



# Challenges in the Management of Trusted Platforms

Thomas Hardjono  
TCG Infrastructure WG Co-Chair

DMTF Alliance Partner Technical Symposium  
March 27, 2008, San Jose CA

# Contents

- The Challenge of Trusted Computing
- Background on the TCG
- Overview of the TPM
- Managing Trust
- DMTF Work Register
- Conclusions & Outlook



# The Challenge of Trustworthy Computing

- Trustworthy Computing
  - How to create a safer computing environment that is faced with increasing frequency and sophistication of attacks
  - Protect end-user data
  - Enable trusted eCommerce transactions
  - Hardware-rooted trust
- Increase the level of trust in the computing platforms
  - Increase consumer confidence in Internet use
    - End-points in the global Internet are end-user PCs/PDAs
  - Reduce risks in business conducted over the Internet
    - Financial Services, Insurance, Government, Healthcare
  - Increase in transaction volume and value
- Increase trust in broader types of computing platforms
  - Laptops, Desktops, PDA, Servers, Mobile Phones, Network gear, etc.
- Communicate Trust
  - Attestations and assertions about platforms
  - Part of trust-negotiations in transactions



# Technical Challenge & Approach

- Challenge:

- Allow communicating platforms to dynamically accept and execute code supplied by other platform over the Internet
- Allow a platform connect and interact with remote platforms.
- Protection of data from misuse.

- Approach:

- Turn the entire platform into a trustworthy environment.
- Enable a platform to *prove* that a given software environment is a protected environment.
- Hide secrets until the correct software environment is arrived at



