Trusted Computing in Action: An Educational Open House

October 18, 2016
Seoul, South Korea
Welcome!

**Trusted Computing in Action: An Educational Open House**
Open to Registered Members and Non-Members

**Grand Ballroom A (Lower Level)**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
</table>
| 8:30am - 9:00am | Welcome and Introduction to Trusted Computing Group  
  Joerg Borchert, TCG President and Chairman & Mark Schiller, TCG Executive Director |
| 9:00am - 9:30am | Introduction to Trusted Computing Concepts and the Trusted Platform Module (TPM) 2.0  
  Trusted Computing Group Experts                                                   |
| 9:30am - 10:30am | Trusted Computing Benefits for Storage  
  Trusted Computing Benefits via Networking  
  The Benefits of Trusted Computing for Embedded, IoT and Automotive Systems  
  Trusted Computing Group Experts                                                   |
| 10:30am - 10:45am | Coffee/Tea & Networking Break (Foyer)                                                      |
| 10:45am - 11:15am | A Survey of Trusted Computing Work and Focus Areas  
  Trusted Computing Group Leadership Team                                           |
| 11:15am - 12:00pm | Keynote Presentation: Korea Cybersecurity Vision and Strategy Overview  
  Jung-Su Song, Director General: Ministry of Science, ICT and Future Planning  
  Introduction by Jing de Jong-Chen, TCG Vice President                           |
| 12:00pm - 12:45pm | Lunch - Grand Ballroom C (Lower Level)                                                   |
| 12:45pm - 2:00pm | Spotlight on TCG Technologies in Use  
  TCG Member Demonstrations                                                        |
Dr. Joerg Borchert
TCG President and Chairman

Joerg Borchert is Vice President of Chip Card & Security ICs at Infineon Technologies North America. He started his career at Siemens AG in 1988 and moved to Siemens Semiconductor which became Infineon Technologies in 1999.

In September 2010, Joerg took over the responsibility for Chip Card and Security for the Americas. Currently, he and his team are involved in semiconductor security solutions for the smart grid and mission critical embedded systems of which, he has contributed to four patent filings.
Board of Directors Update

Joerg Borchert, Infineon Technologies AG
TCG President and Chairman
Anti-Trust Reminder

TCG Bylaws, Section 2.6

• The Members of the Corporation understand that in certain lines of business they may be direct competitors and that it is imperative that they and their representatives act in a manner which does not violate any state, federal or international antitrust laws and regulations.

• Without limiting the generality of the foregoing, the Members of the Corporation acknowledge that the Corporation prohibits any agreement or discussions directed at entering into any agreement on costs, prices, quantity or quality of production levels, methods or channels of distribution, markets, customers or any other topic that may be construed as a violation of antitrust laws. Accordingly, each Member will counsel its representatives on the importance of limiting the scope of their discussions to the topics which relate to the purposes of the Corporation, whether or not such discussions take place during formal meetings, informal gatherings, or otherwise.
Welcome: First Time Attendees

TCG Board of Directors and Committee Chairs would like to welcome the following first-time attendees registered for the Members Meeting:

- Shivaun Albright, HP, Inc
- Arkadiusz Berent, Intel
- Sunhwa Im, Samsung
- Hiroshi Isozaki, Toshiba
- John Kang, Bright Plaza, Inc
- Wonchol Kim, Samsung
- Jaehyun Lee, Samsung
- Seungjae Lee, Samsung
- Dennis Matton, Microsoft
- Jerome Quevremont, Thales Communications & Security
- Igor Sloutsker, Intel
- Michael Velten, Fraunhofer-Institut AISEC
- Ioa-Silviu Vlascean, Huawei
- Marion Vogt, AMOSSYS
- Kerstin Wilde, Infineon Technologies
Welcome: New Members in 2016

Promoter:
- Dell (upgraded from Contributor)
- Huawei Technologies Co. Ltd. (upgraded from Contributor)

Contributor:
- American Express
- Raytheon
- TaoBao China Software Co., Ltd
- VIA Alliance Semiconductor Co., Ltd.

Adopter:
- CoreOS, Inc.
- Micro Focus
- Renesas
- Wibu-Systems
- Unigen DataStorage Corporation
2016 Board of Directors Officers

Dr. Joerg Borchert  
President and Chairman  
Infineon Technologies AG

Jing De Jong-Chen  
Vice President  
Microsoft Corporation

Dr. Claire Vishik  
Secretary  
Intel Corporation

Joe Pennisi  
Treasurer  
Lenovo

Mark Schiller  
Executive Director
2016 Board of Directors

Dean Liberty
AMD

Stacy Cannady
Cisco Systems

Frank Molsberry
Dell

Seigo Kotani, PhD
Fujitsu Limited

Shiva Dasari
Hewlett Packard Enterprise

Boris Balacheff
HP, Inc

Yi Zhang
Huawei Technologies

Dimitrios Pendarakis
IBM

Seth Ross
Juniper Networks, Inc.

