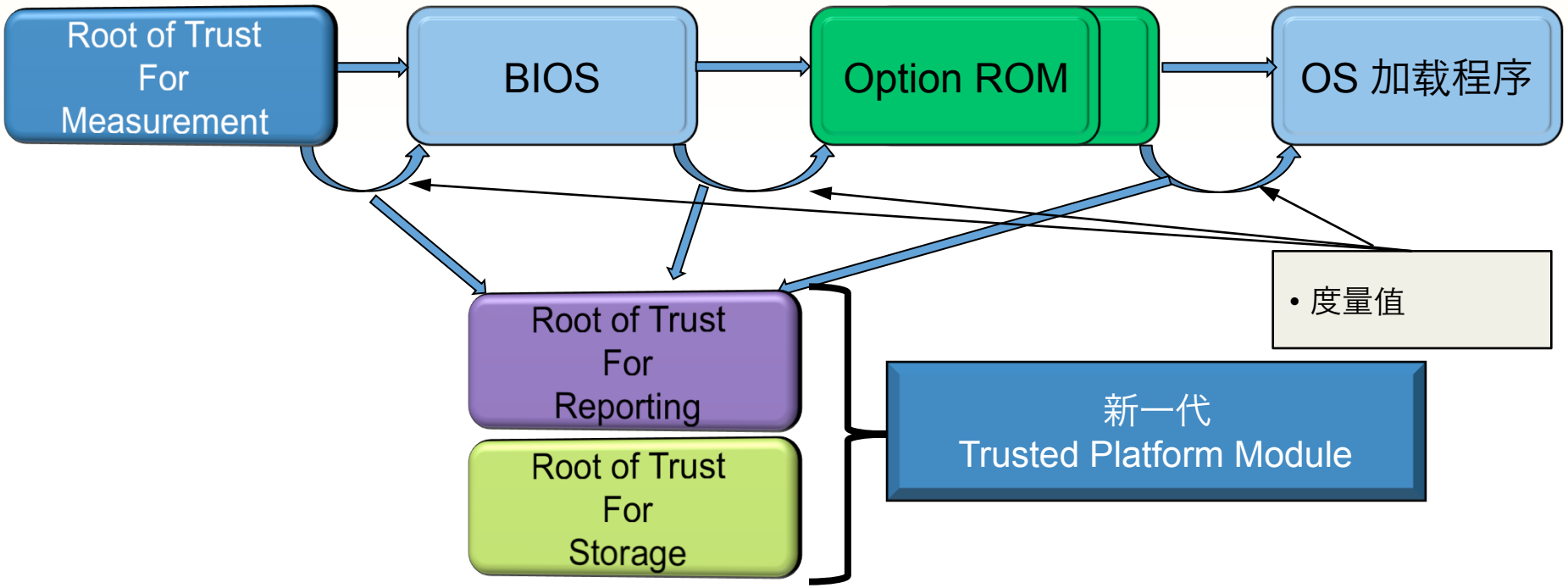
Root of Trust

- 必须信任的系统要素，因为无法检测到异常行为。



