Trusted Computing Group

Introduction and Brief Technical Overview T10

Robert Thibadeau, Ph.D.

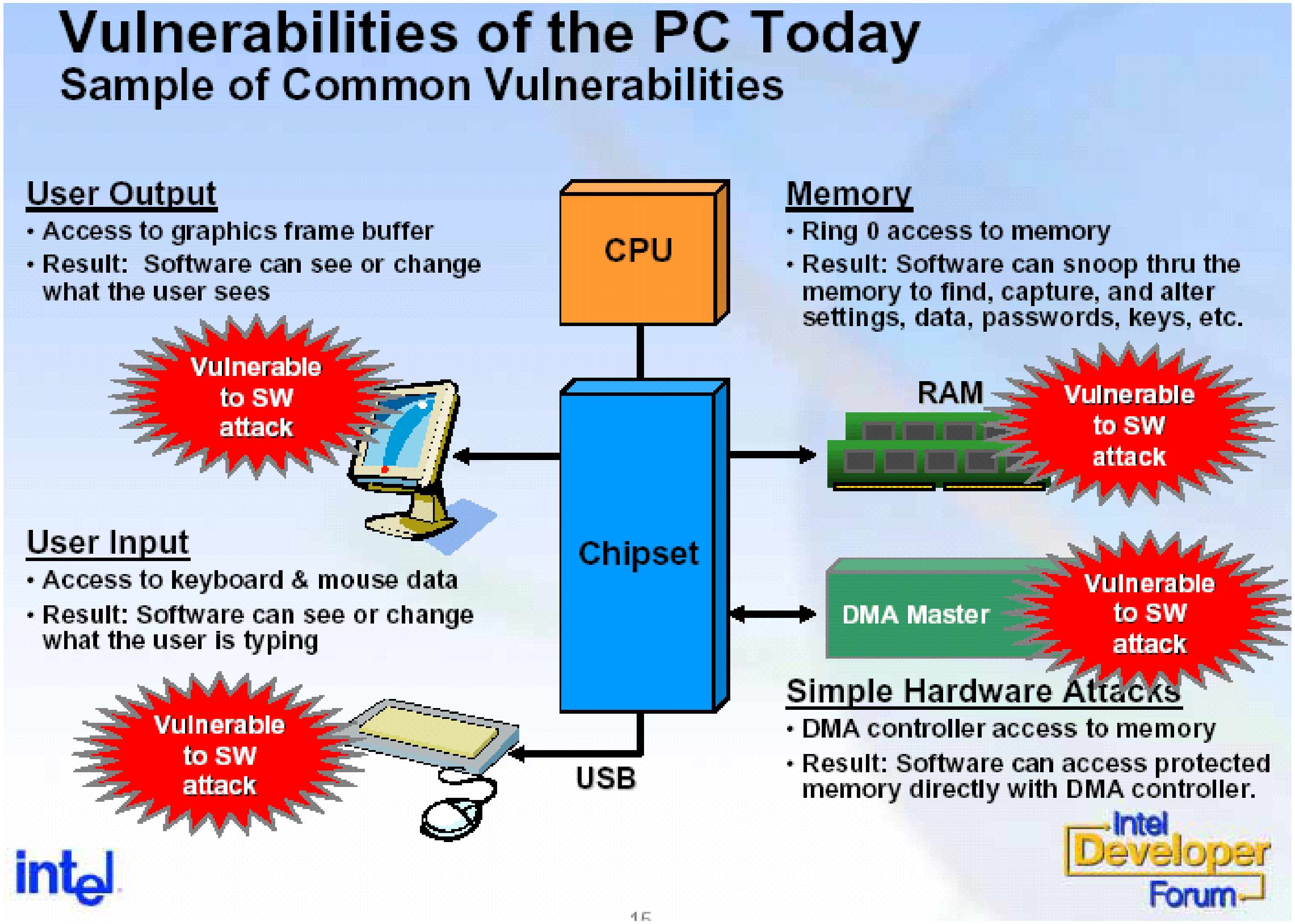
Seagate Research

May 2005

Agenda

- Security Processing
  - Roots of Trust
- TCG Standards Group Intro
- TCG Technical Concepts
- Trusted IN/OUT Proposal
- Discussion

The Need for Trusted Computing



Vulnerabilities of the PC Today

Sample of Common Vulnerabilities

User Output

- Access to graphics frame buffer
- Result: Software can see or change what the user sees

User Input

- Access to keyboard & mouse data
- Result: Software can see or change what the user is typing

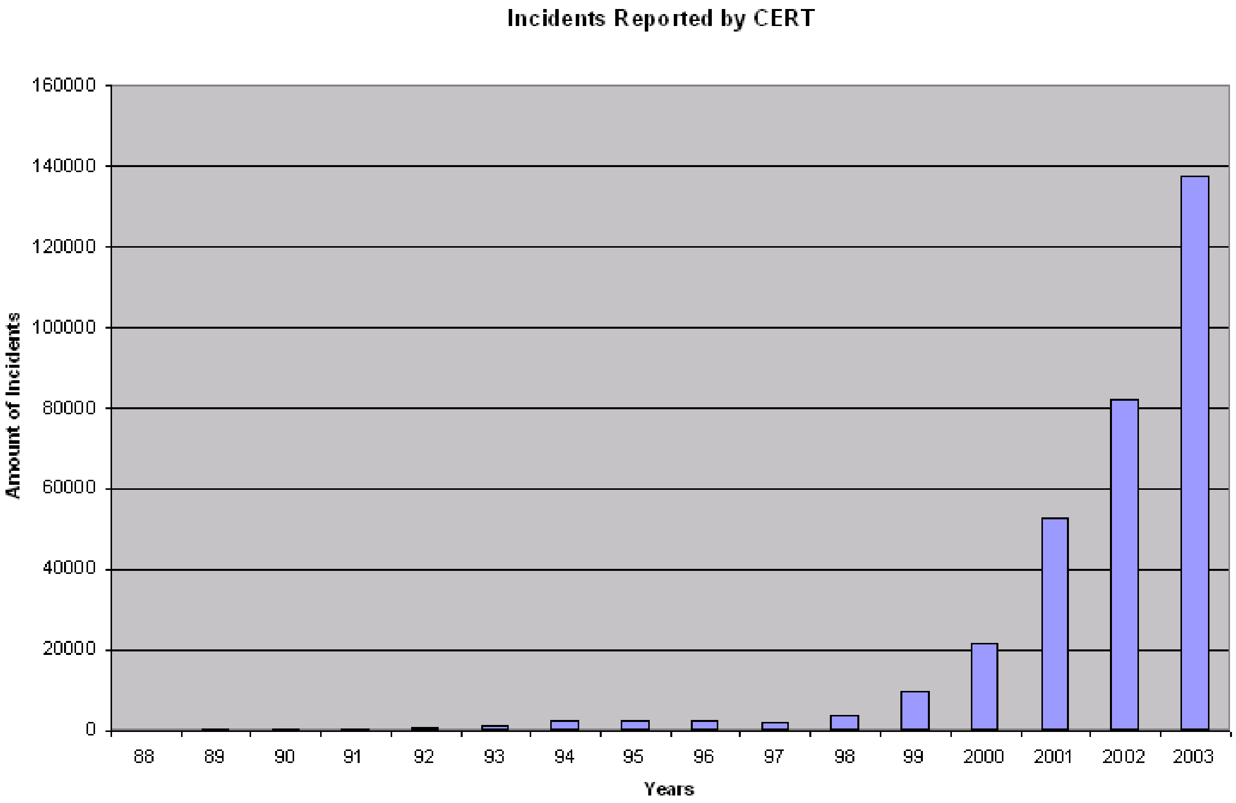
Memory

- Ring 0 access to memory
- Result: Software can snoop thru the memory to find, capture, and alter settings, data, passwords, keys, etc.

