Introduction to Trusted Computing and the TCG

Thomas Hardjono
THardjono@SignaCert.com

IEEE CommSoc/Bay Area
December 8, 2005

Contents

- The Challenge of Trusted Computing
- Features & Benefits of Trusted Platforms
- The TPM
- Platform Authentication and TNC
- TCG Certificates
- Summary

TRUSTED COMPUTING GROUP™

Introduction

The Challenge of Trusted Computing

The Challenge of Trusted Computing

- Trusted 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 PC platform
  - Increase consumer confidence in Internet use
  - Reduce business risks, specially for security-conscious sectors
    - Financial Services, Insurance, Government, Healthcare
  - Increase in transaction volume and value with hardware enforced protections
- Increase trust in other platforms
  - Laptops, Desktops, PDA, Servers, Mobile Phones, Network gear, etc.

TRUSTED COMPUTING GROUP™

Technical Challenge & the TP Solution

- Challenge:
  - Allow communicating platforms to dynamically accept and execute code supplied by the network.
  - Allow a platform connect and interact with remote platforms.
  - Protection of data from misuse.
- Solution:
  - Turn the entire platform into a trusted environment.
  - Enable a platform to prove that a given software environment is a protected environment.
  - Secrets are protected until the correct software environment exists
    - Only then are secrets released into that environment.

TRUSTED COMPUTING GROUP™

Features of Trusted Platforms

What distinguishes TPs

Features of a Trusted Platform

1. Protected Capabilities
   - The set of commands with exclusive permission to access Shielded Locations (SL).
   - SL are places (memory, register, etc.) where it is safe to operate on sensitive data.
   - The TPM implements protected capabilities and shielded-locations.
2. Integrity Measurement and Storage
   - The Process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform.
   - The storing those metrics and the placement digests of those metrics in Platform Configuration Registers (PCR).

TRUSTED COMPUTING GROUP™

Features of a Trusted Platform (cont)

3. Integrity Reporting

- The process of attesting to the contents of integrity storage (i.e. PCRs).
- Philosophy: a platform may be permitted to enter any state possible (including insecure states), but it may not be permitted to lie about states that is was or was not in.
- Multiple *Roots of Trust* in TPM (i.e. keys)

4. Attestations

- The process of vouching for the accuracy of information (e.g. in the PCRs).
- Attestations by the TPM and Platform
- Attestation digitally signed using various TPM-bound and Platform-bound certificates.

TRUSTED COMPUTING GROUP™

Benefits of using TP Features

- Integrity self-protection of a platform
  - Building blocks to turn the platform into a trusted environment.
  - Allow to prove that a given software environment is a protected environment.
  - Secrets encrypted to a given platform configuration
    - Decipherable only by the platform in that configuration
- Platform Authentication (Remote Attestations)
  - *Platform Authentication*: a platform proves to another that it is in a given integrity-state
  - Examples:
    - Network-End-Point Integrity (Trusted Network Connect)
    - Web-services transactions – platform identity based

TRUSTED COMPUTING GROUP™

Overview of the TPM

Trusted Platform Module

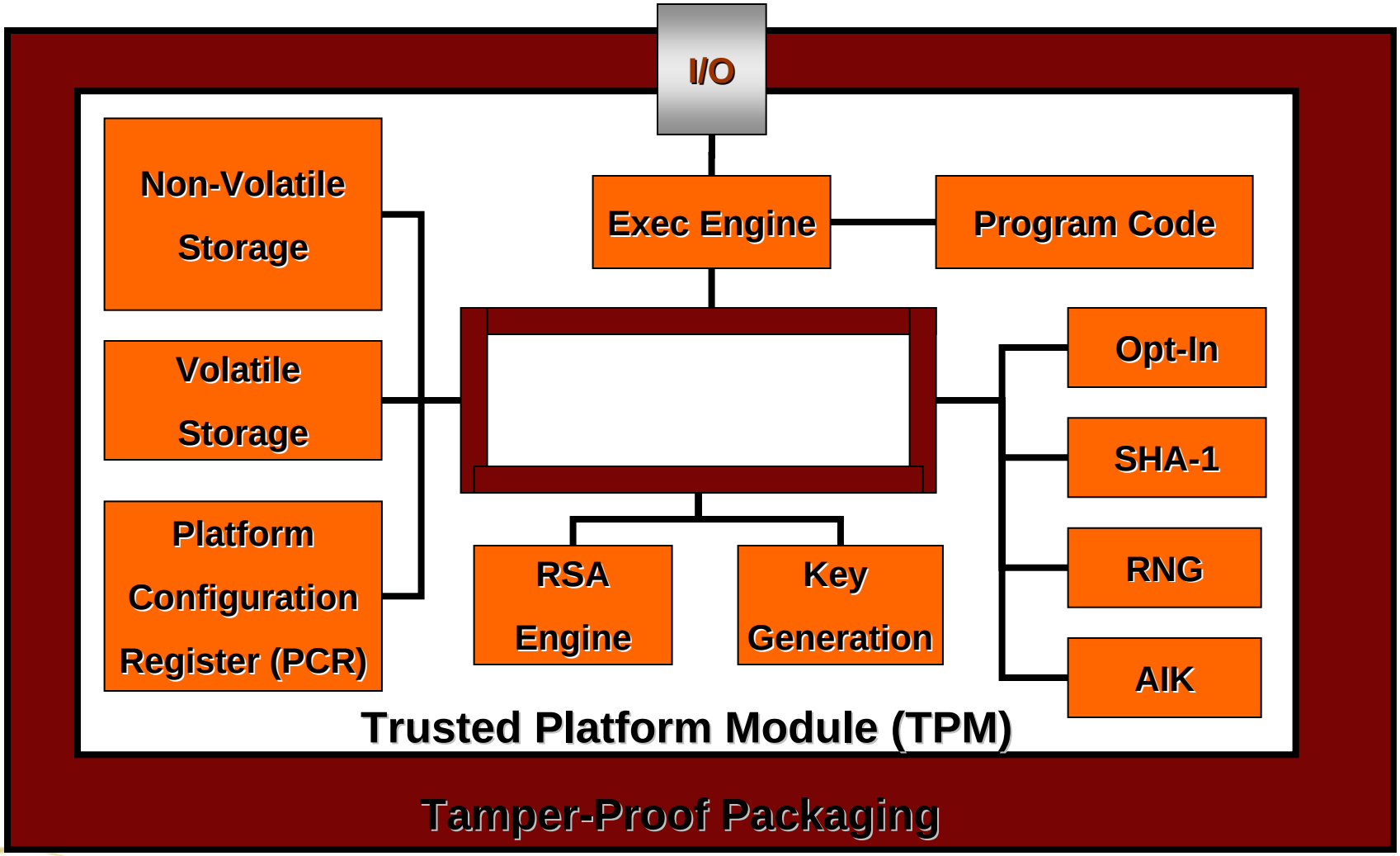
What is a TPM?