# Background on the TCG

The Trusted Computing Group

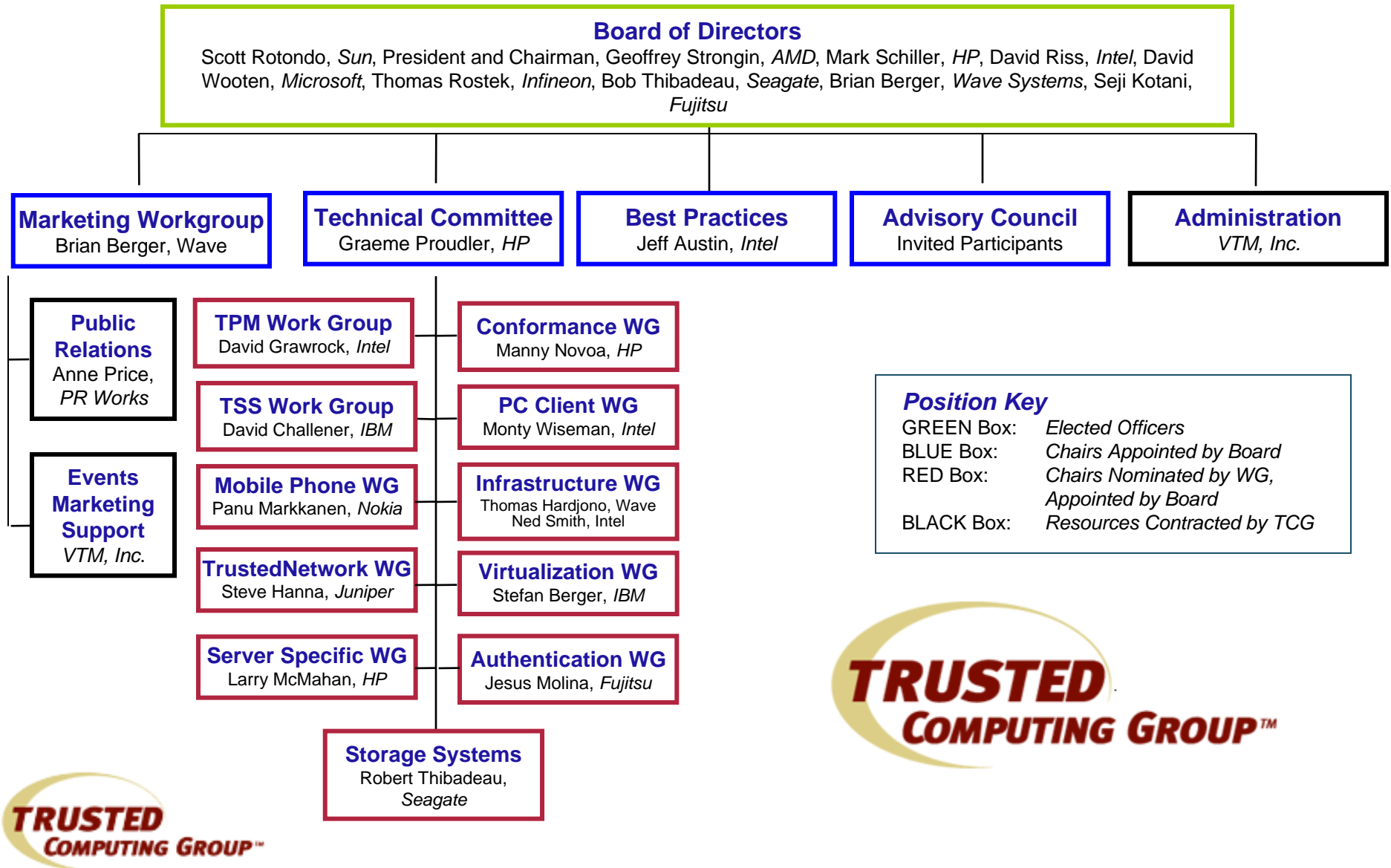


# Brief History of the TCG

- The Trusted Computing Platform Alliance (TCPA)
  - Established by the 5 founders in 1999
    - Intel, AMD, IBM, HP and MSFT
  - Charter focused on TPM1.1 and TSS
  - TPM1.1 specifications publicly released at end of 2002
- The Trusted Computing Group (TCG)
  - Established in March 2003 as continuation of TCPA
  - Charter and Bylaws expanded:
    - TPM1.2 and TSS for 1.2
    - Infrastructure Services
    - Peripherals (with or without a TPM)
    - PDAs, Mobile Phones, Servers
  - Organization structure expanded
  - Levels of membership, Liason Program, elected BoD members, etc.



# Structure of the TCG



# TCG Membership

160+ Total Member Companies as of May 2007

## Promoters

AMD  
Hewlett-Packard  
IBM  
Intel Corporation  
Microsoft  
Sony Corporation  
Sun Microsystems, Inc.

## Adopters

Ali Corporation  
American Megatrends, Inc.  
Enterasys Networks  
Foundry Networks Inc.  
Foundstone, Inc.  
Gateway  
Industrial Tech. Research Institute  
iPass  
OSA Technologies  
Silicon Integrated Systems Corp.  
Softex, Inc.  
Toshiba Corporation  
Winbond Electronics Corporation

## Contributors

Agere Systems  
ARM  
ATI Technologies Inc.  
Atmel  
AuthenTec, Inc.  
Broadcom Corporation  
Comodo  
Dell, Inc.  
Extreme Networks  
Fujitsu Limited  
Fujitsu Siemens Computers  
Funk Software, Inc.  
Gemplus  
Giesecke & Devrient  
Hitachi, Ltd.  
Infineon  
InfoExpress, Inc.  
Juniper Networks  
Legend Limited Group  
M-Systems Flash Disk Pioneers  
Meetinghouse Data Communications  
Motorola Inc.  
National Semiconductor  
nCipher  
Network Associates  
Nokia

## Contributors

NTRU Cryptosystems, Inc.  
NVIDIA  
Philips  
Phoenix  
Renesas Technology Corp.  
RSA Security, Inc.  
SafeNet, Inc.  
Samsung Electronics Co.  
SCM Microsystems, Inc.  
Seagate Technology  
Shang Hai Wellhope Information  
Silicon Storage Technology, Inc.  
Standard Microsystems Corporation  
STMicroelectronics  
Sygate Technologies, Inc.  
Symantec  
Synaptics Inc.  
Texas Instruments  
Transmeta Corporation  
Trend Micro  
Utimaco Safeware AG  
VeriSign, Inc.  
VIA Technologies, Inc.  
Vodafone Group Services LTD  
Wave Systems  
Zone Labs, Inc.