Simple Hardware Attacks

- DMA controller access to memory
- Result: Software can access protected memory directly with DMA controller.

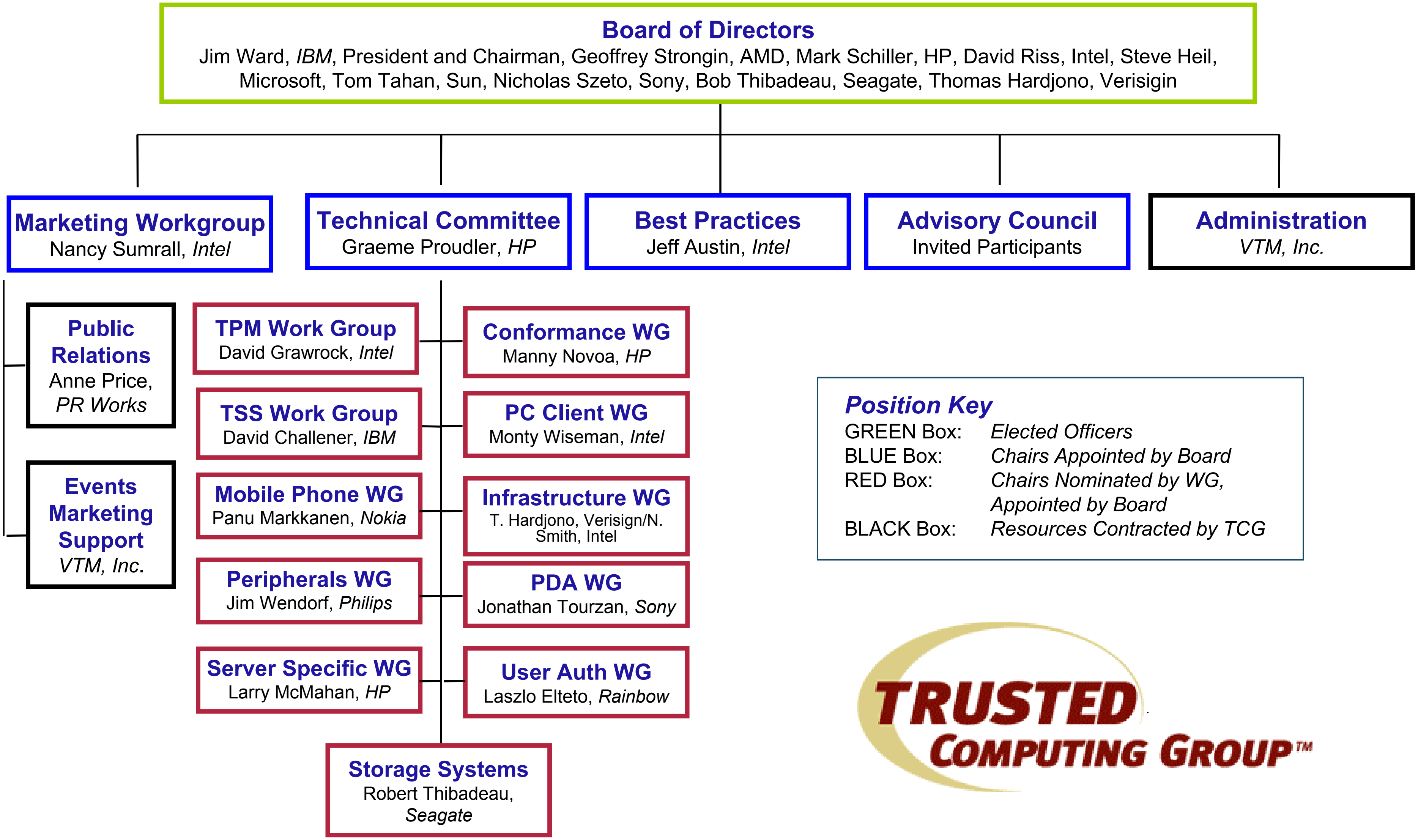
What it Means in Real World



- **Innovation is needed:**
  - **Clients software and hardware**
  - **Networks**
  - **Infrastructures**

TCG Organization

www.trustedcomputinggroup.org



Board of Directors
Jim Ward, *IBM*, President and Chairman, Geoffrey Strongin, AMD, Mark Schiller, HP, David Riss, Intel, Steve Heil, Microsoft, Tom Tahan, Sun, Nicholas Szeto, Sony, Bob Thibadeau, Seagate, Thomas Hardjono, Verisigin

Marketing Workgroup
Nancy Sumrall, *Intel*

Technical Committee
Graeme Proudler, *HP*

Best Practices
Jeff Austin, *Intel*

Advisory Council
Invited Participants

Administration
VTM, Inc.

Public Relations
Anne Price, *PR Works*

Events Marketing Support
VTM, Inc.

