Trusted Computing Group

Introduction and brief technical overview

July 2nd, 2003

Agenda

- TCG introduction
- TCG architecture and brief technical overview

TCG Mission

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

TCG Structure

- TCG is incorporated as a not-for-profit corporation, with international membership
  - Open membership model
    - Offers multiple membership levels: Promoters, Contributors, and Adopters
    - Additional zero fee Liason and Advisory Level Participation Levels under consideration
  - Board of Directors
    - Promoters and member elected Contributors
    - Decision by supermajority (2/3)
  - Typical not-for-profit bylaws
  - Industry typical patent policy (Reasonable and Non Discriminatory) for all specification work
  - Working Groups
    - Technical/Marketing
    - Decision making by majority and supermajority

Current TCG Membership

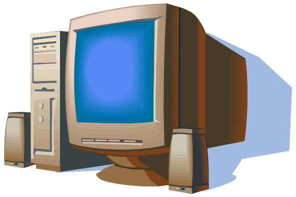
- Promoters:
  - AMD*, Hewlett Packard*, IBM*, Intel*, Microsoft*, initially
  - Additional promoters will be added
- Contributors:
  - Atmel*, Broadcom*, Comodo*, Gemplus*,Fujitsu*, Infineon*, Phoenix Technologies*, Phillips*, National Semiconductor*, Nokia*, NTRU*, Nvidia*, Rainbow Technologies*, STMicroelectronics*,Standard Microsystems*, Seagate* Sony*, Utimaco*, VeriSign*, Wave Systems*
- Adopters:
  - ALi Corp.*, ATI*, Fujitsu-Siemens*, M-Systems*, Silicon Integrated Systems*
- A number of additional companies have expressed interest and intent to join

* Other names and brands may be claimed as the property of others.

Motivations for TCG

- Name change distinguishes TCG as different from TCPA
  - TCPA has acknowledged TCG as the successor industry standard organization for evolving these specifications
- Incorporation enables structural improvements that will promote accelerated specification development
  - Governance model similar to other Standard Setting Orgs
  - Industry-accepted reciprocal RAND IP policy
- Increased resources and broader governance
  - TCG financially supported by all members
- All companies are welcome to join TCG
  - Agree to bylaws, pay dues, etc…

Technical Workgroups



- Technical Committee
  - Technical Committee
- Work groups operational
  - Conformance (Common criteria)
  - Trusted Platform Module (TPM)
  - TPM Software Stack (TSS)
  - PC Specific Implementation

- Work groups being defined:
  - Server Specific Implementation
  - PDA Specific Implementation
  - Mobile Phone Implementation
  - Infrastructure

- Other work groups:
  - Charter Development Committee
  - Marketing
- Additional work groups anticipated

Implementation Status

- Trusted Platform Modules (TPM) based on 1.1b specification available from TPM vendors
  - Atmel
  - Infineon
  - National Semiconductor
- Compliant PC platforms shipping now
  - IBM* ThinkPad notebooks and NetVista desktops
  - HP* D530 desktops
  - More expected soon
- TSS and TPM 1.2 currently in IP Review

* Other names and brands may be claimed as the property of others.

TCG Policy Position

Privacy Effect of TCG Specifications

TCG is committed to ensure that TCG specifications provide for an increased capability to secure personally identifiable information.

TCG Policy Position

Open Platform Development Model

TCG is committed to preserving the open development model that enables any party to develop hardware, software or systems based on TCG Specifications. Further, TCG is committed to preserving the freedom of choice that consumers enjoy with respect to hardware, software and platforms.

TCG Policy Position

Platform Owner and User Control

TCG is committed to ensuring owners and users of computing platforms remain in full control of their computing platform and to require platform owners to Opt-in to enable TCG features.

