Trusted Computing Group
Introduction and Brief Technical Overview for SNIA Security Workgroup

Robert Thibadeau, Ph.D.

Seagate Research

February, 2004

Note: Borrowed (very) Heavily from TCG presentations…Including TCG Marketing Workgroup and Monty Wiseman’s RSA Conference Presentation

www.trustedcomputinggroup.org

Agenda

- TCG Standards Group Intro
- TCG Technical Concepts
- TPM Architecture
- How it Works Together
- Discussion

TRUSTED COMPUTING GROUP™

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.

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 other) attacks (or accidents).

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

TCG Membership as of 1/28/04

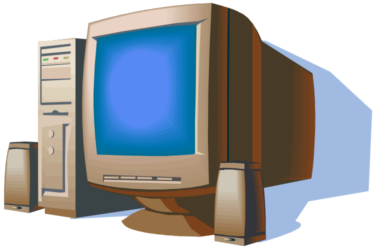
- Promoters and Board:
  - **AMD*, Hewlett Packard*, IBM*, Intel*, Microsoft*, Seagate*+, Sony*, Sun Microsystems*, and Verisign*+**
- Contributors:
  - Agere Systems*, ARM*, ATi Technologies*, Atmel*, Broadcom Corporation*, Comodo*, Fujitsu Limited*, Fujitsu-Siemens Computers*, Gemplus*, Infineon*, 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*, Texas Instruments*, Utimaco Software AG*, VeriSign Inc.*, Wave Systems* .. (55)
- Adopters:
  - Ali Corporation*, Gateway*, M-Systems*, Silicon Integrated Systems*, Softex*, Toshiba*, Winbond Electronics*

TRUSTED COMPUTING GROUP™

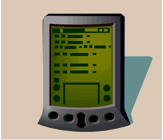
* Other names and brands may be claimed as the property of others.

+ 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

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
  - Intel D865GRH motherboard
  - 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.

Storage Charter

- Basic-Storage-Unit (BSU) Centric
  - Disc Drives, Removable Optical, Flash
- Enterprise Storage, too
  - The Enterprise Storage (sub)System as a building block
  - Securing the inside of the Enterprise Storage System (as a host platform with BSU building blocks inside it)
  - Coordinate *closely* with SNIA Security – large overlap in industry membership.
- Just Starting up NOW

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 with user control and privacy

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

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**

TPM is only one trusted building block

No bulk encryption, for example.

