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

Trusted Computing Pools for China Ecosystem

Yan Li, Chief Cloud Solution Architect

DCSG Technology Marketing

Xin Liu, Nationz, Product Manager

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

Agenda

- Security trends and concerns
- The foundation for best secure processing
- Meeting the security challenge:
- Technologies and use models to mitigate pain points

  Virtualization Technology enhances workload isolation

  Trusted Execution Technology provides visibility and enforcement point

- Next Generation TPM standards for China
- China ecosystem enabling for Trusted Cloud
- Summary

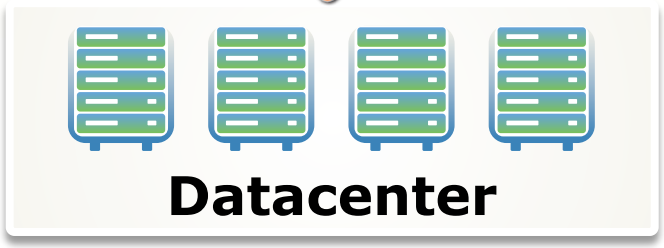
Security in the Enterprise Trends

Security Concerns Growing for Datacenter and Cloud

Trend:
Shift in types of attack

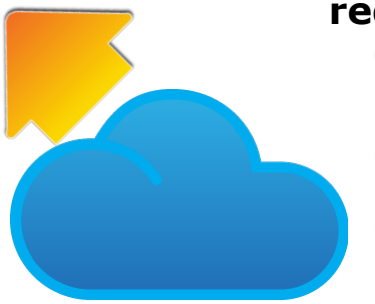
Platform as a target, not just software

Stealth and control as objectives



Trend:
Increased compliance concerns, costs

UK Data Protection Act, FedRAMP, Payment Card Industry (PCI), etc. require security enforcement and create audit needs



Trend:
Changes in architectures require new protections

Virtualization and multi-tenancy

3rd party dependencies

Blurred boundary

Security Concerns Limit Adoption of Cloud

Better Security is Essential for Cloud Growth

IT Pro survey of key concerns:

57%
Avoid putting workloads with compliance mandates in cloud[1]

61%
Say lack of visibility inhibiting private cloud adoption[1]

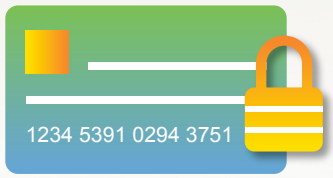
55%
Lack of control over public cloud[1]

[1] McCann 2012 State of Cloud Security Global Survey, Feb 2012

Server Security Technologies

Focus: Security and Trust Built-In

Hardened Foundation for Computing



Identity Protection and Fraud Deterrence

Detection and Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

Pain Point #1: Isolation

Isolating Workloads on Shared Infrastructures is Critical

A major concern of shared infrastructure

Lack traditional guarantees of physical separation

Multiple workloads may tamper or interact with each other

Homeland Security's Subcommittee Hearing:
Cloud Computing: What are the Security Implications?[1]

Multi-Tenant Solutions:
The Pros, the Questions and Integration Concerns[2]

Security Guidance for Critical Areas of Focus in Cloud Computing[3]

*Other names and brands may be claimed as the property of others

[1] http://www.govtrack.us/congress/committee.xpd?id=A0995/Security/3817_Homeland_Security_Hearing_Cloud_Computing_Implications.htm
[2] http://www.itbusinessedge.com/cm/blogs/lawson/multi-tenant-solutions-the-pros-the-questions-and-integration-concerns/?cs=45181&page=2
[3] https://cloudsecurityalliance.org/csaguide.pdf

Pain Point #2: Enforcement

New Controls Needed to Enforce Protection of Infrastructure

Pre-runtime environment target of new attacks

Protections abstracted away by virtualization and cloud

Low-level attacks are hard to detect and can be difficult to recover from

WEBROOT®

Mebromi: The First BIOS Rootkit in the Wild[1]

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

NIST Guidelines Seek to Minimize Risk of BIOS attacks[2]

Science & Technology Security & Trust

US Dept of Homeland Security Cyber Security Research & Development Broad Agency Announcement (BAA): BAA 11-02[3]