TCG does NOT

- Does NOT Certify software or applications
- Does NOT Define mechanisms that would prevent user choice of what software runs on a Trusted Platform
- Does NOT Certify any keys of any sort!
- Does NOT Implement Third Party servers/services
- Does NOT Create any databases…

Onto a technical overview…

Goals of the TCG Architecture

TCG defines mechanisms that aid in

- **Protecting user keys and information**
- **Protecting the user's computing environment**

Whilst…

- **Ensuring the user's choice of using these mechanisms**
- **Protecting user's privacy**

Design Goal: Deliver security <u>with</u> user control and privacy

Features

Basic TPM functionality

Integrity Metrics Storage

- Storage of Integrity Metrics information

As well as

Other cryptographic functions

- H/W Random Number Generator
- Hash functions

Platform Attestation

- Owner Created Platform Attestation Identity Keys (AIK)
- Attesting to platform TCG properties
- Attesting to platform measured integrity metrics

Protected Storage

- Key operations protected by TPM's hardware
- No access to private key data
- Protection may include platform integrity

PCR – Platform Configuration Register

Features

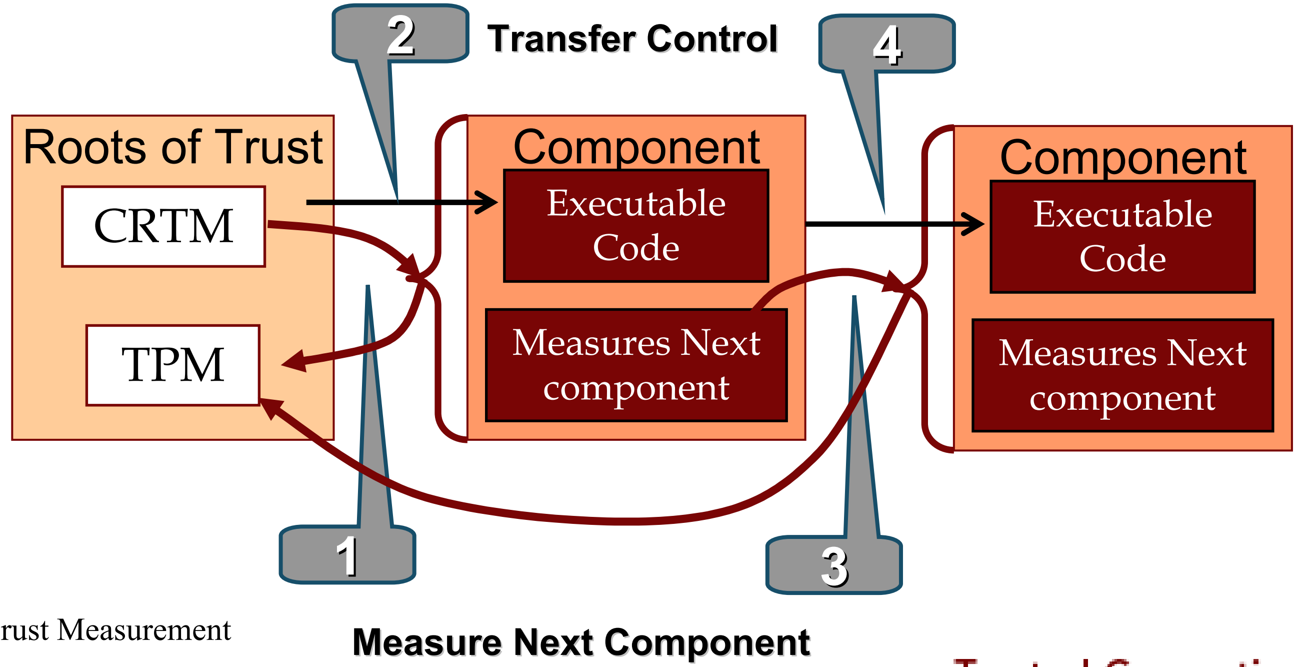
Integrity Metrics

•TPM is a **passive** device

•TPM can store Integrity Metrics information that is reported to it

•Integrity Metrics information reported to TPM can be invalidated but not counterfeited

•This mechanism supports the creation of a “Chain of Trust”