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

TRUSTED COMPUTING GROUP™

[1] TPM specifications must be implementable in software

TPM Overview



TRUSTED COMPUTING GROUP™

TPM Functionality

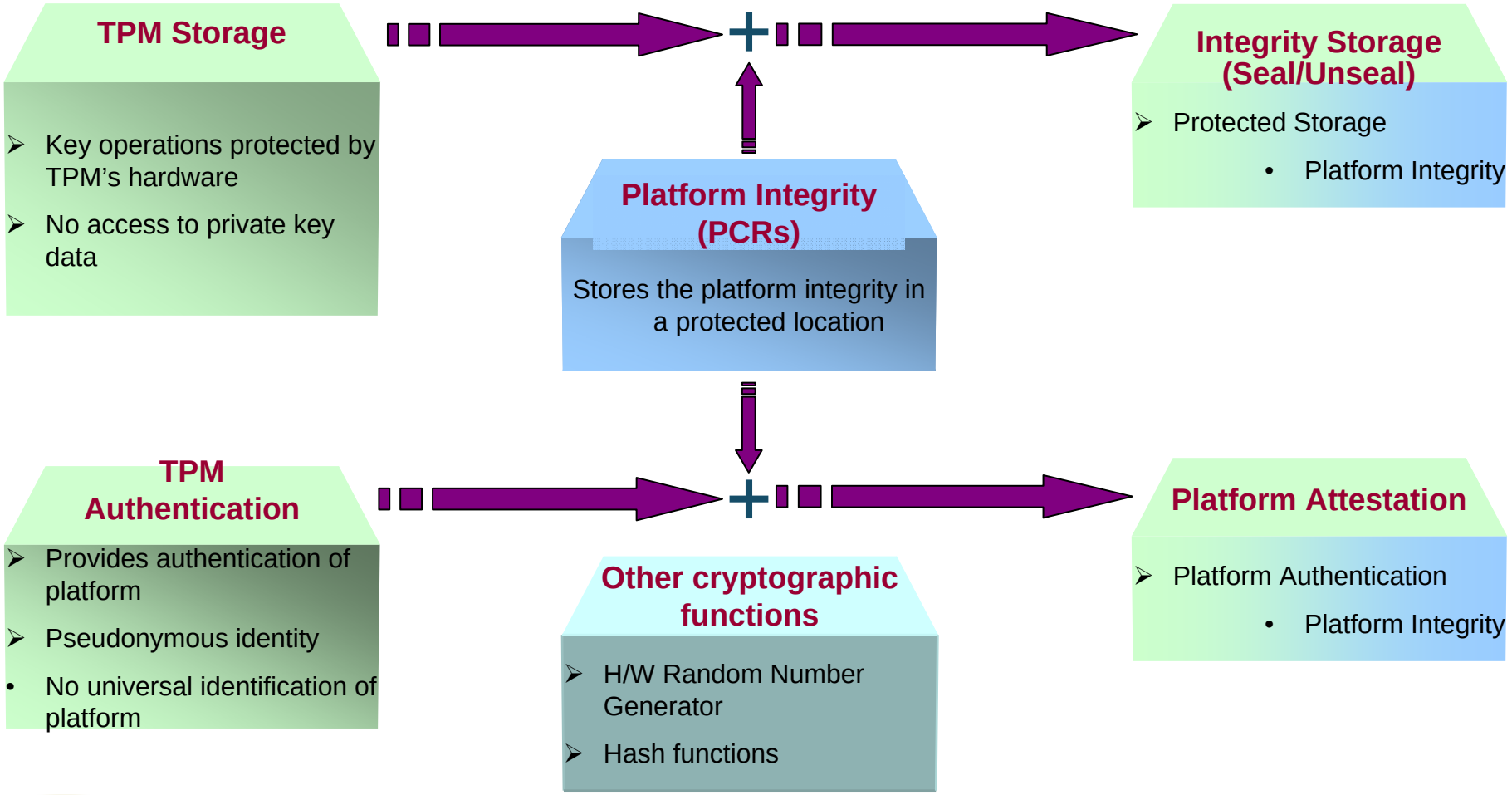
- Monotonic Counter
- Tick Counter
- Digital Signature
- NV Storage
- Delegation
- Clear Endorsement Key
- Transport Session
- Context Management
- Locality
- Random Number Generator
- RSA Engine
- Sha-1 Engine
- Platform Configuration Registers (PCR)
- Key Storage
- Public-Key Enrollment
- Zero-knowledge Proof Engine
- Anonymous and Pseudo-anonymous Identity