# Overview of the TPM

## Trusted Platform Module



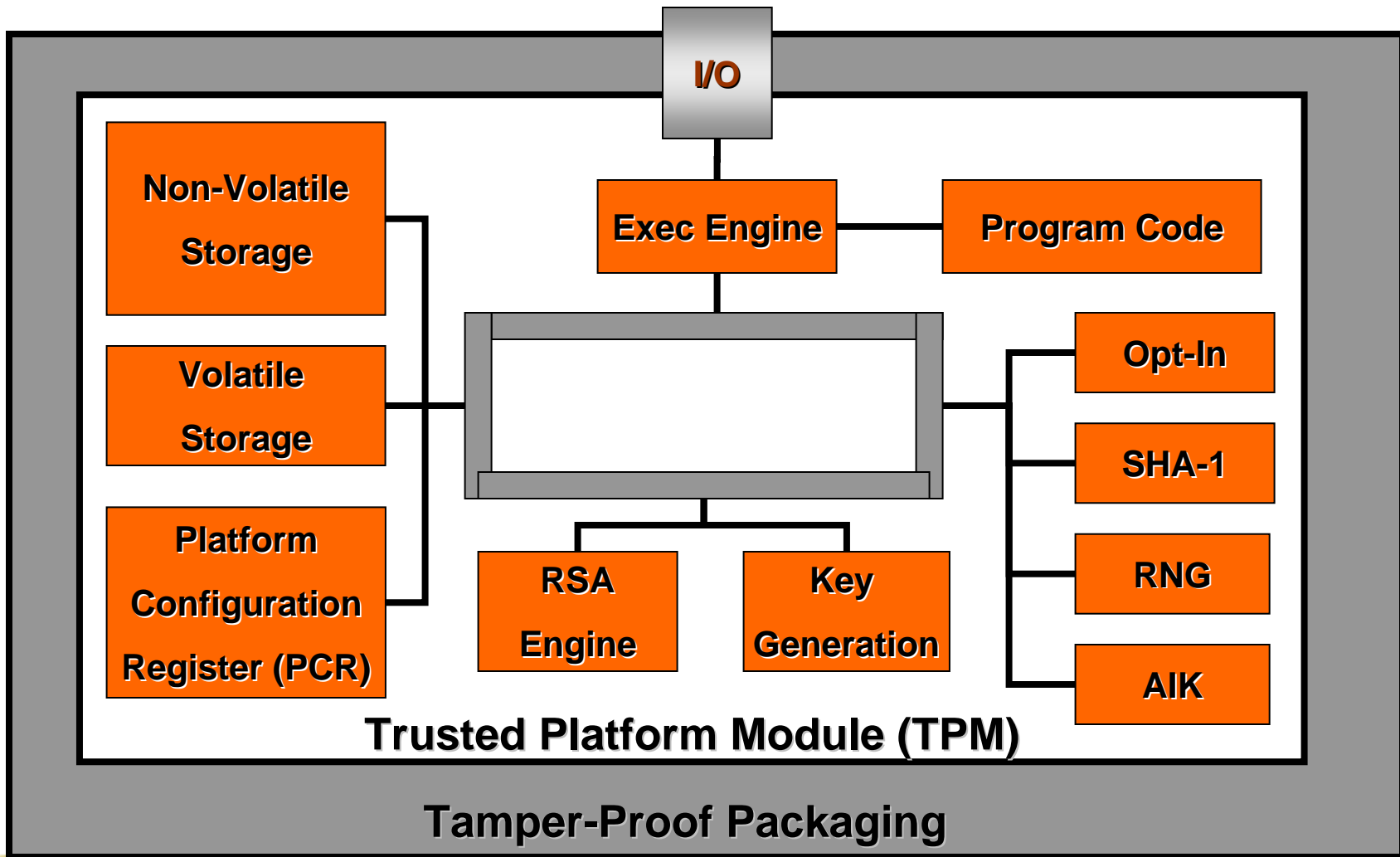
# What is a TPM?

- Defines hardware device<sup>1</sup> functionality
  - Not an implementation
- The TPM h/w cannot be physically removed
  - Bound to the platform
- The TPM contains
  - Cryptographic engine
  - Protected storage
- Functions and storage are isolated
  - Provides a “Trust Boundary”

