The Trusted Platform Module Specifications

Patrick George

Gemplus

Overall Presentation Goals

- Introduce the Trusted Computing Group (TCG)
- Provide a medium/high level view of the Trusted Platform Module (TPM)
  - Architecture
  - Functionality
  - Use cases
- Discuss the relationships between smart cards and TPM in Trusted Computing architectures

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

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 Organization

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, *VeriSign*

Marketing Workgroup
Brian Berger, Wave Systems

- **Public Relations**
  Anne Price, *PR Works*
- **Events Marketing Support**
  VTM, Inc.

Technical Committee
Graeme Proudler, *HP*

- **TPM Work Group**
  David Grawrock, *Intel*
- **TSS Work Group**
  David Challener, *Lenovo*
- **Mobile Phone WG**
  Janne Uusilehto, *Nokia*
- **Peripherals WG**
  Colin Walters, *Comodo*
- **Server Specific WG**
  Larry McMahan, *HP*
  Marty Nicholes, *HP*
- **Conformance WG**
  Randy Mummert, Atmel
- **PC Client WG**
  Monty Wiseman, *Intel*
- **Infrastructure WG**
  Thomas Hardjono, VeriSign
  Ned Smith, Intel
- **Storage Systems**
  Robert Thibadeau, *Seagate*
- **Hard Copy WG**
  Brian Volkoff, *HP*

Advisory Council
Invited Participants

Administration
VTM, Inc.

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™

TCG Membership

110 Total Members as of August 18, 2005
7 Promoter, 71 Contributor, 32 Adopter

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

Contributors
Agere Systems
American Megatrends, Inc.
ARM
ATI Technologies Inc.
Atmel
AuthenTec, Inc.
AVAYA
Broadcom Corporation
Certicom Corp.
Citrix Systems, Inc.
Comodo
Dell, Inc.
Endforce, Inc.
Ericsson Mobile Platforms AB
Extreme Networks
France Telecom Group
Freescale Semiconductor
Fujitsu Limited

Contributors
Fujitsu Siemens Computers
Funk Software, Inc.
Gemplus
General Dynamics C4 Systems
Giesecke & Devrient
Hitachi, Ltd.
Infineon
InfoExpress, Inc.
InterDigital Communications
iPass
Lenovo Holdings Limited
Lexmark International
M-Systems Flash Disk Pioneers
Meetinghouse Data Communications
Mirage Networks
Motorola Inc.
National Semiconductor
nCipher
NEC
Network Associates
Nevis Networks, USA
Nokia
NTRU Cryptosystems, Inc.
NVIDIA
OSA Technologies, Inc
Philips
Phoenix
Pointsec Mobile Technologies

Contributors
Renesas Technology Corp.
Ricoh Company LTD
RSA Security, Inc.
SafeNet, Inc.
Samsung Electronics Co.
SCM Microsystems, Inc.
Seagate Technology
SignaCert, Inc.
Sinosun Technology Co., Ltd.
SMSC
STMicroelectronics
Sygate Technologies, Inc.
Symantec
Symbian Ltd
Synaptics Inc.
Texas Instruments
Trend Micro
TriCipher, Inc.
UPEK, Inc.
Utimaco Safeware AG
VeriSign, Inc.
Vernier Networks
Vodafone Group Services LTD
Wave Systems
Winbond Electronics Corporation
Zone Labs, Inc.

Adopters
Advanced Network Technology Labs
Apani Networks
Apere, Inc.
BigFix, Inc.
Bradford Networks
Caymas Systems
Cirond
CPR Tools, Inc.
Credant Technologies
Fiberlink Communications
Foundry Networks Inc.
Foundstone, Inc.
Industrial Technology Research Institute
Infosec Corporation
Lockdown Networks
Marvell Semiconductor, Inc.
MCI
PC Guardian Technologies
Safend
Sana Security
Senforce Technologies, Inc
Silicon Integrated Systems Corp.
Silicon Storage Technology, Inc.
Softex, Inc.
StillSecure
Swan Island Networks, Inc.
Telemidic Co. Ltd.
Toshiba Corporation
ULi Electronics Inc.
Unisys
Websense