TRUSTED COMPUTING GROUP™

TPM Feature and Function

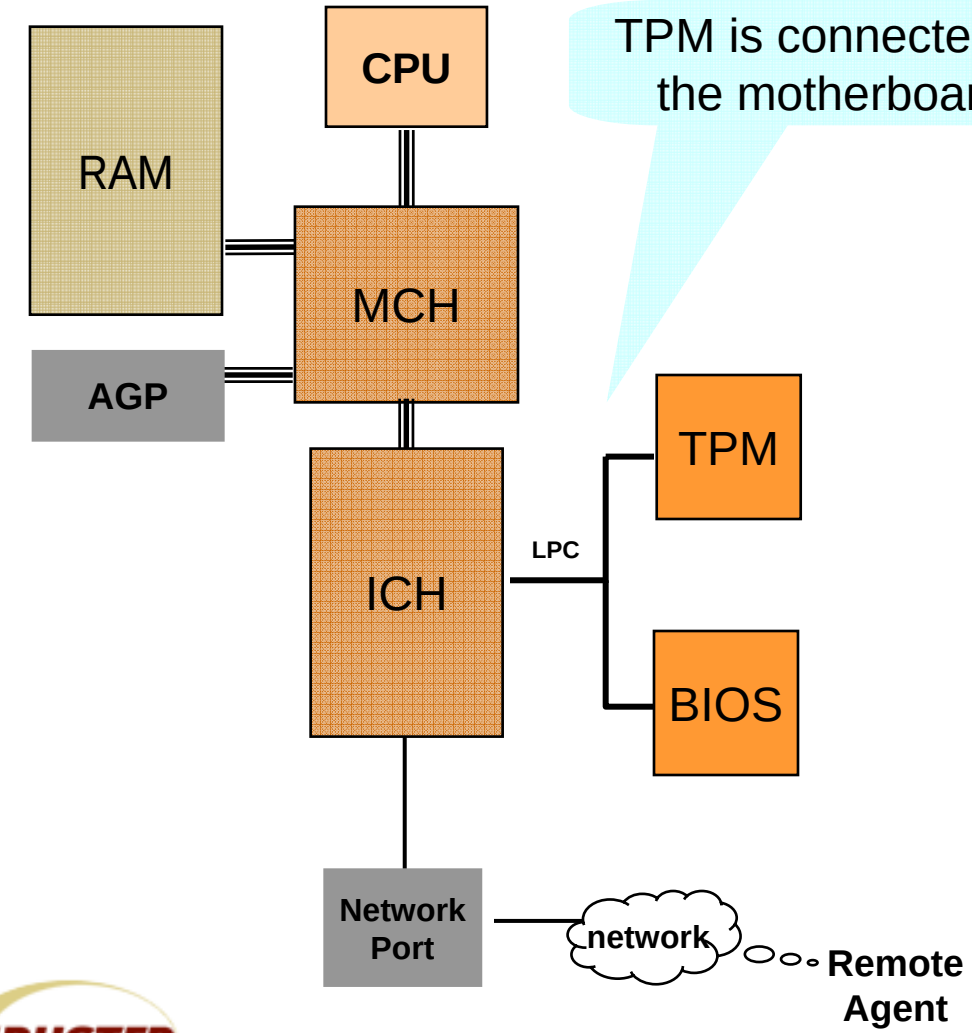
Base Features

Integrity Features



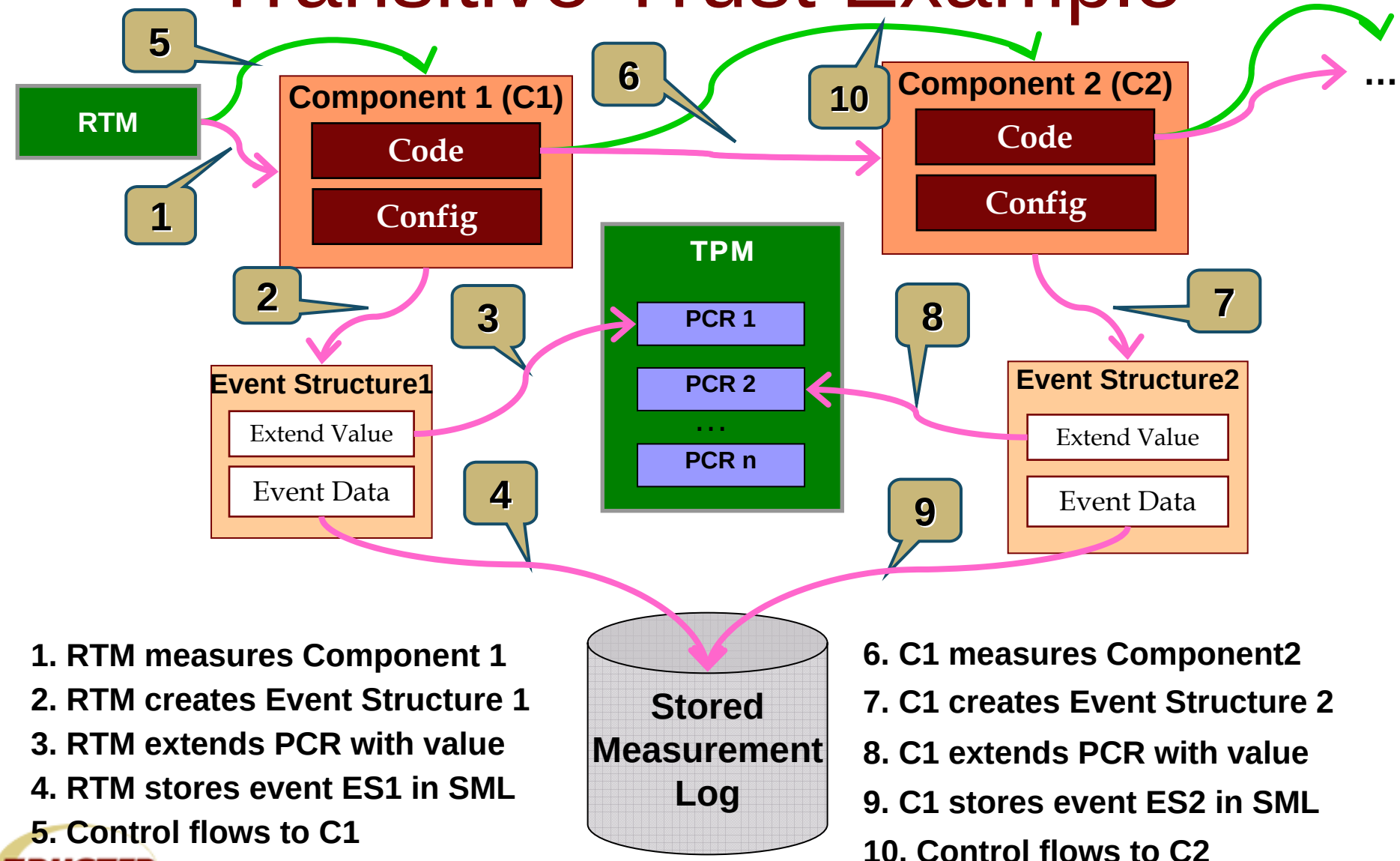
PCR – Platform Configuration Register

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

Transitive Trust Example



1. RTM measures Component 1
2. RTM creates Event Structure 1
3. RTM extends PCR with value
4. RTM stores event ES1 in SML
5. Control flows to C1