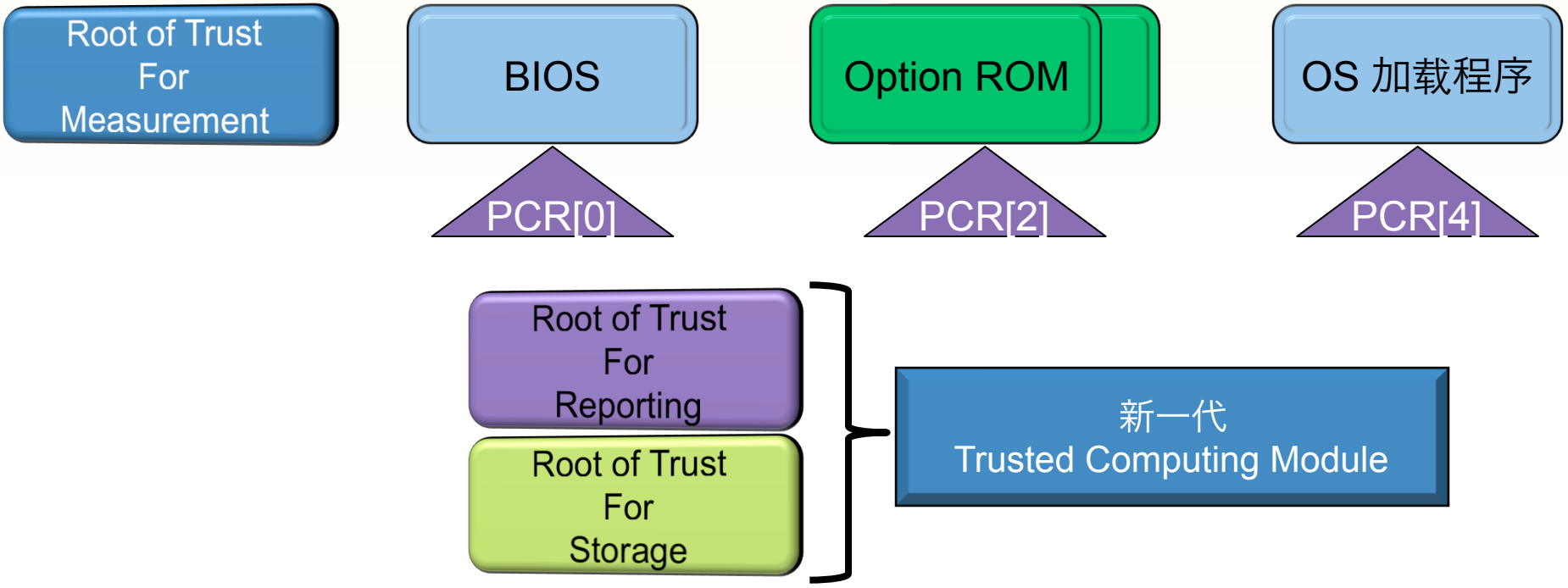
信任链

- 由 RTM 启动的一连串关联度量
- 提供启动顺序“审核”