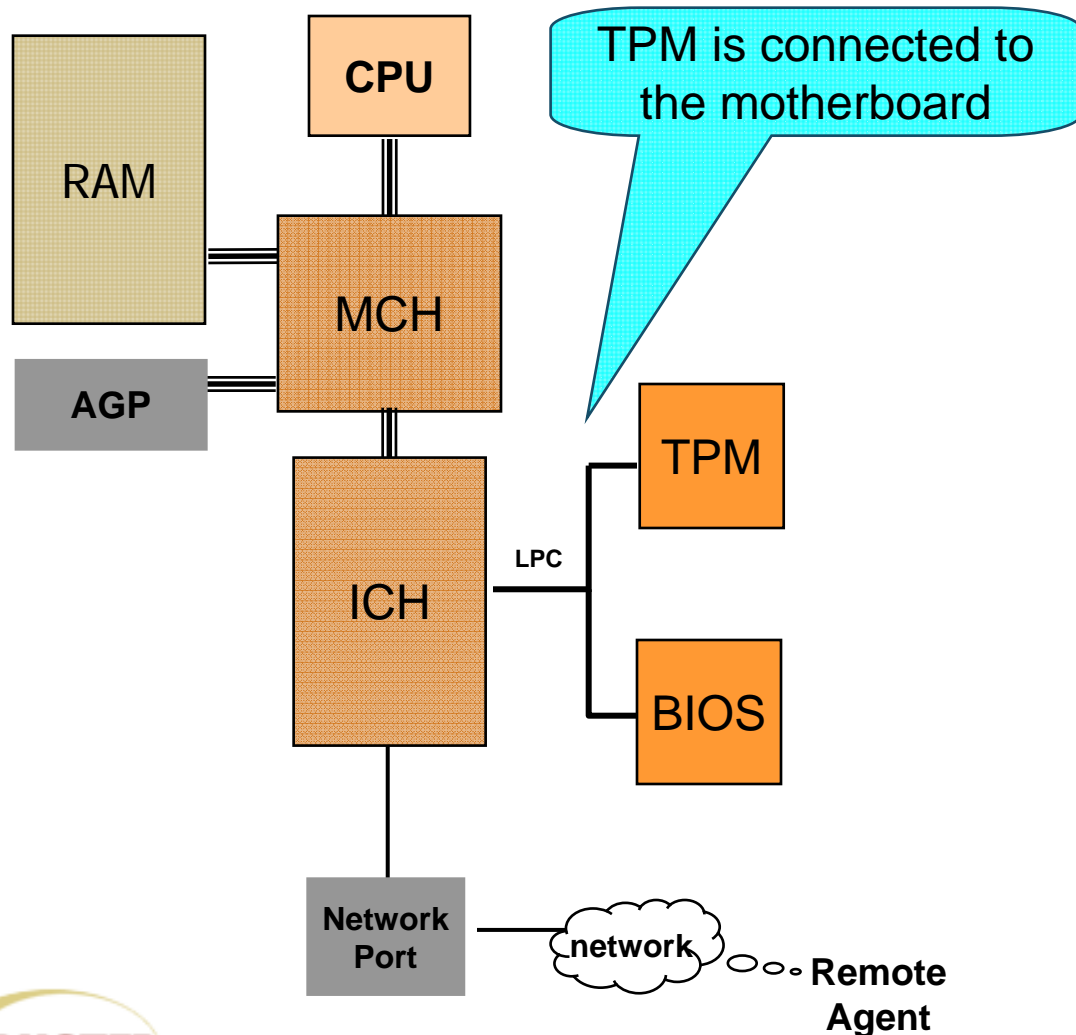


<sup>1</sup> TPM specifications must be implementable in software

# TPM Overview

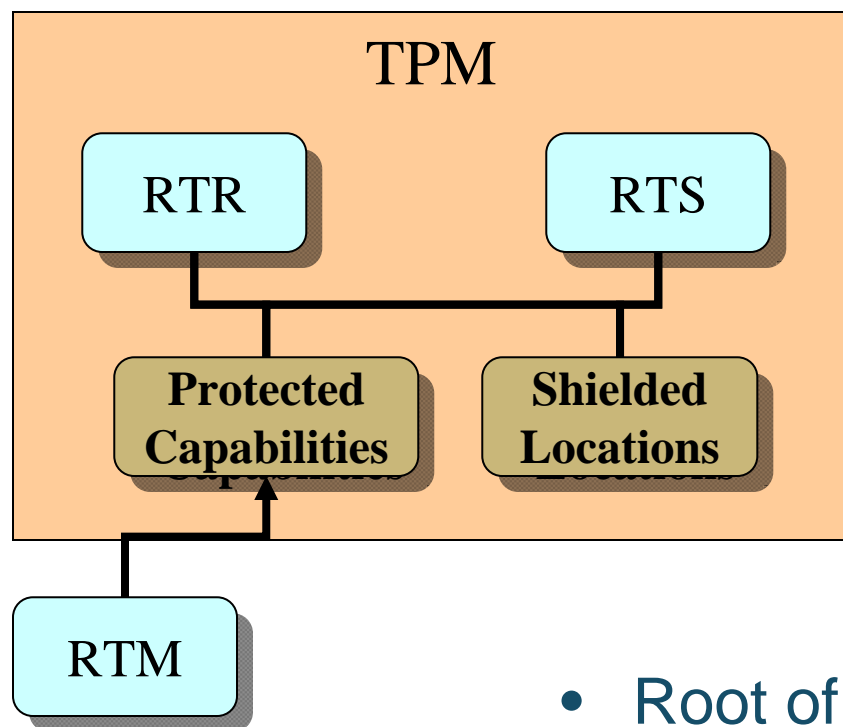


# TCG PC Client H/W Design



- In 1.1b all designs used the LPC bus
  - LPC bus was not required
- In 1.2 all designs **MUST** use the LPC bus