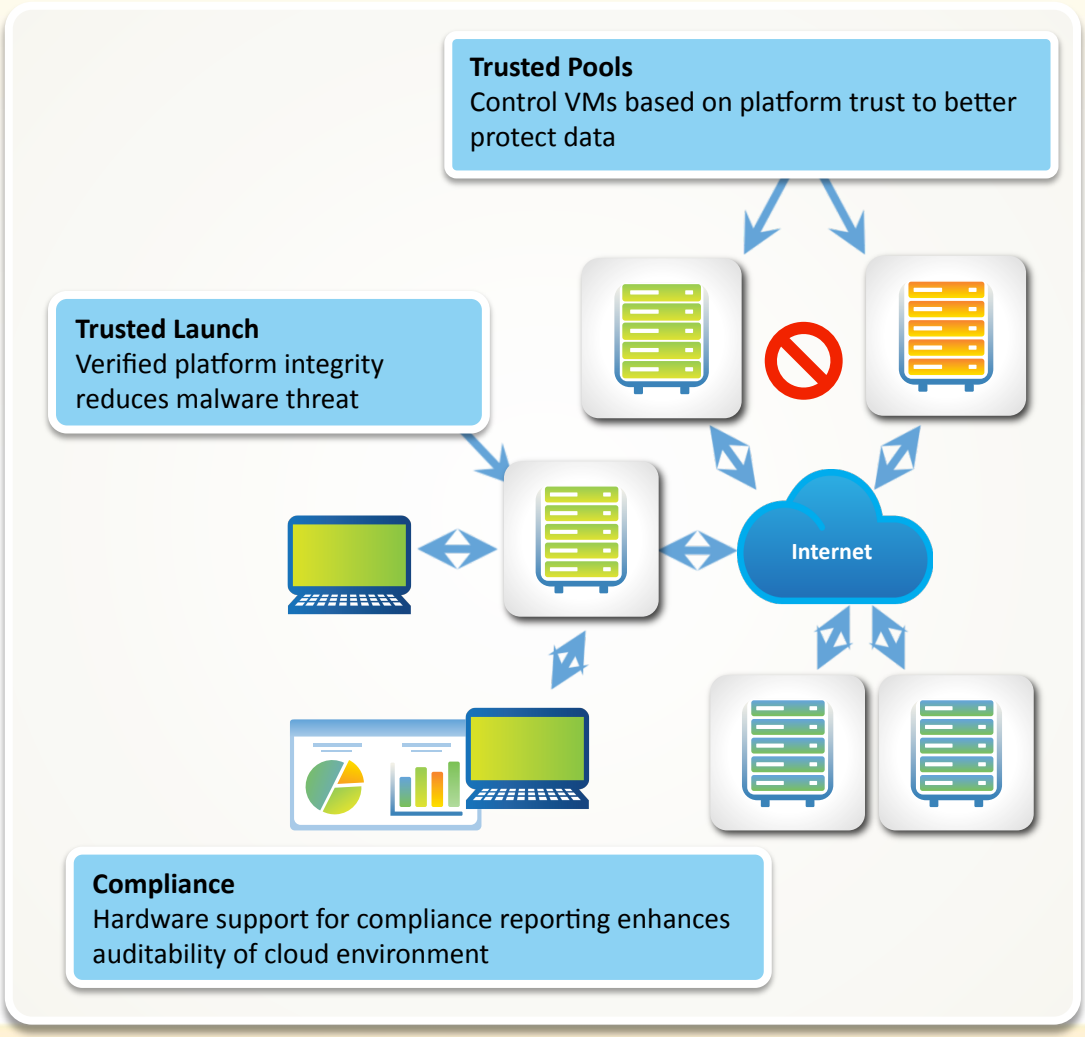
Collen http://www.outlookseries.com/A0995/Security/3817_Homeland_Security_Hearing_Cloud_Computing_Implications.htm
http://www.itbusinessedge.com/cm/blogs/lawson/multi-tenant-solutions-the-pros-the-questions-and-integration-concerns/?cs=45181&page=2
https://cloudsecurityalliance.org/csaguide.pdf

Trusted Execution Technology

Hardens and Helps Control the Platform

TXT:

- Enables isolation and tamper detection in boot process
- Complements runtime protections
- Hardware based trust provides verification useful in compliance
- Trust status usable by security and policy applications to control workloads



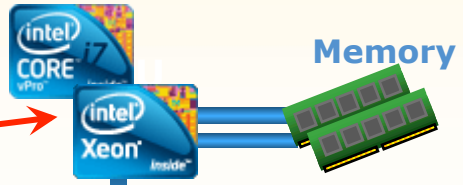
TXT Ingredients

Trusted Execution Technology extensions for measured launch & memory protection (SMX)

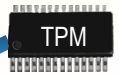
Processor contains hardware to authenticate AC Modules and perform measurements

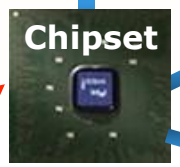
VT-d chipset feature blocks device access (e.g DMA) to protected memory pages

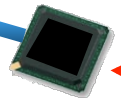
SINIT AC Module
BIOS AC Module



Memory





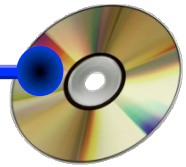


Intel Authenticated Software

3rd party TPM
stores and reports trusted environment measurements

BIOS / Flash
BIOS AC Module and platform initialization

3rd party Software
VMM/OS uses TXT mechanisms to establish a measured launch environment



Agenda

- Security trends and concerns
- The foundation for best secure processing
- Meeting the security challenge:
- Technologies and use models to mitigate pain points

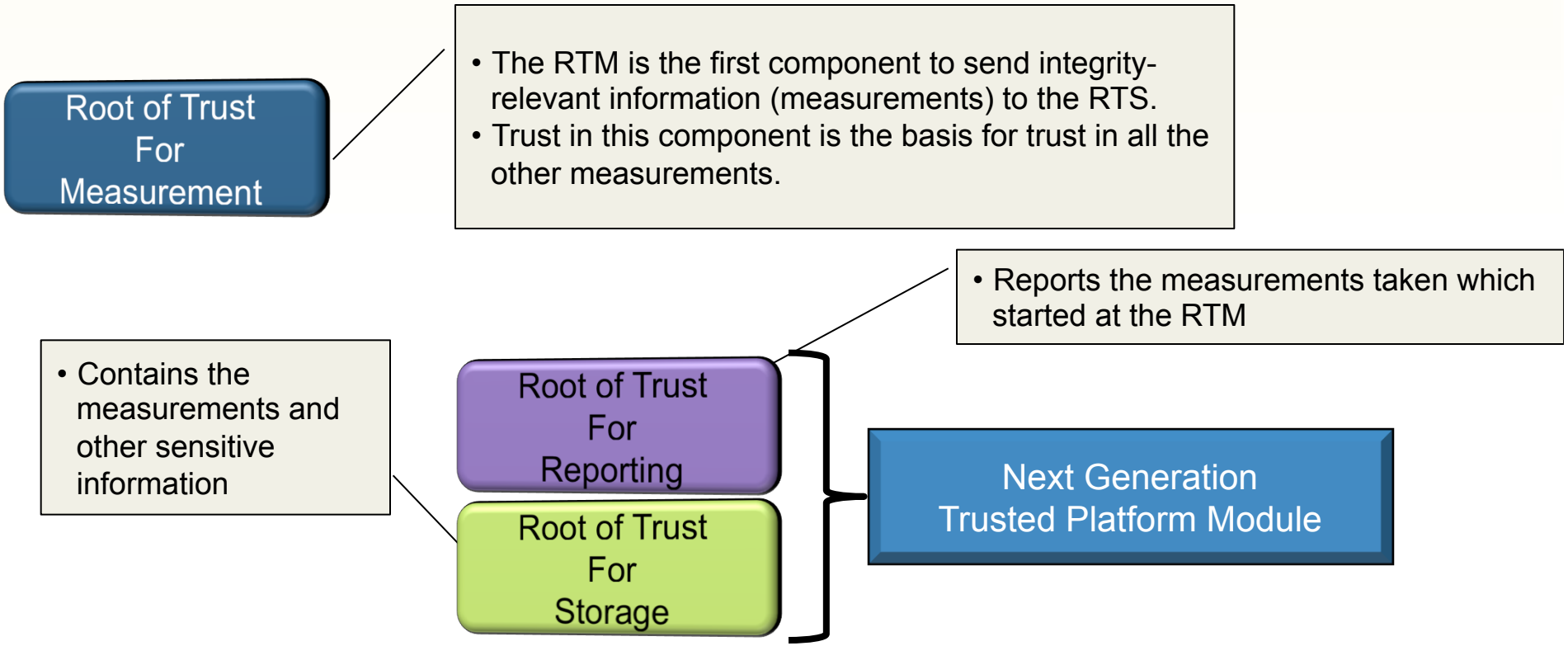
  Virtualization Technology enhances workload isolation