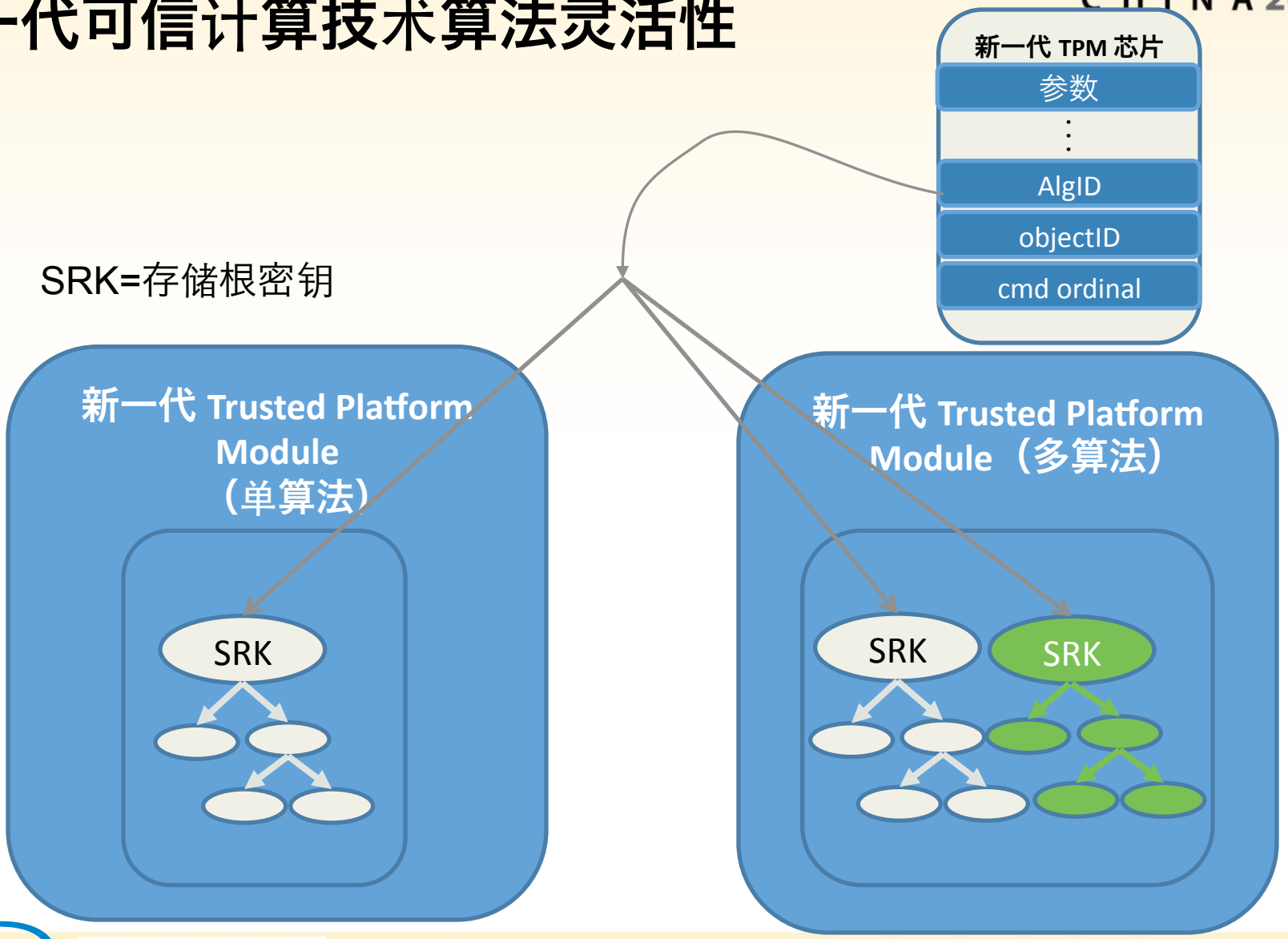


PC 客户端应用程序

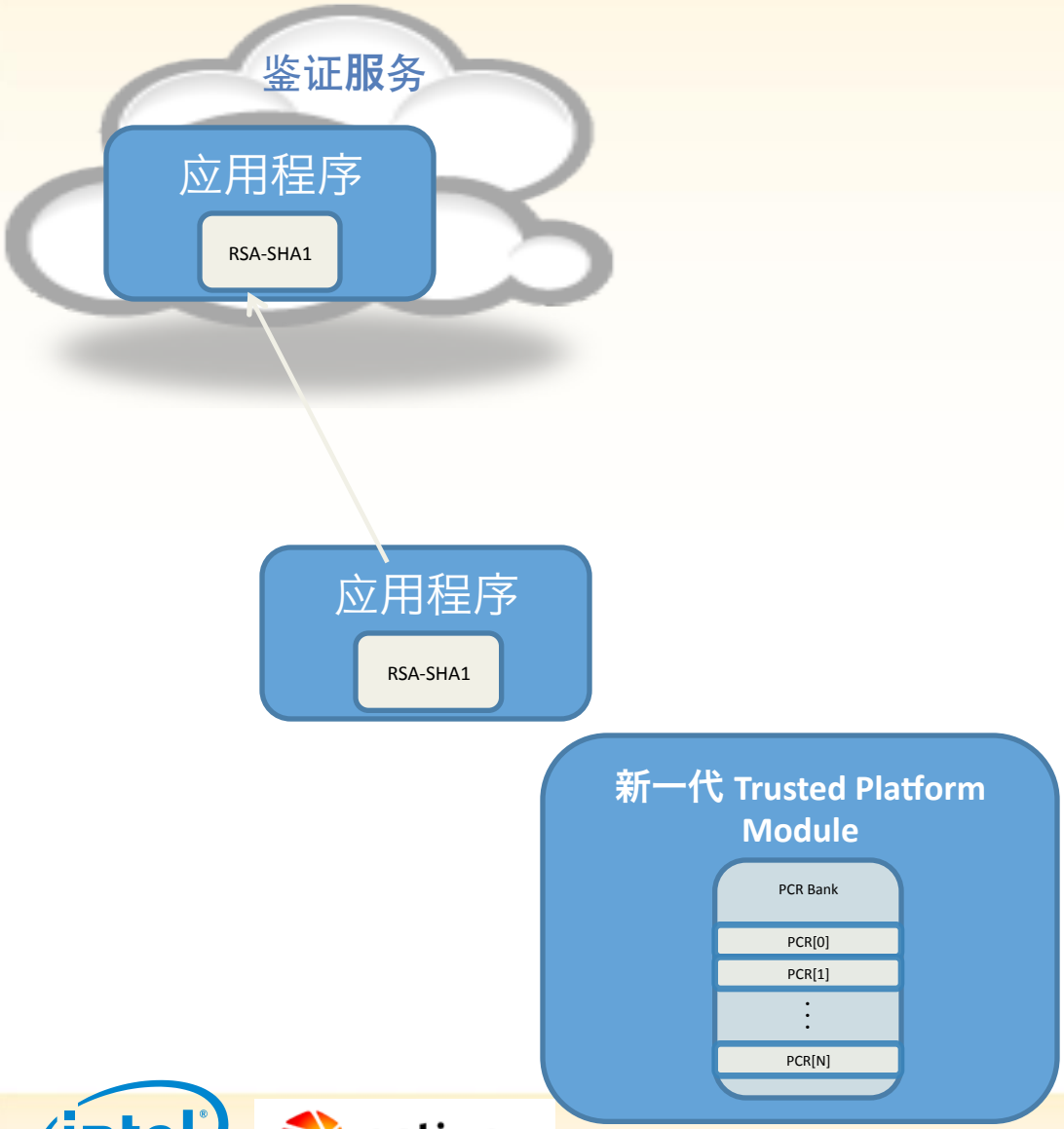
- 将 BIOS 组件与平台配置注册表 (PCR) 相对应



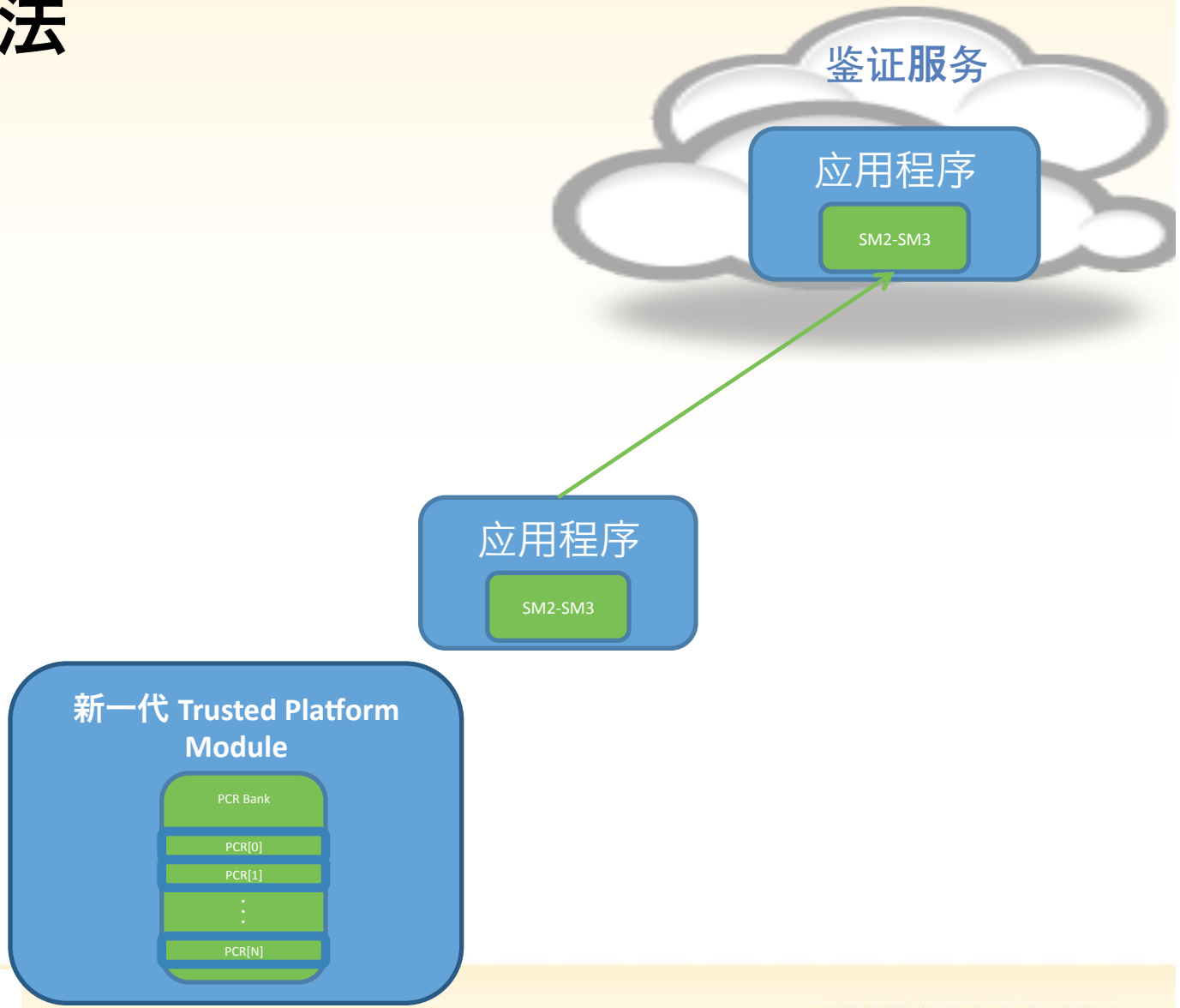
新一代可信计算技术算法灵活性



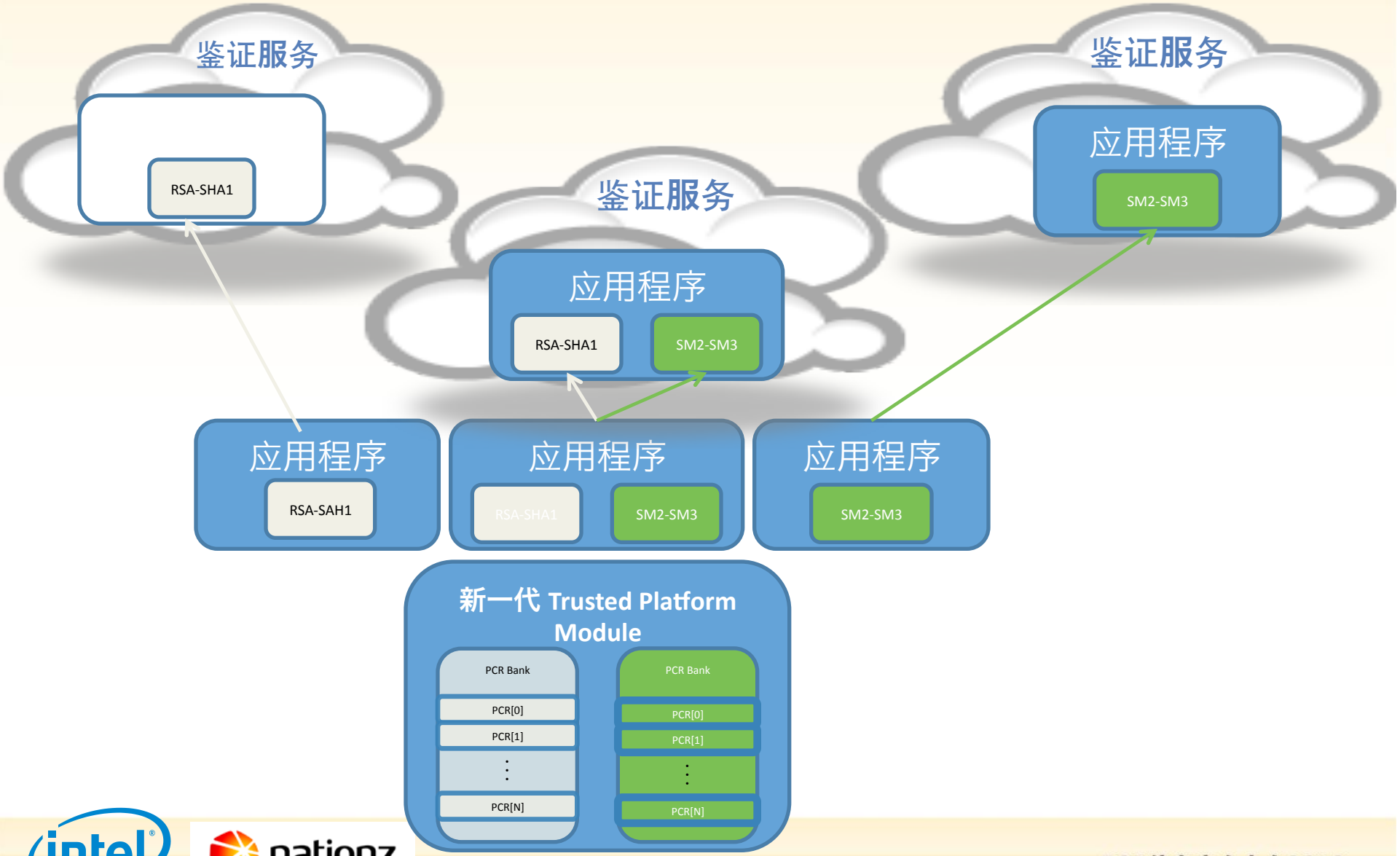