TRUSTED COMPUTING GROUP™

TCG Specifications

- Trusted Platform Module (TPM) Specification 1.2
- TCG Software Stack (TSS) Specification 1.1
- TCG PC Specific Implementation Specification 1.1
- Infrastructure Specifications
  - Reference Architecture for Interoperability
  - Trusted Network Connect (TNC) specifications
- Generic Server Specification

TRUSTED COMPUTING GROUP™

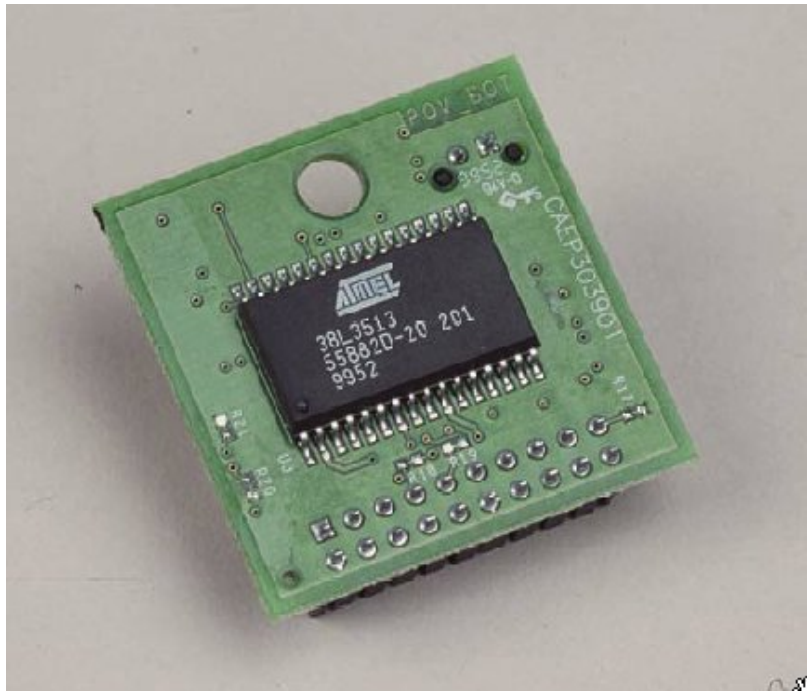
Trusted Platform

- A platform is trusted if it always behaves in the expected manner for the intended purpose
  - Is the platform what it claims to be?
  - Has the platform been modified or compromised?
  - How are the secrets stored by the platform protected?
  - Does it embed a genuine TPM?

TRUSTED COMPUTING GROUP™

Trusted Platform Module (TPM)

- A silicon chip that performs all TPM v1.x functions, including:
  - Store platform integrity measurement
  - Generate and store a private key
  - Hash files using SHA-1
  - Create digital signatures
  - Anchor chain of trust for keys, digital certificates and other credentials



TRUSTED COMPUTING GROUP™

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 (EAL3+ min. required)
  - Communications channel to main processor (LPC typical)
- Non-volatile memory
  - Owner information (on/off, owner auth secret, configuration)
  - Platform attestation information
- Integrity metrics 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