6. C1 measures Component2
7. C1 creates Event Structure 2
8. C1 extends PCR with value
9. C1 stores event ES2 in SML
10. Control flows to C2

TRUSTED COMPUTING GROUP™

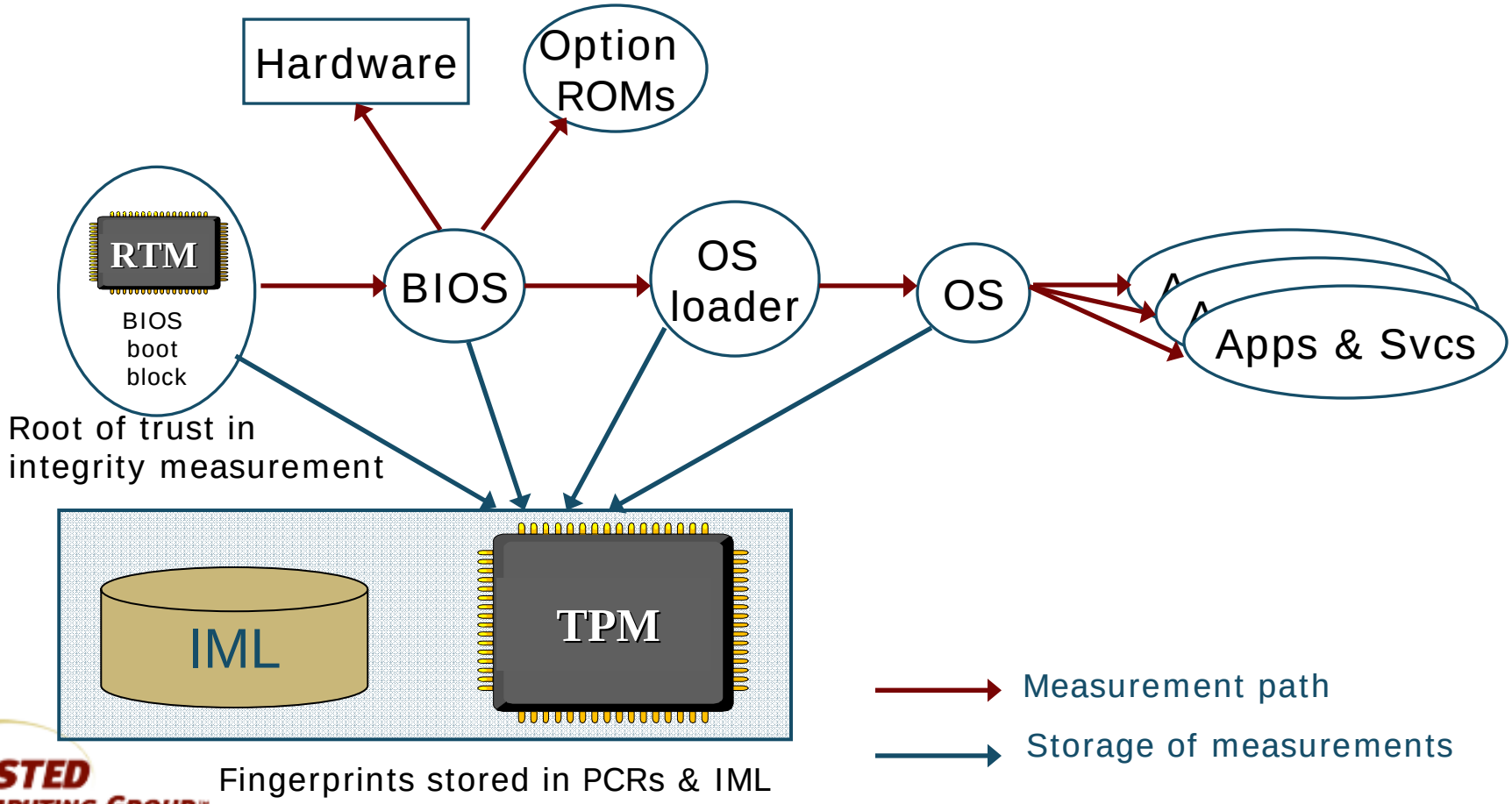
Platform Configuration Registers (PCRs)

- Stores cumulative configuration
- Update is an Extend operation:
  - [PCR] = SHA-1 {[PCR] + Extend value}
  - Value:
    - It is infeasible to calculate the value A such that:
      - PCRdesiredValue = Extend (A)
- Initialized to zero at TPM_Init or TPM_HASH_START
- Parsing of PCRs via Platform Specific Specifications
  - Achieve standard expected behavior

TRUSTED COMPUTING GROUP™

Collecting Platform Configuration State a.k.a. “Measurement”

- Platform Configuration Registers (PCR) contain Sha-1 hash values (Finger Print).
- Information about the sequence of measurement operations are stored in the “Integrity Measurement Log”. (IML)
- RTM is tamper resistant



