Trusted Computing Group (TCG) and the TPM 1.2 Specification

Nancy Sumrall
Intel Corporation - Safer Computing Initiatives Manager
Desktop Platforms Group

Manny Novoa
Hewlett Packard – Principal Member, Technical Staff
Personal Systems Group

intel
Intel Developer Forum

Safer Computing Track – Fall IDF

Tuesday

- LT Overview
  SCMS-16
- TCG & TPM v1.2
  SCMS-17
- LT Architecture
  SCMS-18
- Tech Showcase
  Every Day
  Birds of a Feather Lunches
  Tuesday & Wednesday

Wednesday

- Privacy Method for Assuring Trust
  SCMS-19
- Opt-In Strategy
  SCMS-156
- Trusted Mobile KB Controller
  SCMS-24
- Software for LT
  SCMS-20
- Fundamentals of NGSCB
  SCMS-21
- Migrating Apps to NGSCB
  SCMS-22

Thursday

- TPM Recovery
  SCMS-25
- TCG Credentials
  SCMS-157
- TPM Mfg & Testing
  SCMS-180

= Overview
= Medium Technical
= Highly Technical

Objectives

After this class, you will understand:

- Structure of the Trusted Computing Group (TCG)
- TCG policies regarding TCG specifications
- TPM 1.2 Feature Set and definitions
- TCG Next Steps

Agenda

- Trusted Computing Group Organization
- TCG Policy Statements
- TCG Support and Management Services
- TPM 1.2 Feature Set
- Summary
- Next Steps

TCG Mission

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

TCG Structure

- TCG is incorporated as a not-for-profit corporation, with international membership
  - Offers multiple membership levels
    - Promoters, Contributors, and Adopters
  - Board of directors
    - Promoters and elected Contributors
  - Typical not-for-profit bylaws
  - Provides a reciprocal RAND patent licensing policy
  - Multiple working groups

Current TCG Membership

- **Promoters:**
  - **AMD*, Hewlett Packard*, IBM*, Intel*, Microsoft*, initially**
  - **Additional promoters will be added**
- **Contributors:**
  - **ATi Technologies*, Atmel*, Broadcom Corporation*, Comodo*, Fujitsu Limited*, Gemplus*, Infineon*, Legend Limited Group*, National Semiconductor*, Nokia*, NTRU Cryptosystems, Inc.*, NVIDIA*, Phoenix*, Philips*, Rainbow Technologies*, Seagate*, Shang Hai Wellhope Information*, Sony*, Standard Microsystems*, STMicroelectronics*, Texas Instruments*, Utimaco Software AG*, VeriSign Inc.*, Wave Systems***
- **Adopters:**
  - **Ali Corporation*. Fujitsu-Siemens Computers*, M-Systems*, Silicon Integrated Systems*, Softex***
- **A number of additional companies have expressed interest and intent to join**

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

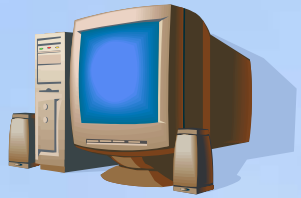
TCPA and TCG

- TCG has adopted published TCPA specifications as a starting point
- TCPA has acknowledged TCG as the industry standard organization for evolving these specifications
- TCPA work groups have ceased operation
- TCG work groups have commenced operation
- TCPA Members have been invited to join TCG by the TCG Board and by the TCPA Steering Committee

Motivations for TCG

- Name change distinguishes TCG as different from TCPA
- Incorporation enables structural improvements that will promote accelerated specification development
  - Governance model similar to other standards orgs
  - Broader platform scope– PCs, servers, PDAs, mobile phones
  - Broader software scope – TSS (TCG Software Stack)
  - Industry-accepted reciprocal RAND IP policy
  - Logo program to enable end-user confidence in products
- Increased resources and broader governance
  - TCG supported by all members
  - More resources will improve development and communications
- Companies must choose to join TCG
  - Agree to bylaws, pay dues, etc…

Technical Workgroups



- Technical Committee
  - TC - Graeme Proudler (HP)
- Operational Work groups
  - Conformance (Common criteria) – Michael Angelo (HP)
  - Trusted Platform Module (TPM) – David Grawrock (Intel)
  - TPM Software Stack (TSS) – Dave Challener (IBM)
  - PC Client Specific Implementation – Monty Wiseman (Intel)
  - PC Server Specific Implementation – Michael Angelo (HP)
  - PDA Specific Implementation – Jonathan Tourzan (Sony)
  - Mobile Phone Implementation – Jukka Parkkinen (Nokia)

- Marketing Work Group
  - MWG – Nancy Sumrall (Intel)
- Additional work groups anticipated

Implementation Status

- Trusted Platform Modules (TPM) based on 1.1b specification available from TPM vendors
  - Atmel
  - Infineon
  - National Semiconductor
- Compliant PC platforms shipping now
  - IBM* ThinkPad notebooks and NetVista desktops
  - HP* D530 desktops
  - More expected soon
- Increasing application support for TPM 1.1b
  - Softex*, Wave Systems*, Verisign*, RSA*, Checkpoint*, Verisign*
- TSS v1.1b and TPM 1.2 currently in IP Review

Note: Modules shown are for test & debug. Actual system implementation may vary.