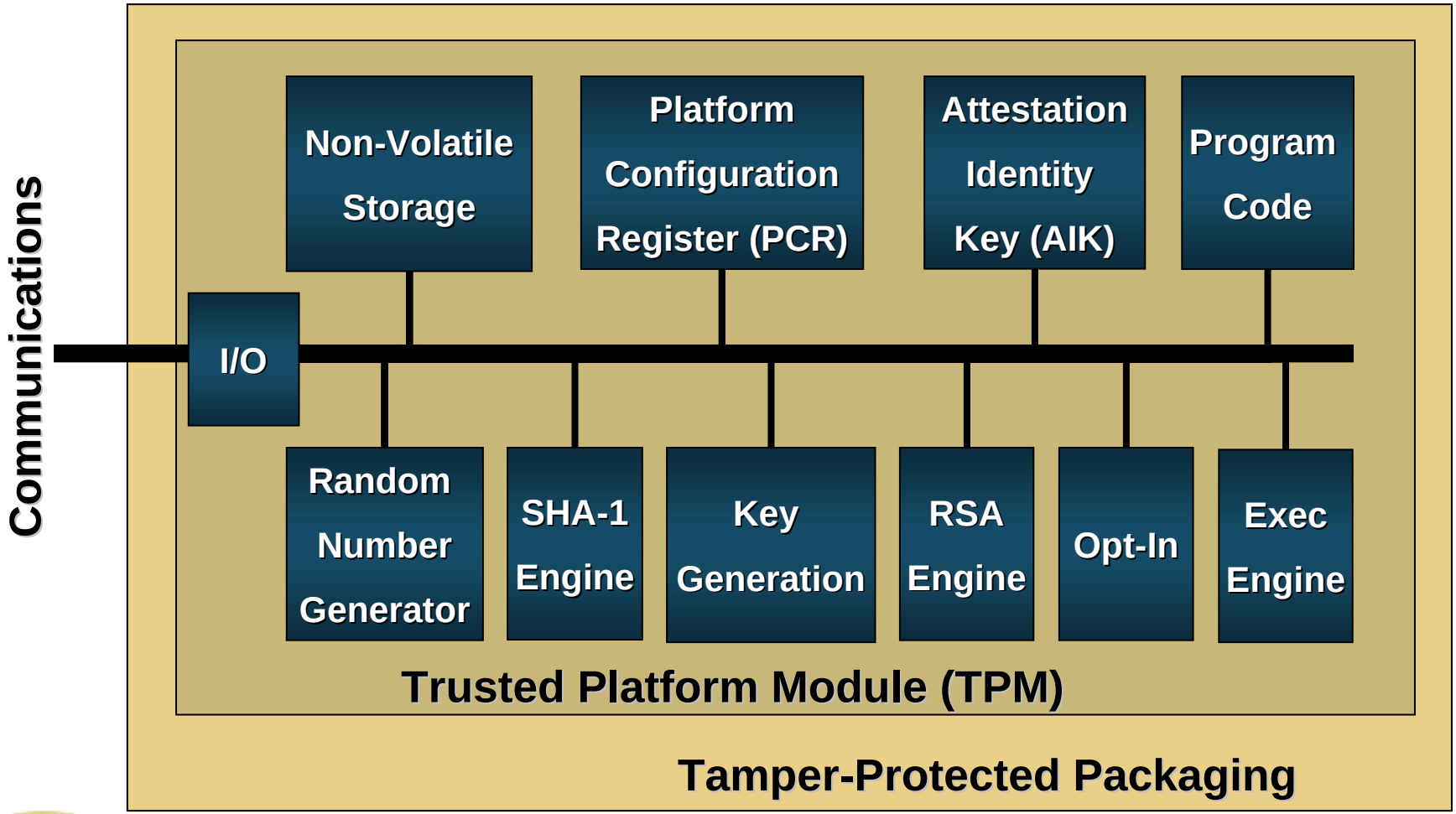
TRUSTED COMPUTING GROUP™

TPM Architecture (cont'd)

- Asymmetric cryptography engine
  - RSA support mandatory (512 through 2048 bit key length), other algorithms optional. 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
- 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.

