IBM Research

Integrating TCG Technology in Linux

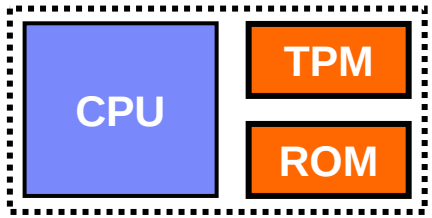
January 25, 2005
IBM Tokyo Research Laboratory
Seiji Munetoh

What are the fundamental TCG Components?

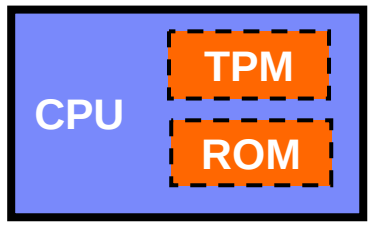
- Hardware based Root of Trust
  - TPM (Trusted Platform Module)
  - Write protected Boot ROM
- Software Support
  - TSS (TCG Software Stack)
  - TPM Device Driver
  - Trusted Boot Support (Trust Measurement)
- Infrastructure
  - Credentials – PKI

Hardware

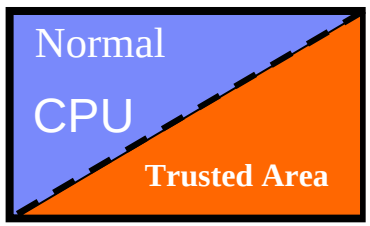
- TPM Protects
  - Identity (Private Keys)
  - Integrity (Platform Configurations)
- TPM for Embedded Platform…
  - Discrete TPM
    - TPM for PC Platform (LPC bus)
    - Atmel AT97SC3201S supports I2C bus!
  - CPU Embedded TPM
    - Intel PXA27x (Also supports Trusted ROM)
  - Software TPM with Strong Separation
    - ARM11 TrustZone?