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

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

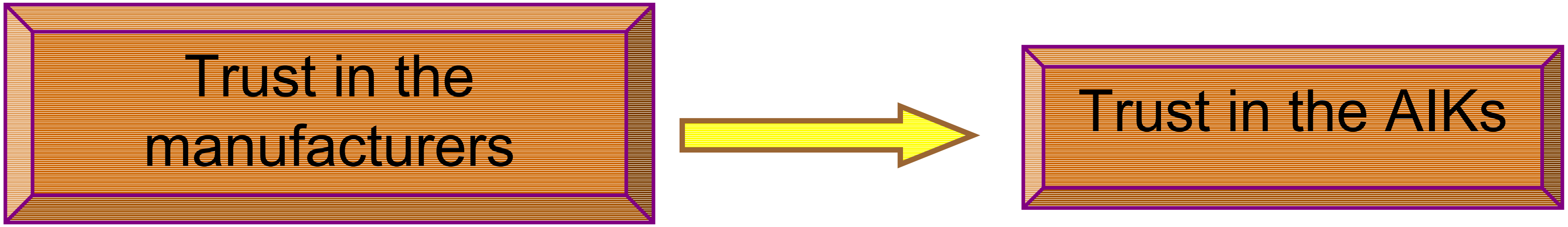
Authentication & Attestation

- 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

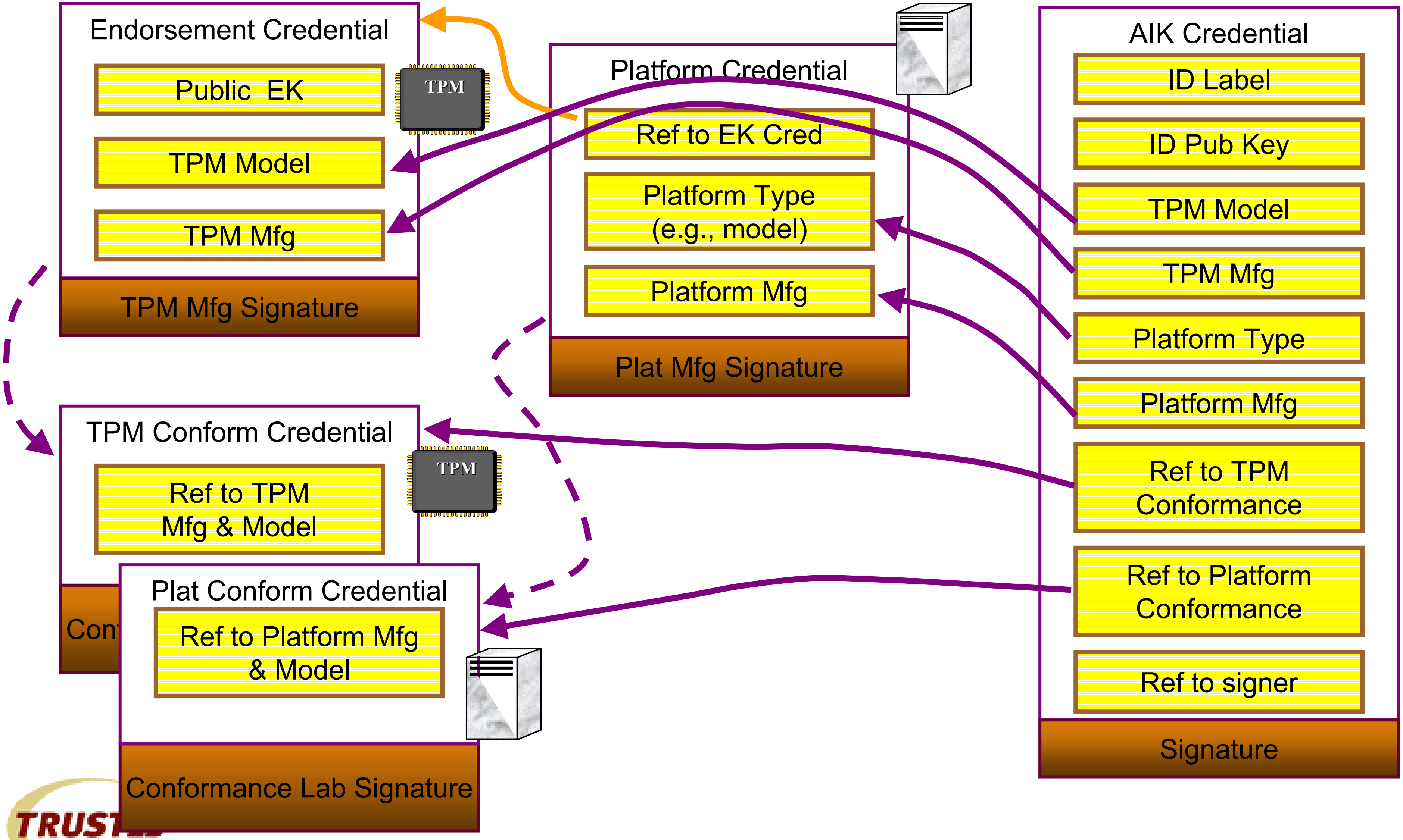
Trust in the AIKs

- 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

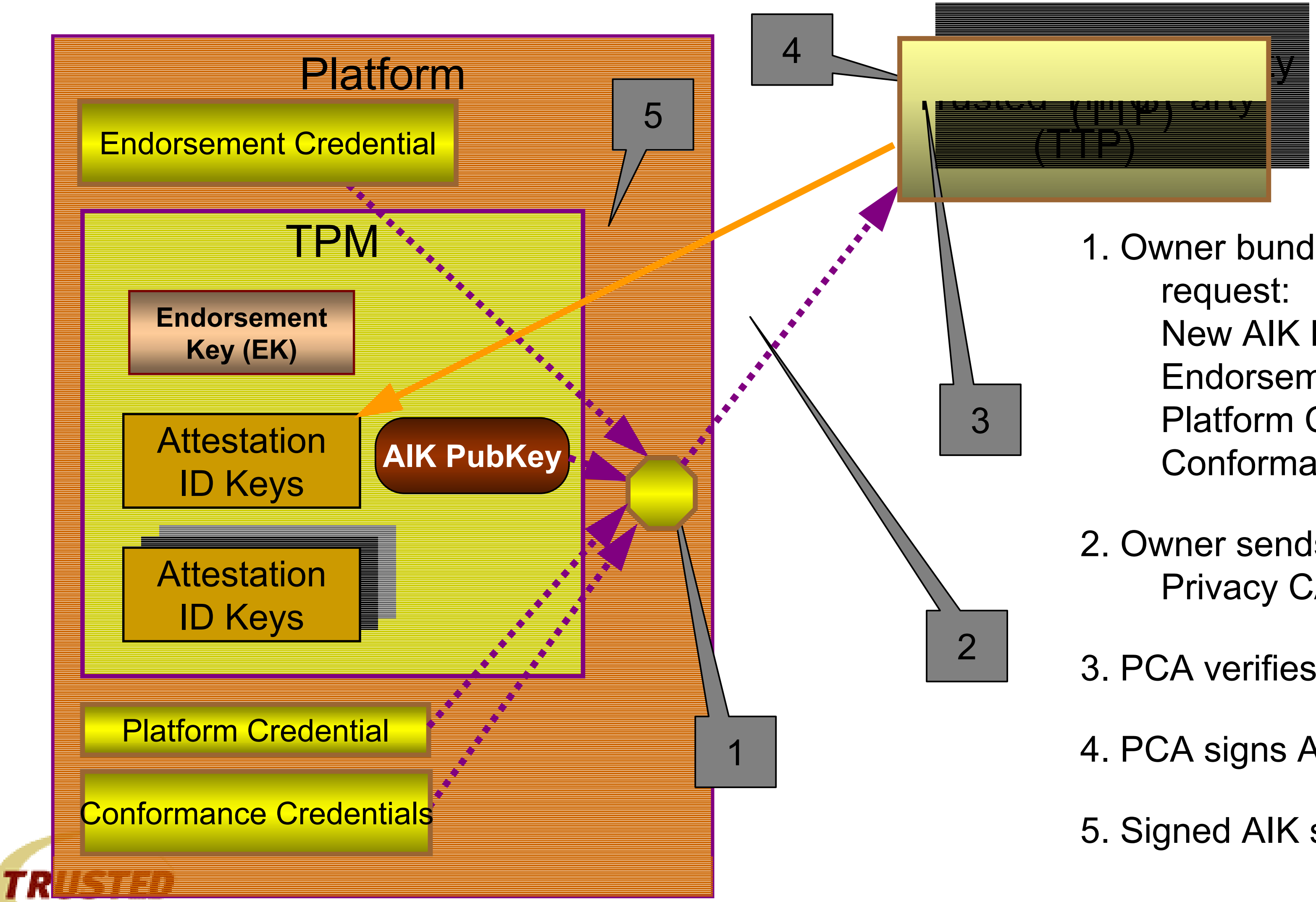
Con