  Trusted Execution Technology provides visibility and enforcement point

- Next Generation TPM standards for China
- China ecosystem enabling for Trusted Cloud
- Summary

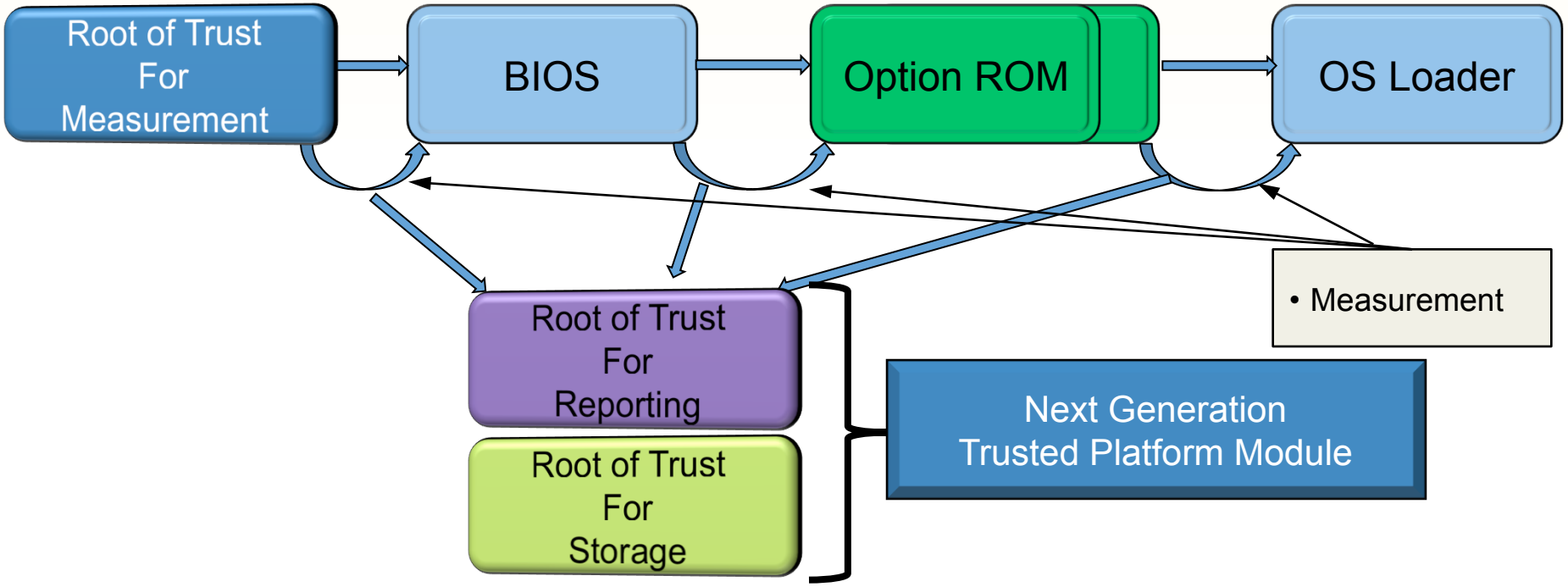
Root of Trust

- System elements that must be trusted because misbehavior is not detectable.



