



Virtualizzazione & sicurezza ICT

11 novembre 2010

Nuovi orizzonti per la virtualizzazione

Gianluca Ramunno
Politecnico di Torino

Attribuzione

- Il materiale di queste slide è stato preparato da:
 - Stephane Lo Presti (University of London, UK)
 - Suen Chun Hui (TU Munich, DE)
 - per il Politecnico di Torino
 - Davide Vernizzi, Emanuele Cesena
 - Gianluca Ramunno, Andrea Atzeni
 - Sviluppato in parte durante per il progetto Open Trusted Computing - <http://www.opentc.net>
- Rilasciato sotto la seguente licenza:
 - Creative Commons Attribution-Share Alike 3.0 Unported License.

Licenza

- This work is licensed under the
 - Creative Commons Attribution-Share Alike 3.0 Unported License
- You are free to
 - Share: copy, distribute and transmit the work
 - Remix: adapt the work
- Under the following conditions:
 - Attribution.
 - Share Alike

Licenza

- To view a copy of this license, visit
 - <http://creativecommons.org/licenses/by-sa/3.0/>
 - Or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.
- To view a copy of the Legal Code (the full license), visit
 - <http://creativecommons.org/licenses/by-sa/3.0/legalcode>

Agenda

- Nuovi orizzonti
- Tecnologia: Trusted Computing e supporto hardware alla virtualizzazione
- Uso combinato di Trusted Computing e virtualizzazione
- Esempi di scenari applicativi

Nuovi orizzonti

- Obiettivi tradizionali della virtualizzazione
 - Consolidamento di server
 - Prototipazione, indipendenza dall'hardware
- Requisiti di sicurezza per la virtualizzazione
 - difesa contro malware (rootkit, virus ...)
 - isolamento delle macchine virtuali
- Paradigma emergente (R&D)
 - Cambiare il punto di vista
 - La sicurezza da requisito diventa un obiettivo

Nuovo paradigma in sintesi

- Uso combinato delle tecnologie di
 - Trusted Computing
 - Virtualizzazione
 - in particolare supporto hardware
- Obiettivi
 - Contrastare attacchi software alla piattaforma
 - Contrastare semplici hardware (“open case”)

Tecnologia: Trusted Computing

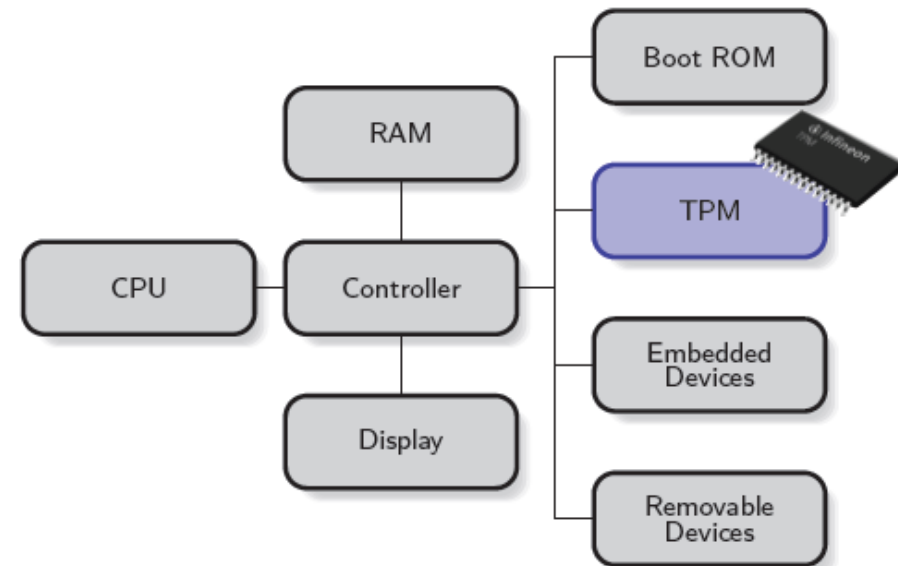
- Trusted Computing
 - Concetti e tecnologie non nuove: TCSEC
- Trusted Computing Group (ex TCPA)
 - Consorzio industriale
 - Specifiche per piattaforme x86, mobile ed embedded
- Trusted Computing Base (Orange Book)
 - L'insieme dei componenti che sono critici per la sicurezza di un sistema, nel senso che bug presenti nel TCB possono mettere a rischio le proprietà di sicurezza dell'intero sistema