CRTM=Core Root of Trust Measurement

Features

Platform Attestation

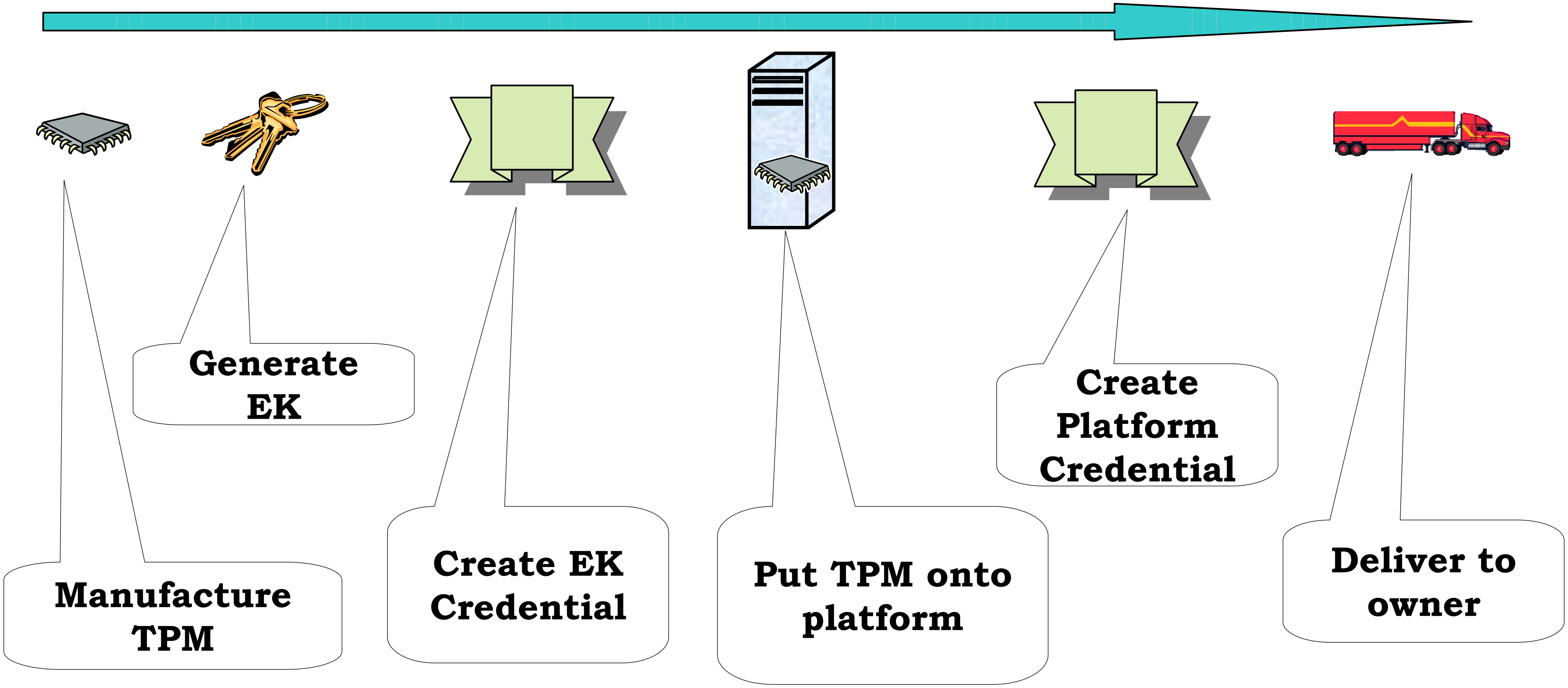
- TPM contains an endorsement key under total control of owner/user
- TPM can be used to created multiple pseudonymous AIK (Attestation Identity Keys)
- An AIK:
  - ✓ Is not linked to the TPM's Endorsement key
  - ✓ Does not require to contain any Personal Identifying Information (PII)
  - ✓ Is generated inside the TPM
  - ✓ Is only ever used by the TPM in order to attest to platform properties or integrity metrics information
- TPM supports mechanism to demonstrate to third-party that an AIK is a valid TPM AIK without associating it to a specific TPM