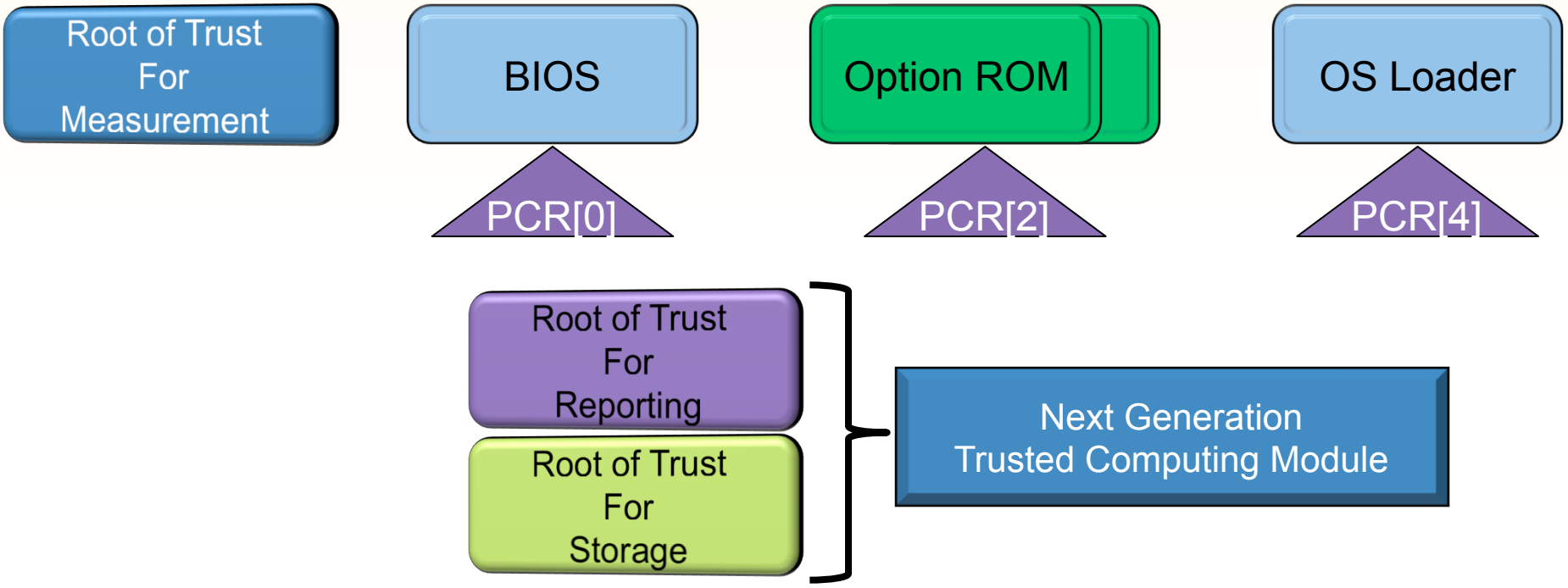
Chain of Trust

- A cohesive set of measurements started by RTM
- Provides an “audit” of boot sequence