Discrete TPM



Embedded TPM

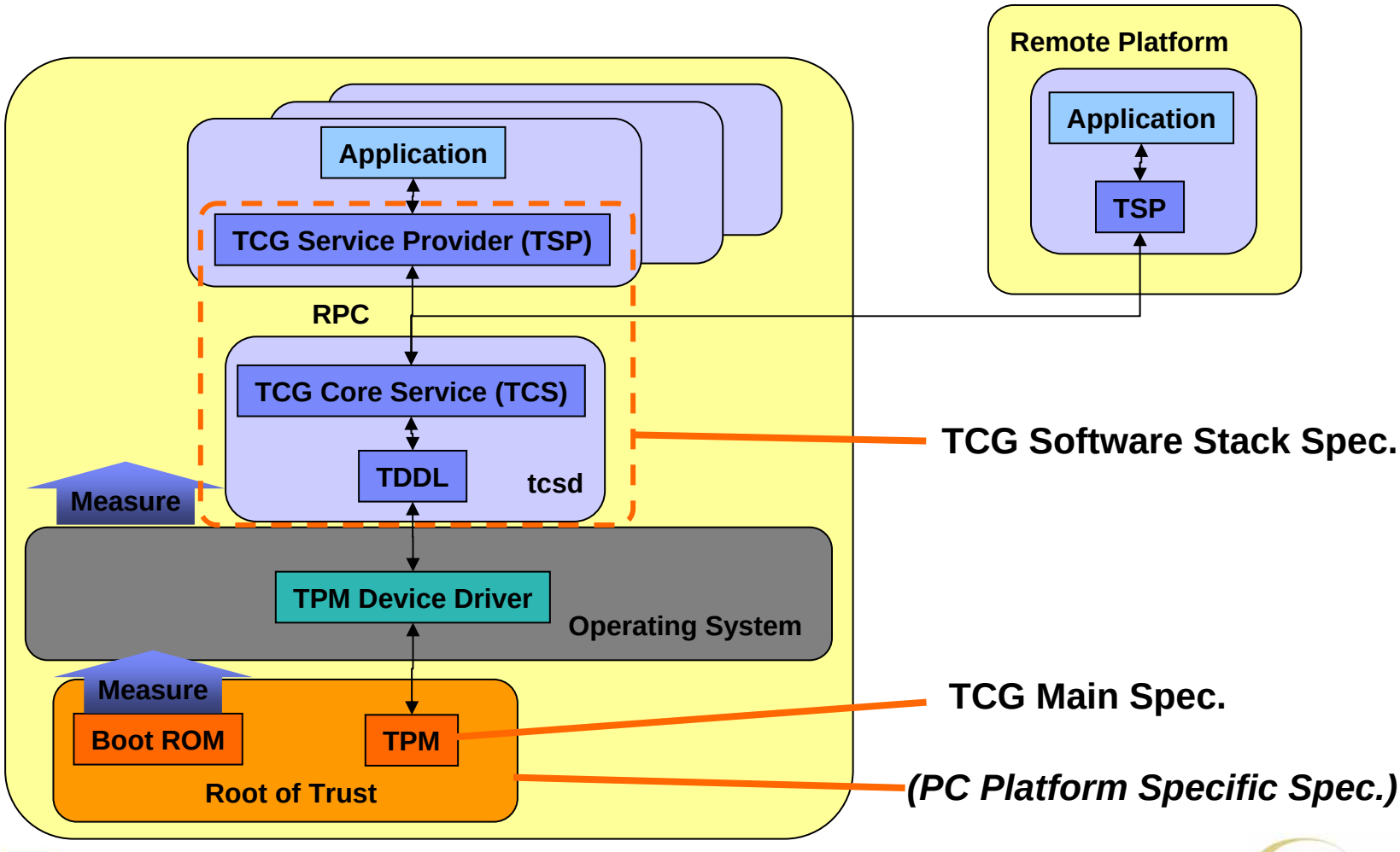


Software TPM

Software

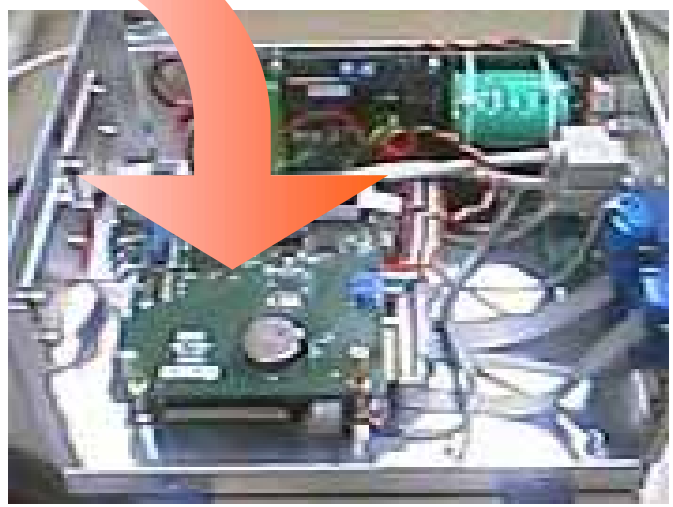
- Specifications
  - You can download them from TCG site
    - TPM Main Specification v1.1b and v1.2
    - TCG Software Stack (TSS) Specification v1.1
- Opensource Implementation from IBM
  - TPM Device Driver for LINUX (GPL)
    - http://sourceforge.net/projects/tpmdd/
  - TSS (TCG Software Stack) for LINUX (CPL)
    - http://sourceforge.net/projects/trousers

TCG Components Overview



Take a look at the technical detail of our demonstration

PC104 TPM Board

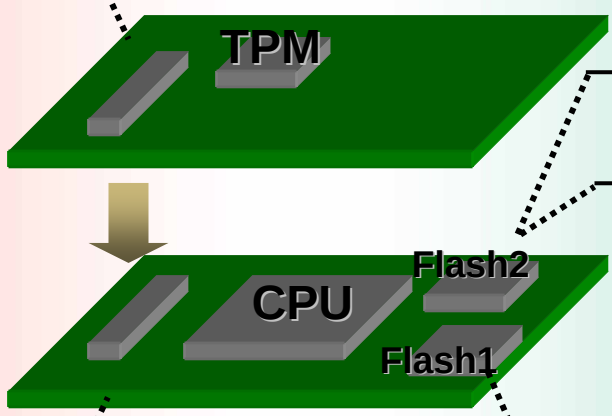


Arcom Viper (Industry Controller based on XScale and Linux)

Bill Of Materials

PC104 TPM Daughter Board

TPM : Atmel AT97SC3291S
I2C bus controller : Philips PCA9564
Battery backup (for RTC)