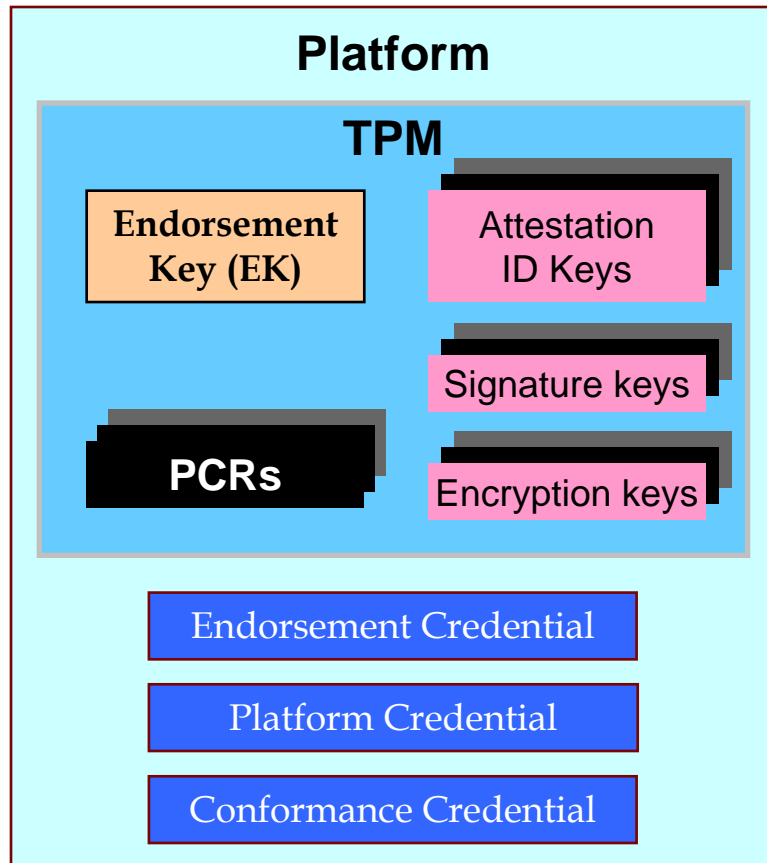
# Functional TPM Diagram



- Root of Trust for Reporting RTR
  - Provides cryptographic mechanism to digitally sign TPM state and information
- Root of Trust for Storage RTS
  - Provides cryptographic mechanism to protect information held outside of the TPM

- Root of Trust for Measurement
  - Provided by platform to measure platform state
  - Defined by platform specification
- Interaction between RTR and RTS is important TPM capability

# Generic Architecture

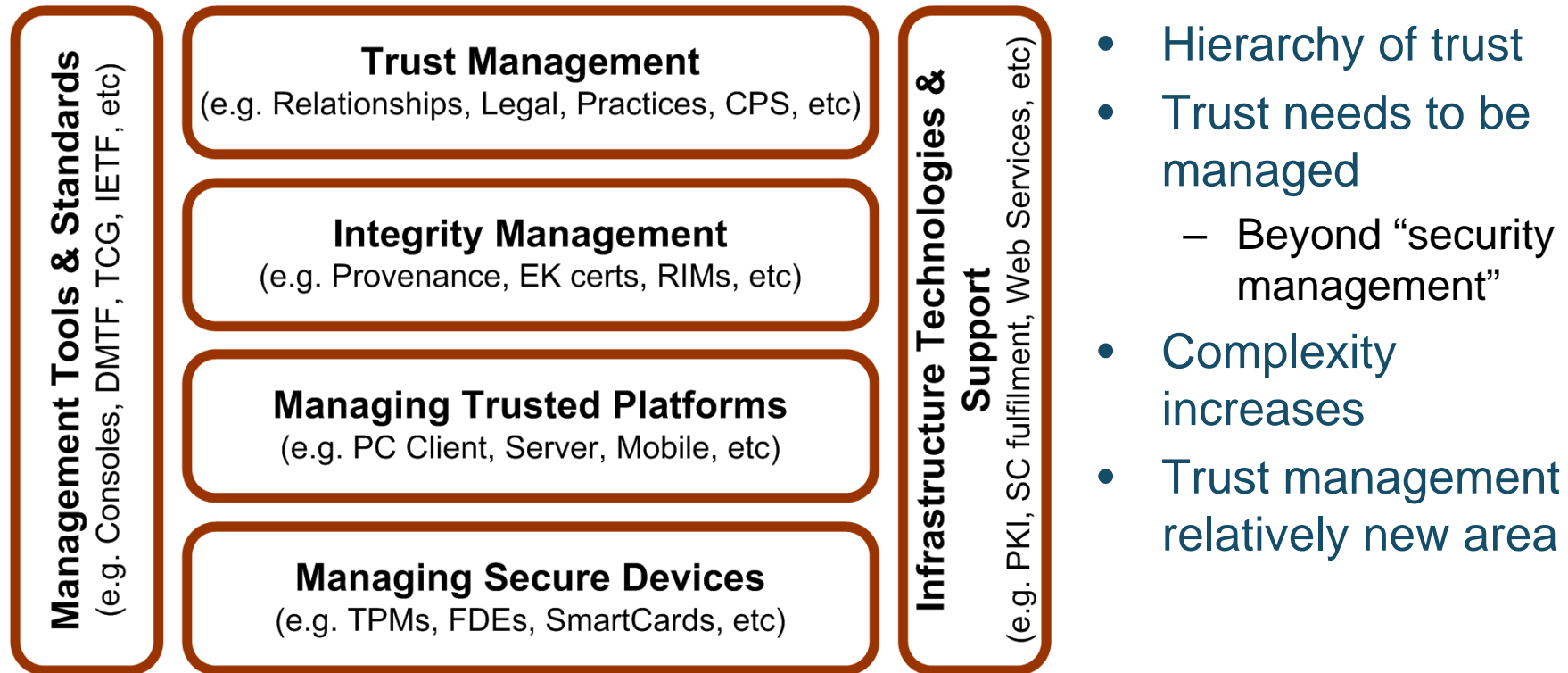


- TPM attached to platform
- Credentials held outside TPM
  - Endorsement credential normally provided by TPM manufacturer
  - Platform credential normally provided by platform manufacturer
  - Conformance credential provided by lab
- TPM can load and use a virtually unlimited number of AIK, signature and encryption keys