Concetto di trust

- **Attenzione!**
 - Trust non è sicurezza
- Trusted system (Trusted Computing Group)
 - Un sistema “trusted” si comporta nel modo atteso per uno scopo particolare
- Trustworthy system (National Security Agency)
 - Un sistema “trustworthy” è un sistema che non fallisce

Panoramica su Trusted Platform

- Obiettivi
 - Protected storage
 - Integrity reporting
- Principi
 - Roots of Trust
 - Trust Transitivo
- Caratteristiche
 - “Protected capabilities”
 - “Shielded locations”

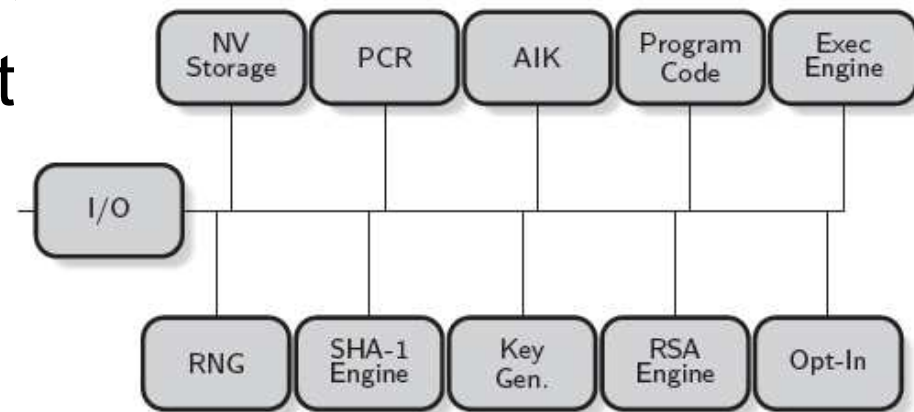


Panoramica su Trusted Platform: Roots of Trust

- Componenti che devono essere trusted
 - un cattivo comportamento non può essere rilevato
- RoT for Measurement (RTM)
 - Motore di elaborazione capace di effettuare misurazioni di integrità affidabili
- RoT for Storage (RTS)
 - Motore di elaborazione capace di mantenere “riassunti” accurati delle misure di integrità
- RoT for Reporting (RTR)
 - Motore di elaborazione capace di riportare affidabilmente le informazioni del RTS