Java Middleware

With Integrity Check Capability

TCG Enabled Linux

TPM Device Driver and TSS
LSM Modules: IMA and LIDS

Arcom Viper

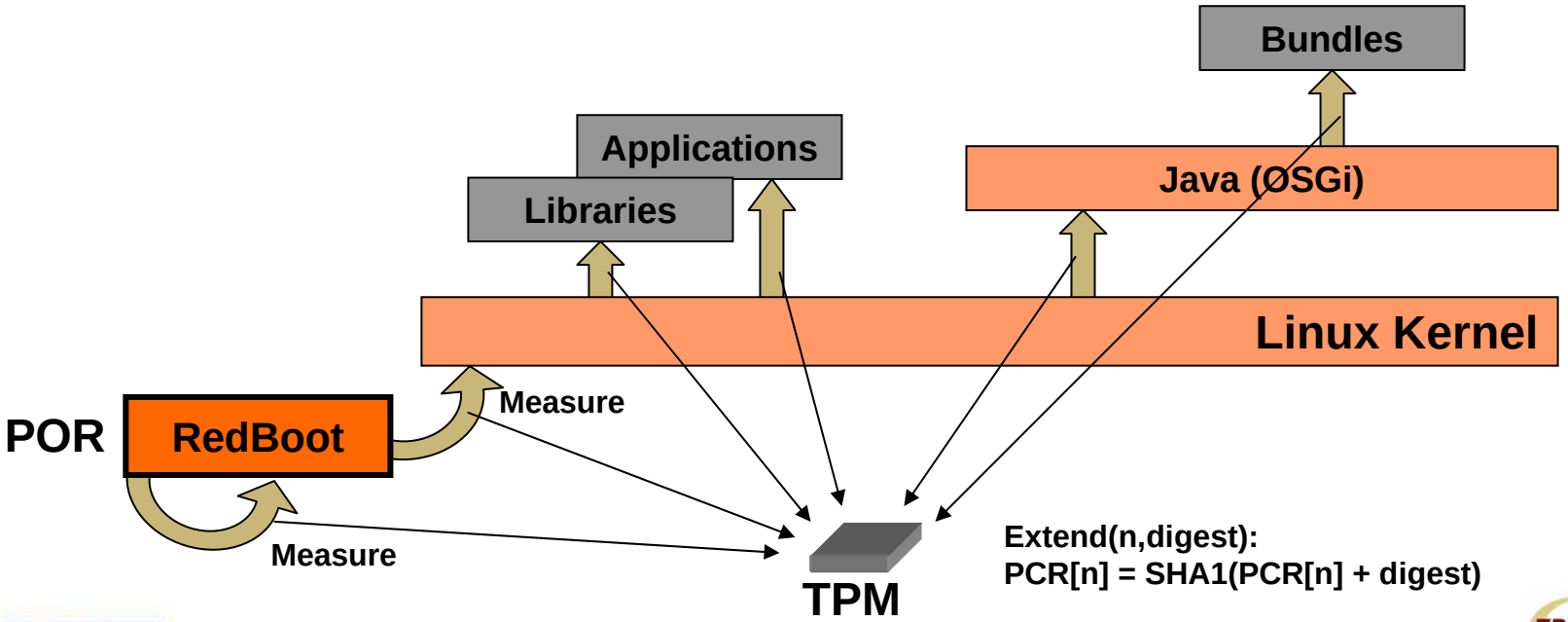
CPU: Intel XScale (PXA255 400MHz)
Memory: 32M Flash, 64MB SDRAM
Platform: PC104

