Trusted Mobile Keyboard Controller Architecture

Sundeep Bajikar
Security Architect
Mobile Platforms Group
Intel Corporation

September 17, 2003

Safer Computing Track – Fall IDF

Tuesday

- LT Overview
  SCMS-16
- TCG & TPM v1.2
  SCMS-17
- LT Architecture
  SCMS-18
- Tech Showcase
  Every Day
  Birds of a Feather Lunches
  Tuesday & Wednesday

Wednesday

- Privacy Method for Assuring Trust
  SCMS-19
- Opt-In Strategy
  SCMS-156
- **Trusted Mobile KB Controller**
  MOB-147 / SCMS-24
- Software for LT
  SCMS-20
- Fundamentals for NGSCB
  SCMS-21
- Migrating Apps to NGSCB
  SCMS-22

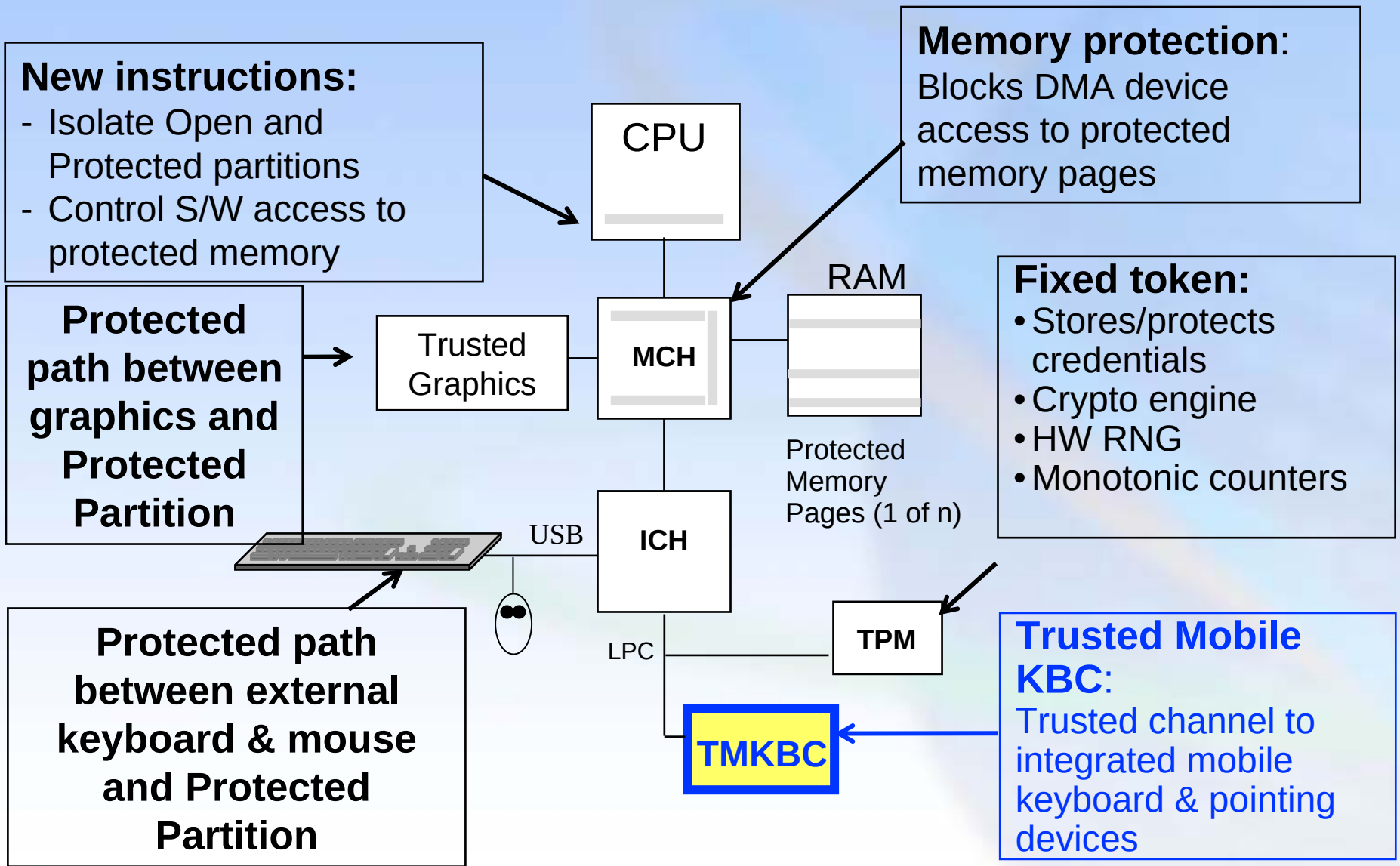
Thursday

- TPM Recovery
  SCMS-25
- TCG Credentials
  SCMS-157
- TPM Mfg & Testing
  SCMS-180

= Overview