# Managing Trust

# Managing Trust



- Management tools & standards required
- Trust infrastructure:
  - Today limited to PKI and Identity Management
  - Support for Integrity Management

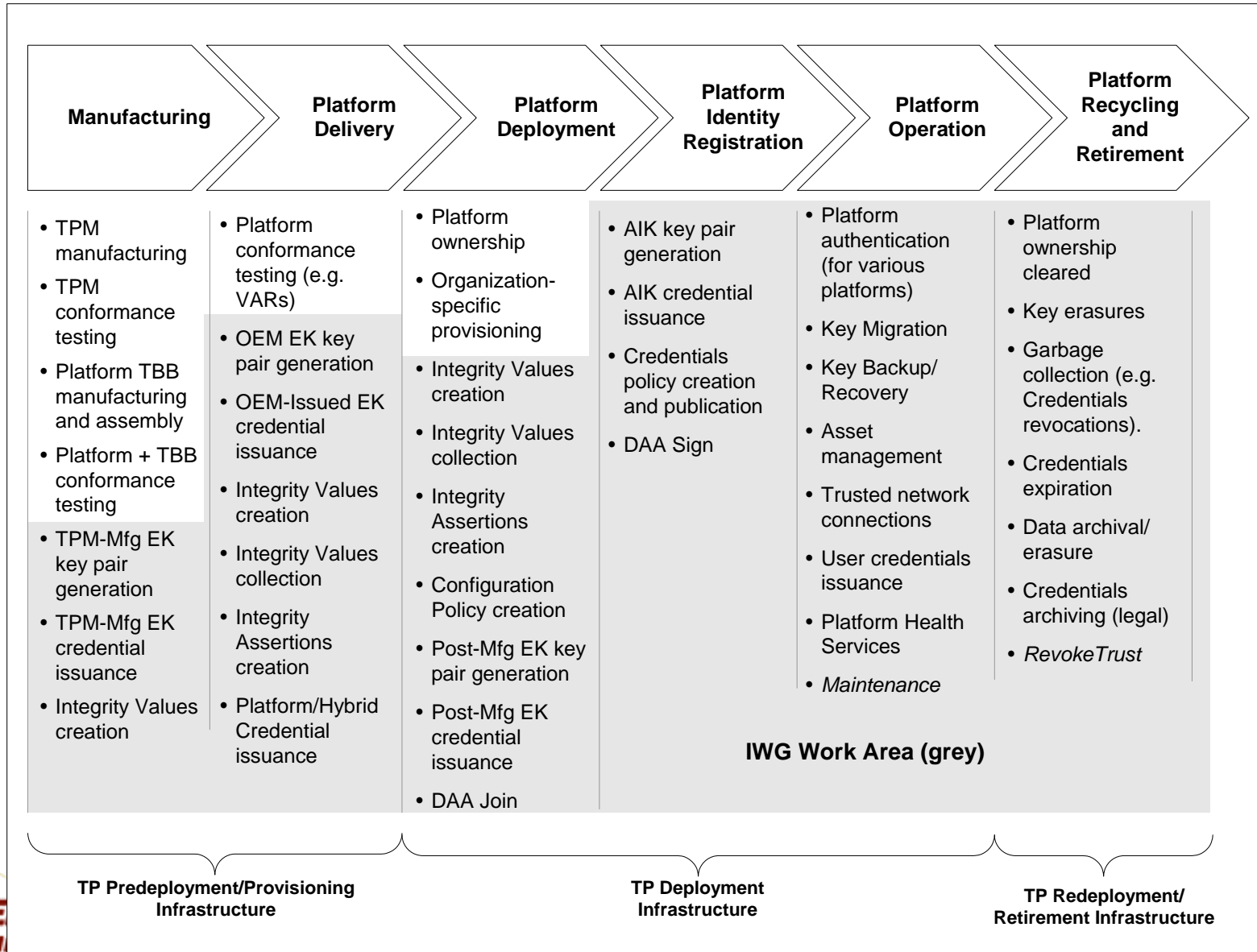


# TCG Trusted Platform Lifecycle

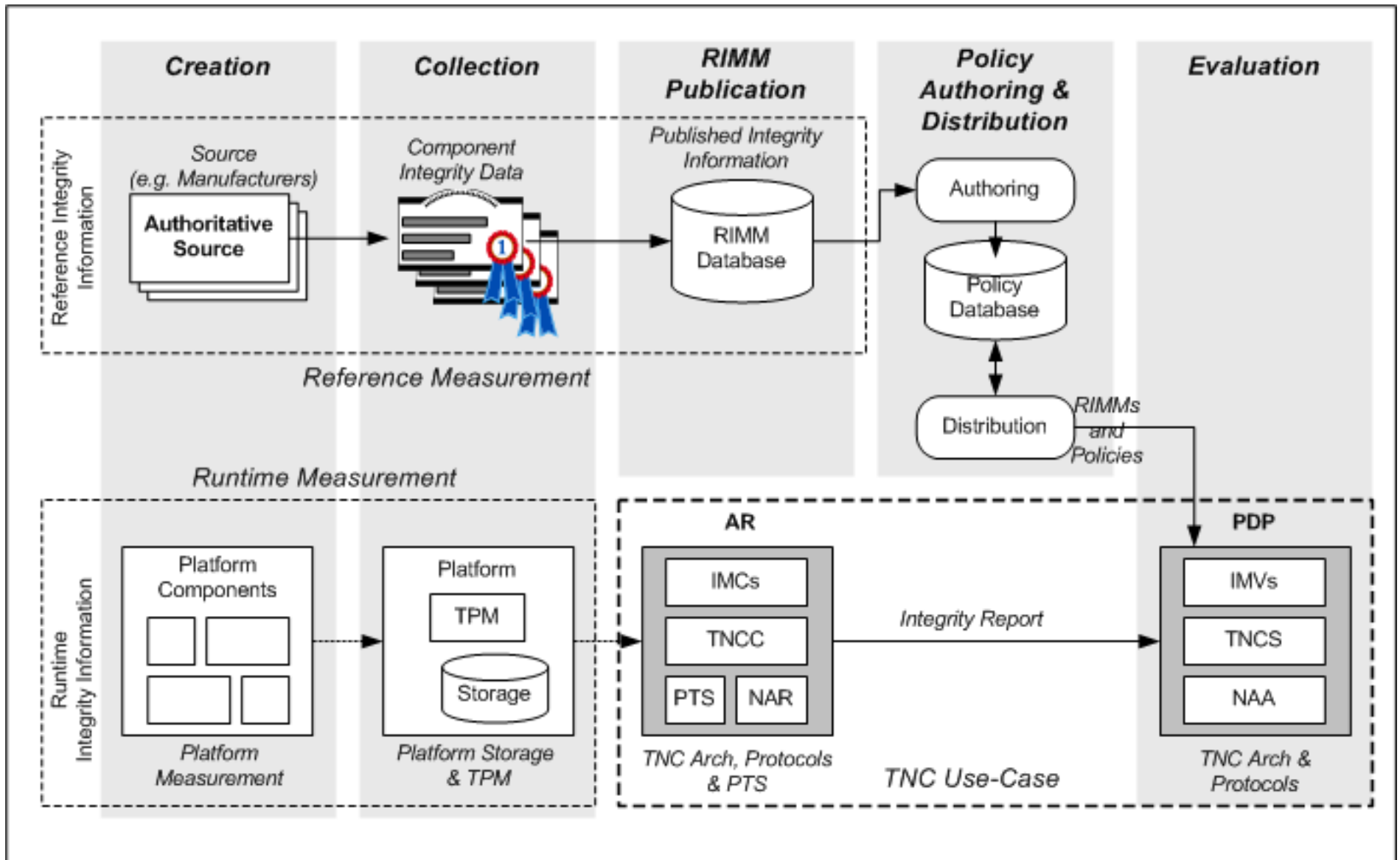
- Framework:
  - a) For understanding *trust management*
    - e.g. Legal issues, Privacy issues, Compliance, etc.
  - b) For identifying tasks/issues in *platform management*
    - e.g. who/when issues TPM credentials, take-ownership, etc
  - c) For identifying requirements for *management tools*
    - e.g. local/remote management, field-upgrades, logs, etc
  - d) For understanding *integrity management*
    - Who issues RIMs, proving transitive-trust, etc
  - e) For identifying *infrastructure* support for (a) – (d)



# The Trusted Platform Lifecycle



# TCG Integrity Management





# DMTF Work Register

# Goal

- Develop a common set of profiles for managing TCG objects within an industry standard management model
  - Trusted Platform Module (TPM)
  - Secure Storage Device (SSD)
  - Trusted Platform (TP)
- As additional trusted components or capabilities are defined, add use cases or augment work register to address new requirements



# Alliance Constraints

- DMTF and TCG have different IPR rules
- Only published TCG standards may be used for Alliance work
- Alliance work will take place in Desktop and Mobile Work Group (DMWG)



