Addressing Mobile Security through Industry Standards

Janne Uusilehto,

Chairman, Mobile Phone Work Group

3GSM World Congress

February 16, 2006 - Barcelona, Spain

Agenda

1. Why mobile platforms need standards-based security
2. Who is Trusted Computing Group
3. Trusted Computing Group's mobile security initiative
4. Summary and questions

TRUSTED COMPUTING GROUP™

Why Add Trust to the Mobile Platform?

- Mobile phones can be used for computing tasks, Internet access, e-commerce, content download etc.
- Increasing variety and popularity of services require more trust and security in the device, service, content and network
- Convergence of Internet and mobile domains requires a common trust approach
- Malware, spam and physical theft of devices can be a threat

Security is of utmost importance yet has been approached in a non-standardized manner

TRUSTED COMPUTING GROUP™

Time is right for mobile security standardization

"IDC agrees that there is unlikely to be a major outbreak until the start of **2008**"

"Despite this intense vendor - and media-driven speculation - the necessary conditions required for viruses or worms to pose a real rapidly spreading threat to more than 30 percent of enterprise mobile devices will not converge until year-end **2007**" (Gartner)

"A lot of this (cell phone attacks) is **hyped** to create a market that doesn't exist," said Neil MacDonald, group vice president and research director at Gartner Inc. "The market will exist eventually because the devices are becoming more powerful, but the **threat today is minimal and overblown**."

TRUSTED COMPUTING GROUP™

Source: Eweek.com. News.com

Why Standardize Security: Benefits to the **Industry**

- Allows the industry to pool scarce resource of top experts, prioritize key issues, and enable wider peer review for flaws
- Creates a broader base of customers for the supply chain, eventually lowering costs and speeding time to market
- Prevents fragmentation, enhances interoperability and reduce R&D costs

TRUSTED COMPUTING GROUP™

Why Standardize Security: Benefits to the **Users**

- Increases confidence that their devices will work as intended
- Prevents virtual and physical theft of content and data and unauthorized use
- Lowers cost and speeds adoption of new systems, meaning users get more features and better security at lower costs

TRUSTED COMPUTING GROUP™

Approaching Standards

- No standards body was addressing the overall issue of mobile device security and trust
- Industry began working together via the Trusted Computing Group
  - Successful already in driving security standards
  - Work can be leveraged, shortening standards and product development cycles
- Organization has 130+ members and a dedicated Mobile Phone Work Group
  - Mobile group members include Authentec, Ericsson, France Telecom, Infineon, Intel, Lenovo, Motorola, Nokia, Philips, Samsung, Sony, ST Microelectronics, Texas Instruments, VeriSign, Vodaphone, Wave Systems, and many others

TRUSTED COMPUTING GROUP™

Agenda

1. Why mobile platforms need standards-based security
2. Who is Trusted Computing Group
3. Trusted Computing Group's mobile security initiative
4. Summary and questions

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 Membership (December 2005)