TRUSTED COMPUTING GROUP™

TPM Block Diagram



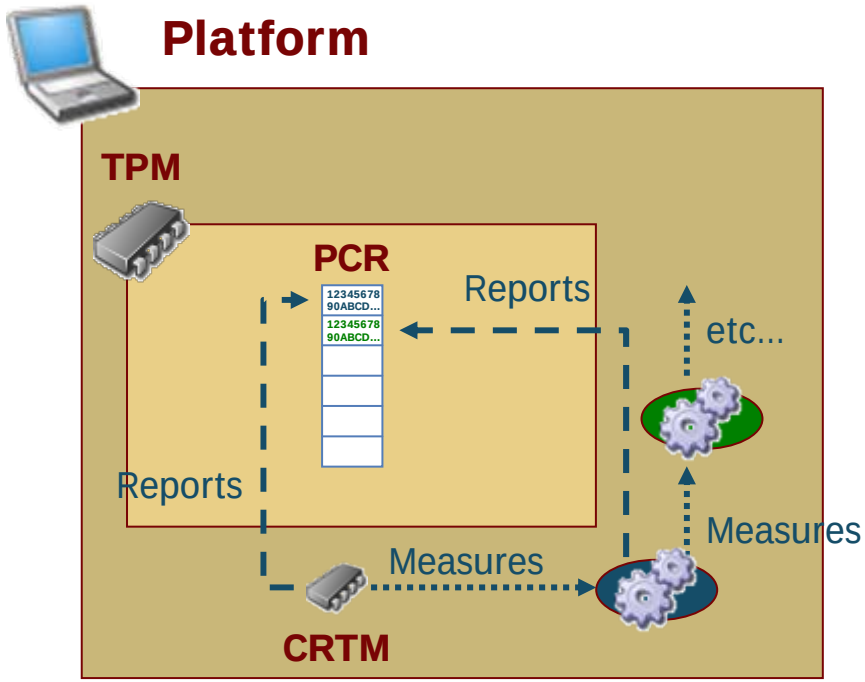
TRUSTED COMPUTING GROUP™

TPM 1.1b Functions

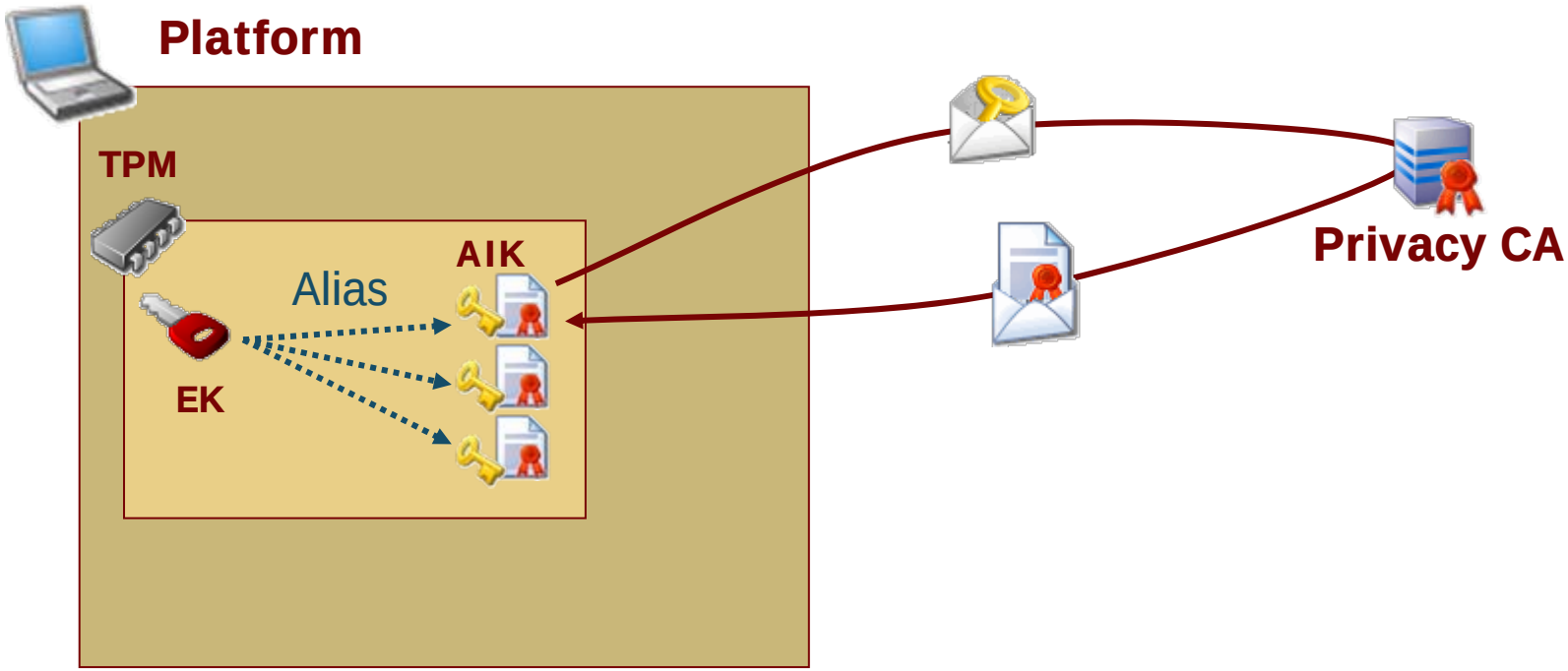
- Asymmetric key functions
  - On-chip key pair generation
  - Digital signature
  - Encryption/decryption of keys
- Secure storage and secure reporting of platform configuration information
  - Enable verifiable attestation of the platform configuration
  - Including creation of Attestation Identity Keys (AIK)
- An Endorsement Key (EK)
  - Anonymously establish that AIK were generated in a TPM
- Initialization and management functions
  - Allow platform owner to turn functionality on or off
  - Reset the chip
  - Take ownership while protecting the user privacy
  - Opt-in