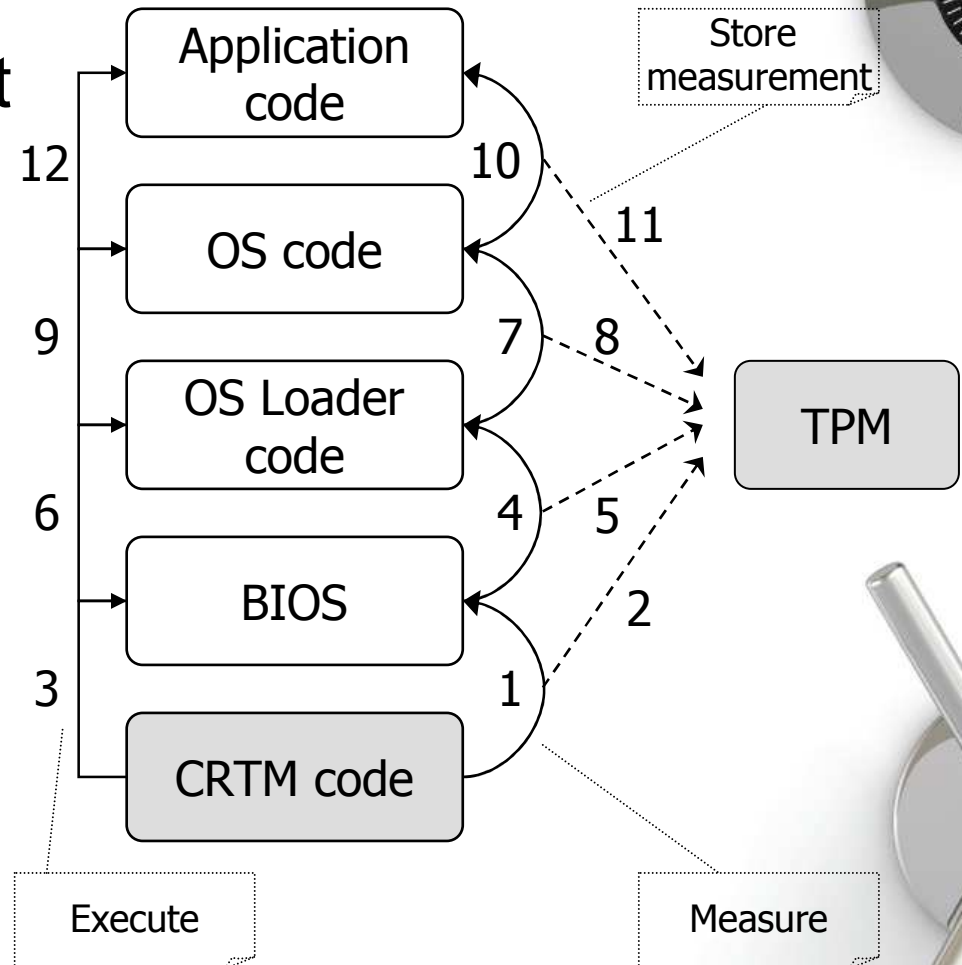
Trusted Platform Module (TPM)

- Due versioni
 - 1.1b: obsoleto
 - 1.2: disponibile
- Hardware
 - Chip a basso costo ~2\$
 - microprocessore 16-bit @ 33MHz (Infineon)
- Functionalities
 - RSA 2048-bit, SHA-1
 - True Random Number Generator, ...



Catena di trust

- Trust transitivo
 - A partire da (Core) Root of Trust for Measurement
- Ogni componente
 - Carica
 - Misura
 - Esegue il componente seguente



Tecnologia: Cenni su virtualizzazione hardware

- Tecnologie per piattaforme x86
 - Intel TXT (LT)
 - AMD-V (SVM)
- Differenti stack di privilegi
 - Replica dei ring 0-3
- Partizionamento della memoria (MMU)
- Partizionamento I/O (IOMMU)
- Late launch (D-CRTM)

Uso combinato di Trusted Computing e virtualizzazione

- Virtualizzazione Trusted
 - Uso della virtualizzazione per sicurezza di x86
 - Idealmente sostitutivo dei tradizionali security kernels
- Per frameworks di sicurezza “general purpose”
 - Adatto per molti scenari applicativi
 - Ideally comprising all application purposes
- Utilizzato tra gli altri in progetti R&D
 - OpenTC (Open Trusted Computing)
 - EMSCB (European Multilateral Security Computing Base)