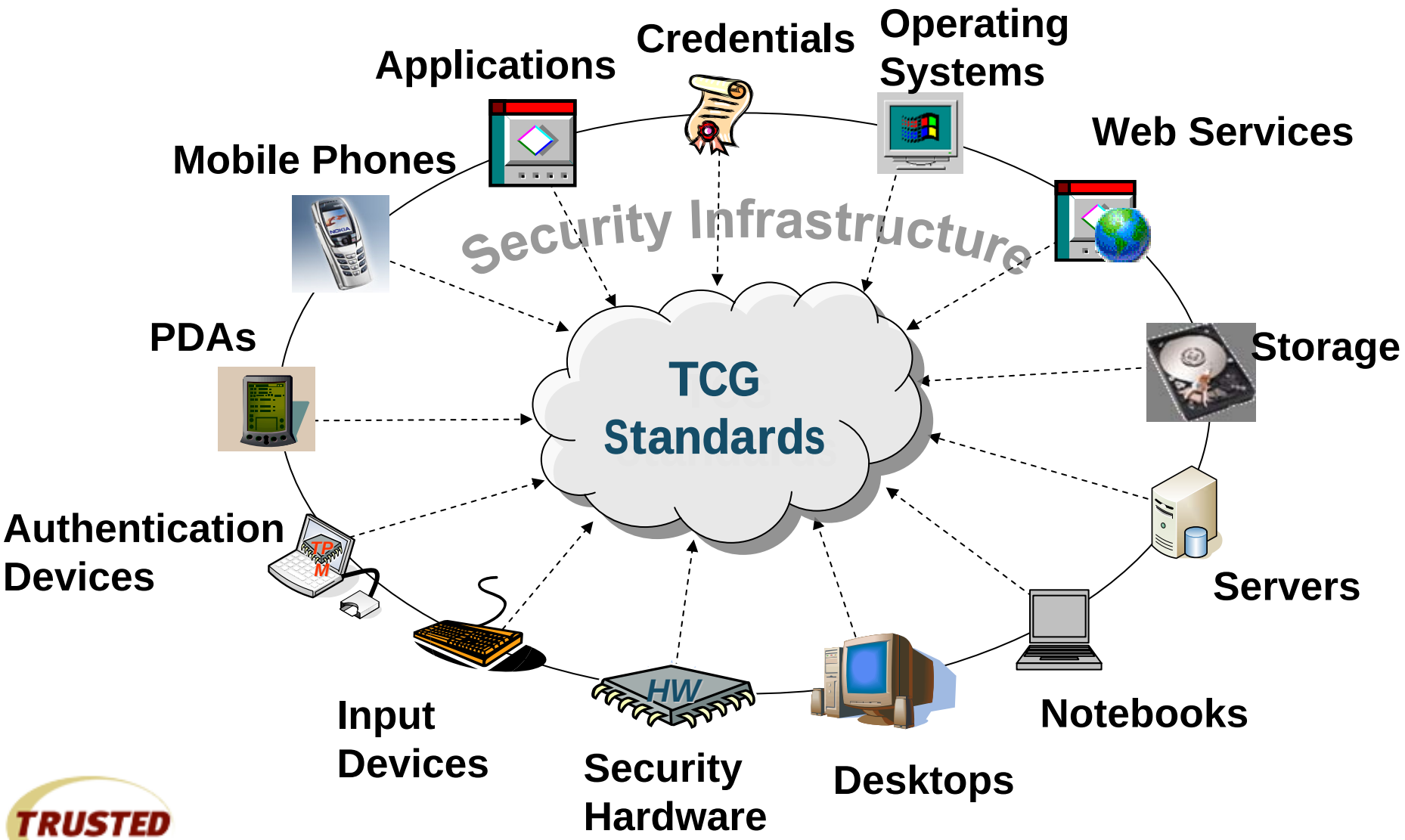
- **131** Total Member companies
- 6 Promoter members
- 77 Contributor members
- 48 Adopter members

Promoters

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

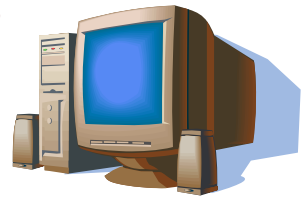
TRUSTED COMPUTING GROUP™

Trusted Computing: The "BIG" Picture

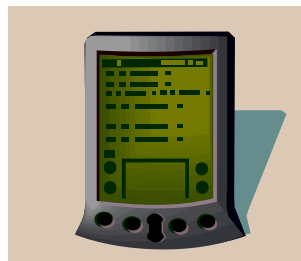


TRUSTED COMPUTING GROUP™

Technical Workgroups



- Technical Committee
- Technical Work groups
  - Trusted Platform Module (TPM)
  - TPM Software Stack (TSS)
  - PC Specific Implementation
  - Peripheral Implementation
  - Server Specific Implementation
  - Storage Systems Implementation
  - **Mobile Phone Work Group**
  - Conformance (Common Criteria)
  - Infrastructure
  - Trusted Network Connect
- Marketing Work Group