Fingerprints stored in PCRs & IML

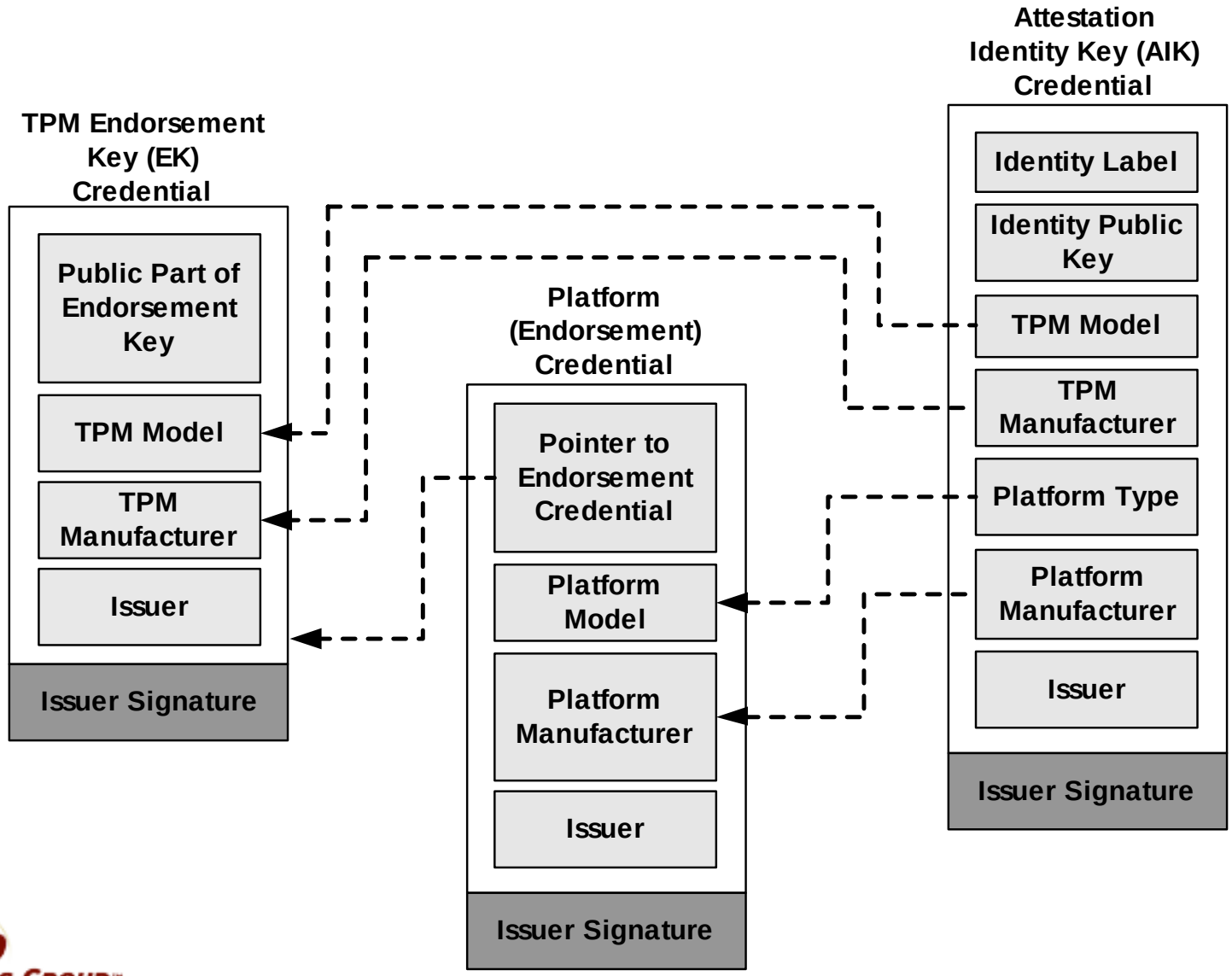
Certificates in TCG

Building Blocks for Platform Identities

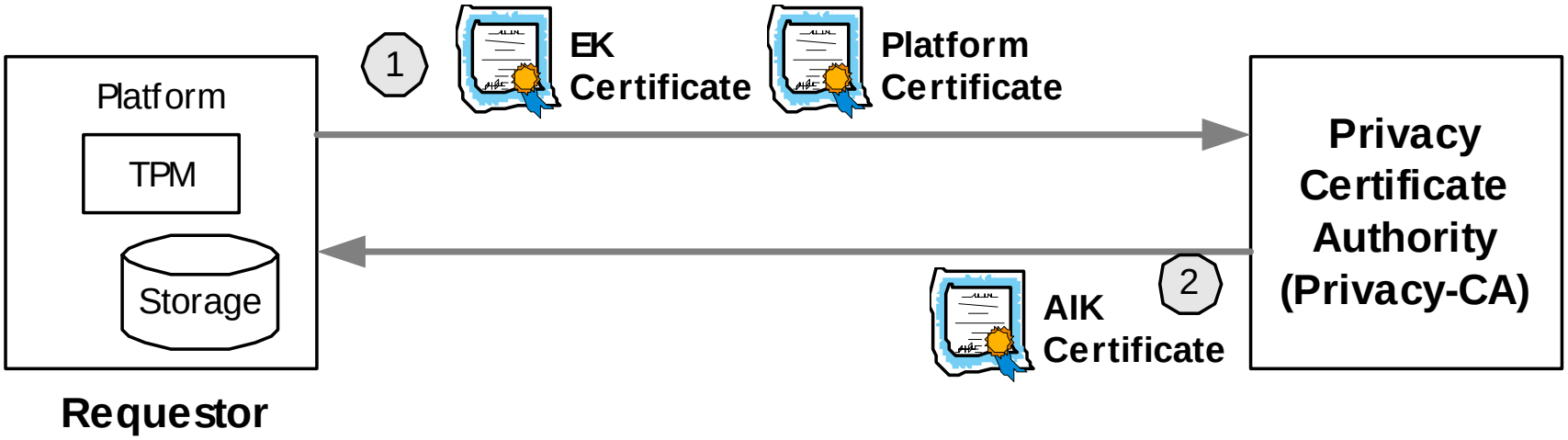
Relevant Certificates in Trusted Platforms

- TPM-Manufacturer Certificate (EK-Certificate):
  - Each TPM chip has unique internal RSA key pair and Certificate
    - Referred to as Endorsement Key (EK) and EK-certificate
  - Issued & made present in the TPM by the chip Manufacturer
  - Used internally by TPM
- Platform (Endorsement) Certificate
  - Attests that a platform has TPM and Trusted Building Block (TBB)
  - Issued by a Platform Manufacturer (e.g OEM) or Lab
- AIK-certificates:
  - Attests to the fact that a TPM has the AIK and the AIK is tied to a valid TPM EK Credential and a valid Platform Credential
  - Issued by Privacy-CA – a “blinding” certificate
  - Used to digitally-sign proofs about existence of active TPM chip
- SKAE-certificates:
  - Standard X509 cert with extension containing AIK-cert portions.