Boot Flash

Work as CRTM(Core Root of Trust Measurement)
TCG Enabled RedBoot

Transitive Trust

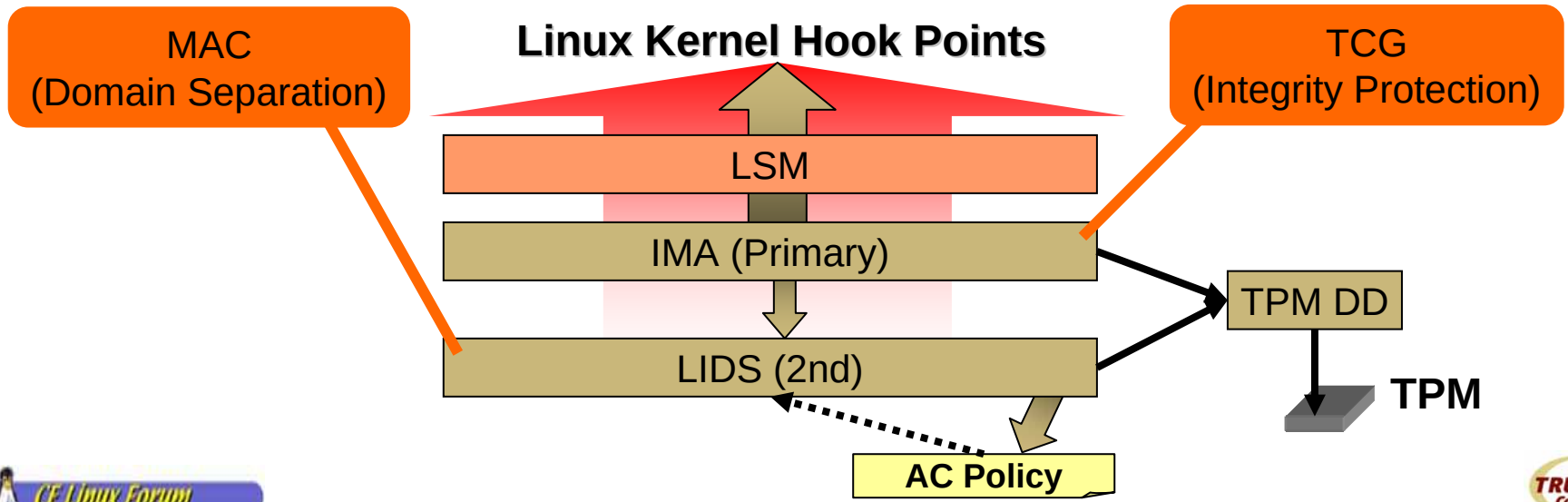
- Integrity Measurement Strategy
  - RedBoot measure itself and Kernel Image
  - Kernel measures Executables, Shared libraries and Loadable Kernel Modules
  - The OSGi bundle loader measures integrity of each bundle JAR file before loading it



Linux - Security Enhancement

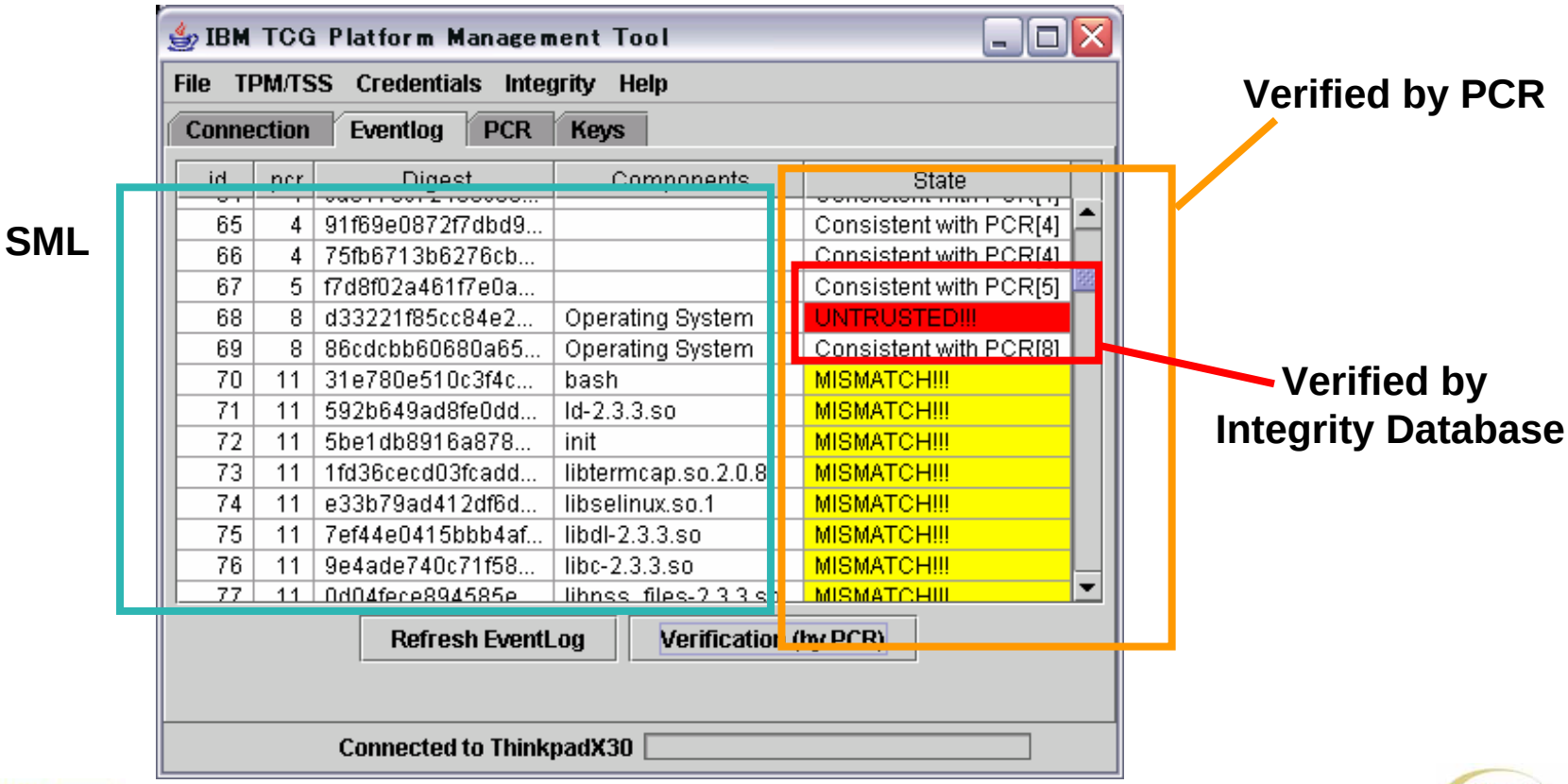
- LSM (Linux Security Module)
  - LISD (Linux Intrusion Detection System)
    - MAC Policy Enforcement
  - IMA (Integrity Measurement Architecture)
    - Integrity Measurement