Darren Krahn
Google (Contributor Advisor)
Recent Specifications Published

Embedded Systems Work Group

- [PC Client Work Group EFI Protocol Specification Errata Version 0.5](#) (July 2016)
- [TCG Guidance for Securing Resource-Constrained Devices Version 1 Revision 17](#) (August 2016)
- [TCG TPM I2C Interface Specification Family 2.0, Level 00, Revision 1.0](#) (October 2016)
Upcoming Members Meetings

February 2017 Members Meeting
• Dates: February 6-9, 2017
• Location: San Diego Marriott Del Mar, Del Mar, California

June 2017 Members Meeting
• Dates: June 12-15, 2017
• Location: Park Hyatt Hamburg, Hamburg, Germany

October 2017 Annual Members Meeting
• Dates: October 23-26, 2017
• Location: Vancouver Marriott Pinnacle Downtown Hotel, Vancouver, BC
This Week’s Member Meetings

Mark Schiller, Executive Director
Schedule: Tuesday afternoon

2:00pm - 5:00pm
- Junior Ballroom C: Open
- Junior Ballroom B: Certification Program Committee (CPC)
- Topaz (3rd Floor): Marketing
- Junior Ballroom A: DICE Architectures
- Coral (3rd Floor): Embedded Systems
- Grand Ballroom B: Open

6:00pm - 8:00pm
- Seoul Walking Tour
  Tour will depart from the Millennium Seoul Hilton
  Sign Up for the Tour at the Registration Desk
# Schedule: Wednesday

<table>
<thead>
<tr>
<th>Time</th>
<th>Junior Ballroom C</th>
<th>Junior Ballroom B</th>
<th>Topaz (3rd Floor)</th>
<th>Junior Ballroom A</th>
<th>Coral (3rd Floor)</th>
<th>Grand Ballroom B</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00am - 9:00am</td>
<td>TPM Software Stack (TSS)</td>
<td>Storage</td>
<td>Board of Directors</td>
<td>Mobile Platform/TMS</td>
<td>DICE Architectures</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>9:00am - 12:00pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00pm - 1:00pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00pm - 5:00pm</td>
<td>TPM Software Stack (TSS)</td>
<td>Open</td>
<td>Board of Directors</td>
<td>Open</td>
<td>Embedded Systems: Vehicle Services</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>5:15pm - 6:30pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Grand Ballroom A**

- TCG Award Ceremony
  - Cocktail and Appetizer Reception and Award Ceremony
## Schedule: Thursday

<table>
<thead>
<tr>
<th>Time</th>
<th>Junior Ballroom C</th>
<th>Junior Ballroom B</th>
<th>Topaz (3rd Floor)</th>
<th>Junior Ballroom A</th>
<th>Coral (3rd Floor)</th>
<th>Grand Ballroom B</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00am - 9:00am</td>
<td>Trusted Platform Module (TPM)</td>
<td>Open</td>
<td></td>
<td>Virtualized Platform</td>
<td>Embedded Systems: Network Equipment</td>
<td>Storage</td>
</tr>
<tr>
<td>9:00am - 12:00pm</td>
<td></td>
<td></td>
<td>Board of Directors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00pm - 1:00pm</td>
<td></td>
<td></td>
<td></td>
<td>Lunch - Grand Ballroom C (Lower Level)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00pm - 5:00pm</td>
<td>Open</td>
<td>DICE Architectures</td>
<td>Board of Directors</td>
<td>Virtualized Platform</td>
<td>Embedded Systems: Internet of Things</td>
<td>Open</td>
</tr>
</tbody>
</table>
Floor Plan – 3rd Floor

1. AMBER ROOM
2. TOPAZ ROOM
3. CORAL ROOM A+B+C
   3a. CORAL ROOM C
   3b. CORAL ROOM B
   3c. CORAL ROOM A
4. JADE ROOM A+B
   4a. JADE ROOM B
   4b. JADE ROOM A
TCG Representatives

Mark Schiller  
Executive Director

Amanda Parenti  
Associate Executive Director

Stephanie Schultz  
Staff

Paul Lanning  
Staff

Molly Nelson  
Staff

• Have a comment?
• Have a future Member Meeting location to recommend?
• Want to provide feedback to TCG or to its staff?
• Need a piece of paper?

Stop by the registration desk and leave the TCG staff a comment.  
Every comment is important and very much appreciated!
The Trusted Computing Group: Overview

Mark Schiller, Executive Director
Who is TCG? : Mission

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.
Who is TCG?

The Trusted Computing Group (TCG) is an international industry standards group focused on Trusted Computing since its founding in 2003.