TCG Certificates Relationship



The Privacy CA

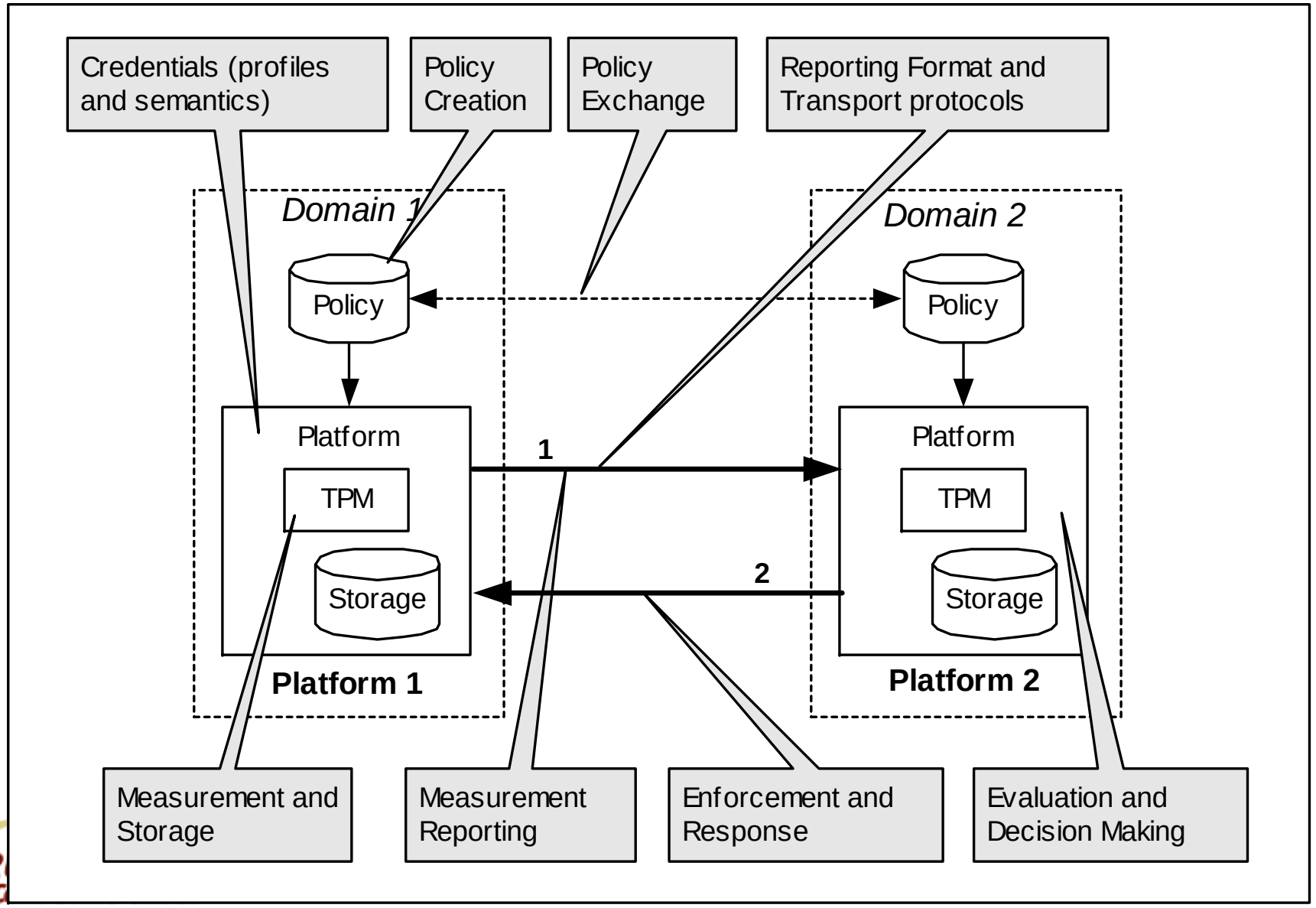


- The Privacy-CA issues AIK-certificates
  - Trusted not to reveal EK-certificate contents
  - AIK-certificates issued encrypted to the TPM
    - Decipherable only by the same TPM
  - Unlimited number of AIK-certificates per platform
    - Prevent correlation of Privacy Identifying Information (PII)
  - AIK-certs used to protect application-credentials enrollment
    - Subject Key Attestation Evidence (SKAE) extension in X509