TRUSTED COMPUTING GROUP™

The Trusted Computing Solution

- Enable a trusted environment
  - Dynamic platform communication with the network
  - Protection of data
  - Remote communication
- Enable a platform to prove that a given software environment is a protected environment
- Secrets are protected until the correct software environment exists
  - Only then are secrets released

TRUSTED COMPUTING GROUP™

Agenda

1. Why mobile platforms need standards-based security
2. Who is Trusted Computing Group
3. Trusted Computing Group's mobile security initiative
4. Summary and questions

TRUSTED COMPUTING GROUP™

TCG's Mobile Phone Work Group (MPWG)

- The group works on the extension of Trusted Computing concepts and benefits to mobile devices
- The group builds on existing specifications and concepts to **address specific characteristics of mobile devices**
  - Ex. connectivity and limited capability
- The technical work will continue to enable different business models of the mobile industry

TRUSTED COMPUTING GROUP™

Threats for mobile environment

- Viruses and worms
- Denial of service
- Att
- Ma
- To
  pe
- Tra
  ma
- Violation of privacy: ID applications, personal information
- Loosing money: e-cash, unauthorized phone calls, etc.
- st
- st own
- rmation
- tection, copying electronic tickets, etc.
- Device is portable – easy to steal

TCG addresses threats from device architecture level

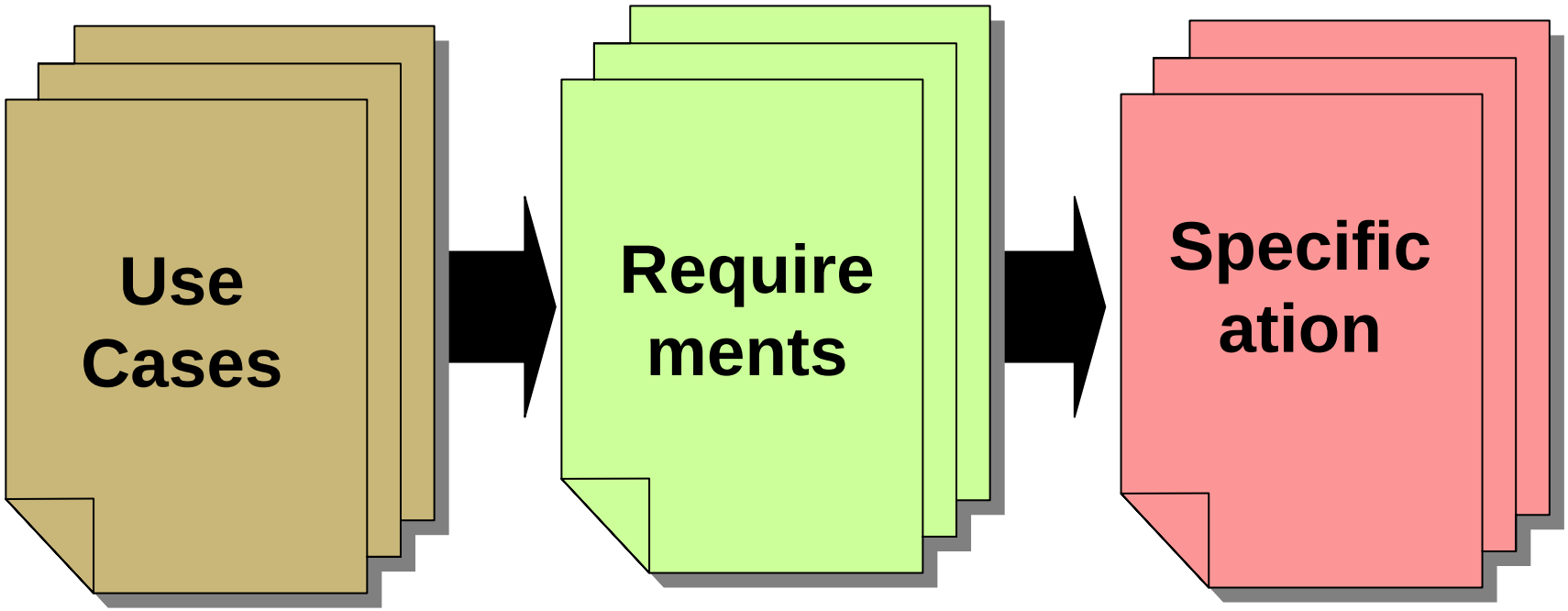
TRUSTED COMPUTING GROUP™

TCG Deliverables

- Step 1: Use Cases
  - Consolidated collection of usage scenarios that are describing the usage of mobile devices in trusted environment, concentrated on exploring added value for mobile devices.
  - Get industry input, additional participation, create support for industry working together to address security issues
- Step 2: Requirements
  - List of high-level requirements (functional and non-functional) related to the adoption of trusted computing platform for mobile devices.
- Step 3: Mobile Security Specification
  - Extensions and modifications required for TCG main specification to be adopted for mobile devices.

TRUSTED COMPUTING GROUP™