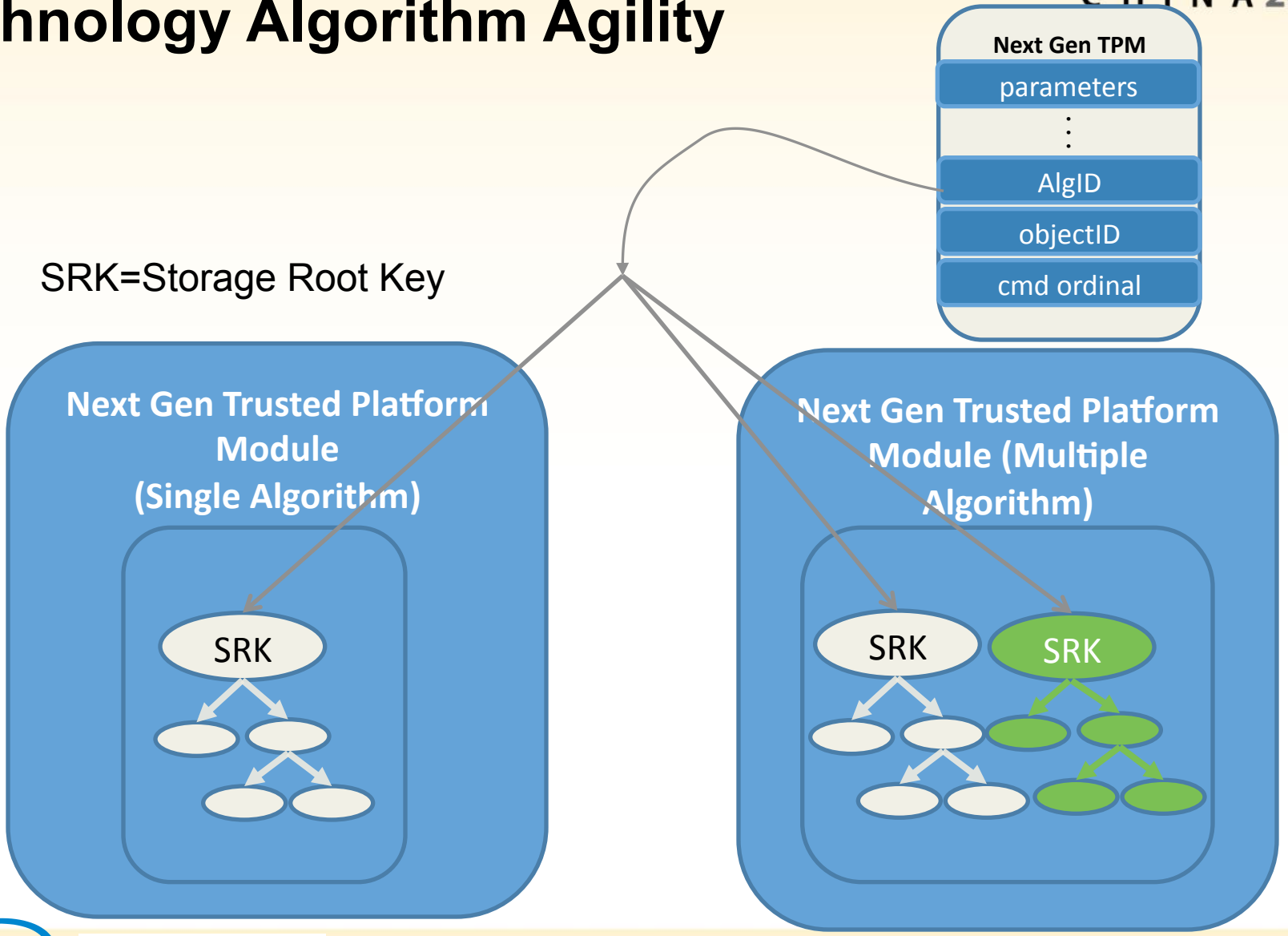


PC Client Application

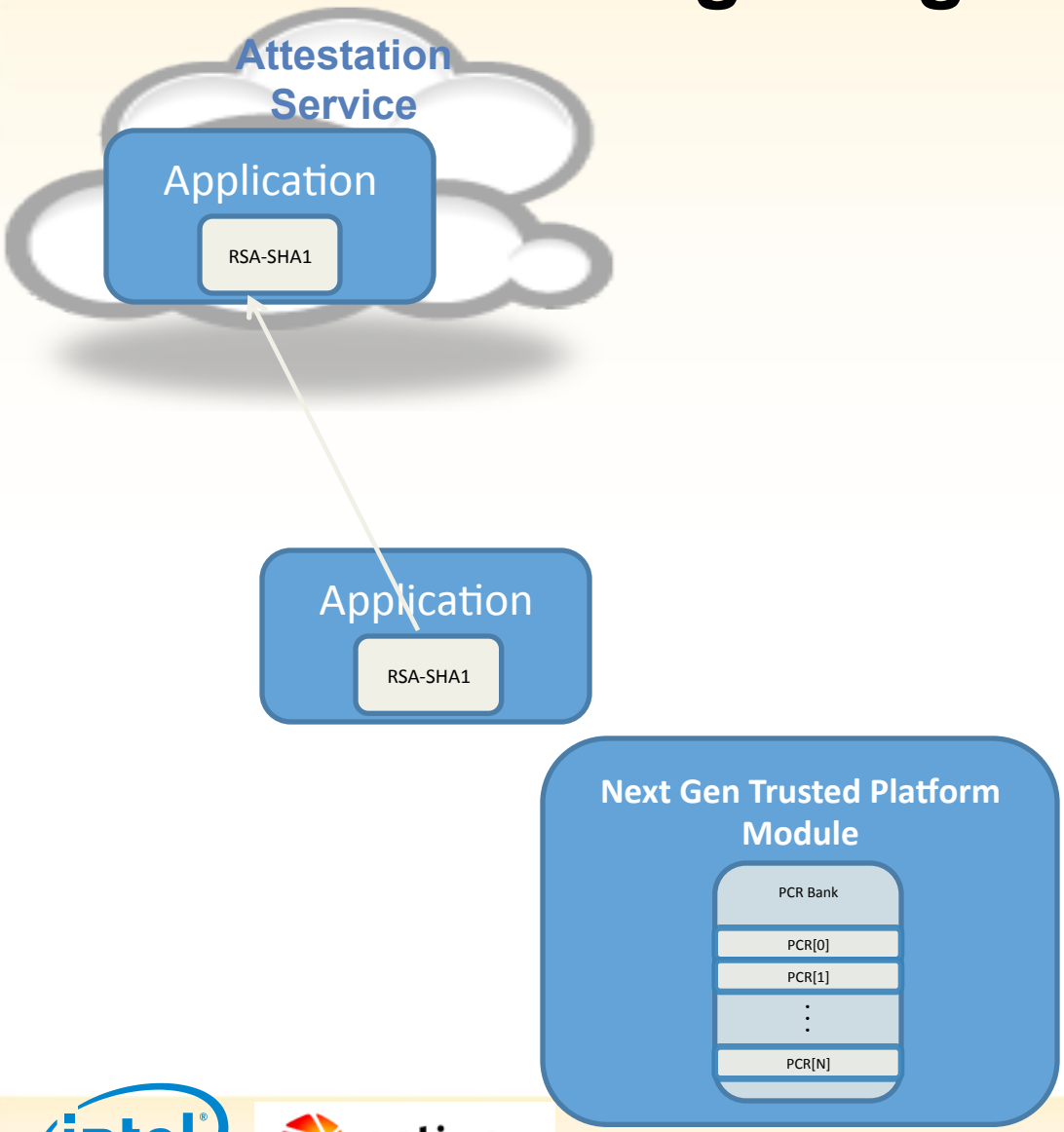
- Maps the BIOS components to Platform Configuration Registers (PCRs)



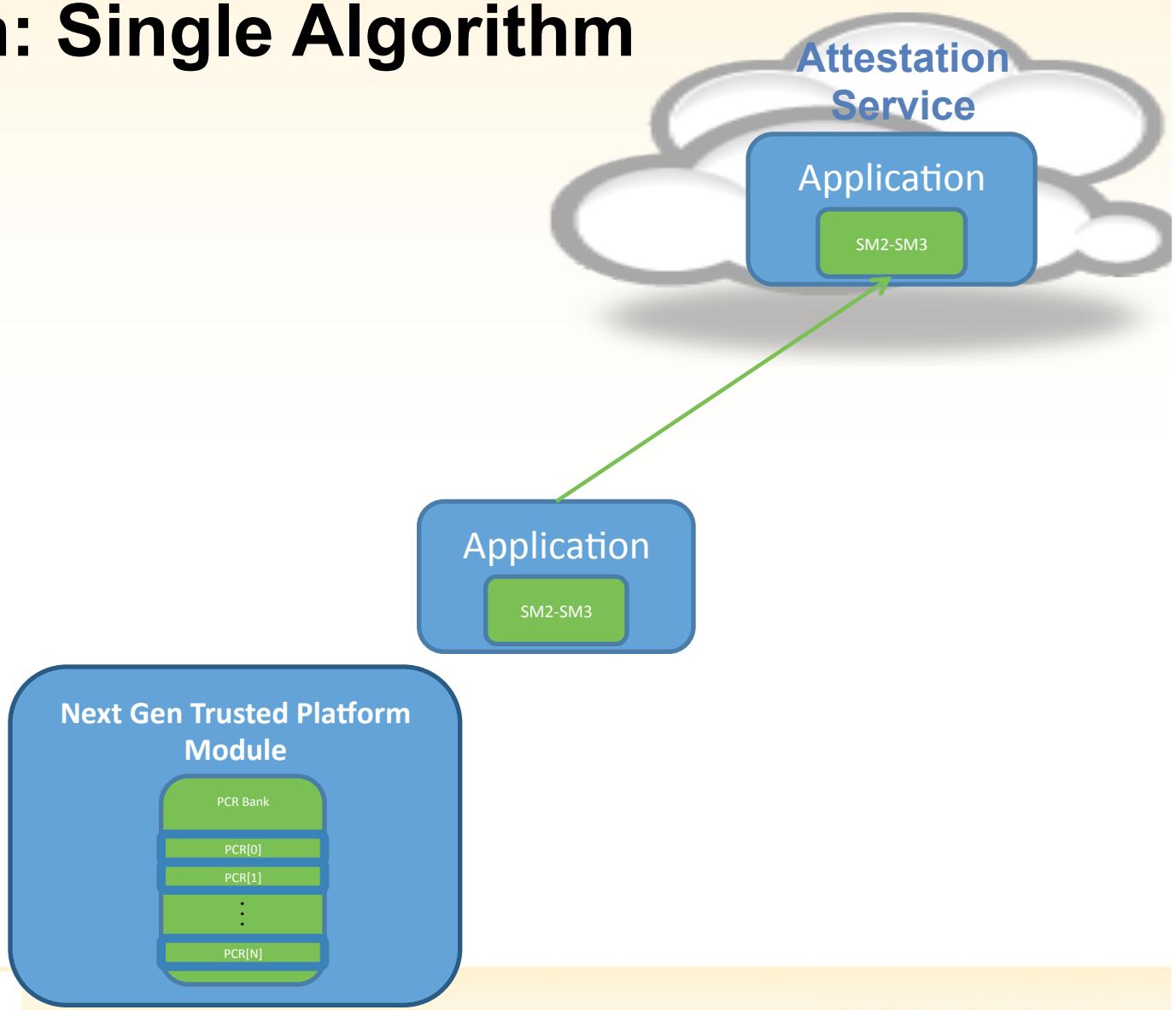
Next Generation Trusted Computing Technology Algorithm Agility



