



TCG activities on Mobile Security standardization



**Mr. Janne Uusilehto, Nokia
Chairman, TCG MPWG
Embedded Security Seminar
September 12, 2005**

■ Trusted Computing Definition

*Hardware and Software
behave as designed*

Why TCG works on mobile security

- Mobile phones becoming more sophisticated enable them to be used for basic computing tasks
- Increasing variety and popularity of mobile data services require more trust and security in the device, service, content and network
- Convergence of Internet and mobile domains require common trust approach

Scope of Mobile Phone Work Group

- The group will work on the **adoption of TCG concept for mobile devices** to enable different business models in market environment of open terminal platform
- The group will enhance TCG as needed to **address specific features of mobile devices** like their connectivity and limited capability

Threats for mobile environment

- Viruses and worms
- Denial of Service
- Attacks by others
- Malware
- Trojans
- Data leakage
- Theft
- Violation of privacy. ID applications, personal information
- Loosing money: e-cash, unauthorized phone calls, etc.
- Information leakage, copying electronic tickets, etc.
- Device is portable – easy to steal

TCG addresses threats from device architecture level

Time is right for mobile security standardization

"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

enterprise

year or

"IDC
major

WDSGlobal handles data support calls for Hewlett-Packard, Nokia, Orange, Sony Ericsson and T-Mobile. In the last quarter, it received just 10 end-user enquiries about smart phone viruses out of the 275,000 calls it fielded--equating to 0.0036 percent of all calls.

"A lot of this (cell phone attacks) is hyped to create a n't exist," said group vice search director The market ally because the ning more e threat today verblown."

■ TCG Mobile Deliverables

■ 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.

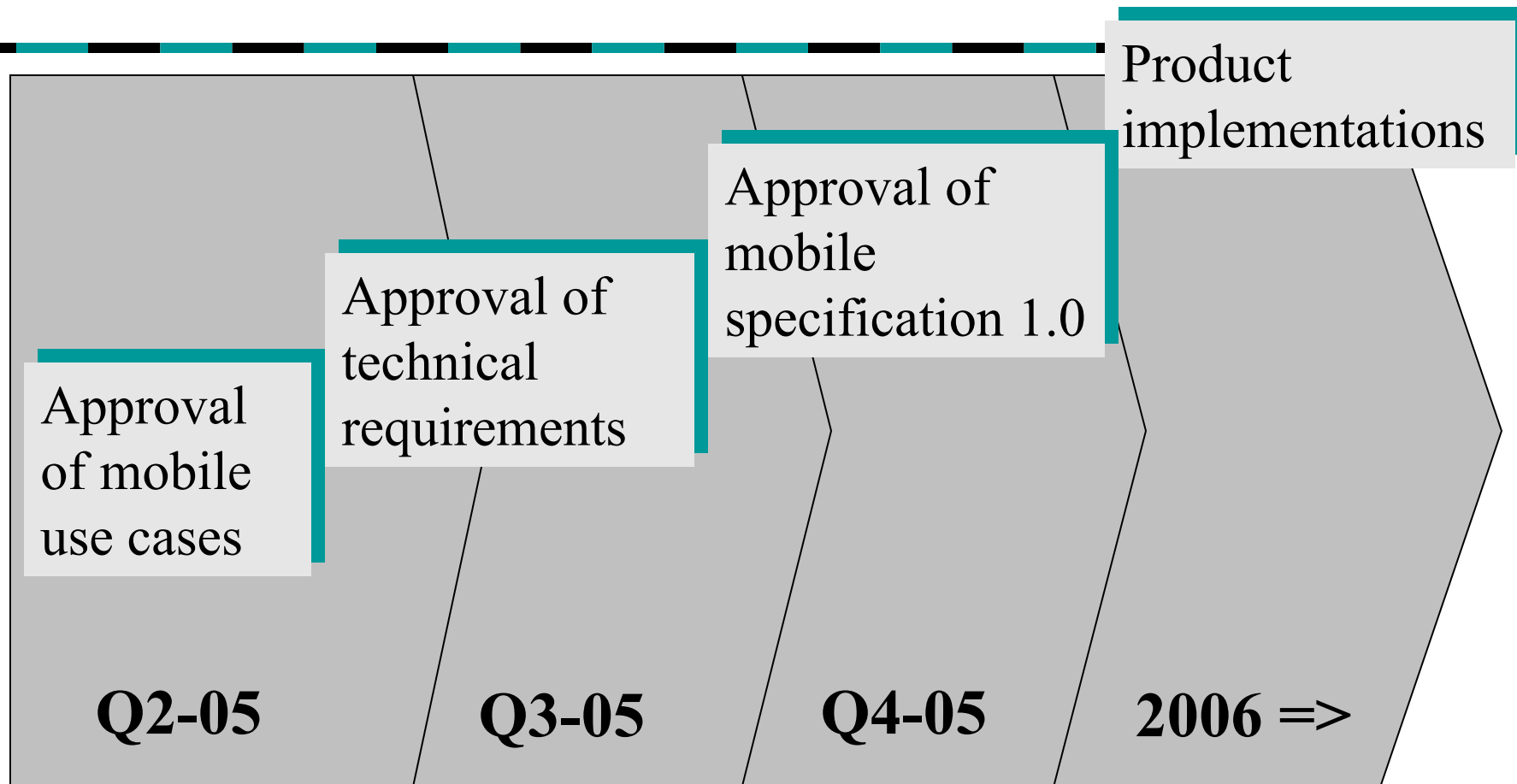
■ Requirements:

- List of high-level requirements (functional and non-functional) related to the adoption of trusted computing platform for mobile devices.

■ Mobile specific specifications:

- Proposal of extensions and modifications required for TCG main specification to be adopted for mobile devices.

TCG Mobile Security roadmap



Benefits of standardized security 1/2

- Prevents fragmentation, enhancing interoperability and reducing R&D costs.
- Allows wider peer review for flaws, hence affecting a higher quality end result
- Reduces the risks, and increases confidence in manufactureres supporting the required functionality
- Increases confidence in consumer and business users in trusting their device to work as intended

Benefits of standardized security 2/2

- Standardized interfaces allow terminal manufacturers to expand their supplier base
- Standardized interfaces allow hardware component providers to expand their customer base
- Allows the industry to pool the scarce resource of top experts
- Allows for the industry to come together and collectively decide priority items



TCG Mobile Security Use Cases



Introduction

- These Use Cases 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

■ Use Case classification

- **Substantive** use cases describe functionality that *is likely to be required* of all Devices implemented according to the technical specifications (Use Case 1)
- **Application specific** use cases describe functionality that *may not be required* of all Devices implemented according to the technical specifications (Use Cases 2-6)

■ 1. Platform Integrity

- Ensure the **use of authorized** operating system(s) and hardware
- Platform integrity maintenance means that the platform HW and principal elements of the platform SW are **in the state intended** by the Device Manufacturer.

■ 2. Device Authentication

- Assists a Service or Network Provider in **end user authentication** when the device identity has been bound to an end user identity
- Prove the **identity of the device** itself
- Device should be able to store and protect all identities
- Device should use the appropriate identities depending on the context

3. Robust DRM Implementation

- By employing **trusted computing** principles, techniques and specifications, device manufacturers can establish a robust DRM implementation
- This use case proposes a **hardened implementation** of the DRM specification

4. SIMLock/Device Personalisation

- Ensure that a mobile **device remains locked** to a particular network until it is unlocked in an authorized manner
- Mechanisms to deter **device theft** need to be in place
- Subsidising entities need to be assured that End Users cannot move their device to another Network Provider or Service Provider without authorisation

■ 5. Secure Software Download

- Goal for the use case is for the device to **securely download** application software, application software updates, firmware updates or patches
- Software download may be triggered by the end user, device manufacturer or network provider

6. Secure channel between device and UICC

- Some security sensitive applications may be implemented partly in the UICC and partly in the device
- UICC and device should be aware of each others' trust status in order to
 - avoid malicious software on the device interfering with applications
 - avoid a compromised device-UICC interface interfering with applications

Summary

- TCG Mobile Phone Work Group works to specify mobile security in device hardware and relevant software layers
- TCG Mobile Phone Work Group has published a set of use cases to form the basis of the TCG mobile security specification
- The specification is expected to be ready for product implementations in early 2006