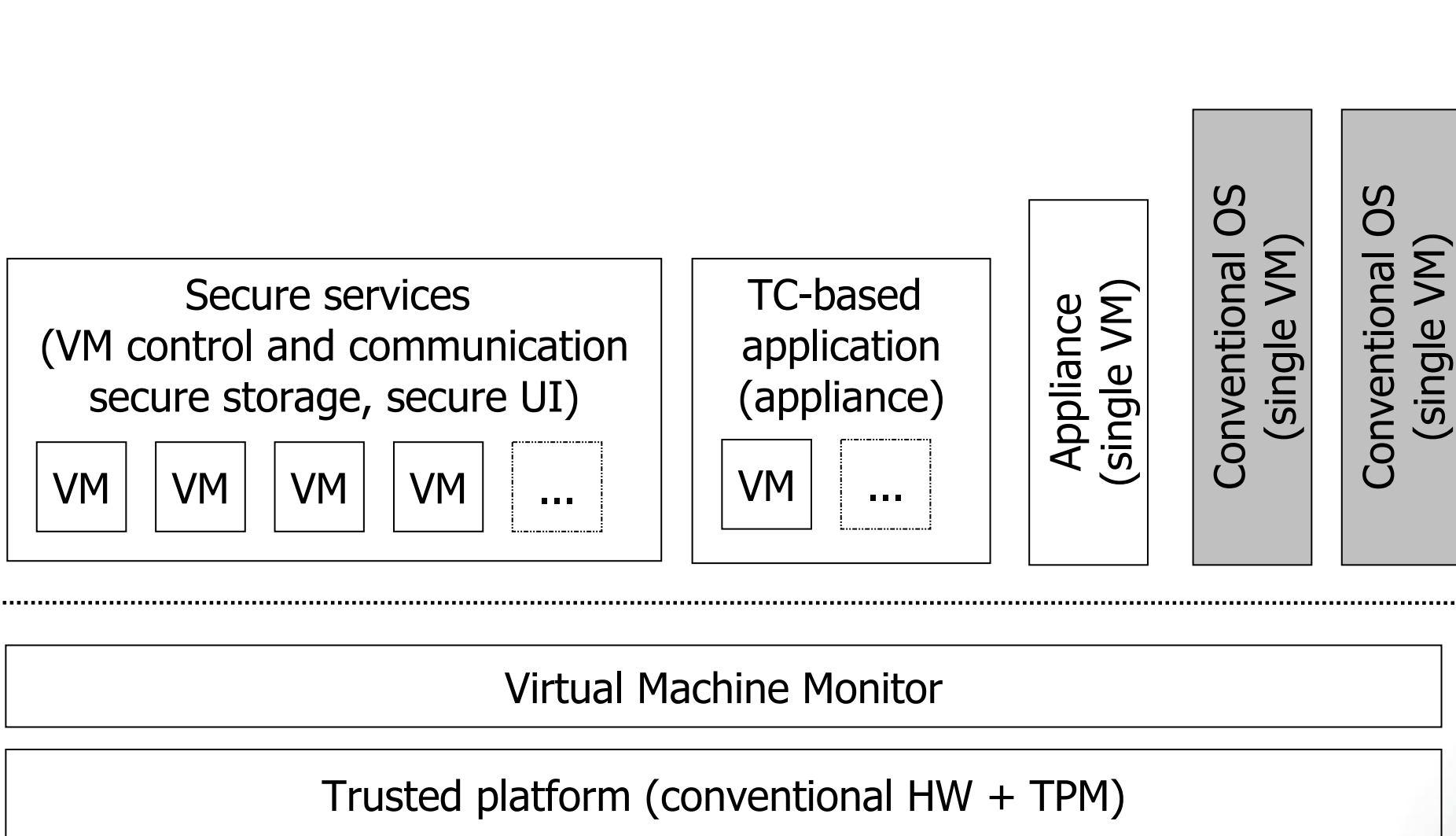


Uso combinato di Trusted Computing e virtualizzazione

- TPM usato come Root of Trust hardware
 - Molti servizi realizzati in software
- Virtualizzazione per ottenere isolamento di memoria
- Servizi di sicurezza in piccole macchine virtuali: Secure GUI, Secure Storage, Virtual TPMs, ...
 - Possono essere misurate (trusted)
 - Insieme al Virtual Machine Monitor (VMM) formano il Trusted Computing Base (TCB)
- Anche applicazioni utente critiche per la sicurezza possono essere isolate in VM e misurate
 - Le comunicazioni tra VM sono soggette a politiche di controllo di flusso di informazioni gestite dal VMM