TRUSTED COMPUTING GROUP™

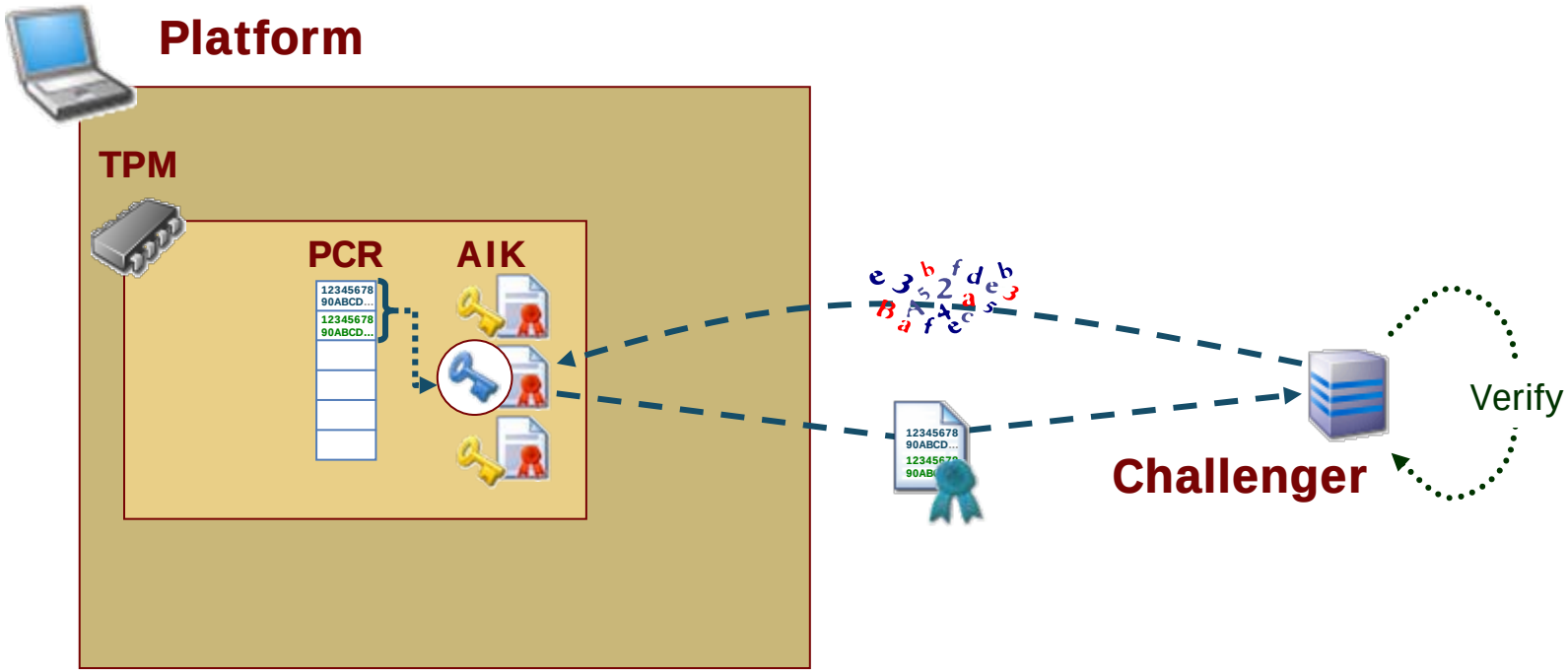
Integrity Measures



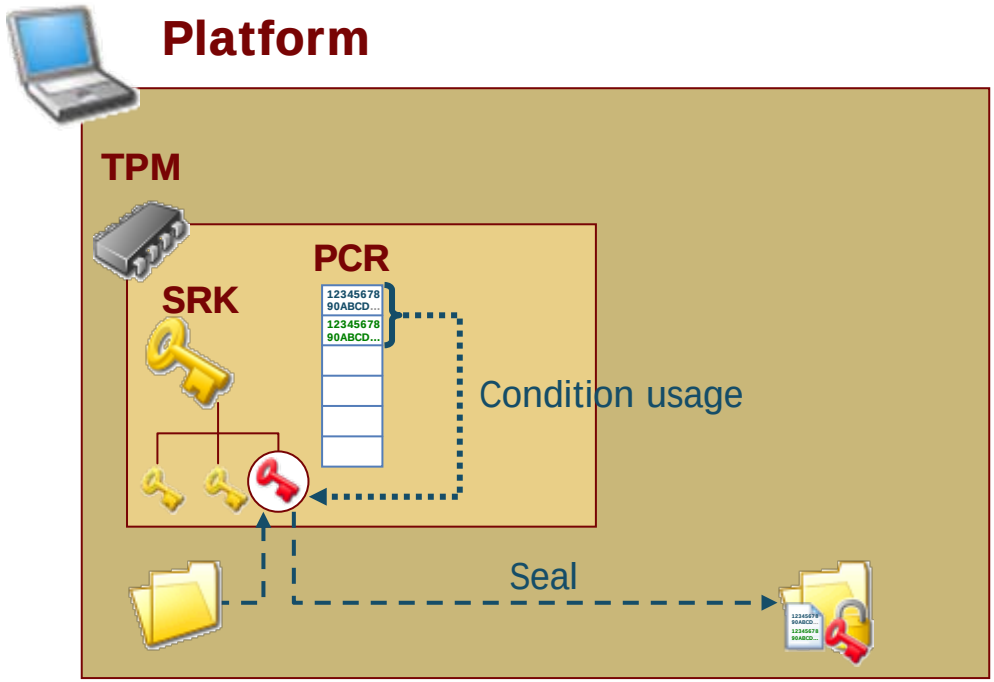
Platform Identities



Platform Attestation



Sealed Storage



TPM 1.2 New Functions

- TPM 1.1b backward compatibility
- Direct Anonymous Attestation
  - Protocol to remotely prove that a key is held in *some* hardware
  - Combine device strong authentication with privacy protection
  - Complement attestation functions in 1.1b
- Locality
  - Allows the TPM to differentiate between commands from different LOCAL sources
    - Normal application
    - Trusted application
    - Trusted OS
    - Trusted chip set
  - Enables more than one simultaneous root of trust to exist per platform

TRUSTED COMPUTING GROUP™

TPM 1.2 New Functions (cont'd)

- Delegation
  - Allow TPM owner to delegate other entities to use specific owner-authorized commands without allowing access to other commands in the TPM
- Non-volatile storage
  - Allow system software or firmware to store information on the TPM
- Others
  - Optimized transport protection
  - Monotonic counters
  - Tick counter

TRUSTED COMPUTING GROUP™

TPM Use Cases

- Secure Boot
  - Different from authenticated boot
  - Prevent the platform from booting if a difference exists between the actual boot process and the expected boot process
  - Can be achieved by using non volatile memory (or Data Integrity Registers in TPM1.1b) to hold the critical integrity measures