TPM Work Group
David Grawrock, *Intel*

TSS Work Group
David Challener, *IBM*

Mobile Phone WG
Panu Markkanen, *Nokia*

Peripherals WG
Jim Wendorf, *Philips*

Server Specific WG
Larry McMahan, *HP*

Conformance WG
Manny Novoa, *HP*

PC Client WG
Monty Wiseman, *Intel*

Infrastructure WG
T. Hardjono, Verisign/N. Smith, Intel

PDA WG
Jonathan Tourzan, *Sony*

User Auth WG
Laszlo Elteto, *Rainbow*

Storage Systems
Robert Thibadeau, *Seagate*

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*

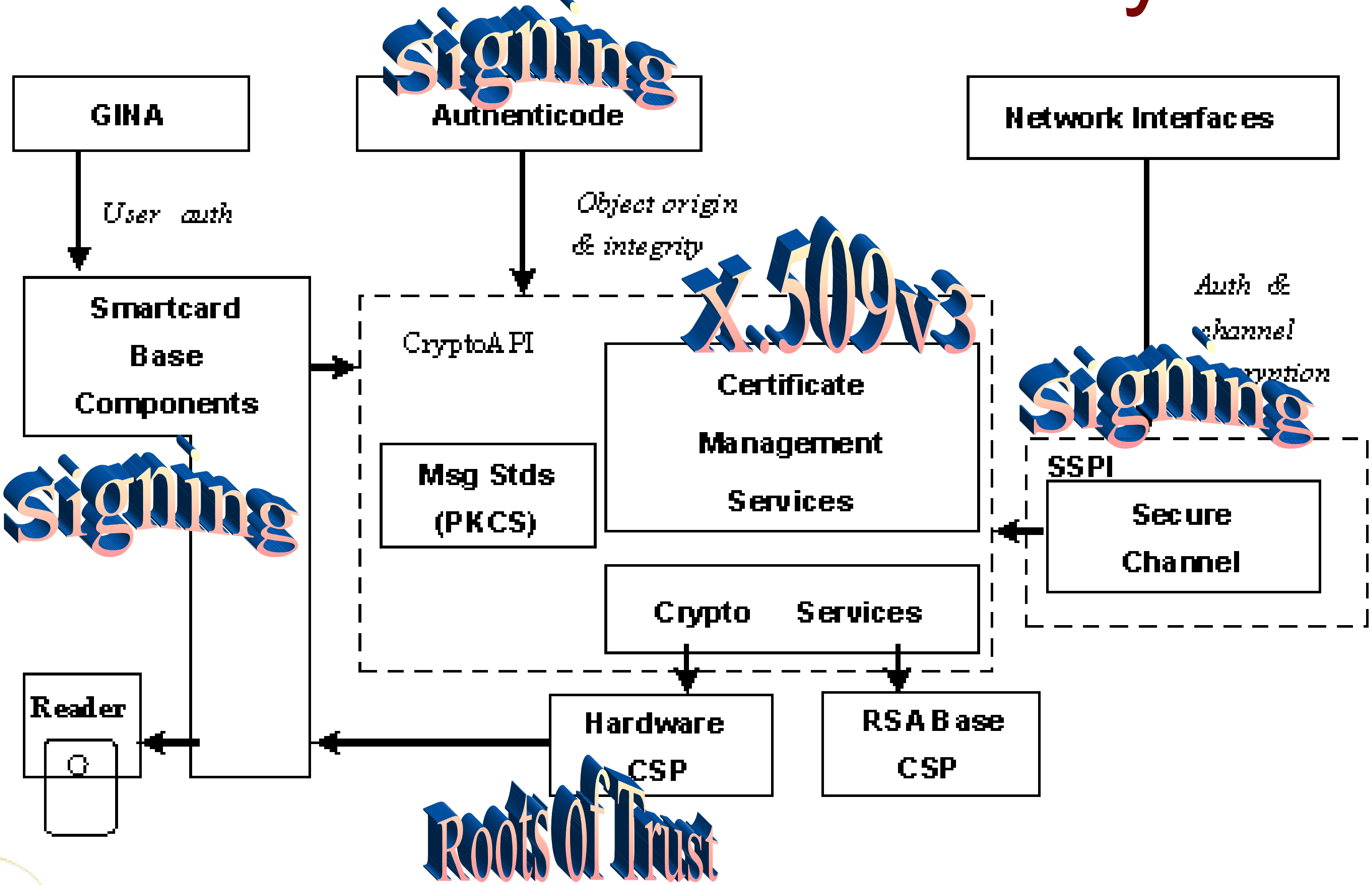
TRUSTED COMPUTING GROUP™

What is Trust? – it does what was intended to do.

- It is cryptographic SIGNING
  - PlaintextMessage + Signed(Hash(PlaintextMessage))
    - Hash = Reduces message to 20 Bytes (2^160th number)
    - Sign = Encrypts with a private key that only the corresponding public key can decrypt and verify
  - Microsoft signs the Microsoft software proving it is the software from Microsoft…
  - X signs Y and Y signs Z -- **Chain of Trust**
- An X.509 Certificate is a cryptographically SIGNED attestation of a fact or claim.
  - Basis for Trust in ALL BANKING WORLDWIDE
  - Basis for Trust in Windows and Linux and Web

TRUSTED COMPUTING GROUP™

Windows Core Security



What is a Root of Trust?

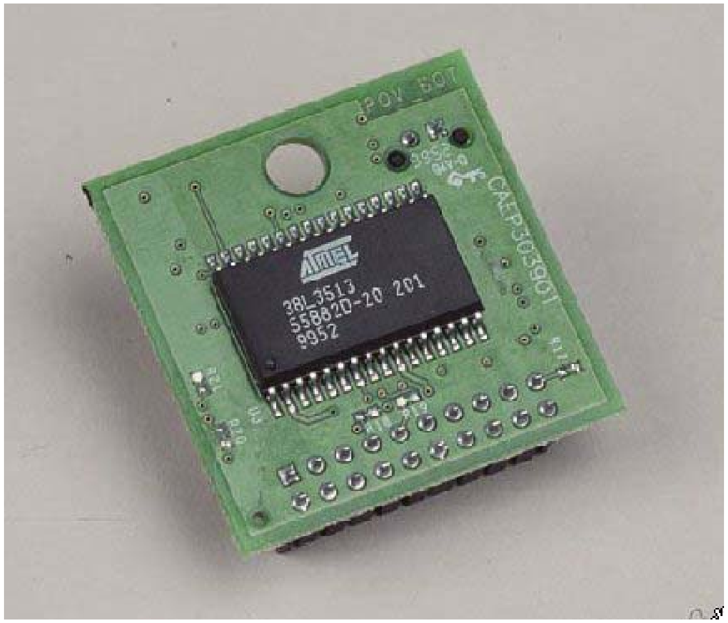
- Hardware that *you can't* ***change*** **that can sign** and therefore start off a chain of trust.
- A TPM is a tiny processor on the motherboard that can sign and can't have the firmware modified.
- Disk Drives are roots of trust against network attacks since you can't upload firmware to change them.
  - Of course, much 'hardening' needs to happen.

TRUSTED COMPUTING GROUP™

The Trusted Platform Module

A silicon chip that performs all TPM v1.1 functions, including:

- Can store OS status information
- Generate and store a private key
- Hashes files using SHA-1
- Creates digital signatures
- Anchors chain of trust for keys, digital certificates and other credentials



Basic Conceptual Motivation

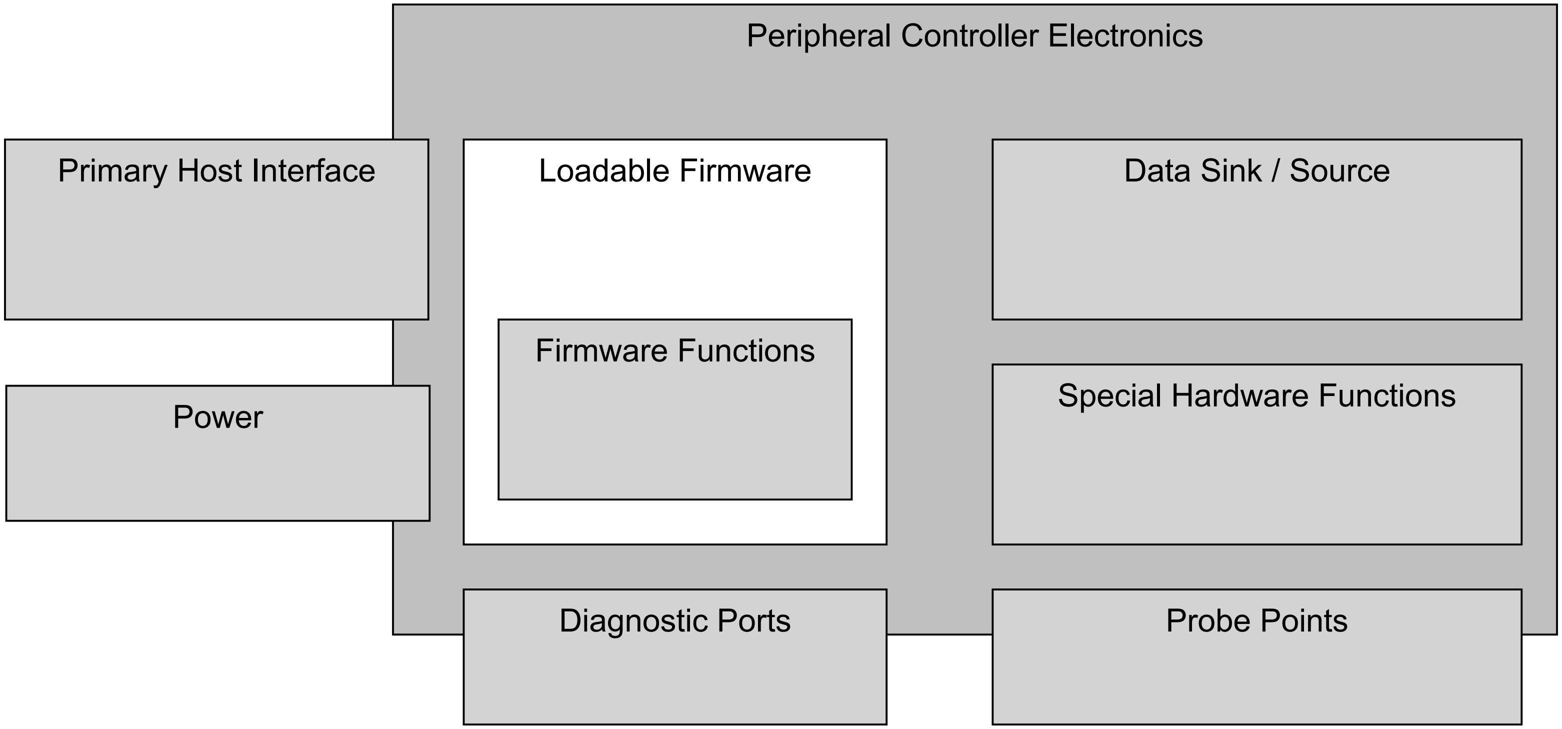
- Internet-connected devices will always have untrusted activities going on inside of them, so …
- Create internal trustable sub-units and secure paths … the building blocks, so …
- In the future, you (IT) can know the trusted subsystem won't be compromised even if exposed to Internet (and limited physical) attacks (or accidents).