= Medium Technical
= Highly Technical

intel

TMKBC in Mobile LT Platform Architecture



LT architecture details provided in the Safer Computing Track

Agenda

- Mobile trusted input requirements
- Trusted Mobile Keyboard Controller (TMKBC) architecture
- TMKBC implementation examples
- Design Considerations

Mobile Trusted Input Requirements

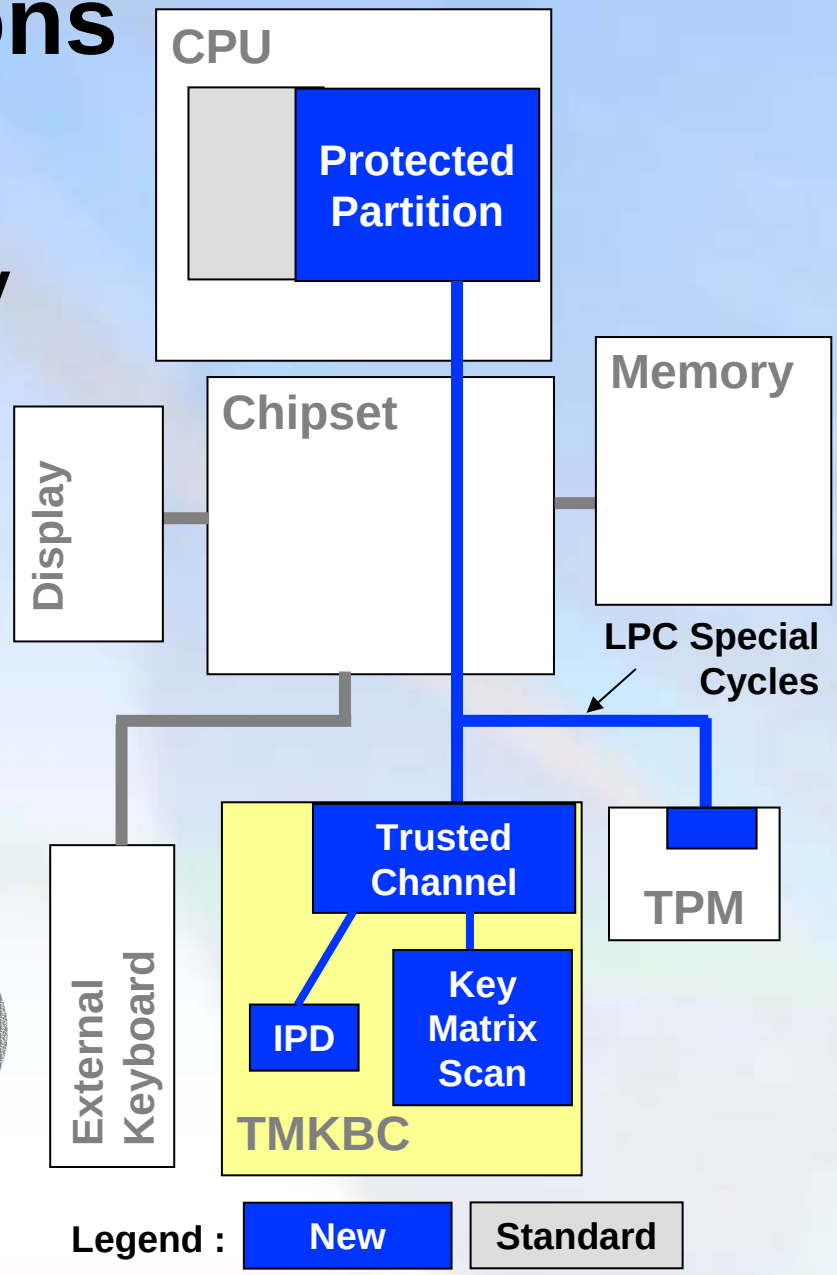
- Protect end-user input from malicious S/W
  - Snooping, modification, false insertion
- Provide non-repudiation for transactions
- Protect input from standard devices
  - Notebook integrated key matrix
  - Notebook pointing devices
  - External USB keyboard and pointing devices
- Protection from physical hardware attack is outside the scope