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

1.1b User and IT Benefits

- **Benefits for today's applications**
  - **More secure storage of files, personally identifiable information and digital secrets**
  - **More secure authentication, e-mail, and communications**
  - **Low-cost authentication**
- **Benefits for new applications**
  - **More secure remote access through a combination of machine and user authentication**
  - **More secure data decryption through confirmation of platform integrity prior to decryption**

TCG Policy Position

Privacy Effect of TCG Specifications

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

TCG Policy Position

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

TCG Policy Position

Backwards Compatibility

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

TCG Support & Management Services

- **VTM* (Vital Technical Marketing)**
  - **TCG's Technical Management and Marketing Company**
  - **Contact information: 503-291-2562**
  - **Email: admin@trustedcomputinggroup.org**
- **PR Works***
  - **Anne Price (TCG PR)**
  - **Contact information: 602-840-6495**
  - **Email: press@trustedcomputinggroup.org**
- **Kavi* - Website management**

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

More Info

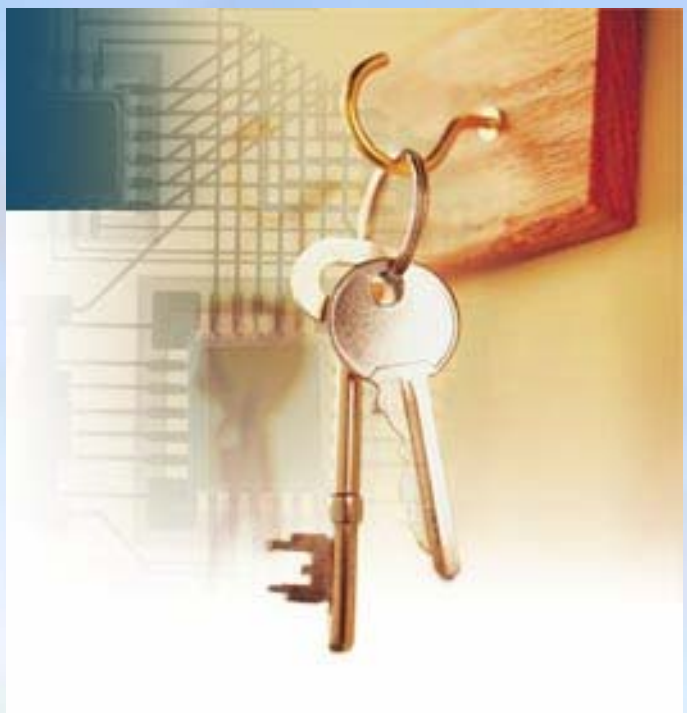
- **TCG site, www.trustedcomputinggroup.org, includes membership list, how to join TCG, PR contacts and specification info**
- **TCG Annual Members Meeting**
  - **November 12-14th, Orlando, FL**
  - **www.trustedcomputinggroup.org/events/**

Trusted Platform Module 1.2 Feature Set

intel

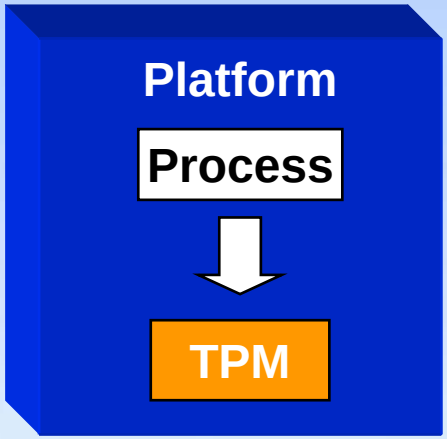
Intel Developer Forum

1.2 Feature Set Overview



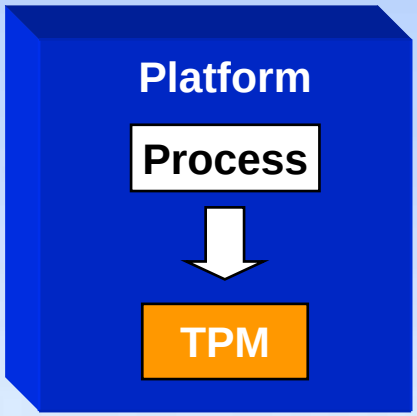
- Locality
  - PCR attributes
  - PCR Selection changes
- NV Storage
- Delegation
- Revoke Trust
- Direct Anonymous Attestation
- Infrastructure Enhancements
  - Monotonic counter
  - Transport Protection
  - Tick counting