TRUSTED COMPUTING GROUP™

TCG Storage/Peripherals Use Cases

- Enroll a Device with a Platform (establish trust)
  - Platform trusts peripheral, peripheral trusts Platform
- Now you can connect and disconnect device at will
  - TCG TPM on Motherboard and the Device recognize each other and user has to do nothing

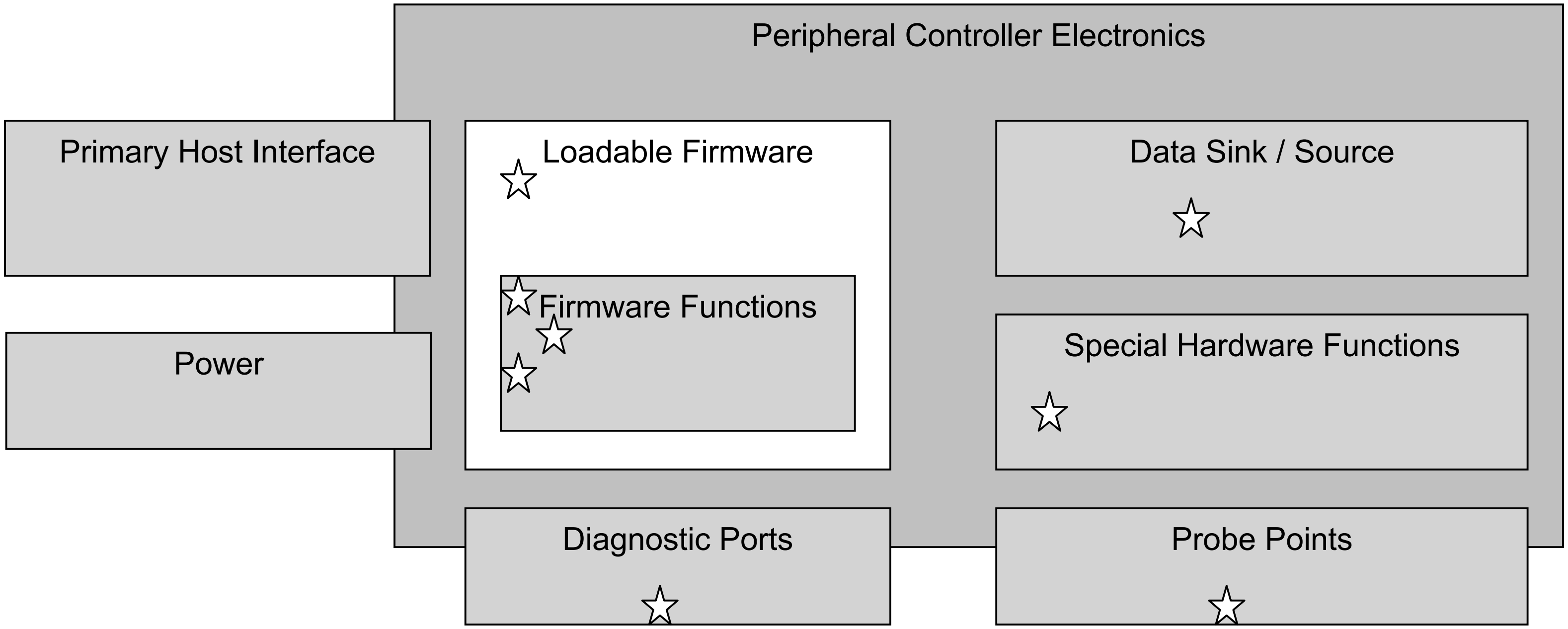
General Risk Model for a Peripheral



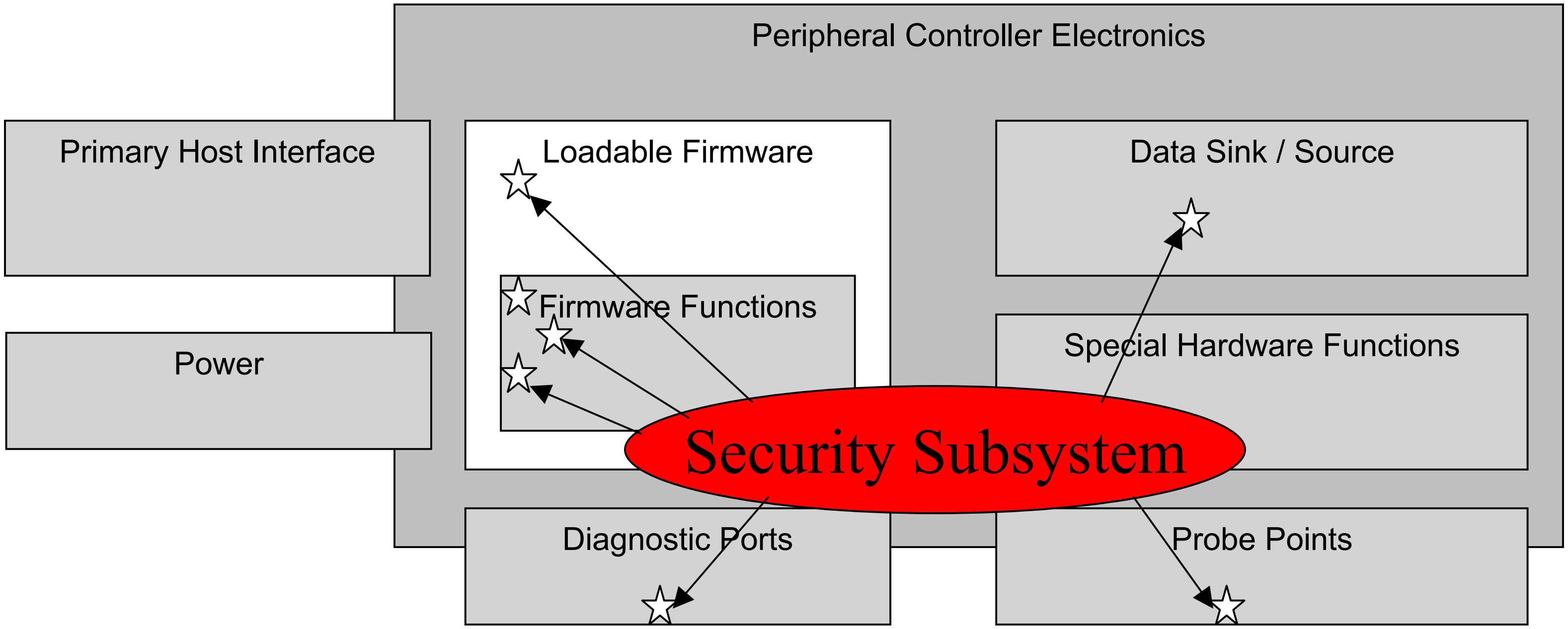
The general risk model shows four major channels of attack in a peripheral:

1. **Primary host interface**
2. **Power**
3. **Diagnostic ports**
4. **Probe points**

Access Control over Points of Vulnerability



Access Control over Points of Vulnerability



Summary

The security subsystem is controlled differently than the main purpose of the device

Trusted IN/OUT Proposal

Bit Byte	7	6	5	4	3	2	1	0
0	operation code (B5h)							
1	reserved			rstrict	spid			
2	pkt_typ	sp_ctrl		rstrict	ipid			
3	restricted							
4	(msb)							
5		key reference						
6								
7								(lsb)
8	(msb)	transfer length						
9								(lsb)
10	reserved							
11		control						

SPID

- Security Protocol ID
  - Protocol for controlling security subsystem
    - E.g., Smart Card – ISO 7816 (probably a hundred variants today)
    - TCG Protocol

Value	Description
0h	Request for an X.509 certificate (see 1.3)
1h – 6h	Reserved.
7h – Ch	Restricted to TCG.
Dh - Fh	Vendor specific.

IPID

- Integrity Protocol ID
  - DoS Attacks – Allows upstream filtering
  - OSD Compatibility – Allows Same Object Authentication

Value	Description
0h	No integrity protection.
1h	Hashed.
2h	Keyed hashed (HMAC).
3h	SHA-1.
4h	SHA-256.
5h - Dh	Reserved.
Eh - Fh	Vendor specific.

Discussion

BACKUP

Issues of the moment..

- What is TCG and what is it doing?
- What is it NOT doing
  - It is not doing DRM or Content Protection
  - But it is an enabler of that, privacy protection, and many other things that improve system reliability, availability, and predictability
- Why we are suggesting a Trusted Send/Receive as a container for messaging
  - Messaging needs to be session oriented and confidential – may be slow (inexpensive but limited) or fast.

TCG Mission

Develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms

Building Blocks

- **TPM (Trusted Platform Module)**: A hardware source of trust for platform hosts (PCs, Servers, PDAs, Phones, etc.)
- **Peripherals, Storage** : Making these devices provide other components of trust. (Harden the component hardware).
- **Infrastructure** : Across Platform Communications
- **Outside TCG Proper:** Intel's LaGrande Protected Execution Processor, and AMDs Secure Execution Machine, Microsoft's Next Generation Secure Computing Base (NGSCB) running on these processors.

TCG System Benefits

- Benefits for today’s applications
  - **Measurable security for data (files) and communications (email, network traffic)**
  - **Hardware protection for Personally Identifiable Information (Digital IDs)**
  - **Strong protection for passwords : theft of data on disk provides no useful information**
  - **Lowest cost hardware security solution : no token to distribute or lose, no peripheral to buy or plug in, no limit to number of keys, files or IDs**
- Benefits for new applications
  - **Safe remote access through a combination of machine and user authentication**
  - **Enhanced data confidentiality through confirmation of platform integrity prior to decryption**

TPM Provides Enhanced Protection for Business

Usage	Protection	Examples
Hardened Data Protection	Helps protect the integrity and confidentiality of data assets through hardware-based protection of encryption keys	**Email, file encryption**
Hardened Electronic Digital Signatures	Increases confidence in digital signature operations by providing hardware-based protection of Digital IDs. Prevents cloning by performing signature operation in tamper resistant hardware.	**Online purchases, contracts**
Hardened User Authentication	Helps protect integrity and confidentiality of user login credentials. Can also act as the “something you have” in multi-factor authentication scenario	**Can replace smart cards, secure tokens**
Hardened Platform Authentication	Helps to ensure that only authorized platforms and users gain access to corporate network and that security policy settings / security software haven't been attacked.	**Virtual Private Networks (VPN)**

Value proposition speaks to urgent needs of security-minded businesses

TRUSTED COMPUTING GROUP™

TCG Structure

- TCG is incorporated as a not-for-profit corporation, with international membership
  - Open membership model
    - Offers multiple membership levels: Promoters, Contributors, and Adopters
  - Board of Directors
    - Promoters and member elected Contributors
  - Typical not-for-profit bylaws
  - Industry typical patent policy (Reasonable and Non Discriminatory) for all published specifications
  - Working Groups

TRUSTED COMPUTING GROUP™

TCG Membership

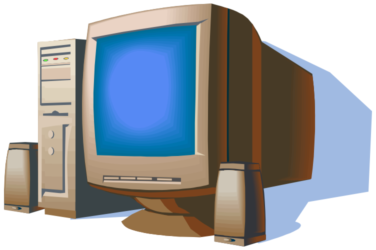
- Promoters and Board:
  - **AMD*, Hewlett Packard*, IBM*, Intel*, Microsoft*, Seagate*+, Sony*, Sun Microsystems*, and Verisign*+**
- Contributors:
  - Agere Systems*, ARM*, ATi Technologies*, Atmel*, Broadcom Corporation*, Comodo*, DELL*, Fujitsu Limited*, Fujitsu-Siemens Computers*, Gemplus*, Infineon*, Legend Limited Group*, Motorola*, National Semiconductor*, nCipher*, Nokia*, NTRU Crytosystems, Inc.*, NVIDIA*, Phoenix*, Philips*, Rainbow Technologies*, RSA Security*, Seagate*, Shang Hai Wellhope Information*, Silicon Storage Technology*, Standard Microsystems*, STMicroelectronics*, Symantec*,Texas Instruments*, Utimaco Software AG*, VeriSign Inc.*, Wave Systems* .. (75)
- Adopters:
  - Ali Corporation*, Gateway*, M-Systems*, Silicon Integrated Systems*, Softex*, Toshiba*, Winbond Electronics*

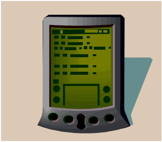
* Other names and brands may be claimed as the property of others.

+ Elected Contributor member elected to 1 yr term.

Technical Workgroups

(organized by conceptual, not governance hierarchy)





- Technical Committee Charters Work Groups:
  - Trusted Platform Module (TPM)
    - TPM Software Stack (TSS)
      - PC Specific Implementation
      - Server Specific Implementation
      - PDA Specific Implementation
      - Mobile Phone Specific Implementation
  - InfraStructure
    - User Authentication
  - Peripherals
    - Storage

  - Conformance (e.g., Common Criteria, FIPS)
  - Best Practices
- Additional work groups anticipated

TRUSTED COMPUTING GROUP™

Implementation Status

- Trusted Platform Modules (TPM) based on 1.1b specification available from multiple vendors
  - Atmel*, Infineon*, National Semiconductor*
- Compliant PC platforms shipping now
  - IBM* ThinkPad notebooks and NetVista desktops
  - HP* D530 desktops, Selected Laptops
  - Intel D865GRH motherboard
  - Dell Latitudes (100% in Gov)
  - More expected soon
- Application support by multiple ISV's
  - Existing familiar applications are using TCG/TPM through standard cryptographic APIs like MC-CAPI and PKCS #11
- TPM 1.2 Specification announced Nov. 5, 2003
- **Peripherals and Storage Chartered January 2004**.