TRUSTED COMPUTING GROUP™

Use Case: Platform Authentication & Trusted Network Connect

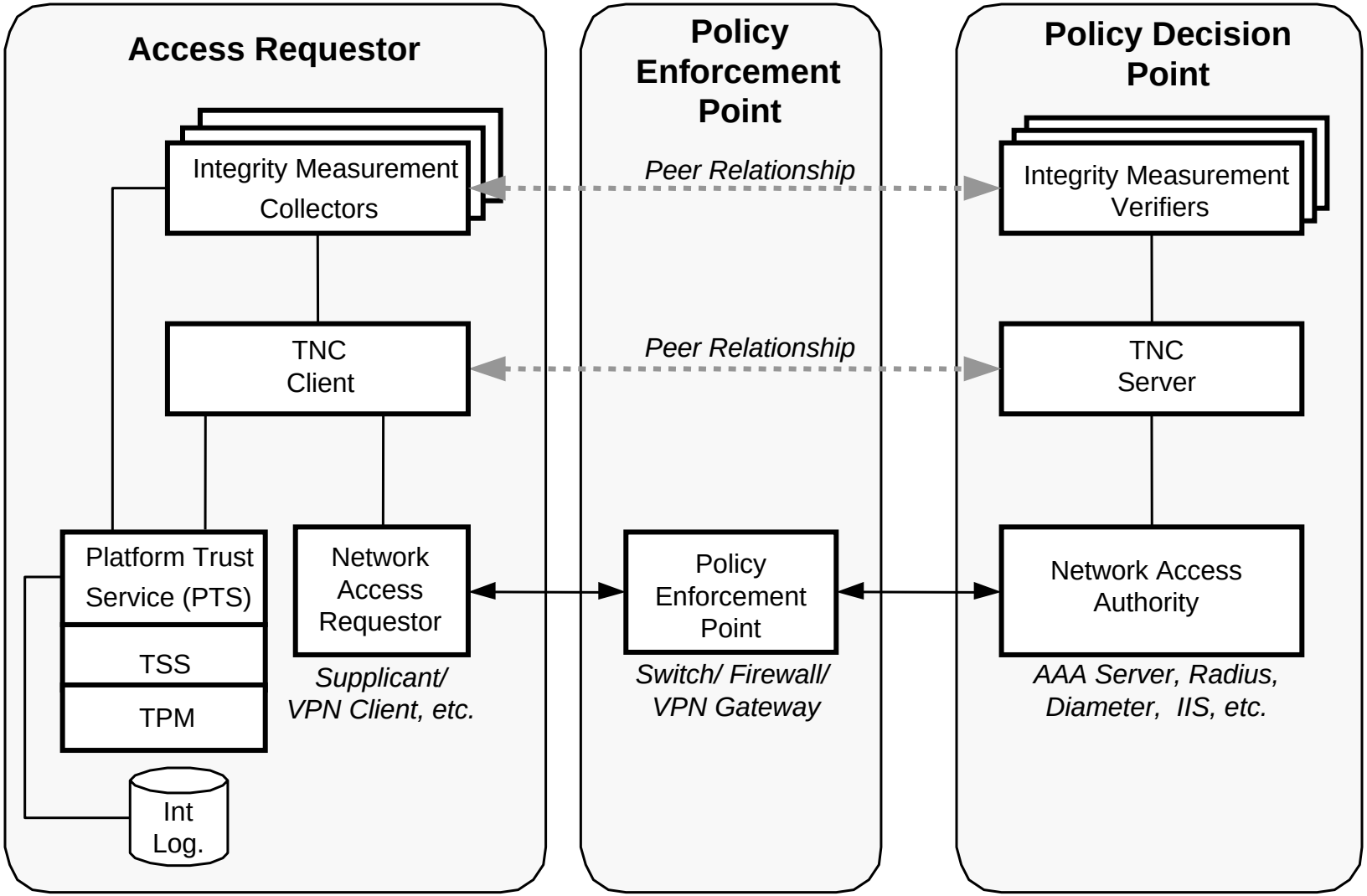
Platform Authentication Features



Trusted Network Connect

- Problem:
  - to diminish/remove threat due to virus and malware introduced to the Enterprise network via end-user devices (e.g. laptops).
- Solution:
  - Deploy *Trusted Access Control* in the context of networking at layer-2/3 (eg. 802.1X, EAP, IP, IPsec)
  - Integrity measurement and verification based on trusted platform features.
  - Client reports its integrity information through an Integrity Handshake with the Server.
  - Server evaluates Client status against policy.
  - Failed Clients redirected to remedial network (e.g. VLAN)

TNC Architecture



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.

TRUSTED COMPUTING GROUP™

TCG Membership

125+ Total Members as of November 2005

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

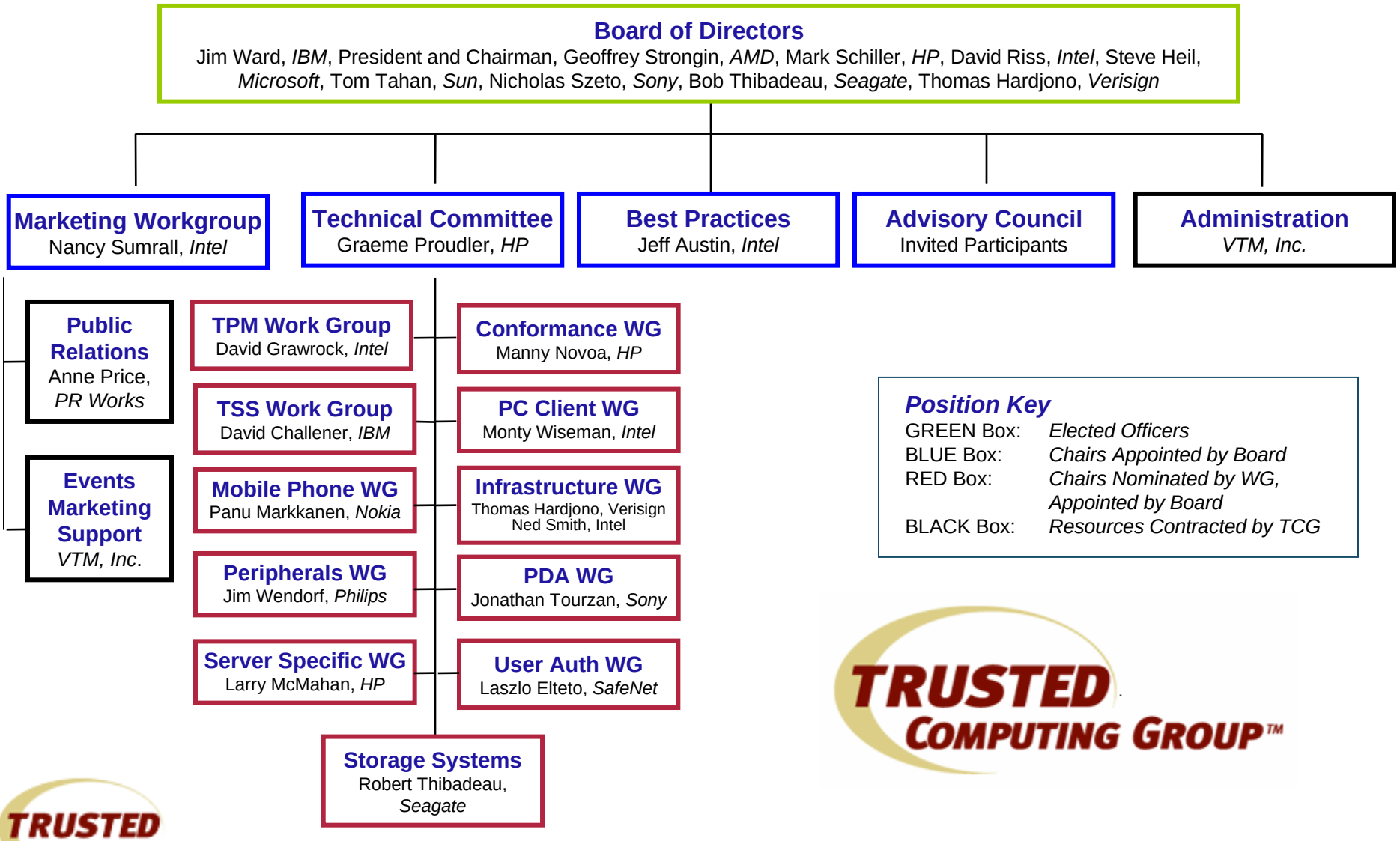
Adopters
Ali Corporation
American Megatrends, Inc.
Enterasys Networks
Foundry Networks Inc.
Foundstone, Inc.
Gateway
Industrial Tech. Research Institute
iPass
OSA Technologies
Silicon Integrated Systems Corp.
Softex, Inc.
Toshiba Corporation
Winbond Electronics Corporation

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.