- You know us for our technical specs & guidance such as:
  - Trusted Platform Module (TPM 2.0)
  - Self Encrypting Drive (SED)
  - Trusted Network Communications (TNC)
Trusted Computing Group Organization Structure (2016 August)

Board of Directors

- Marketing Work Group
  - Public Relations
  - Events Marketing Support

- Technical Committee
  - Embedded Systems
  - Infrastructure
  - Mobile Platform
  - PC Client
  - Security Evaluation
  - Server
  - Storage
  - Trusted Network Communications (TNC)
  - Trusted Platform Module (TPM)
  - TCG Software Stack (TSS)
  - Virtualized Platform
  - Persistent Memory

- Solutions Work Groups
  - Trusted Mobility Solutions
  - Trusted Multi-tenant Infrastructure
  - Compliance

- Certification Program Committee
- Japan Regional Forum
- Greater China Regional Forum
- Admin

New Work Group

DICE Architectures

*Device Identifier Composition Engine
Trusted Computing Group Organization Structure (2016 August)
Trusted Computing Group Organization Structure (2016 August)
TCG: Membership

Including Commercial, Liaison, Invited Experts and Government participants: 100+ MEMBER ORGANIZATIONS

Promoters

Contributors

Adopters

Current Membership List Available: http://trustedcomputinggroup.org/membership/members/companies/
Trusted Computing Group Membership
Available Levels of Membership**

- **Contributor:**
  Highest Value/All Benefits**
  $15,000/year

- **Associate:**
  Solution Workgroups
  $10,000/year

- **Adopter:**
  RAND Obligation & Compliance Program Value
  $7,500/year

*Small Adopter level available for entities of less than 100 employees

**Note: Promoter Membership level with Director privileges by Board invitation only
Recommended: Contributor Level Membership

Contribute to Specs &

Vote to ensure your needs are met
Recommended: Contributor Level Membership

Early Specification Access enabling…

…Leadership Product Development
Recommended: Contributor Level Membership

Full Community Participation
(incl. Japan/China Regional Forums)

& Maximized Learning via
Workgroups and Solutions Teams
Recommended: Contributor Level Membership

Demonstrate Thought Leadership to Customers…

…Assume TCG Leadership Roles
Baseline Benefits (all membership levels):

– RAND Licensing Benefits/Obligation from/to Members

– Participation in Marketing Programs (such as RSA), PR and events

– Compliance/Certification Program Participation
Marketing Program Benefits

• TCG technology product demos at Tradeshows
• Press Release Participation
• PR and Media Opportunities
• Speaking Opportunities
Contributor Benefits Recap:

- Contribute to Specs and Vote to ensure your needs are met
- Early Access to Specs for product work
- Full Community Participation and Maximized Learning Opportunities (including Greater China and Japan Regional Forums)
- Demonstrate Thought Leadership to your Customers (including access to formal TCG Workgroup leadership roles)
TCG Membership Benefits At-a-Glance

<table>
<thead>
<tr>
<th>TCG Membership Levels</th>
<th>Contributor</th>
<th>Associate</th>
<th>Adopter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Dues (USD)</td>
<td>$15,000</td>
<td>$16,000</td>
<td>$7,500*</td>
</tr>
</tbody>
</table>

**MEMBERSHIP BENEFITS**

- **Voting Rights**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Chairpersons Candidacy (for Workgroups)**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Nominate a Representative as a Contributor Advisor to the Board**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Participate in TCG Work Groups and Committees**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Number of Participants**
  - Contributor: Unlimited
  - Associate: Unlimited
  - Adopter: Unlimited

- **Intellectual Property**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Members Meetings (3 per year)**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Attend Interoperability & Compliance Plugfests**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Certification Program**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Work-in-Progress Specifications**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Work-in-Progress Best Practices, Reference Documents**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Conduct Review and/or Comment on Specs & Reference Documents**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Supporting Materials of Specs & Reference Documents**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Industry/Government Technical Experts Via Workgroups**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Participate in the Greater China and Japan Regional Forums**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Published Specifications**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Marketing Programs**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Access to Members-only & Public Web site**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Subscription to email lists**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

- **Listed as a Member on TCG Web site**
  - Contributor: Full Participation
  - Associate: Limited Participation
  - Adopter: Limited Participation

*Additional Benefits for Organizations with less than 100 Employees: $2,000

RAND Licensing Benefits/Obligation from/to All Members

- Full Participation
- Limited Participation

*For companies with less than 100 employees.
Associate Benefits
• Significant Baseline Benefits with:
  – Partial Community & Meeting Participation
    • Currently for Cloud and Mobile Solutions
      (Additional Solutions Groups expected)
    • Plenary Sessions General Meeting Participation

Adopter Benefits
• Significant Baseline Benefits with:
  – Meeting Participation (Limited to Plenary Sessions)