Attestation: Single Algorithm

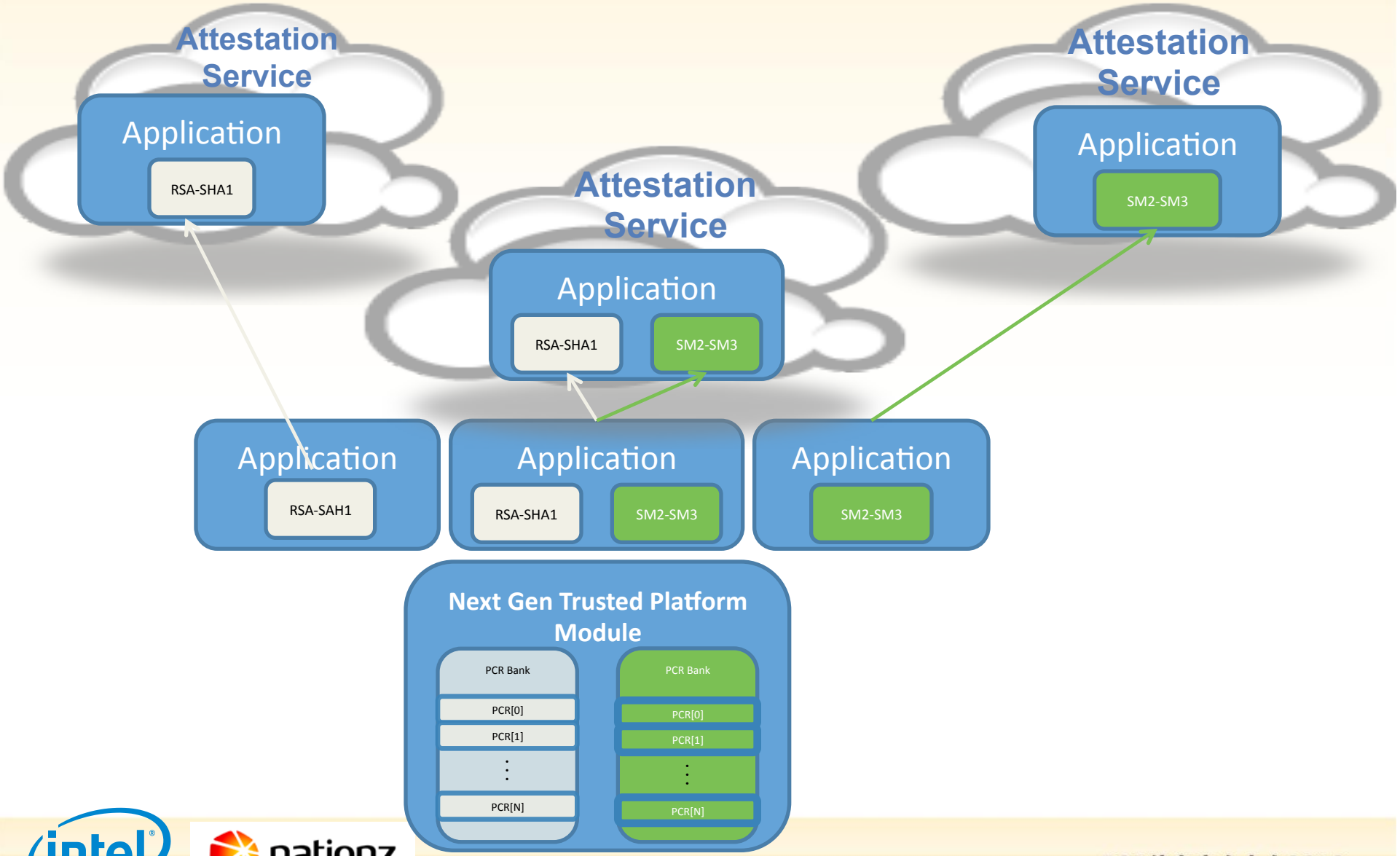


Attestation: Single Algorithm



Attestation: Multi-Algorithm

RSA CONFERENCE CHINA 2012



Getting Consistent Implementations Trusted Platform Module 2.0

RSA CONFERENCE CHINA 2012

- The specification becomes its own first implementation
  - Can simultaneously develop and validate the spec and the test suite
  - Debugged test suite available before the first hardware Trusted Platform Module
- May shorten the hardware development process
  - Adapt code from specification rather than develop from scratch
- Objective: Lead to more regularity of implementations
  - Improves trustworthiness of the system because of consistency of Trusted Platform Module implementations

Specification Structure

- Part 1 is the informative description of a TPM and its methods

- Part 2 contains the normative definition of the interface elements
  - Tables used to define structures
  - Table annotations allow automated tools to extract the necessary C-code structure definitions and generate the marshaling and unmarshaling code

- Part 3 is the normative definition of the TPM commands
  - Narrative description of each command
  - Tables defining the interface parameters (commands and response)
  - Detailed actions written in C-code
  - It is likely that C-code in Part 3 will be used as-is in a lot of implementations