Features

Protected Storage

- TPM is a small passive device that only has the minimal non-volatile memory
- When Ownership of TPM is taken, a Storage Root Key (SRK) is generated by the TPM to be protected inside the TPM
- Unlimited number of cryptographic keys can then be created by, or protected by the TPM using that SRK.
- Small amounts of data – No Bulk Encryption – can then be protected using TPM keys
- TPM keys and data can be protected by means of authorization data and/or Integrity Metrics information

Trusted Platform Manufacturing steps



Manufacture TPM

Generate EK

Create EK Credential

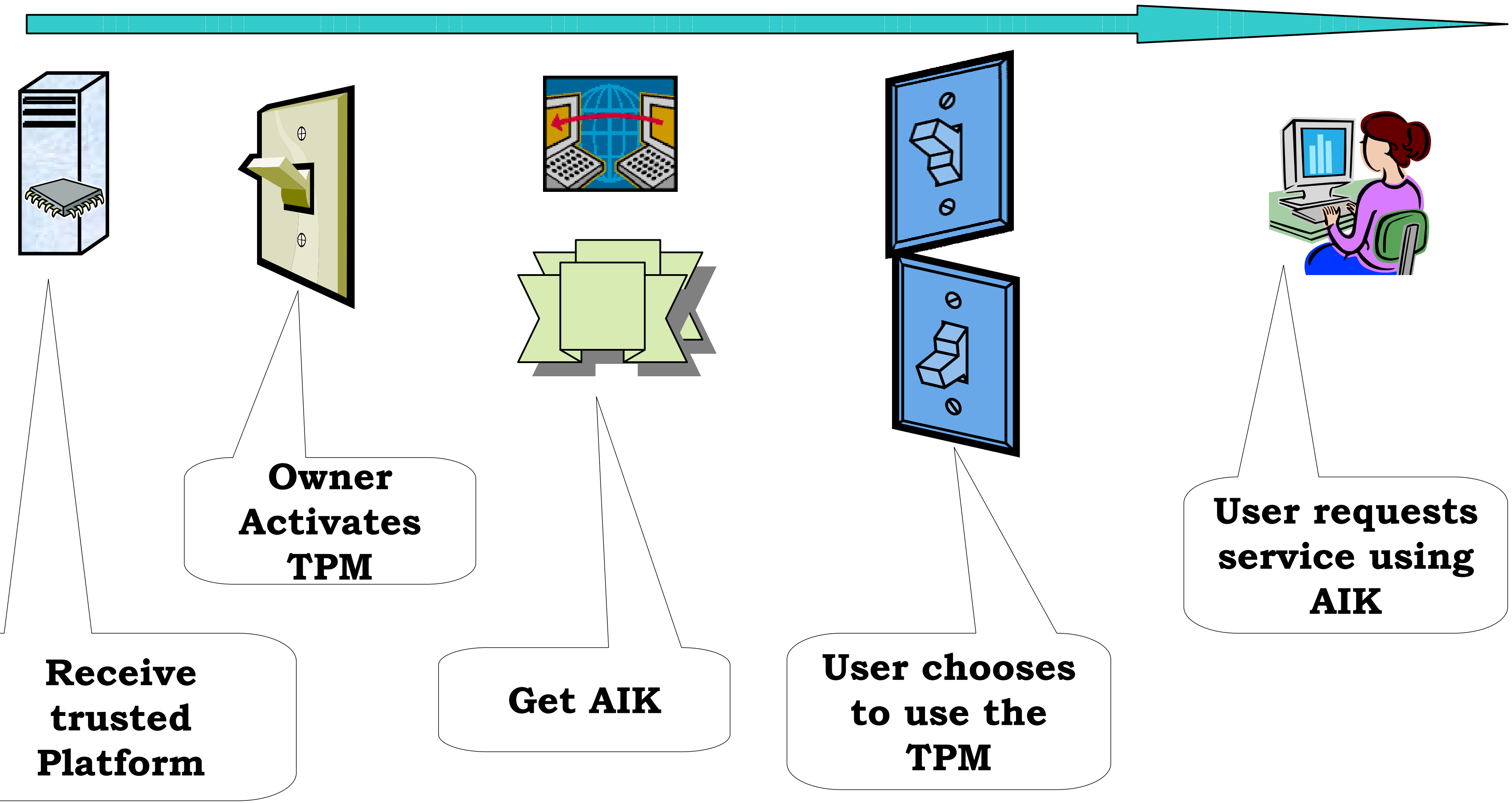
Put TPM onto platform

Create Platform Credential

Deliver to owner

Trusted Computing Group

Platform Deployment and Use



Design concepts

Platform Ownership

- The Platform Owner is the TPM owner. A user of a trusted platform may or may not be the Owner

- In Corporate IT environment, Platform Owner could be IT Administrator. In this case, the employee would be the user

- At home, Platform Owner could be the individual consumer

- Privacy positive design has been pursued to ensure Platform Owner ultimate control on the use of TPM mechanisms

Design Concepts

Platform Ownership

Owner Opt-in, individual users can Opt-out, and Platform Owner is re-settable

- The Platform Owner can:
  - Control the use of the TPM
  - Remotely authorize owner-controlled commands

- A Platform User can:
  - Deactivate the TPM temporarily
  - Disable the TPM by being physically present at the platform

In Conclusion

TCG is about developing and promoting open, vendor-neutral, industry standard specifications for trusted computing with a commitment to provide for an increased capability to secure personally identifiable data.