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

Goals of the TCG Architecture

TCG defines mechanisms that

- Protect user keys (digital identification) and files (data)
- Protect secrets (passwords)
- Enable a protected computing environment

While…

- Ensuring the user's control
- Protecting user's privacy

Design Goal: Delivering robust security with user control and privacy

TRUSTED COMPUTING GROUP™

TCG Policy Positions

Privacy Effect of TCG Specifications

TCG is committed to ensuring that TCG specifications provide for an increased data capability to secure personally identifiable information

Open Platform Development Model

TCG is committed to preserving the open development model that enables any party to develop hardware, software or systems based on TCG Specifications. Further, TCG is committed to preserving the freedom of choice that consumers enjoy with respect to hardware, software and platforms

TRUSTED COMPUTING GROUP™

TCG Policy Position

Platform Owner and User Control

TCG is committed to ensuring owners and users of computing platforms remain in full control of their computing platform, and to require platform owners to opt-in to enable TCG features

Backwards Compatibility

TCG commits to make reasonable efforts to ensure backward compatibility in future specifications for currently approved specifications

TCG System Benefits

- Benefits for today's applications
  - **Hardware protection for keys used by data (files) and communications (email, network traffic)**
  - **Hardware protection for Personally Identifiable Information (Digital IDs)**
  - **Hardware protection for passwords stored on disk**
  - **Lowest cost hardware security solution : no token to distribute or lose, no peripheral to buy or plug in, no limit to number of keys, files or IDs**

- Benefits for new applications
  - **Safer remote access through a combination of machine and user authentication**
  - **Enhanced data confidentiality through confirmation of platform integrity prior to decryption**

TPM Abstract Architecture

- Module on the motherboard
  - Can’t be removed or swapped
  - Secrets in module can’t be read by HW or SW attackers
- Stores Private Keys
  - Perform the private key operation on board so that private key data never leaves TPM
- Hold Platform Measurements
  - PC measures software, TPM is repository of measurements

TPM Architecture

- Turnkey Secure Module
  - **Internal CPU to implement all TPM commands**
  - **Internal math engine to accelerate computation of asymmetric algorithm operations**
  - **Tamper resistance to prevent physical attacks that might reveal TPM or user secrets.**
  - **Communications channel to main processor (LPC typical)**
- Asymmetric Details
  - **RSA support mandatory, other algorithms optional. 512 through 2048 bit key length. On board key generation.**
  - **On board key cache stores frequently used keys, arbitrary number stored on disk. Off chip keys are protected using key that never leaves TPM.**
  - **Keys can be migrated from one TPM to another – if both the TPM owner and the key owner authorize the operation and if the key has been appropriately tagged at creation**

TPM Architecture (cont'd)

- Integrity Metric Storage
  - **Multiple instances of Platform Configuration Registers (PCR)**
  - **Can be extended (hash with new value) but not cleared**
  - **Key usage can be connected to desired values**
  - **Platform can provide attestation of current values**
- High Quality Random Number Generator
  - **Used to prevent replay attacks, generate random keys**
- SHA-1 Hash Computation Engine
  - **Multiple uses: integrity, authorization, PCR extension, etc.**
- Nonvolatile memory
  - **Owner information (on/off, owner auth secret, configuration)**
  - **Platform attestation information**

Implementation Status

- Trusted Platform Modules (TPM) based on 1.1b specification available from multiple vendors
  - Atmel*, Infineon*, National Semiconductor*
- Compliant PC platforms shipping now
  - IBM* ThinkPad notebooks and NetVista desktops
  - HP* D530 Desktops and nc4010, nc6000, nc8000, and nw8000 Notebooks
  - Intel* D865GRH motherboard
  - Fujitsu* LifebookS notebook PC series
  - More expected soon
- Application support by multiple ISV's
  - Existing familiar applications are using TCG/TPM through standard cryptographic APIs like MC-CAPI and PKCS #11
- TPM 1.2 Specification announced late fall 2003
  - Atmel has announced chips based on new spec; anticipate other TPM vendors to make silicon available soon

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

Common Misconceptions

- The TPM does not measure, monitor or control anything
  - **Software measurements are made by the PC and sent to the TPM**
  - **The TPM has no way of knowing what was measured**
  - **The TPM is unable to reset the PC or prevent access to memory**
- The platform owner controls the TPM
  - **The owner must opt-in using initialization and management functions**
  - **The owner can turn the TPM on and off**
  - **The owner and users control use of all keys**
- DRM is not a goal of TCG specifications
  - **All technical aspects of DRM are not inherent in the TPM**
- TPMs can work with any operating systems or application software
  - **The spec is open and the API is defined, no TCG secrets.**
  - **All types of software can (and will, we hope) make use of the TPM**

TRUSTED COMPUTING GROUP™

Storage Charter

- Basic-Storage-Unit (BSU) Centric
  - Disc Drives, Removable Optical, Flash
  - Coordinate *closely* with SNIA Security, INSIC, INCITS – large overlap in industry membership.
- Focus
  - Key distribution and protection on storage devices
  - Key operations on storage devices (e.g., whole drive encryption, authenticating a host context)
  - Data at rest protection (where’s that device been)?
  - Data protected against host side deletion or alteration (Tunneling, Secure Messaging).
  - On board security manager for OSD

Trusted Send/Receive Concept

- Commands that can hold special security messages that are optionally confidential (and require out of path decryption / encryption)
- Messages have (possibly multiply simultaneous) Sessions (essential for security) to manipulate security bindings or associations (e.g., challenge-response authentication and key exchange, and action)
- There may be more than one security language supported : Native TCG, ISO 7816 ICC Smartcard

More TCG Technical Concepts…

Goals of the TCG Architecture

TCG defines mechanisms that securely

- Protect user keys (digital identification) and files (data)
- Protect secrets (passwords) from being revealed
- Protect the user's computing environment

While…

- Ensuring the user's control
- Protecting user's privacy

Design Goal: Delivering robust security <u>with</u> user control and privacy

TRUSTED COMPUTING GROUP™

Architecture & Usage …

TPM Abstract Architecture

- Module on the motherboard
  - Can’t be removed or swapped
  - Secrets in module can’t be read by HW or SW attackers
- Stores Private Keys
  - Perform the private key operation on board so that private key data never leaves TPM
- Hold Platform Measurements
  - PC measures hardware, firmware, software, TPM is repository of measurements

TRUSTED COMPUTING GROUP™

TPM Architecture

- RSA support mandatory, other algorithms optional. 512 through 2048 bit key length. On board key generation.
- On board key cache stores frequently used keys, arbitrary number stored on disk. Off chip keys are protected using key that never leaves TPM.
- Keys can be migrated from one TPM to another – if both the TPM owner and the key owner authorize the operation and if the key has been appropriately tagged at creation

TPM Architecture (cont'd)

- Integrity Metric Storage
  - Multiple instances of Platform Configuration Registers (PCR)
  - Can be extended (hash with new value) but not cleared
  - Key usage can be connected to desired values
  - Platform can provide attestation of current values
- High Quality Random Number Generator
  - Used to prevent replay attacks, generate random keys
- SHA-1 Hash Computation Engine
  - Multiple uses: integrity, authorization, PCR extension, etc.
- Nonvolatile memory
  - Owner information (on/off, owner auth secret, configuration)
  - Platform attestation information

TRUSTED COMPUTING GROUP™

TPM is only one trusted building block

No bulk encryption, for example.