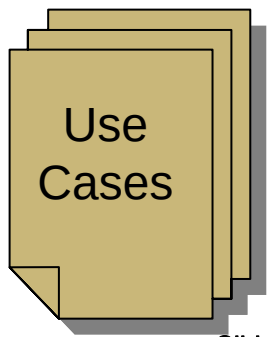
Working Group Process Steps



TRUSTED COMPUTING GROUP™

Use Cases

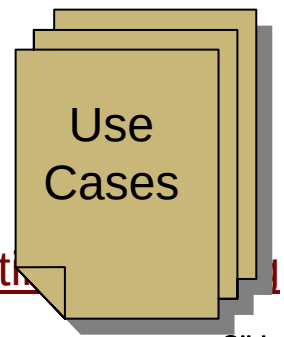
- TCG Use Cases for mobile security intend to outline the application of TCG techniques and specifications to mobile devices
- They have been written to:
  - Guide subsequent technical specification work within the Mobile Phone Working Group
  - Ensure that the work of Mobile Phone Working Group meets real industry needs



TRUSTED COMPUTING GROUP™

Use Cases

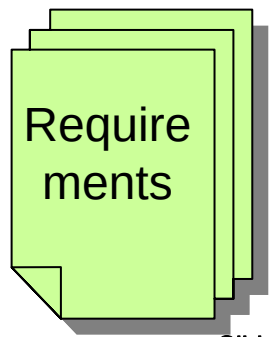
- Platform Integrity
- Device Authentication
- Robust DRM implementation
- SIM lock/Device personalization
- Secure Software download
- Secure channel between device and UICC
- Mobile Ticketing
- Mobile Payment
- Software Use
- Prove Platform and Application integrity to end users
- User Data protection and privacy



Use cases available for download @ www.trustedcomput

Requirements

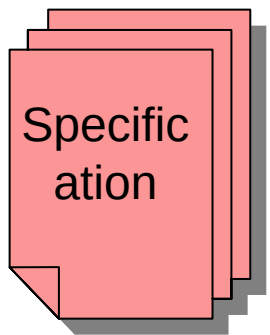
- Technical prerequisites deriving from the real-life use cases
- Baseline for specification, illustrates the conceptual framework
- Examples of planned requirements:
  - Locally verified boot
  - Platform verification authority
  - Secure storage
  - Portability, migration
  - Owner-installed applications
  - Etc.



TRUSTED COMPUTING GROUP™

Specification

- Builds on use cases and requirements
- Ready for product implementation during 1H2006
- Will be posted on www.trustedcomputinggroup.org/Mobile



TRUSTED COMPUTING GROUP™

Agenda

1. Why mobile platforms need standards-based security
2. Who is Trusted Computing Group
3. Trusted Computing Group's mobile security initiative
4. Summary and questions

TRUSTED COMPUTING GROUP™

Summary

- Timing is right for addressing mobile security issues
- Standardized approach brings numerous benefits
- TCG is an industry-wide specification body specializing in security
- TCG MPWG consists of security experts in wireless companies
- TCG MPWG is creating a mobile phone security specification
- Specification ready for product implementation during 1H2006

TRUSTED COMPUTING GROUP™

Thank you.

Questions ?