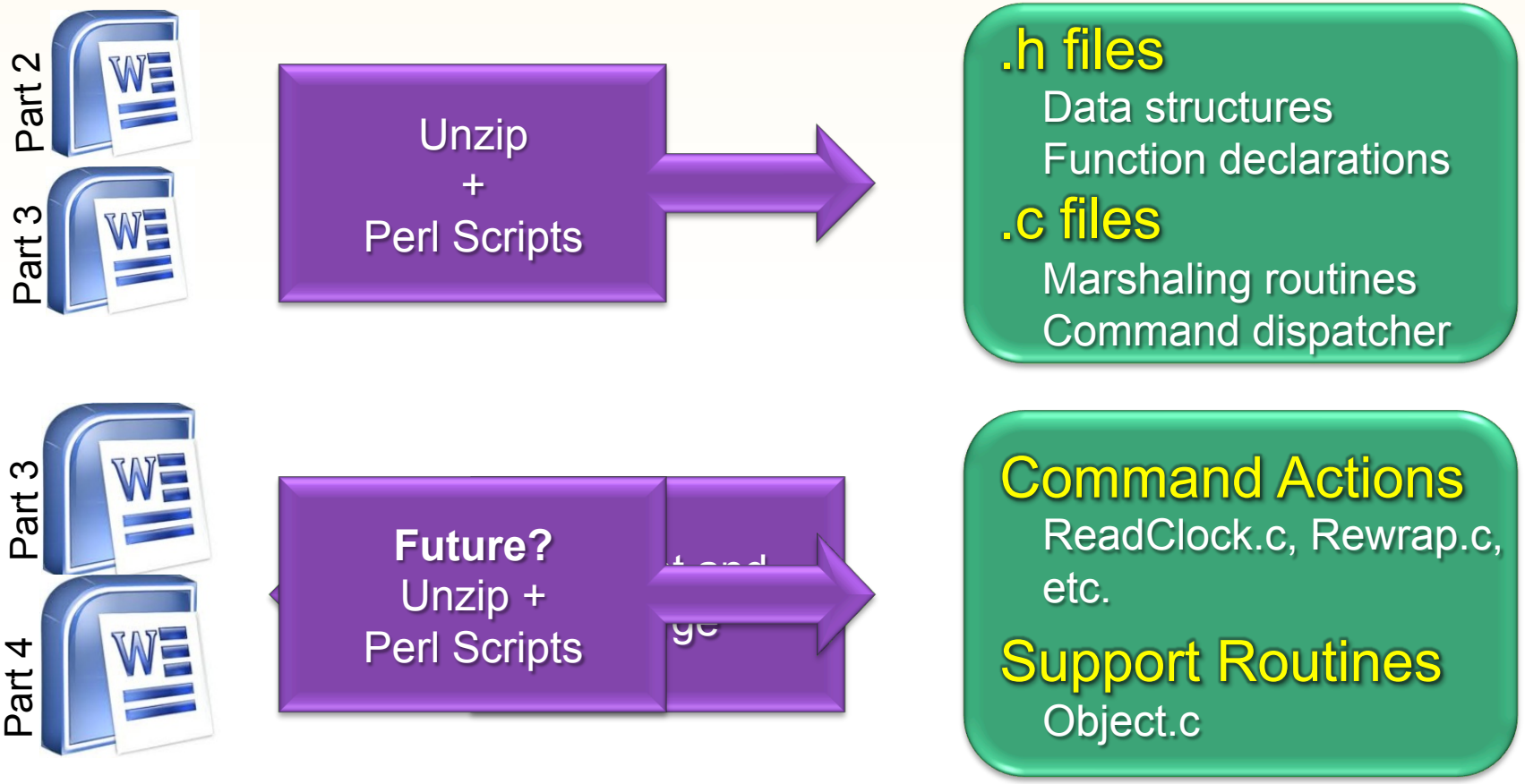
- Part 4 is an informative section that is almost all C-code
  - Contains major subsystems that are implementation-dependent (e.g., NV memory)
  - Contains some framework code that will not be in actual TPMs but which allows construction of an executable reference TPM
    - Allows anyone to build and test the code – just add a crypto library
  - It is expected that large portions of the Part 4 code will be replaced in each implementation