HOW TPM WORKS TOGETHER so far…

Endorsement Key (EK)

- Single 2048 RSA keypair
  - An encryption key
  - But, has very restricted uses
    - Never used in authentication, attestation or other user protocols
    - Cannot be used to encrypt or sign user data
- Relationships:
  - One EK per TPM
    - One-to-one relationship to the TPM
  - One TPM per platform
    - One-to-one relationship to the Platform
  - One EK per Platform
    - One-to-one relationship to the Platform

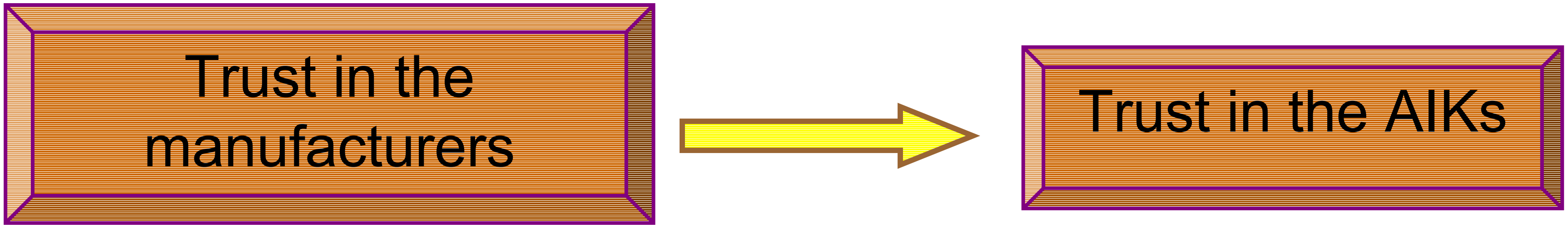
Authentication & Attestation

- Problem:
  - Need an authentication key for:
    - Platform authentication
    - Attestation of platform configuration
    - Protection properties of TPM keys
    - Etc.
  - Can’t use the Endorsement Key (EK)
    - This is a unique key
    - Privacy sensitive
- Solution: Attestation Identity Key (AIK)
  - This is a signature key
  - Only available on the platform that created it
  - Unlimited number of them
    - Can create one per domain

The EK is used to attest to the AIKs

TCG Credential (Signed Public Key) Concepts

- TCG Credentials are used to obtain an AIK
- TCG Credentials provide proof of a valid:
  - TPM
  - Platform



Trust in the manufacturers

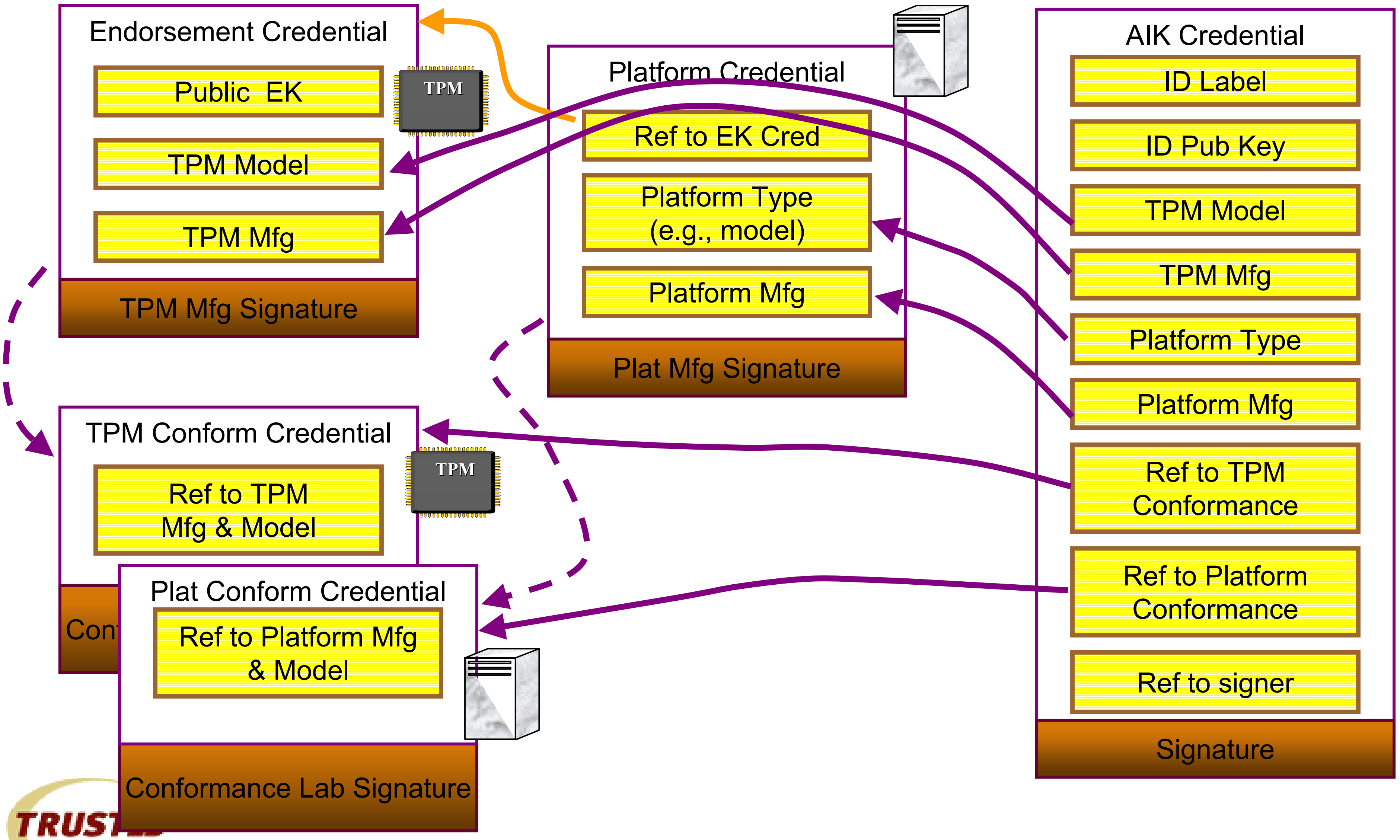
Trust in the AIKs

- Credentials impact manufacturing and distribution of
  - Components and "Finished Platforms"

TPM Credentials

- Types:
  - – **Endorsement Credential**
    - **One per platform**
  - – **Platform Credential**
    - **One per platform**
  - – **TPM Conformance Credential**
    - **One per “model” of platform**
  - – **Platform Conformance Credential**
    - **One per “model” of platform**
  - – **Validation Credentials**
    - **One per component (Optional for a TCG-platform)**
  - – **AIK (Attestation Identity Key) Credential**
    - **Any number per platform**
- Signers
  - – **The “issuer” signs the Credentials**
- Creation and distribution mechanism is not specified by TCG

Credential Relationships



Endorsement Credential

Public EK

TPM Model

TPM Mfg

TPM Mfg Signature

Platform Credential

Ref to EK Cred

Platform Type (e.g., model)