Stacked!



Demonstration – Stored Measurement Log (SML)

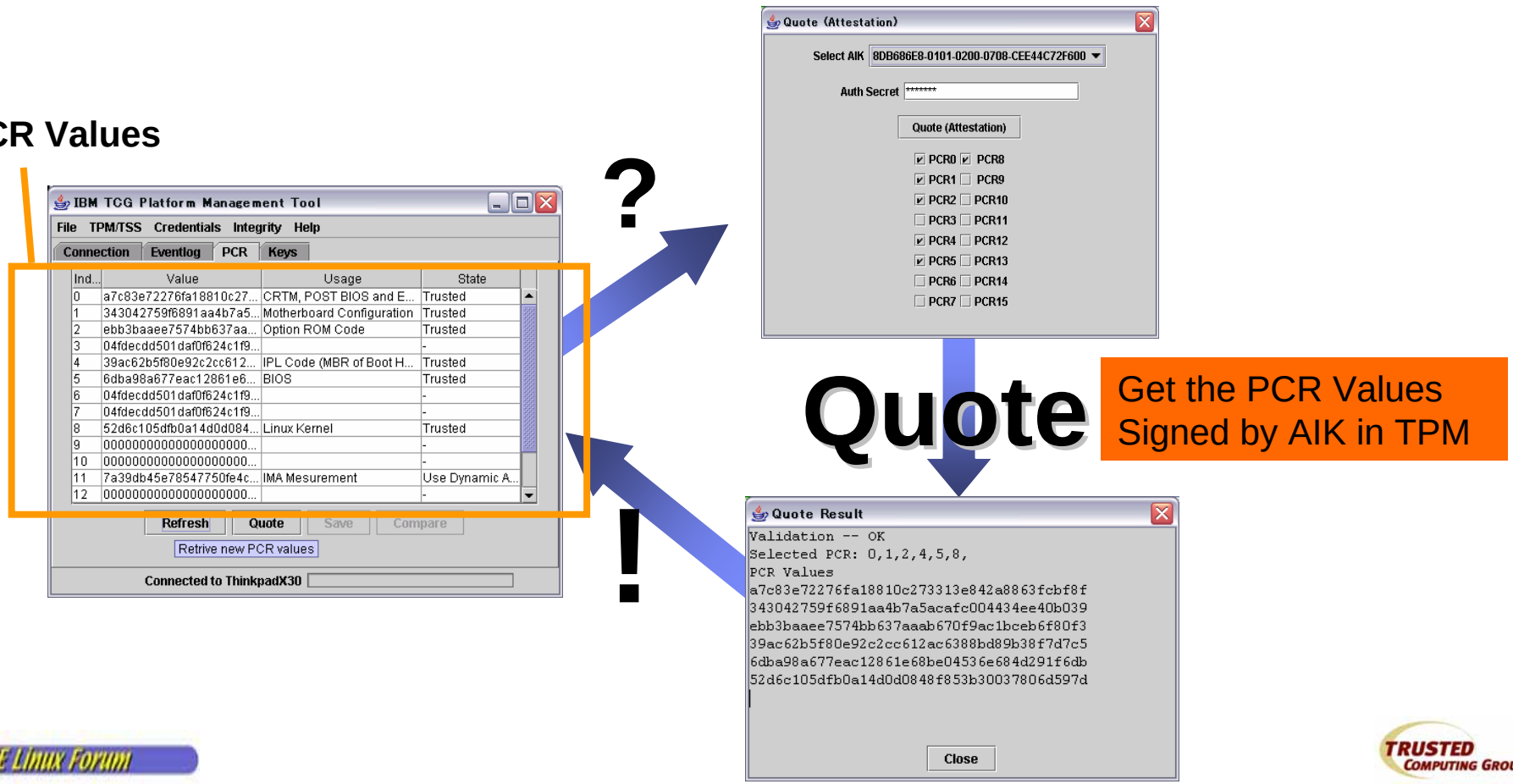
- Contains sequences of related measured values. Each sequence shares a common measurement digest.