鉴证：单算法


鉴证服务
应用程序
RSA-SHA1
应用程序
RSA-SHA1
新一代 Trusted Platform Module
PCR Bank
PCR[0]
PCR[1]
PCR[N]

鉴证：单算法


鉴证服务
应用程序
SM2-SM3
应用程序
SM2-SM3
新一代 Trusted Platform Module
PCR Bank
PCR[0]
PCR[1]
PCR[N]

鉴证：多算法


鉴证服务
RSA-SHA1
鉴证服务
应用程序
RSA-SHA1
SM2-SM3
鉴证服务
应用程序
SM2-SM3
应用程序
RSA-SAH1
应用程序
RSA-SHA1
SM2-SM3
应用程序
SM2-SM3
新一代 Trusted Platform Module
PCR Bank
PCR[0]
PCR[1]
PCR[N]
PCR Bank
PCR[0]
PCR[1]
PCR[N]

获得一致的实施
Trusted Platform Module 2.0

RSA CONFERENCE CHINA 2012

- 该规范成了其自身的首次实施
-
  - 该规范的测试代码，首款 Trusted Platform Module 硬件发布前提供
- 可缩短硬件开发流程
- 改写规范中的代码，而不是从零开发
- 目的：使实施更有规律
- Trusted Platform Module 的一致实施可提高系统的可信性