IBM VIEW OF TCG TECHNOLOGY BUILDING BLOCKS

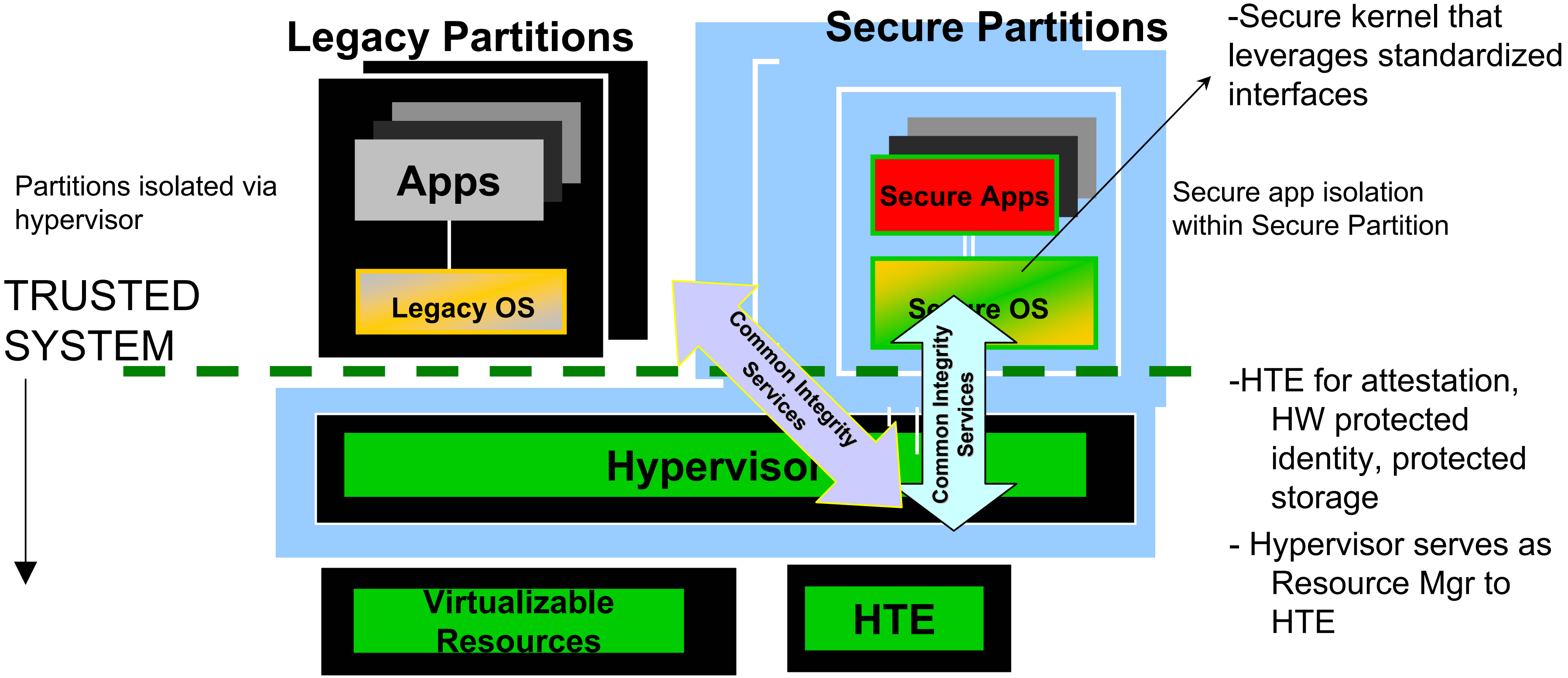
IBM Corporate Security Strategy

Enterprise Security and IBM Common Integrity Services

June 2003

Corporate Security Strategy Team

Secure eBusiness on Demand Computing Architecture



Partitions isolated via hypervisor

-Secure kernel that leverages standardized interfaces

Secure app isolation within Secure Partition

-HTE for attestation, HW protected identity, protected storage

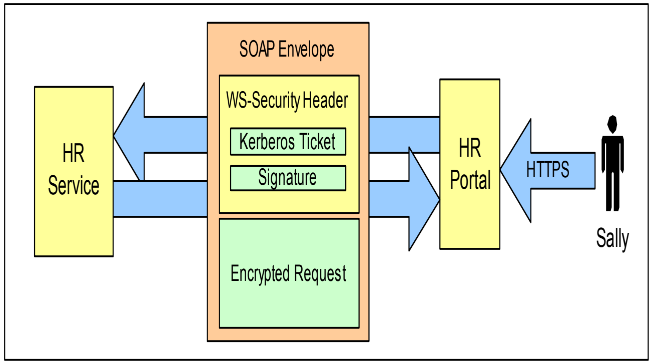
- Hypervisor serves as Resource Mgr to HTE

- Common Trusted System capabilities for Servers, Laptops, Desktops, Mobile Devices, and embedded applications
  - Secure Virtualization implemented via hypervisor on top of platform specific core HW architectures
  - Exploited in system SW via open standards based Common Integrity Services interface

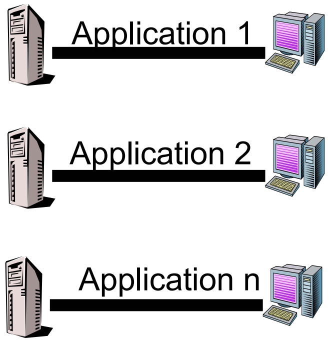
Open Standards via Common Integrity Services

Extending Embedded Integrity

Web Services



High Assurance



Other Initiatives

- Laptops
- Linux
- IGS Services
- Control Systems
- Access & Identity tools

Enables Enhanced Policy Enforcement

- •Databases
- •Collaboration
- •Web Servers
- •Portals
- •Messaging SW
- •Management SW
- •Storage elements
- •Desktops / Laptops
- •Etc…

Trust Management

Server & Systems Management (IBM Director, Tivoli & others)

