TCG Overview

January 25, 2005

Nicholas Szeto
TCG Board Member, Sony
Contents

• Introduction & Overview
• Technical Concepts
• TCG and CELF
• References
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
  - 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

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

### Adopters
- BigFix, Inc.
- Citrix Systems, Inc
- Enterasys Networks
- Foundry Networks Inc.
- Foundstone, Inc.
- Gateway
- Industrial Technology Research Institute
- Interdigital Communications
- Latis Networks, Inc.
- MCI
- Nevis Networks, USA
- PC Guardian Technologies
- Sana Security
- Senforce Technologies, Inc
- Silicon Integrated Systems Corp.
- Silicon Storage Technology, Inc.
- Softex, Inc.
- Telemidic Co. Ltd.
- Toshiba Corporation
- TrioCipher, Inc.
- ULI Electronics Inc.

### Contributors
- Agere Systems
- ARM
- ATI Technologies Inc.
- Atmel
- AuthenTec, Inc.
- AVAYA
- Broadcom Corporation
- Certicom Corp.
- Comodo
- Dell, Inc.
- Endforce, Inc.
- Ericsson Mobile Platforms AB
- Extreme Networks
- France Telecom Group
- Freescale Semiconductor
- Fujitsu Limited
- Fujitsu Siemens Computers
- Funk Software, Inc.
- Gemplus
- Giesecke & Devrient
- Hitachi, Ltd.
- Infineon
- InfoExpress, Inc.
- iPass
- Juniper Networks
- Lenovo Holdings Limited
- Lexmark International
- M-Systems Flash Disk Pioneers
- MCI Nevis Networks, USA
- Microsoft
- Sony Corporation
- Sun Microsystems, Inc.

### Contributors
- Meetinghouse Data Communications
- Motorola Inc.
- National Semiconductor
- nCipher
- Network Associates
- Nokia
- NTRU Cryptosystems, Inc.
- NVIDIA
- OSA Technologies, Inc
- Philips
- Phoenix
- Pointsec Mobile Technologies
- Renesas Technology Corp.
- RSA Security, Inc.
- SafeNet, Inc.
- Samsung Electronics Co.
- SCM Microsystems, Inc.
- Seagate Technology
- SignaCert, Inc.
- Sinosun Technology Co., Ltd.
- Standard Microsystems Corporation
- STMicroelectronics
- Sygate Technologies, Inc.
- Symantec
- Symbian Ltd
- Synaptics Inc.
- Texas Instruments
- Transmeta Corporation
- Trend Micro
- Utimaco Safeware AG
- VeriSign, Inc.
- Vernier Networks
- VIA Technologies, Inc.
- Vodafone Group Services LTD
- Wave Systems
- Zone Labs, Inc.
Product Implementations

- Trusted Platform Modules (TPM) available from multiple vendors
  - Atmel*, Broadcom*, Infineon*, National Semiconductor*, SMSC*, ST Microelectronics*
- 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* Lifebook S7000, E8000, NAH Notebooks, FMV-E625 Desktop
  - More expected soon
- TCG Solutions
  - M-Systems*
  - NTRU*
  - Softex* (Omni Pass and Theft Guard)
  - Utimaco* (SafeGuard)
  - Verisign* (Personal Trust Agent)
  - Wave Systems* (Embassy Trust Suites)
  - Existing familiar applications are using TCG/TPM through standard cryptographic APIs like MS-CAPI and PKCS #11

* Other names and brands may be claimed as the property of others.
TCG Technical Concepts
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
The Trusted Platform Module

A silicon chip that performs functions, including:

- Storing platform status information
- Hashing files using SHA-1
- Generating and storing private keys
- Creating digital signatures
- Anchoring chain of trust for keys, digital certificates and other credentials
Basic TPM Functions

Diagram Revision: 1.1
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
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
TCG and CELF
Possible TCG Collaboration

• TCG has Liaison Program for approved non-profit organizations to participate in TCG Work Groups

• Potential benefits of CELF working with TCG:
  – Obtain TCG Specifications prior to release
  – Work with TCG to make sure their Specifications and policies accommodate Linux and CE devices
TCG Liaison Program Requirements

- If CELF is interested, compatibility between CELF and Liaison Program would need to be evaluated
- Confidentiality and IP
  - CELF needs to be incorporated and able to agree to the necessary terms
- Goals
  - CELF will need to identify exactly what goals it wishes to achieve in working with TCG
- Participation
  - Individuals will need to agree to participate in TCG Work Groups and make some form of commitment
- Otherwise, companies still have the option to participate individually
- Some overlap already between TCG and CELF companies
References

www.trustedcomputinggroup.org
Acronyms

• AIK – Attestation Identity Key
• DAA – Direct Anonymous Attestation
• DIR – Data Integrity Register
• EK – Endorsement Key
• PCR – Platform Configuration Register
• RTM – Root of Trust for Measurement
• TBB – Trusted Building Block
• TCG – Trusted Computing Group
• TCPA – Trusted Computing Platform Alliance
• TPM – Trusted Platform Module
• TSS – Trusted Software Stack

See also TCG Web site for released Glossary