规范结构

包含与实施相关的主要子系统（例如 NV 内存）

- 第 2 部分包含接口元素的标准定义
- 用于定义结构的表
- 表注释允许使用自动化工具提取必要的 C 代码结构定义，并生成封送和解封的代码

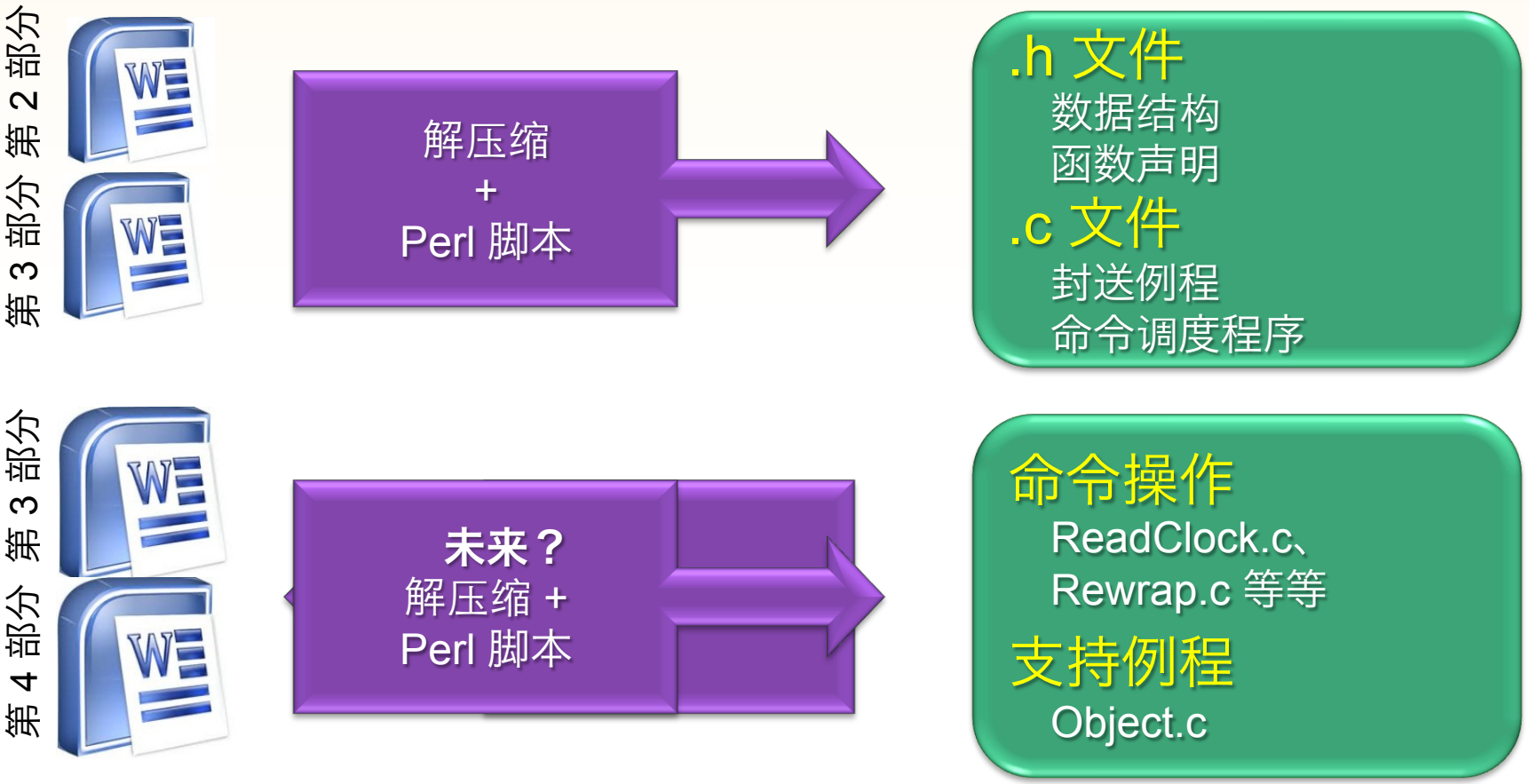
第 3 部分是 TPM 命令的标准定义

- 各命令的叙述性描述
- 定义接口参数（命令和响应）的表
- 用 C 代码编写的详细操作
- 第 3 部分的 C 代码在大量实施中可能会按原样使用

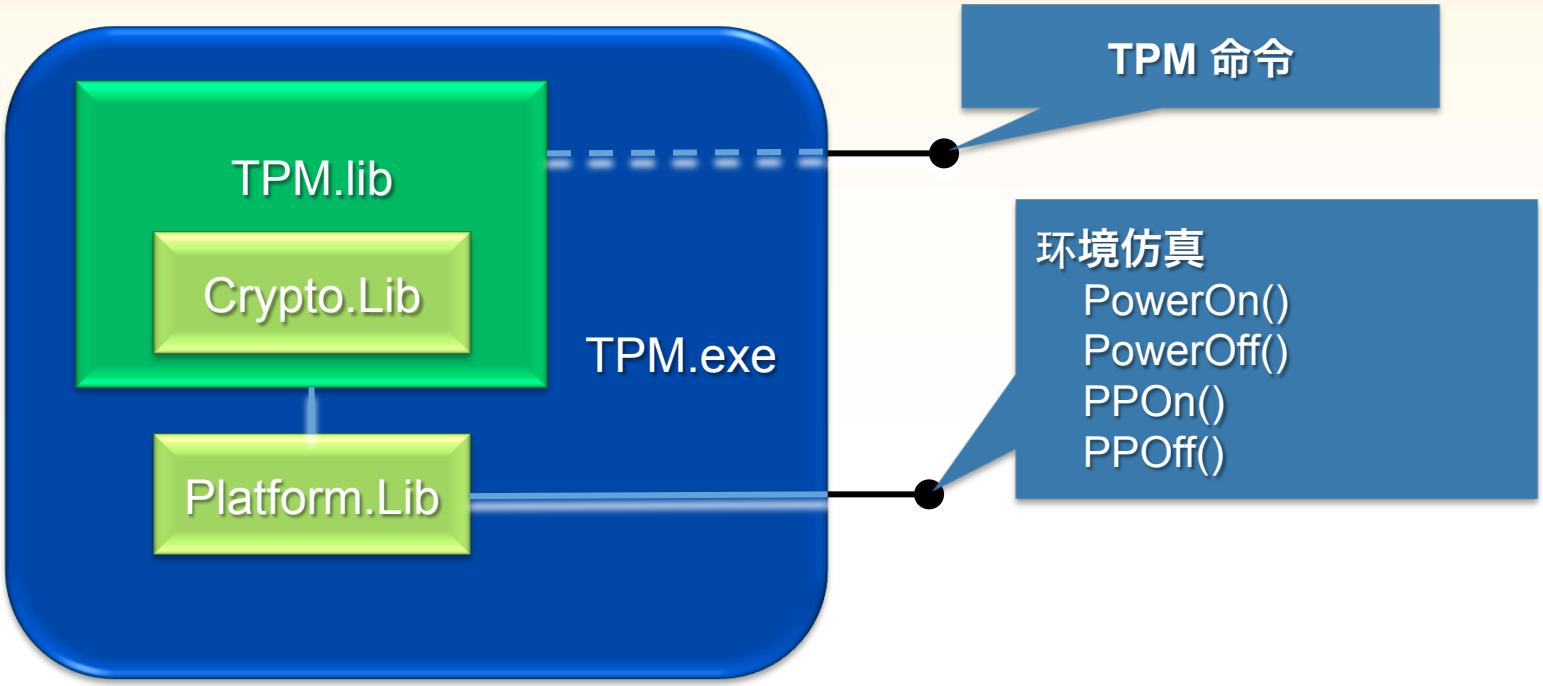
- 第 4 部分提供几乎所有 C 代码的相关信息
- 包含与实施相关的主要子系统（例如 NV 内存）
- 包含不会在实际 TPM 中出现但允许构建可执行参考 TPM 的某个框架代码
  - 允许任何人构建和测试代码 – 只需添加加密库
- 在各项实施中，第 4 部分的大多数代码预计将被替换成其他内容

工具

Specification.docx　　工具　　参考实施



参考实施中的主要模块



Tpm.lib – Vanilla c 代码。无需 OS 直接支持
CryptoLib – 加密例程
PlatformLib – OS 服务（内存、存储…）
TPM.exe – 参考实施显示了两个网络 TCP 端口

议程

- 安全趋势和问题
- 最安全处理的基础
- 安全趋势和问题
- 可信执行技术提供可见性和执行点
- 总结
- 中国生态系统实现可信云
- 总结

中国国内的可信计算池解决方案堆栈和生态系统

开放源代码

Tboot
OAT
TSS
OpenSSL
ODCA

华中科技大学 Huazhong University of Science and Technology
武汉大学

S²C 中标软件

openstack CLOUD SOFTWARE

HUAWEI

Xen

BYOSOFT 百敖软件

nationz

需要业界广泛协作，为新开发人员提供机会

*其他名称及品牌为其各自所有者的资产

总结/行动标语

- 可信计算池使用模型对于适用的云部署至关重要
- 新一代可信计算技术是实施可信计算池的基础
- Intel 和 Nationz 将携手共建可信计算池
- 与 Intel、Nationz* 和本地供应商一起确定协作点，构建解决方案堆栈

谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012