Hypervisor + Common Integrity Services

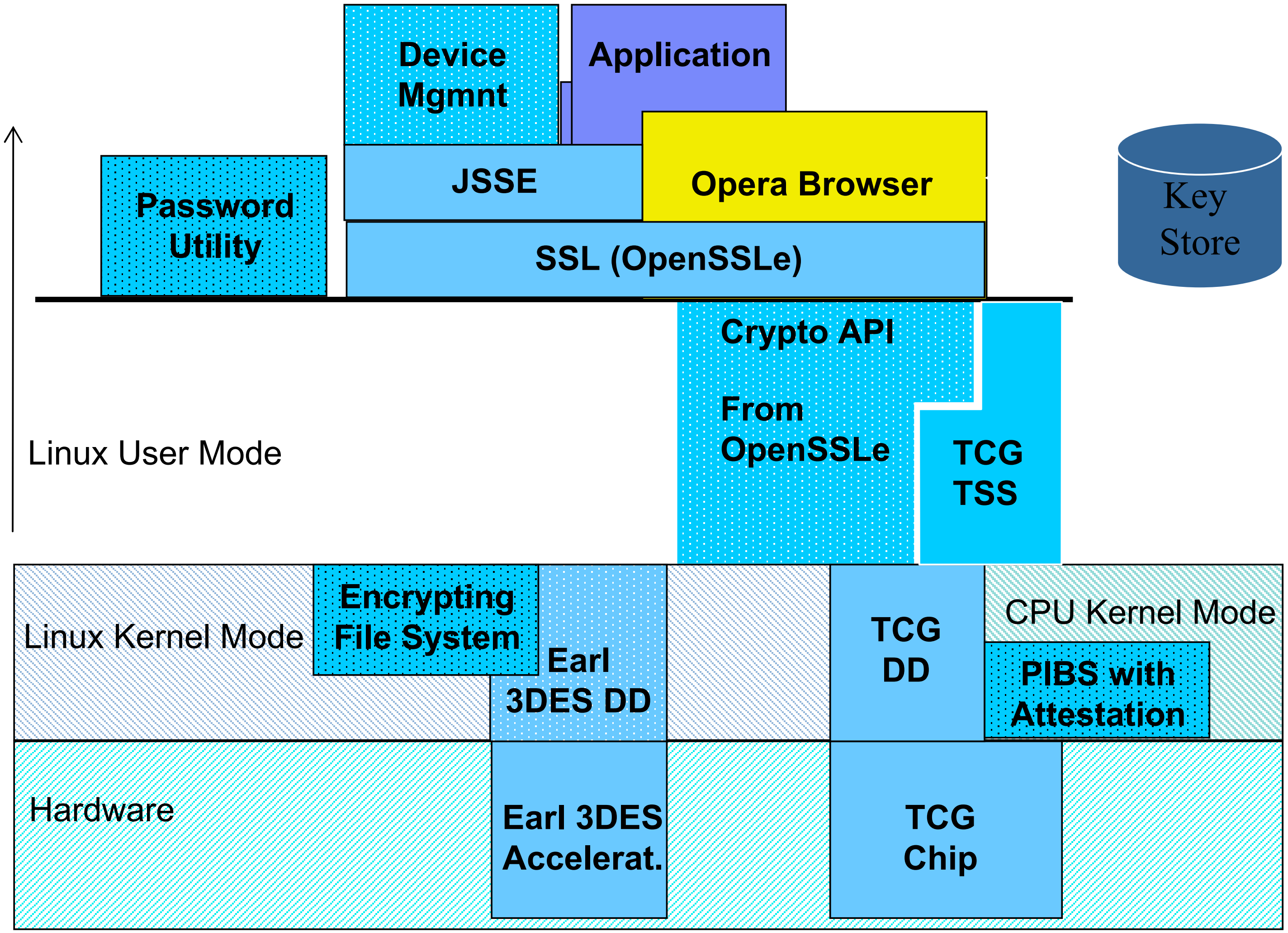
Protected Execution/Process/Memory

TRUSTED SYSTEM

IBM Server & Device Attributes

- •Verifiable System ID
- •Verifiable Envir.
- •Verifiable Boot
- •Verifiable Process
- •HW Crypto Token
- •Protected Storage

Pervasive (Embedded) Linux Exploitation



Summary

- IBM trusted systems vision
  - will embrace open standards for implementing trusted systems
  - is committed to enabling Linux as an operating system that exploits trusted platforms
  - is committed to enabling these open standards across all of our systems platforms
  - intends to leverage trusted platforms across all of our software products and development tools