TRUSTED COMPUTING GROUP™

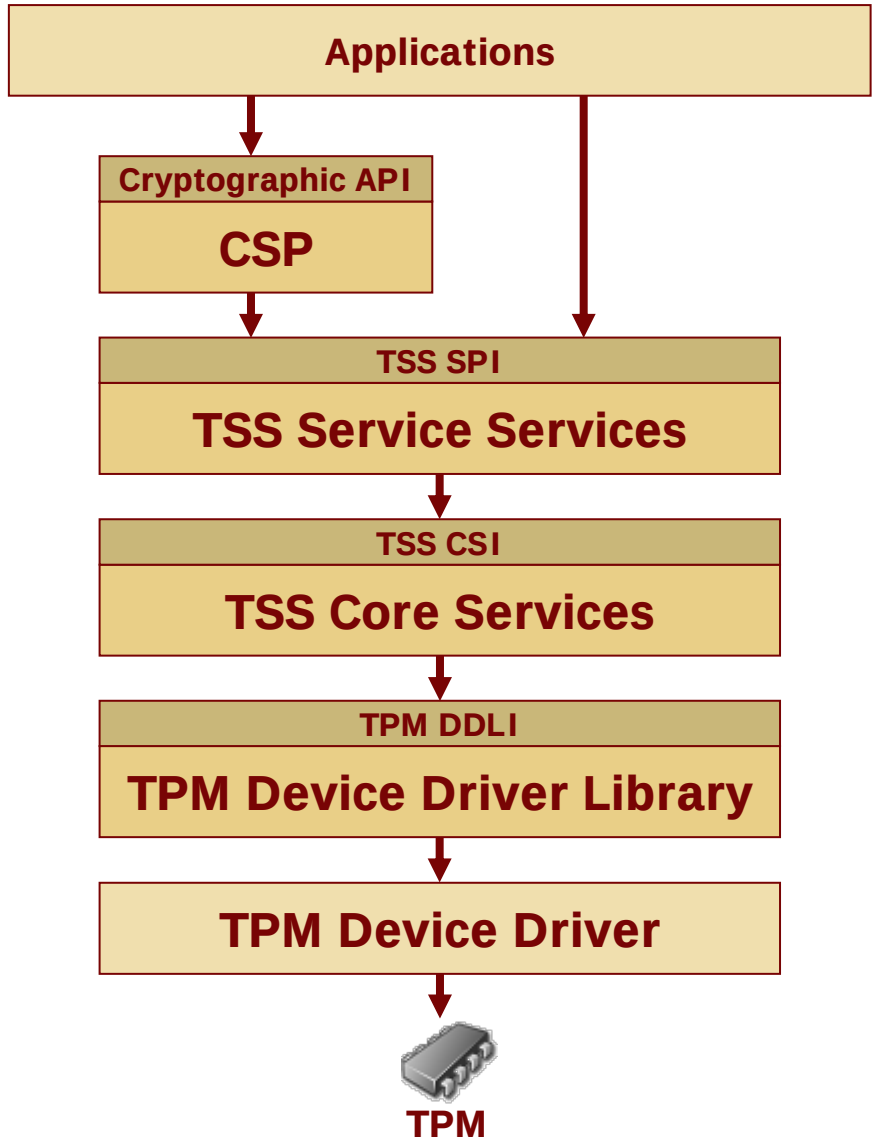
TPM Use Cases (cont'd)

- End-point integrity (TNC)
  - Introduce the notion of "health" of a client computer wishing to gain enterprise network access
    - AV version, OS patches, drivers
  - Authentication server evaluates health level of the client
  - Healthy client allowed network access, unhealthy clients denied or placed into remedial network

TRUSTED COMPUTING GROUP™

TCG Software Stack

- TSS enables application development and interoperability
  - Supply one entry point for applications to the TPM functionality
  - Provides synchronized access to the TPM
  - Hide building command streams with appropriate byte ordering and alignment from applications
  - Manage TPM resources
- Several implementations available
  - IBM
  - Infineon
  - NTRU
  - Open Source (TrouSerS)



TRUSTED COMPUTING GROUP™

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 make use of the TPM

TRUSTED COMPUTING GROUP™

Implementation Status

- Trusted Platform Modules (TPM) based on 1.1b and 1.2 specifications available from multiple vendors
  - Atmel, Broadcom, Infineon, National Semiconductor
- Compliant PC platforms shipping now
  - IBM ThinkPad notebooks, NetVista desktops and eServer xSeries 366 servers
  - HP D530 Desktops and many notebooks
  - Dell Latitude D410, D610 and D810
  - Intel D865GRH motherboard
  - TPM1.2-based are announced
- Application support by multiple ISV's
  - Existing familiar applications are using TCG/TPM through standard cryptographic APIs like MS-CAPI and PKCS#11
  - RSA* Secure ID, Checkpoint VPN, VeriSign PTA

TRUSTED COMPUTING GROUP™

TPM and Smart Cards

From competition to cooperation

TCG Position

How do TPMs compare with smart cards?