Tools

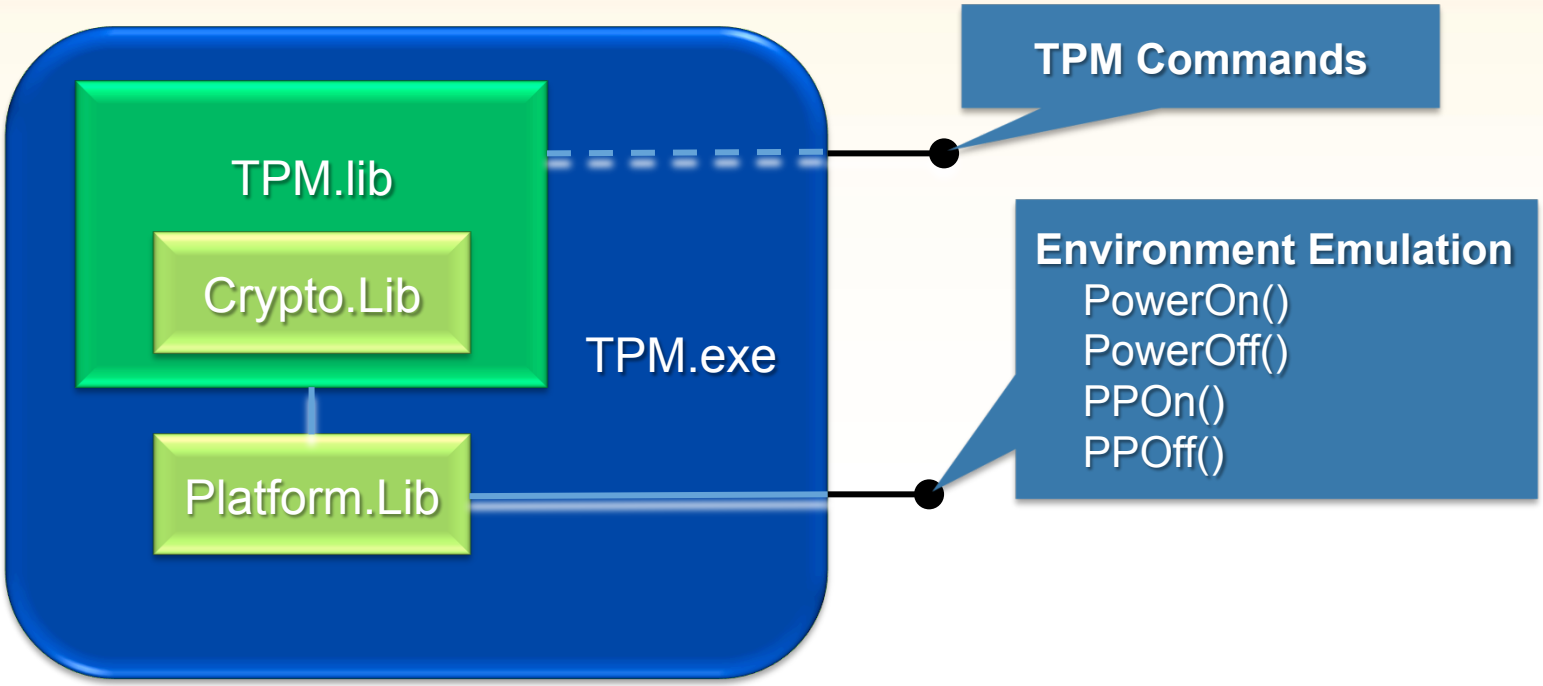
Specification.docx

Tools

Reference Implementation



Major Modules in the Reference Implementation



Tpm.lib – Vanilla c-code. Requires no direct OS support
CryptoLib – Cryptographic routines
PlatformLib – OS services (memory, storage…)
TPM.exe – Reference implementation exposes two network TCP ports

Agenda

- Security trends and concerns
- The foundation for best secure processing
- Meeting the security challenge:
- Technologies and use models to mitigate pain points

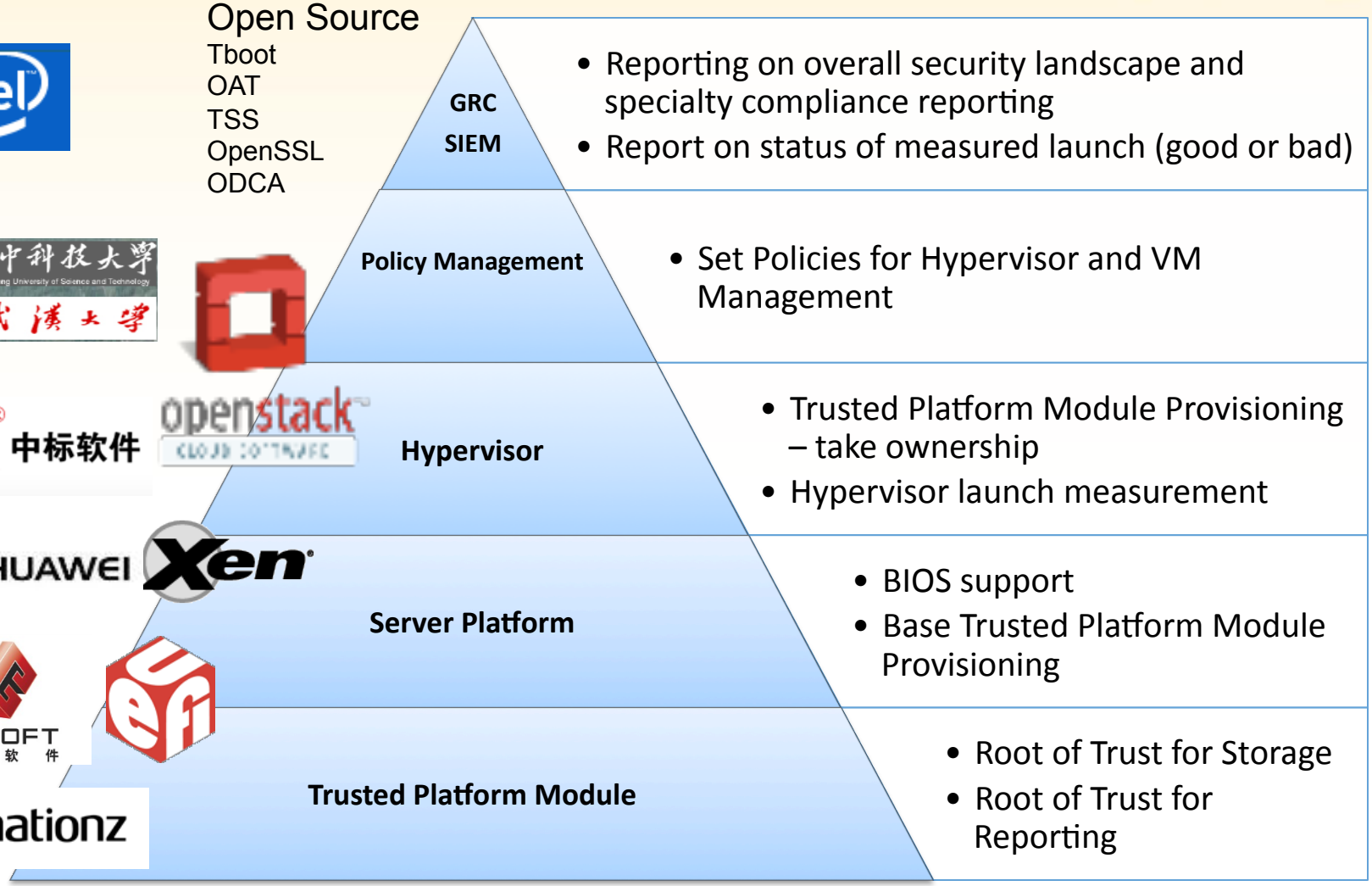
  Virtualization Technology enhances workload isolation

  Trusted Execution Technology provides visibility and enforcement point
- Next Generation TPM standards for China
- China ecosystem enabling for Trusted Cloud
- Summary

Trusted Compute Pools Solution Stack and Ecosystem in China

RSA CONFERENCE CHINA 2012

Open Source
Tboot
OAT
TSS
OpenSSL
ODCA



Requires Broad Industry Collaboration and Brings New Developer Opportunities

RSA信息安全大会2012

*Other names and brands may be claimed as the property of others

Summary/Call to Action

- The Trusted Compute Pools usage model is essential to usable cloud deployments
- Next generation trusted computing technology is the foundation for implementing the Trusted Compute Pools
- Intel and Nationz will work together to enable the Trusted Compute Pools
- Work with Intel, Nationz* and local vendors to identify the collaboration points and enable the solution stack

谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012