LT requires trusted input from user

TMKBC Key Functions

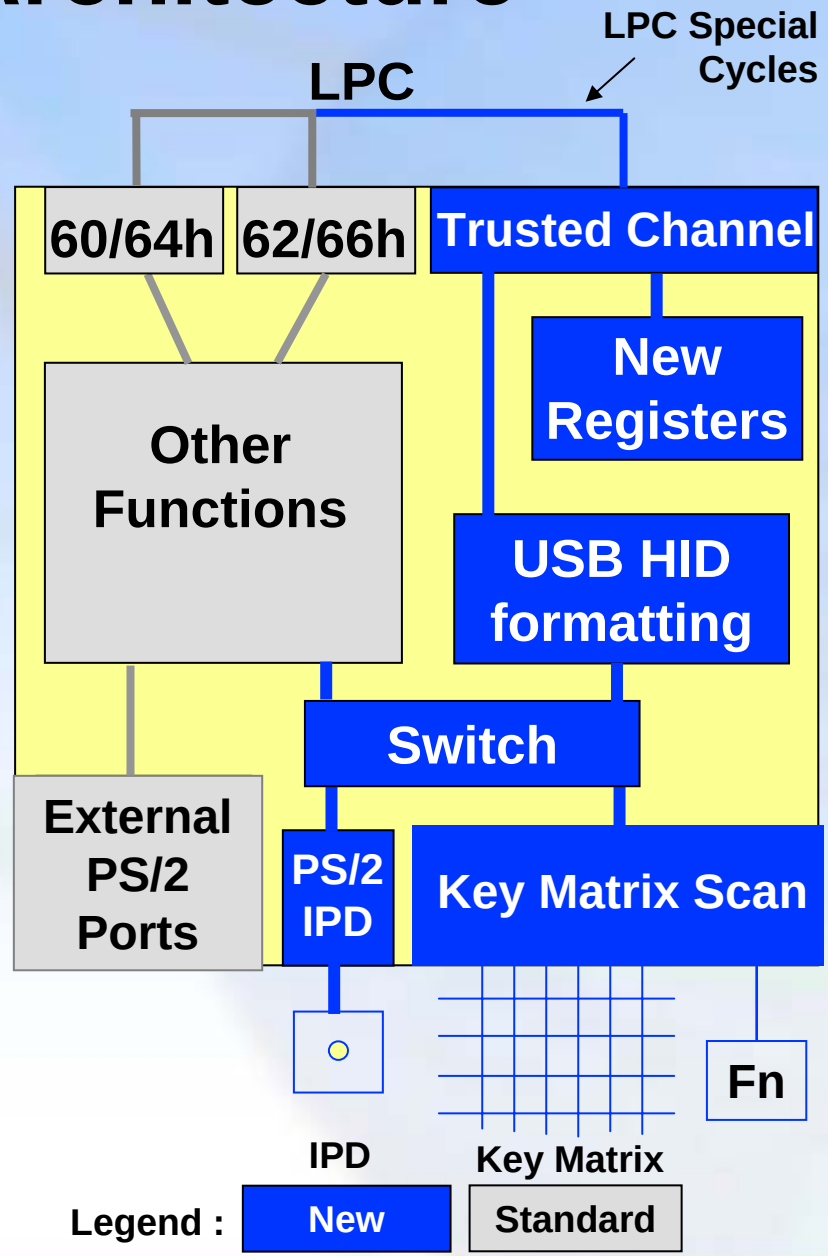
- **Protects input from:**
  - **Notebook's integrated key matrix**
  - **Integrated Pointing Devices (IPD)**
- **Architecture specifies**
  - **Behavioral requirements**
  - **Trusted Channel**