Attestation (Integrity Reporting)

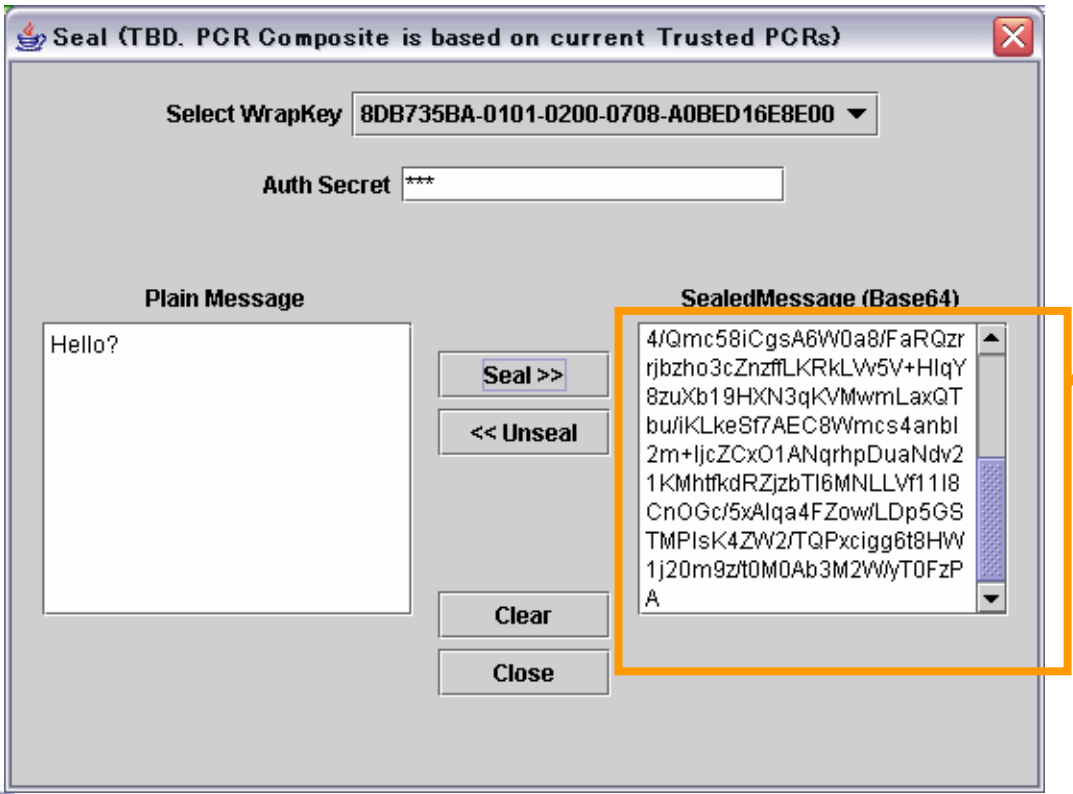
- Root of Trust Reporting
  - To expose shielded-locations for storage of integrity measurements (PCRs).
  - To attest to the authenticity of stored value based on trusted platform identities (AIK).