The TPM is a fixed token that can be used to enhance user authentication, data, communications, and/or platform security.

A smart card is a portable token traditionally used to provide more secure authentication for a specific user across multiple systems.

Both technologies can have a role in design of more secure computing environments.

TRUSTED COMPUTING GROUP™

TPM vs. Smart Card

- Similar hardware capabilities
  - Micro controllers
  - RAM, ROM, Flash
- Common cryptographic services
  - Asymmetric cryptography
  - Hash functions
- Comparable tamper resistance
  - EAL3+ to EAL5
- Specialized close firmware vs. open multi-purpose platform
  - Integrity measures reporting
  - Unique Endorsement Key
  - Locality
- Fixed vs. removable

TRUSTED COMPUTING GROUP™

Other Opinion

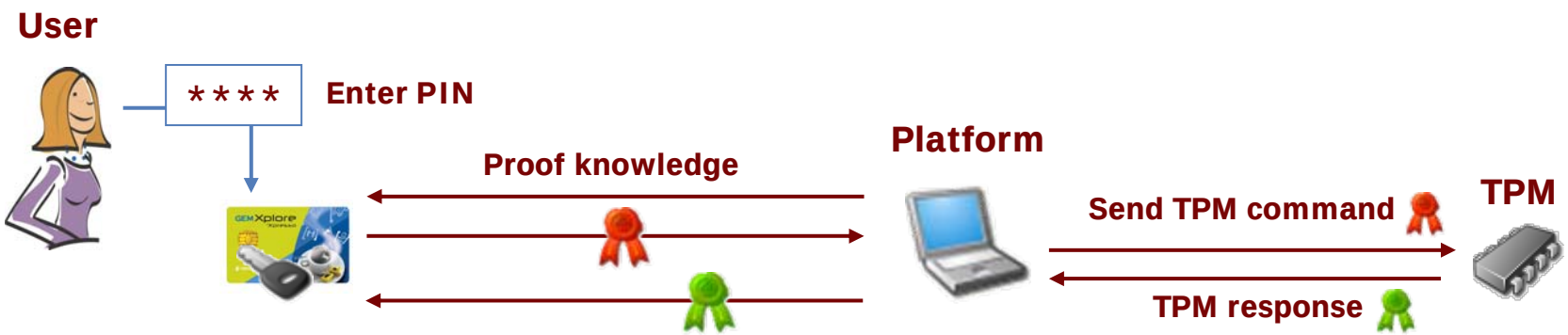
"It can be seen that smart card-based user authentication and TPM-based machine authentication are complementary, rather than competing, technologies." (Dell)

User/Machine Authentication Scenario	Smart Card	TPM
User ID for VPN access		
User ID for domain logon		
User ID for building access		
User ID for secured email		
Platform ID for VPN access		
Platform ID for domain access		
Platform ID for attestation		

TRUSTED COMPUTING GROUP™

A First Step Toward Cooperation

- The TPM user must be authorized before using TPM-protected resources
- User authentication is based on the proof of knowledge a a secret shared between the user and the TPM
- This methods raises security concerns
- A smart card can be used to perform user authentication without exposition the Authorization Data



Other Areas of Cooperation

- Does one security device fit all?
  - Same device for platform and user secrets?
- Separate credentials
  - User credential portability
  - User administration simplification
  - Protection level adequacy
  - User privacy
- Leverage from corporate deployments
  - Logical access to computers
  - Physical access control badges too
- Toward a smartcard-and-TPM cooperative model

TRUSTED COMPUTING GROUP™

TCG Information

- For information on TCG membership and programs

  TCG Administration

  5440 SW Westgate Dr., Suite 217

  Portland, OR 9722

  PH: 503.291.2562 FX: 503.297.1090

  admin@trustedcomputinggroup.org

  www.trustedcomputinggroup.org

- For technical information & specification questions

  techquestions@trustedcomputinggroup.org

TRUSTED COMPUTING GROUP™

TRUSTED COMPUTING GROUP™

Questions