TMKBC architecture specification available from Intel



TMKBC Behavioral Architecture

- Trusted Channel multiplexed on LPC
- Protected and Standard functions are separated
- Entry & exit of New Mode controlled by bit in New Register space



TMKBC adds trusted input handling

TMKBC Trusted Channel

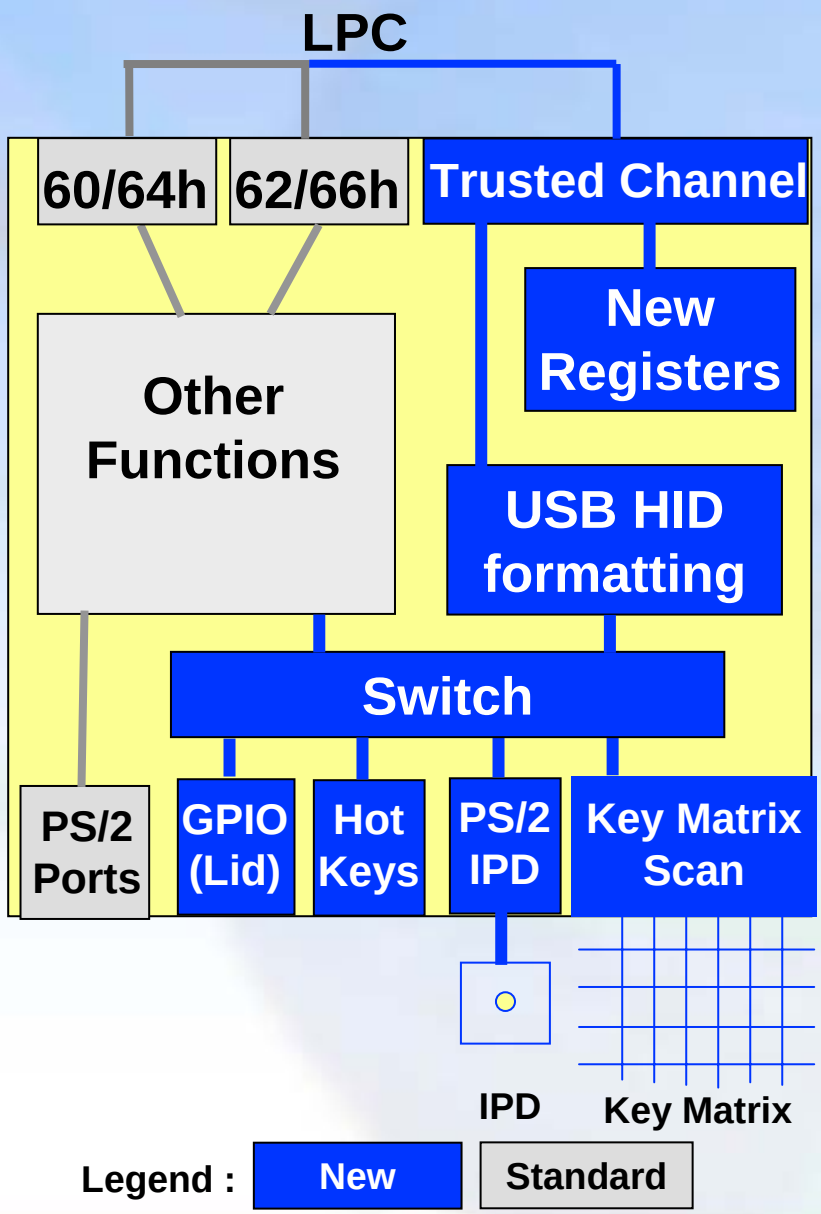
- New registers are mapped to LT protected region
- New LPC special cycles similar to standard I/O Read and I/O Write
  - Only protected system software running in protected partition on main CPU can initiate these cycles
- TMKBC New Registers accessible only via new LPC special cycles
- Enable bit for New Mode mapped to New Register

TMKBC Trusted Channel: Register Overview

- Status registers
- Data registers
- Capabilities registers
- Control registers
- ID registers