# Profiles

- **TPM**
  - Use Cases
    - Discover TPM status and capabilities
    - Configure/Manage TPM
  - Actors
    - Remote Owner
  - Managed Elements
    - Ownership
    - Physical Presence
    - Firmware Update
    - Driver Update
    - EK / EK Cred
    - NV
    - Tick Counter
    - DAA Cred
- **SSD**
  - Use Cases
    - Discover SSD enabled platform status and capabilities
    - Configure/Manage SSD
  - Actors
    - Remote Owner
  - Managed Elements
    - Ownership
    - Lock / Unlock
    - Cryptographic Erase
    - Preboot Authentication
    - Shadow MBR
    - Key Backup Agent
- **TP**
  - Use Cases
    - Discover TP enabled platform status and capabilities
    - Configure/Manage TP
  - Actors
    - Remote Owner
    - Local User(s)
    - Remote User(s)
  - Managed Elements
    - Platform Cred(s)
    - AIK / AIK Cred(s)
    - Delegations
    - RIMMs
    - Migration Authority
    - SSD User Provisioning
    - Security Policies



# Example: TPM Remote Management Operations

Operation Title	Description	Authentication
Query TPM information	Query TPM manufacturer ID, firmware version, driver vendor, driver version.	Optional
Query TPM state	Query TPM ownership, enablement, activation, temporary disablement	Optional
Query TPM capabilities	Query available resources, supported algorithms, used resources of the TPM, EK, NV, Counter, DAA data.	Required
Manage TPM Ownership	Take/Change/Clear TPM ownership	Required
Enable/disable TPM	Change the TPM state to enabled or disabled	Required
Configure TPM capabilities	Adjust TPM capabilities: ability to read TPM internal data, change ordinal audit status, physical lock, enable/disable maintenance, configure NV, tick counter and DAA, manager owner delegation tables	Required
Install EK Credential	Install Endorsement Key Credentials (doesn't this require TOS?)	Required
Revoke Trust	Delete EK and all TPM state	Required
Generate EK	Generate Endorsement Key	Required
Configure Maintenance	Install Maintenance Authority Trust Anchor	Required



# Example: Trusted Drive Operations

Operation Title	Description	Authentication
Initialize	Perform issuance, establish Drive Owner and initial security state	Issuance Authority
Uninitialize	Restore trusted drive to manufacturing security state	Drive Owner
Get Status	Get trusted drive ID, manufacturer details, firmware revision, security state	Drive Owner
Enable Security	Enable TCG SSWG compliant security	Drive Owner
Disable Security	Disable TCG SSWG compliant security	Drive Owner
Unlock Drive	Unlock a trusted drive	Drive Owner / User
Lock Drive	Lock a trusted drive	Drive Owner / User
Erase	Perform cryptographic erase of drive	Drive Owner
Change Drive Owner	Change the trusted drive owner credentials	Drive Owner
Set Backup Agent Credential	Establish backup agent identity	Drive Owner
Authenticate Backup Agent	Authenticate a backup agent	Drive Owner
Backup FDE Security	Backup trusted drive security information	Drive Owner
Restore FDE Security	Restore trusted drive security information	Drive Owner
Update Shadow MBR	Update the shadow MBR within a trusted drive	Drive Owner





# Conclusions and Outlook

# Conclusions & Outlook

- Trusted Computing and Trust
  - Trusted Computing remains a challenge
  - TPMs and Trusted Drive: the first building blocks
- Managing Trust
  - Trust needs to be managed
  - Based on a clear Lifecycle of Trusted Platforms
  - Based on the TCG Integrity Management model
- DMTF-TCG Liaison
  - Work Register to address management of specific devices
    - TPM, Trusted Drives & Trusted Platforms



# Specifications

- <https://www.trustedcomputinggroup.org/specs/>
  - TPM architecture:
    - [https://www.trustedcomputinggroup.org/groups/TCG\\_1\\_3\\_Architecture\\_Overview.pdf](https://www.trustedcomputinggroup.org/groups/TCG_1_3_Architecture_Overview.pdf)
  - TPM specs:
    - <https://www.trustedcomputinggroup.org/specs/TPM/>
  - PC Client specific implementation:
    - <https://www.trustedcomputinggroup.org/specs/PCClient>
  - Key Backup/Migration:
    - [https://www.trustedcomputinggroup.org/specs/IWG/IWG\\_Backup\\_and\\_Migration\\_Services\\_1-00\\_1-00.pdf](https://www.trustedcomputinggroup.org/specs/IWG/IWG_Backup_and_Migration_Services_1-00_1-00.pdf)
  - Certificates:
    - [https://www.trustedcomputinggroup.org/specs/IWG/Credential\\_Profiles\\_V1\\_R1.14.pdf](https://www.trustedcomputinggroup.org/specs/IWG/Credential_Profiles_V1_R1.14.pdf)



# End + Questions