TRUSTED COMPUTING GROUP™

Structure of the TCG



Position Key

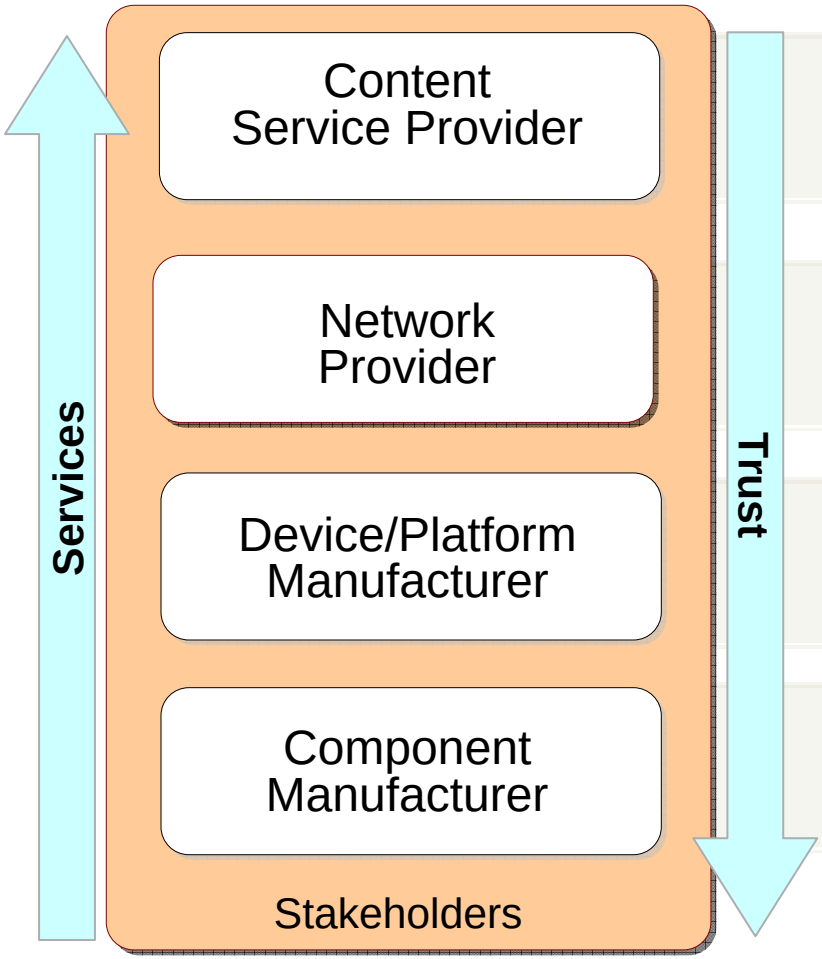
GREEN Box:	*Elected Officers*
BLUE Box:	*Chairs Appointed by Board*
RED Box:	*Chairs Nominated by WG, Appointed by Board*
BLACK Box:	*Resources Contracted by TCG*

TRUSTED COMPUTING GROUP™

TRUSTED COMPUTING GROUP™

Mobile Phone Working Group

Social Trust and Technical Trust



- Often acts on behalf of rights-holders
- Dependent on underlying trust providers
- May require way to prove client trust state

- Network services available only if device operates in a trusted state
- Some dependence on Device Manufacturer

- Device Manufacturer acts as OEM.
- Express levels of trust through platform level credentials and roots-of-trust

- Component trust established through accompanying credentials & measurements
- Trust profiles and conformance/compliance

Something can be trusted if it always behaves

in an expected manner for a particular purpose

TRUSTED COMPUTING GROUP™

Use Cases of the MPWG

- User Data Protection and Privacy
  - Enable the protection of user's personal information, such as identity and address books, from access or copying by unauthorized parties.
- Platform Integrity
  - Ensure device operation occurs with only authorized operating system(s) and hardware.
- Device Authentication
  - Ensure that 1) device authentication may be used to assist in end user authentication, and 2) that it may prove the identity of the device itself.
- Robust DRM Implementation
  - Ensure any implementation of a DRM specification can be trusted to protect the data that users acquire and the content and service providers require .
- SIMLock / Device Personalization
  - Ensure that subsidized mobile devices remain locked to the appropriate network until unlocked in an authorized manner.

Use Cases of the MPWG (cont)

- Secure Software Download
  - Enable the secure download of application software or updates, firmware updates or patches to protect against attacks.
- Secure channel between device and UICC
  - Provide shared functioning for security sensitive applications (e.g., an m-commerce application) that must implemented partly in the UICC and partly in the device.
- Mobile Ticketing
  - Enable new services based on a user purchase of an electronic ticket which is downloaded to the mobile device and used for entry to an event or access to a service.
- Mobile Payments
  - Enable the mobile device to serve as a user's wallet or purse for electronic payments to point of sale devices. Support for a variety of payment sources including credit cards, debit cards, pre-paid funds, and online accounts.
- Software Usage
  - Assure that software applications retain their integrity against attacks, adhere to device user policies, and cannot interfere with other device functions.

The Need for Trusted Mobile Phones

- **Increase in value of content**
  - Increasing richness of multimedia content
  - Advances in network services and bandwidth
  - Content-over-anything (e.g., IP, GPRS, Bluetooth, etc)

- **Merging of Mobile and Home Content**
  - Mobile content as an extension of home content
  - Sharing content across user devices
  - Content anywhere anytime
  - P2P for distribution & scale

- **The need for a Trusted Environment**
  - Safe platforms for content
  - Blurring of boundary of PC Platform and Mobile Phones/PDAs
  - Value of data (individual and corporate)

TRUSTED COMPUTING GROUP™

End + Questions