TMKBC Trusted Channel: Logical Devices

- TMKBC supports up to 15 logical devices
- Expected devices:
  - Keyboard, Mouse
  - Touch pad, Hot Keys
  - GPIO based events
    - e.g. Lid Switch
- USB-like Report Descriptor used to describe each logical device



TMKBC Trusted Channel – Data and Event Reporting

- Data and status registers mapped to New Register space
- Each logical device reports data using standard 8-byte USB HID packets
  - Status register indicates logical device
- Data to/from TMKBC goes via FIFO
  - FIFO must accommodate full USB HID packet
  - Reduces overhead on CPU
- Events reported using existing edge-triggered interrupts

TMKBC Trusted Channel – Entering New Mode

- Protected Software reads Report Descriptors and Capabilities Registers
- Protected Software performs several verification checks
- Protected Software enables New Mode
  - Causes TMKBC to enter New Mode of operation
- Legacy ports are still available for legacy functions
  - E.g. GPIO, power management, etc.

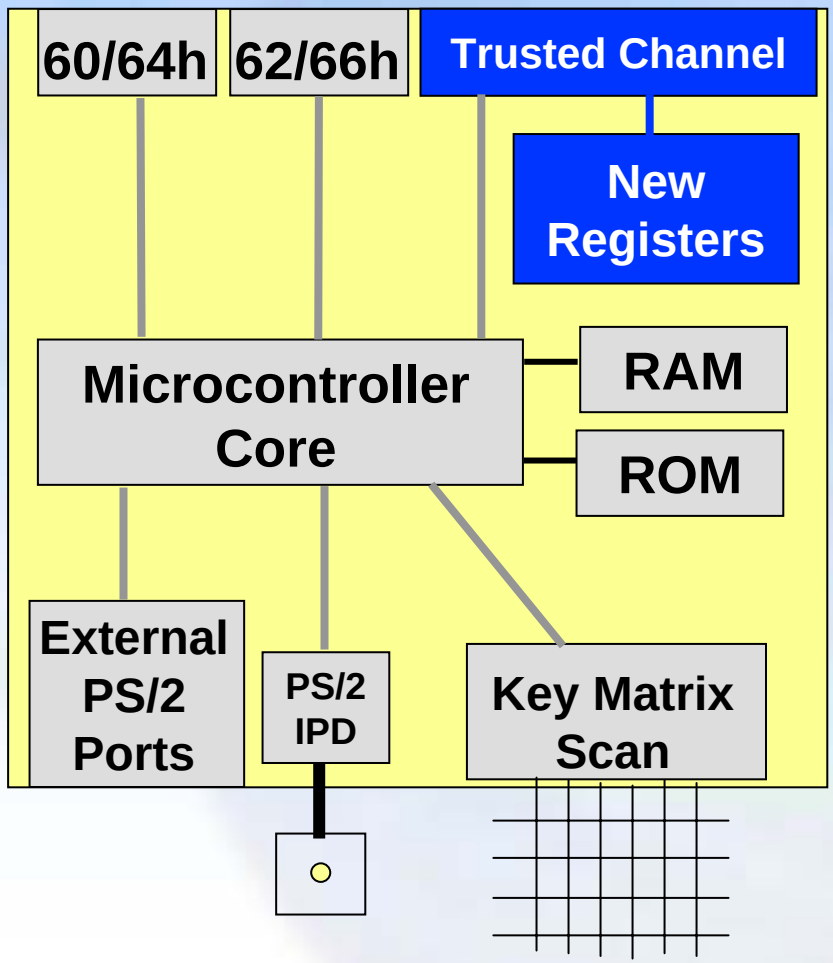
TMKBC Implementations

- TMKBC specification does not require any specific internal architecture
- At least three viable implementations
  - Single microcontroller
  - Single microcontroller with Trusted Mode
  - Dual microcontroller
- Several TMKBC vendors have products under development

