

Who is TCG ?

- develops and supports
 - open, vendor-neutral industry standards for trusted computing
 - across multiple platform types and
 - operating environments
 - industry advocacy programs (logo, etc.)
- an open organization
 - specification documents are free
 - but participation requires paid membership
- www.trustedcomputinggroup.org
- Goals:
 - “. . . enable open and widely available building blocks and common interface stacks that the industry can broadly adopt across multiple platform types and environments. With these open building blocks, the industry can address a range of security needs without compromising functional integrity, privacy or individual rights.”
- TCG Benefits include:
 - Users will have more secure local data storage and a lower risk of identity theft from both external software attack and physical theft.
 - IT organizations will be able to deploy more secure systems and solutions based on open industry standards.
 - Computer, device, and software suppliers will be able to more quickly develop more secure systems and solutions based on open standards.

What do they want from T13 ?

- to reserve two opcodes and three IDENTIFY words

Why ?

- the objective is to have TCG define the transferred data to be common across all platforms
- to create a placeholder with which to implement trusted computing commands
- a similar effort is occurring now in T10 (04-163r0)

How is this different from CPRM ?

Category	CPRM	TCG
Organization	closed (4 members)	<ul style="list-style-type: none"> • open (currently 72 members), • specifications are free, • paying members may influence design and requirements
Roots	Intel, IBM, Matsushita, Toshiba	<u>many</u> hardware manufacturers, content providers, software providers, system builders
Purpose	content protection	protecting hardware, software, and user-owned and created data from external attack; protect content owned by others
Controlled by	content owner	user and content owner
Processor classes	Intel	Intel, AMD, Sun, ARM, Motorola, Atmel, TransMeta, others
OS classes	Microsoft	Microsoft, trusted Linux, Sun, others
Hardware classes	(originally) removeable media, then ATA disks also	storage (all types), keyboard, mice, display, cables, compact flash, PCs, servers, PDAs, phones, networking, TV, wireless, (everything)
License agent	License Management International	TBD
Offline content access and authentication	(not addressed)	TBD
Disaster recovery (keys and data)	(difficult at best)	TBD, varies with hardware type
Encryption	one method	several methods

References:

www.trustedcomputinggroup.org

Teleconference T10/TCG open to all:

... to discuss the proposed TRUSTED COMPUTING IN/OUT commands proposal.

Monday, July 19, 2004,
02:00pm EDT, 1:00pm CDT, 12:00pm MDT, 11:00am PDT

dial-in 866 279 4742
passcode 255 5580

- o Introductions
- o New agenda items
- o Status from T10 CAP meeting and the TCG SSWG
- o Definition of Trusted Commands
 - This will be a technical meeting where we start working on the TRUSTED COMPUTING IN/OUT commands.

TCG Members as of June 17, 2004

Promoter

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

Contributor

Agere Systems
ARM
ATI Technologies Inc.
Atmel
AuthenTec, Inc.
Broadcom Corporation
Comodo
Dell, Inc.
Extreme Networks
Fujitsu Limited
Fujitsu Siemens Computers
Funk Software, Inc.
Gemplus
Giesecke & Devrient
Hitachi, Ltd.
Infineon
InfoExpress, Inc.
Juniper Networks
Legend Limited Group
Meetinghouse Data Communications
Motorola Inc.
National Semiconductor
nCipher
Network Associates
Nokia
NTRU Cryptosystems, Inc.
NVIDIA
Philips
Phoenix

Renesas Technology Corp.
RSA Security, Inc.
SafeNet, Inc.
Samsung Electronics Co.
SCM Microsystems, Inc.
Seagate Technology
Shang Hai Wellhope Information
Silicon Storage Technology, Inc.
Standard Microsystems Corporation
STMicroelectronics
Sygate Technologies, Inc.
Symantec
Synaptics Inc.
Texas Instruments
Transmeta Corporation
Trend Micro
Utimaco Safeware AG
VeriSign, Inc.
VIA Technologies, Inc.
Vodafone Group Services LTD
Wave Systems
Zone Labs, Inc.

Adopter

Ali Corporation
American Megatrends, Inc.
Enterasys Networks
Foundry Networks Inc.
Foundstone, Inc.
Gateway
Industrial Technology Research Institute
iPass
M-Systems Flash Disk Pioneers
OSA Technologies
Silicon Integrated Systems Corp.
Softex, Inc.
Toshiba Corporation
Winbond Electronics Corporation