PCR Values



Seal/Unseal

- TPM_Seal: External data is concatenated with a value of integrity metric sequence and encrypted under a parent key.
- TPM_Unseal decrypts the blob using the parent key and exports the plaintext data if the current integrity metric sequence inside the TPM matches the value of integrity metric sequence inside the blob



Concatenated with PCR Values

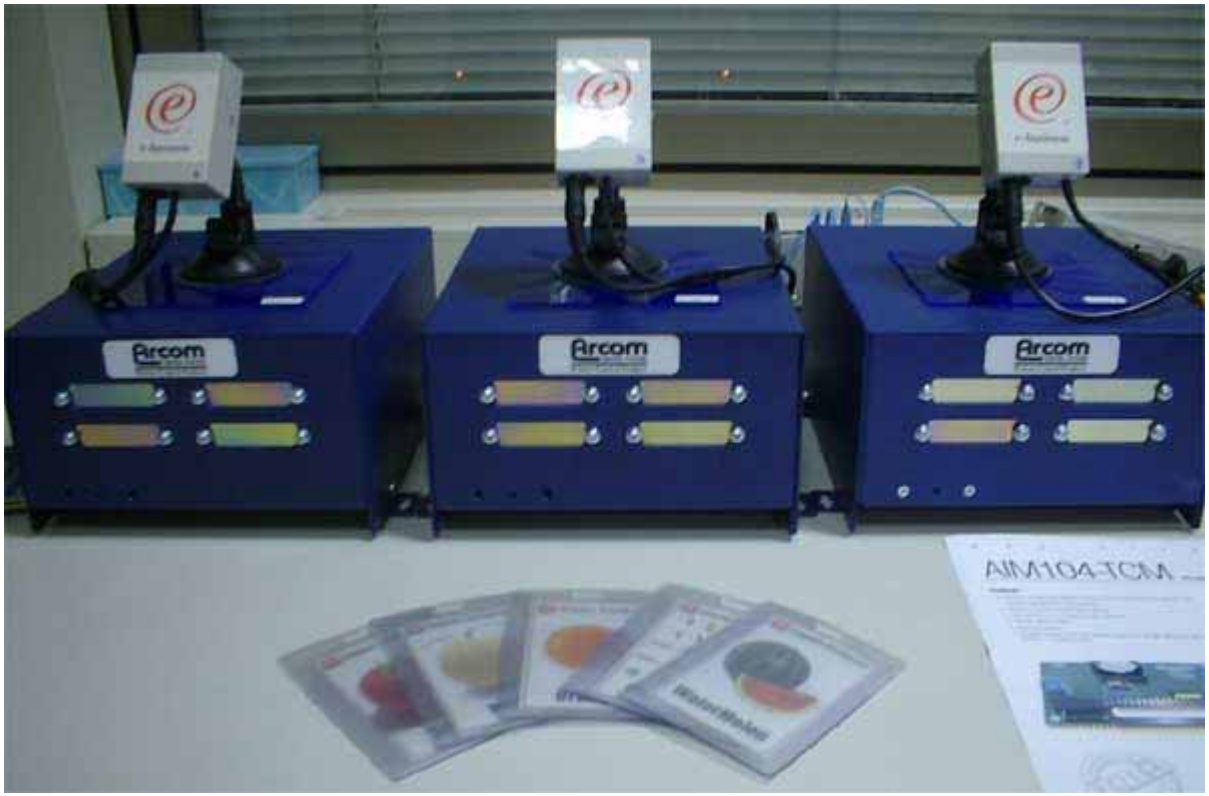
Conclusions

- TCG develop and promote open, vendor-neutral industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms

- Hardware protection for Keys used by various applications
- Hardware protection for Platform Integrity - this achieve an evaluation of assurance
- Lowest cost – standardized security solution

- Future Works
  - Integrity Management and Validation
    - Vulnerability, Provisioning….
  - Credential, Infrastructure

Thank you!



Trusted RFID Gateway will be demonstrate at upcoming RSA Conference.
See you at the IBM booth

Links

- **Trusted Computing Group (TCG)**
  - https://www.trustedcomputinggroup.org/home
- **Linux Intrusion Detection System (LIDS)**
  - http://www.lids.org/
- **Integrity Measurement Architecture (IMA)**
  - http://www.research.ibm.com/secure_systems_department/projects/tcglinux/
  - http://www.research.ibm.com/compsci/project_spotlight/security/
- **TPM Device Driver for LINUX (GPL)**
  - http://sourceforge.net/projects/tpmdd/
-