TMKBC implementation is flexible

Single Microcontroller

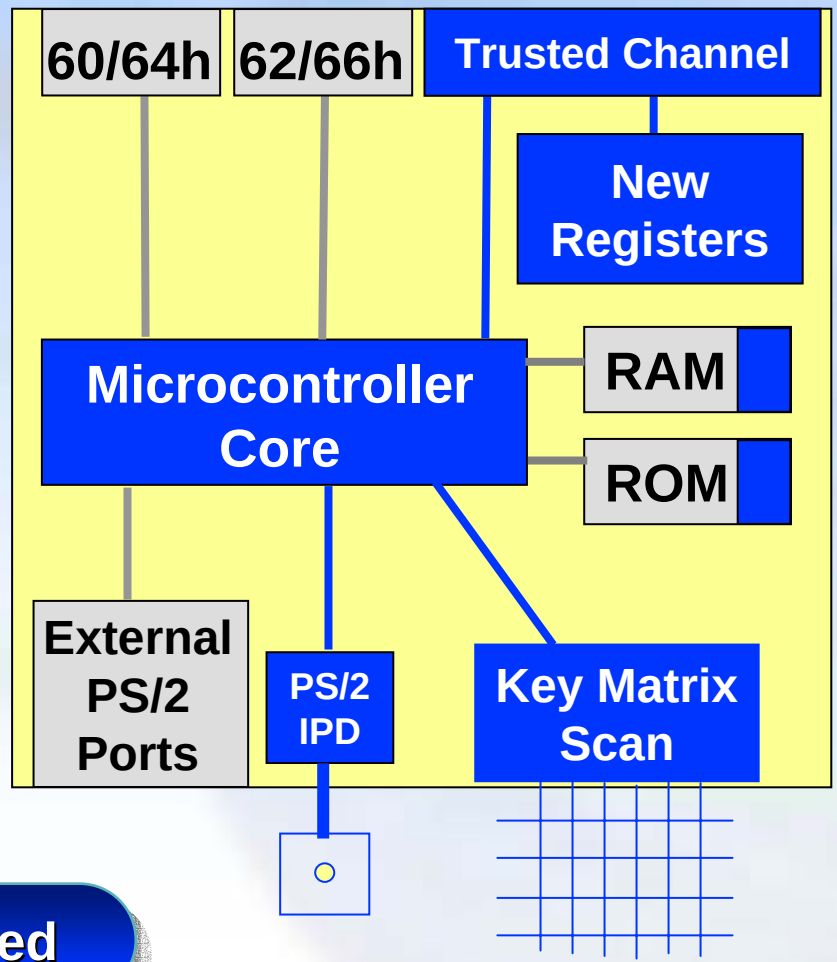
- Add Trusted Channel and New Registers
- Challenges:
  - Entire code base needs certification
  - Any code update needs re-certification