Locality



- Assuming the following
  - A trusted process on a platform
  - The process is trusted to always perform properly
  - The process is not related to the boot of the platform
  - The process may come and go
  - The process may perform measurements
  - The process may only be local to the platform
- The trusted process wants to communicate with the TPM
  - Indicate that process is running
  - Control aspects of measurement and operation of the TPM

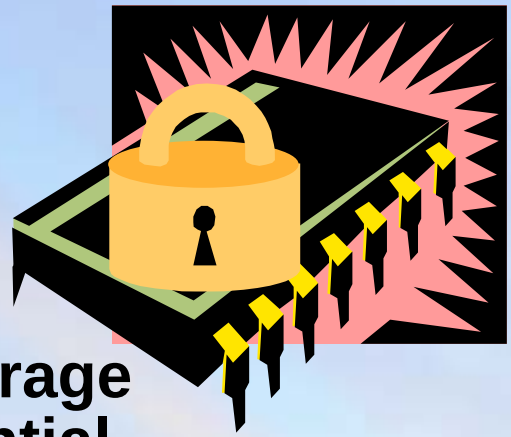
Locality Details



- The trusted process modifies the TPM command transport
  - Indicate that the command comes from only the trusted process
  - Modifier is platform and interface specific
  - TPM internally propagates the modifier for the single command
- TPM provides 4 locality modifiers
- PCR registers now have attributes
  - Extend, read and use can be under control of local process
- New command TPM_PCRReset
  - Only issued by trusted process
  - Only directed to PCR registers that allow reset

NV Storage

- The TPM has NV storage in use for V1.1
  - EK, SRK etc.
  - DIR
- V1.2 was going to add additional requirements
  - More DIR, Bit commands
- Request was made to provide a storage area for the EK and Platform credential
- Many of the NV areas would not be in use all the time (DIR for locality)
- Definition of NV areas are under control TPM Owner.



NV Details

- TPM Owner (or physical presence) authorizes the allocation of a chunk of NV storage
  - Min size is 20 bytes, equating to deprecated DIR register
  - Max size is set by TPM manufacturer
- Rich set of control attributes
  - Authorization to read and or write
  - PCR restrictions on read and or write
  - Locality on read and or write
  - Special read and write restrictions

Delegation

- **A mechanism to allow the TPM Owner to specify other entities or processes that control the TPM**
  - **Delegation done at ordinal granularity**
  - **TPM Owner can delegate right to delegate**
- **Delegations grouped into “families”**
  - The size of the family table allows up to sixteen (16) separate families.
- **Delegations can be stored external to TPM**

RevokeTrust

- RevokeTrust command added
  - Two step process
    - Create authorization value during GenerateEK
    - Present authorization value for RevokeTrust
  - RevokeTrust invalidates the EK and all other key material
  - Somehow need to recreate the endorsement and platform credentials
    - Platform owner needs to communicate with entity willing to issue endorsement and platform credential
- Entity that causes creation of EK needs to store and distribute RevokeTrust authorization value

Direct Anonymous Attestation

- Direct Anonymous Attestation (DAA) provides additional mechanism to prove the validity of an AIK
- Provides alternative to TTP (Trusted Third Party) for AIK Credential
- Based on Zero Knowledge Protocol

Attend SCMS19 on "Privacy Method for Assuring Trust" for more information on DAA

TPM 1.2 Status

- TPM 1.2 Specification entered IP review on August 26, 2003
- Projected spec publication Q4 2003
- Products based on specification expected in 2004
- TCG Software Stack (TSS) V1.1 officially announced on 9/16/03…here at IDF!
- TCG Software Stack (TSS) v1.2 spec work has begun

Summary

- 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
- TPM 1.2 Specification release targeted for Q4 2003

Next Steps

HW Developers	• **Comprehend TPM 1.2 capabilities and roadmap into future product plans**
SW Developers	• **Comprehend TPM 1.2 capabilities and roadmap into future product plans**
IT	• **Ask for and reflect TPM 1.2 back to your vendors**
All	• **Join TCG** https://www.trustedcomputinggroup.org/join/

Acronyms

Acronym	Description
AIK	Anonymous Identity Key. Generated by the TPM on request by the user to represent an pseudo-anonymous identity that is attested to by a credential chain.
DAA	Direct Anonymous Attestation (based on Zero Knowledge Proof)
DIR	Data Integrity Register.
EK	Endorsement Key.
PCR	Platform Configuration Registers.
TPM	Trusted Platform Module as defined by the Trusted Computing Group (TCG) www.trustedcomputinggroup.org
TSS	TCG Software Stack as defined by the Trusted Computing Group (TCG) www.trustedcomputinggroup.org

Thank you for attending.

Please fill out the Session Evaluation Form.