Platform Mfg

Plat Mfg Signature

AIK Credential

ID Label

ID Pub Key

TPM Model

TPM Mfg

Platform Type

Platform Mfg

Ref to TPM Conformance

Ref to Platform Conformance

Ref to signer

Signature

TPM Conform Credential

Ref to TPM Mfg & Model

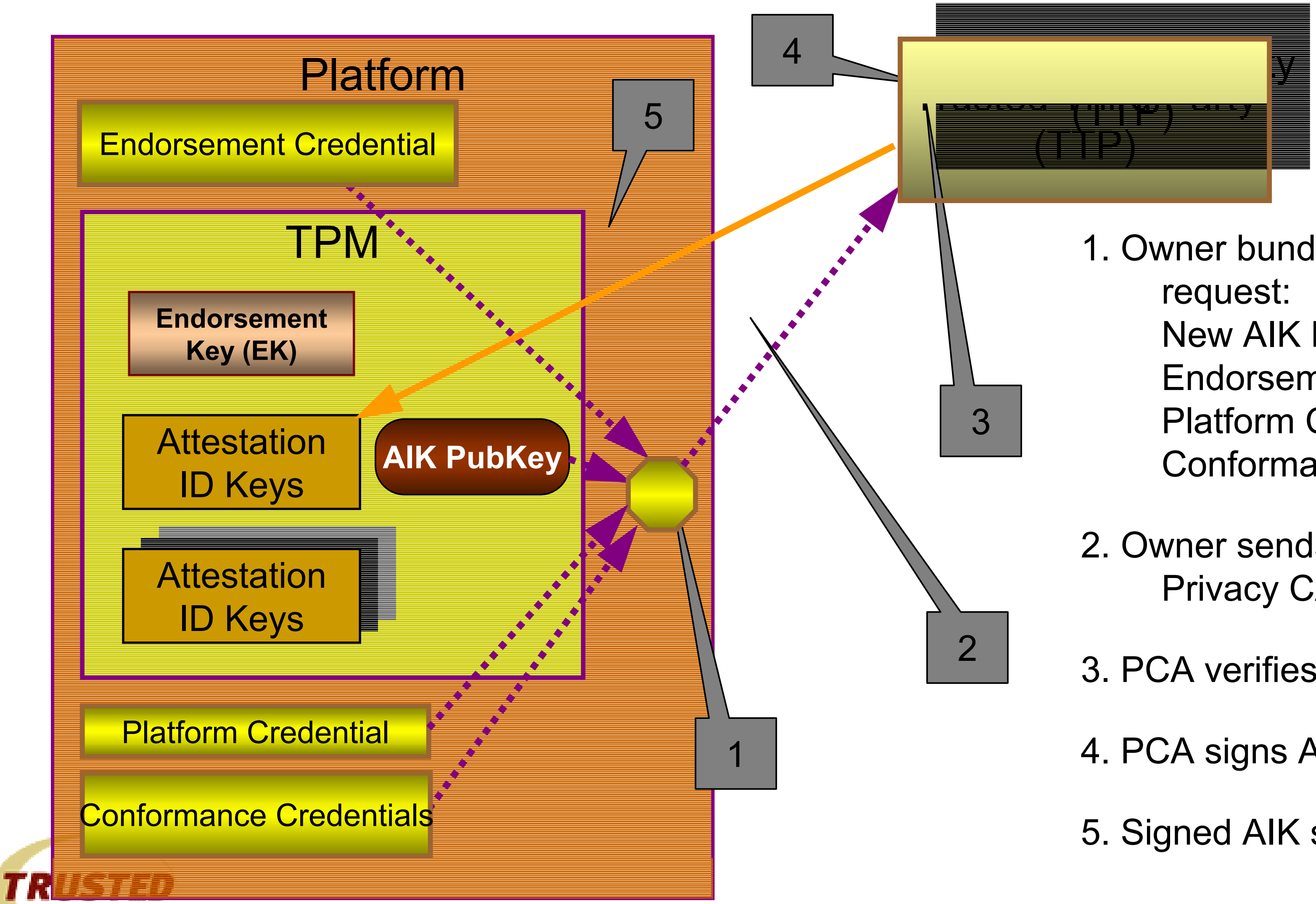
Con

Plat Conform Credential

Ref to Platform Mfg & Model

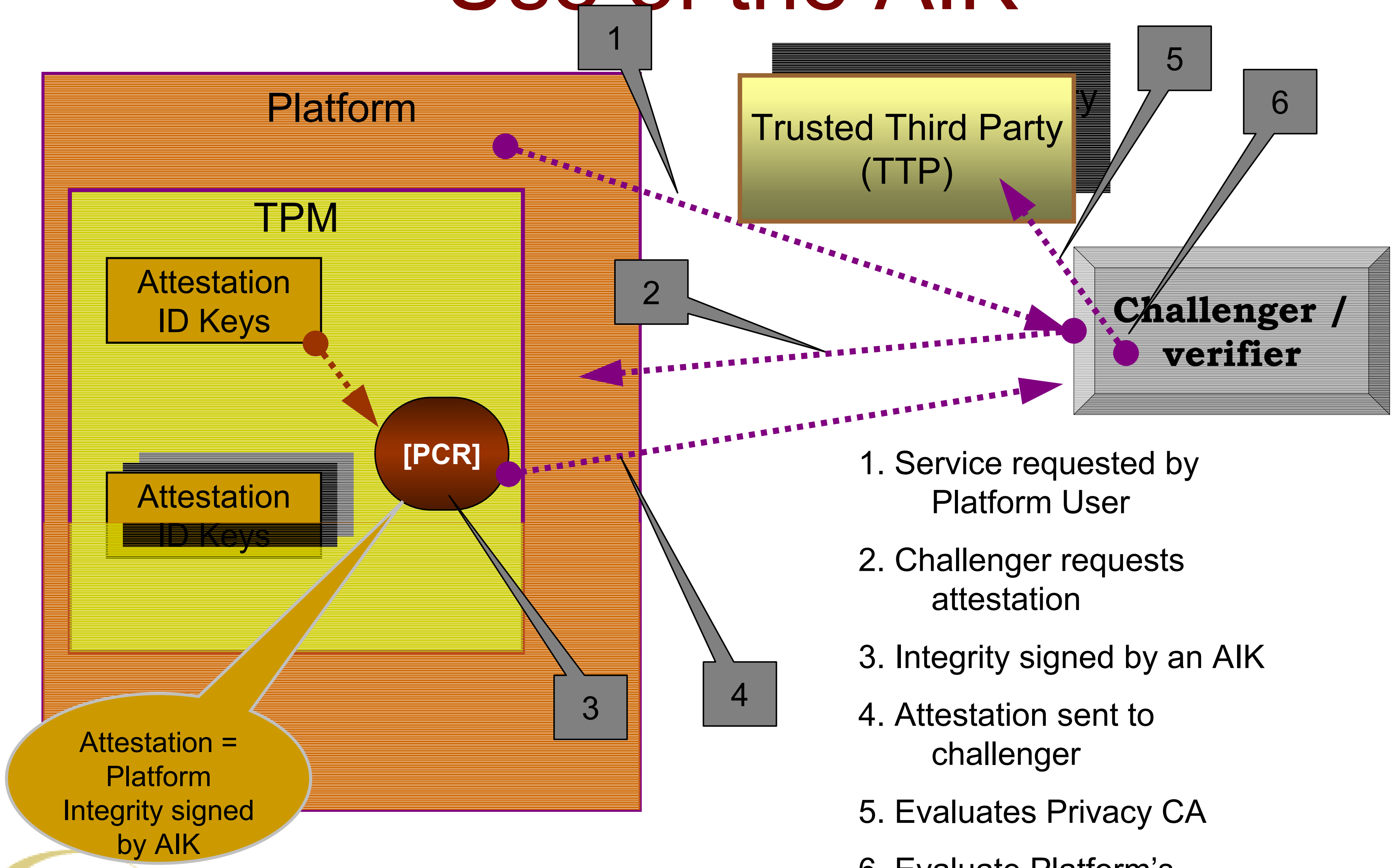
Conformance Lab Signature

Certifying the AIK using the Privacy CA Model



1. Owner bundles into an AIK request:
   New AIK PubKey
   Endorsement Cred,
   Platform Cred,
   Conformance Creds
2. Owner sends AIK request to Privacy CA (PCA)
3. PCA verifies Credentials
4. PCA signs AIK
5. Signed AIK sent to TPM

Use of the AIK



1. Service requested by Platform User
2. Challenger requests attestation
3. Integrity signed by an AIK
4. Attestation sent to challenger
5. Evaluates Privacy CA
6. Evaluate Platform’s Integrity

TRUSTED COMPUTING GROUP™

DONE!

Actually a lot more, but that's enough for now…