High cost of certification

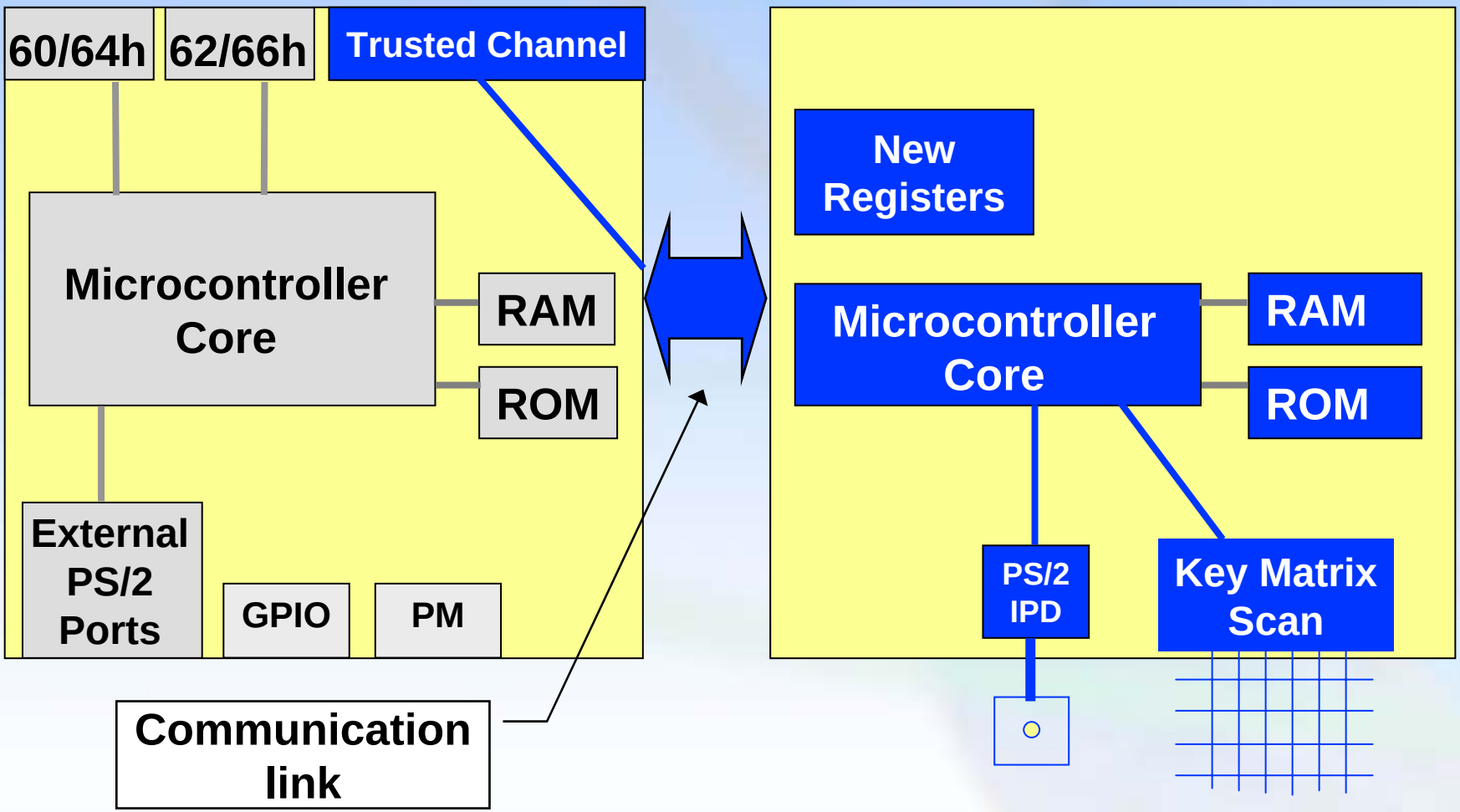
Single Microcontroller with Trust Mode

- Microcontroller has trusted operating mode
  - Regions of ROM and RAM only accessed by trusted code
- Split firmware
  - Trusted code only does key matrix scan and IPD handling