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

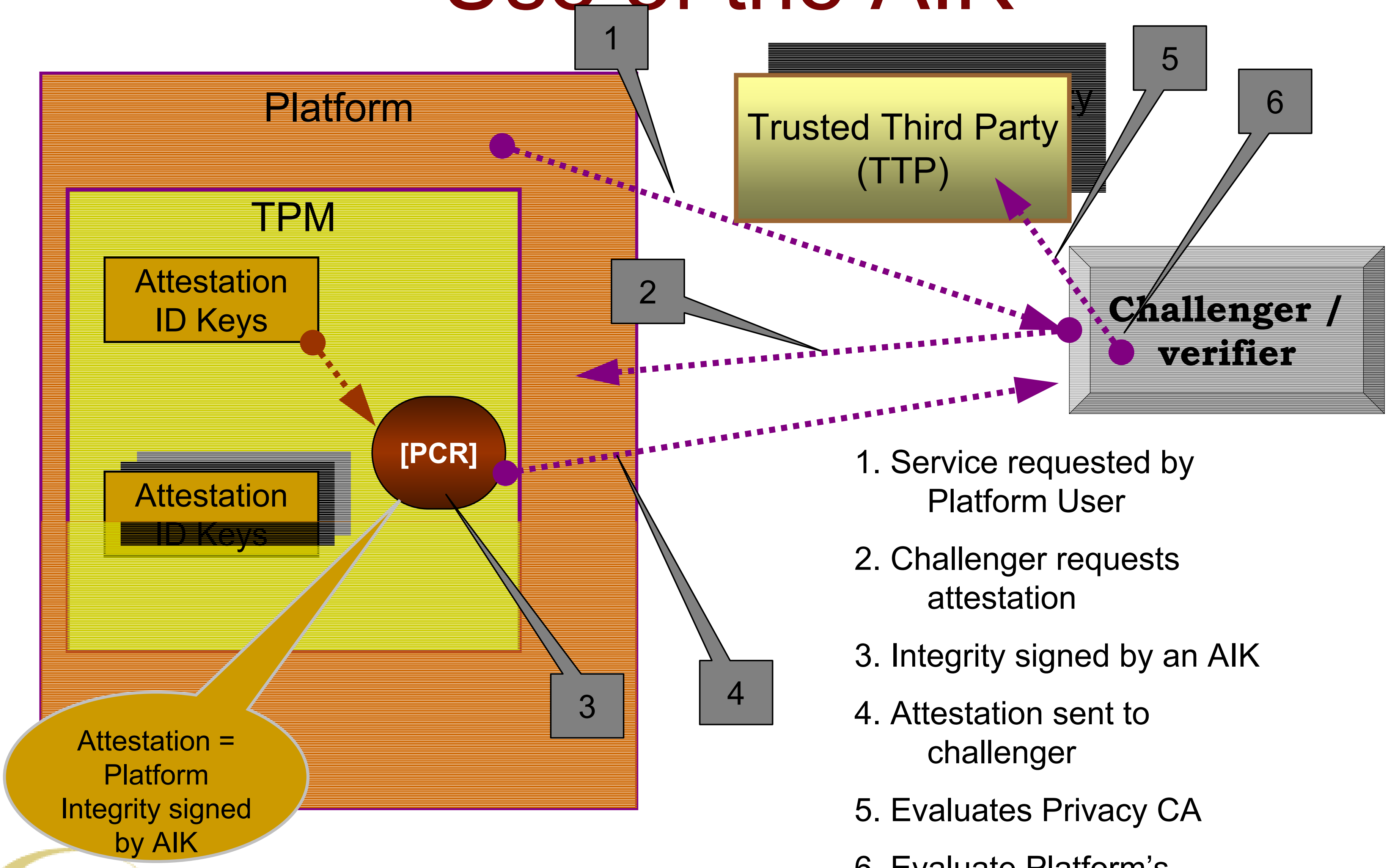
2. Owner sends AIK request to Privacy CA (PCA)

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

DONE!

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

Backup

Summary

- World Class Security
  - Open standards, low cost, owner control
- TCG will develop, define, and promote industry standard specifications for hardware building blocks and software interfaces for trusted computing across multiple platforms and operating environments
  - Current functionality being enhanced and extended
  - New specifications being created
  - Workgroups active in many areas

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

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

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