Only trusted firmware certified

Dual Microcontroller



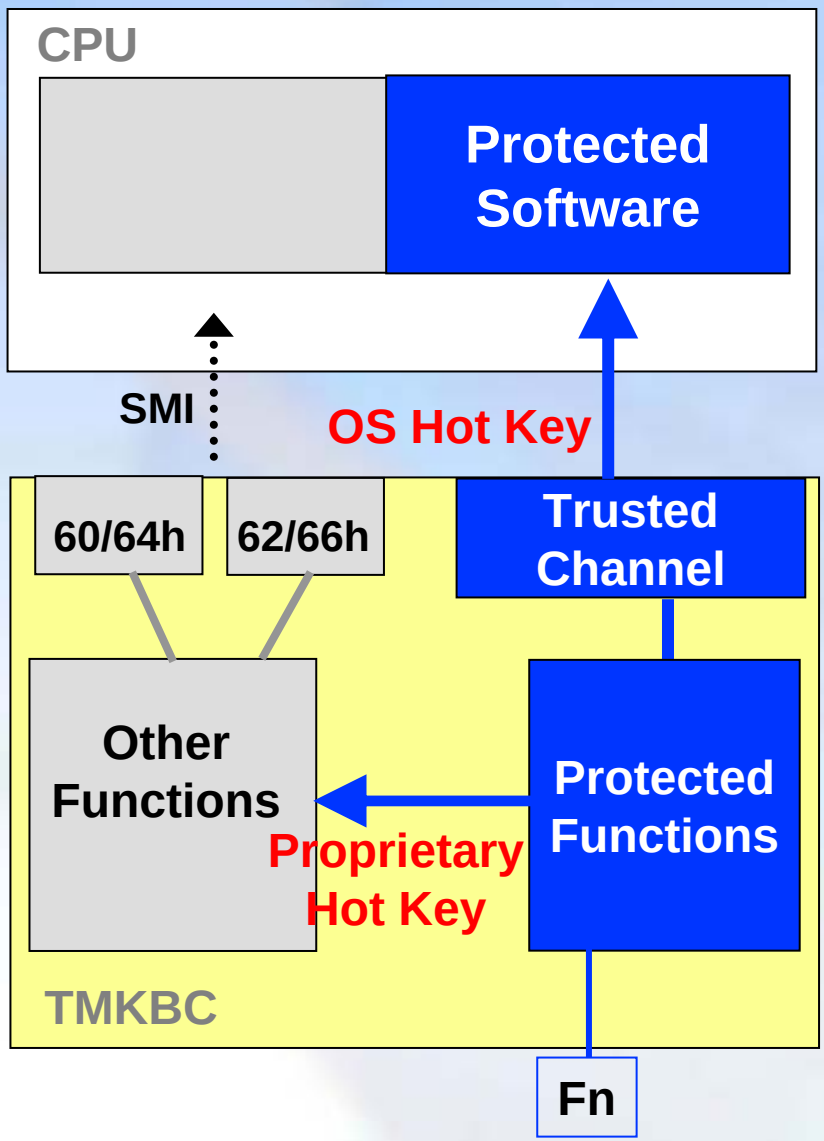
Only one Microcontroller involved with Trusted Input

TMKBC Design Considerations – Boundary Cases

- TMKBC resets and reverts to standard mode on a platform reset or power failure
  - TMKBC must not preserve any secrets, such as prior keystrokes or IPD data
- Protected environment taken down before sleep state entry
  - TMKBC switched back to standard mode by Protected Software

TMKBC Design Considerations - Hot Keys

- TMKBC can internally report Hot Keys from New side to Standard side
- OS-Visible Hot Keys can be reported through Trusted Channel
- Requirements
  - Hot Keys are reported ONLY if Fn key is pressed
  - Fn key cannot be re-mapped using translation table



TMKBC Design Considerations – Error Handling

- TMKBC reports keystroke or IPD errors as part of the standard USB HID packets
  - This is already defined in the USB specification
- Self-Test and other errors reported through Extended Status Register
- For system lockup, TMKBC remains in New Mode until it receives a system hardware reset

TMKBC Design Considerations – Other

- External keyboards and mice are supported via USB
  - Internal PS/2 devices are supported
- Protected code on TMKBC can be field updated
  - Use Signed and/or encrypted update mechanism
  - Firmware update mechanisms are beyond the scope of the TMKBC spec

Implement TMKBC architecture based on design considerations identified

Status

- TMKBC Specification V0.8 available under NDA and license
  - TMKBC V0.8 Specification reviews completed
  - Contact your local Intel representative to get access to the specification
- TMKBC V0.9 Specification planned for end of Q4’2003
- TMKBC V1.0 Specification planned for end of Q2’2004
- TMKBC products in development

Summary

- LT requires trusted input from user
- TMKBC architecture specification available from Intel
- TMKBC specification allows for various implementations & vendor optimizations
- Implement TMKBC architecture based on design considerations identified

Next Steps

- OEMs: Prepare plan for LT platform design
  - Work with KBC vendors to set design goals and understand architecture issues
- KBC Vendors: Design TMKBC based on the guidelines & specifications available from Intel
- ISVs: Evaluate product offerings in the LT timeframe to understand how they can benefit from LT features
- OSVs: Provide support for TMKBC based on the hardware specification provided by Intel

Thank you for attending.

Please fill out the Session Evaluation Form.

Acronyms

- LT = LaGrande Technology
- KBC = Keyboard Controller
- TMKBC = Trusted Mobile KBC
- IPD = Internal Pointing Device
- LPC = Low Pin Count bus
- USB = Universal Serial Bus
- HID = Human Input Device
- TPM = Trusted Platform Module
- OS = Operating System
- I/O = Input / Output
- FIFO = First In First Out buffer