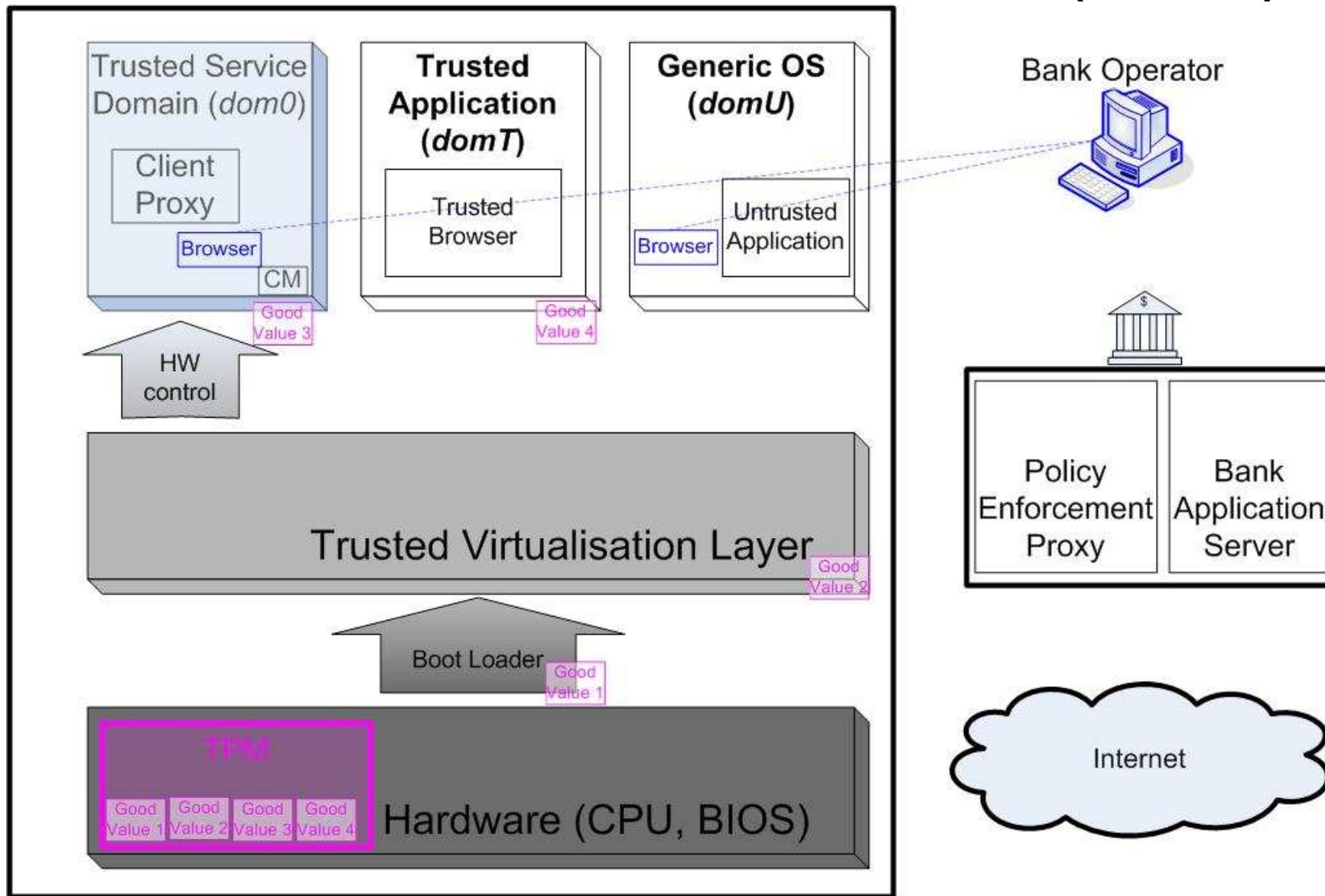
Framework di sicurezza



Hypervisor progettati per la sicurezza: esempi

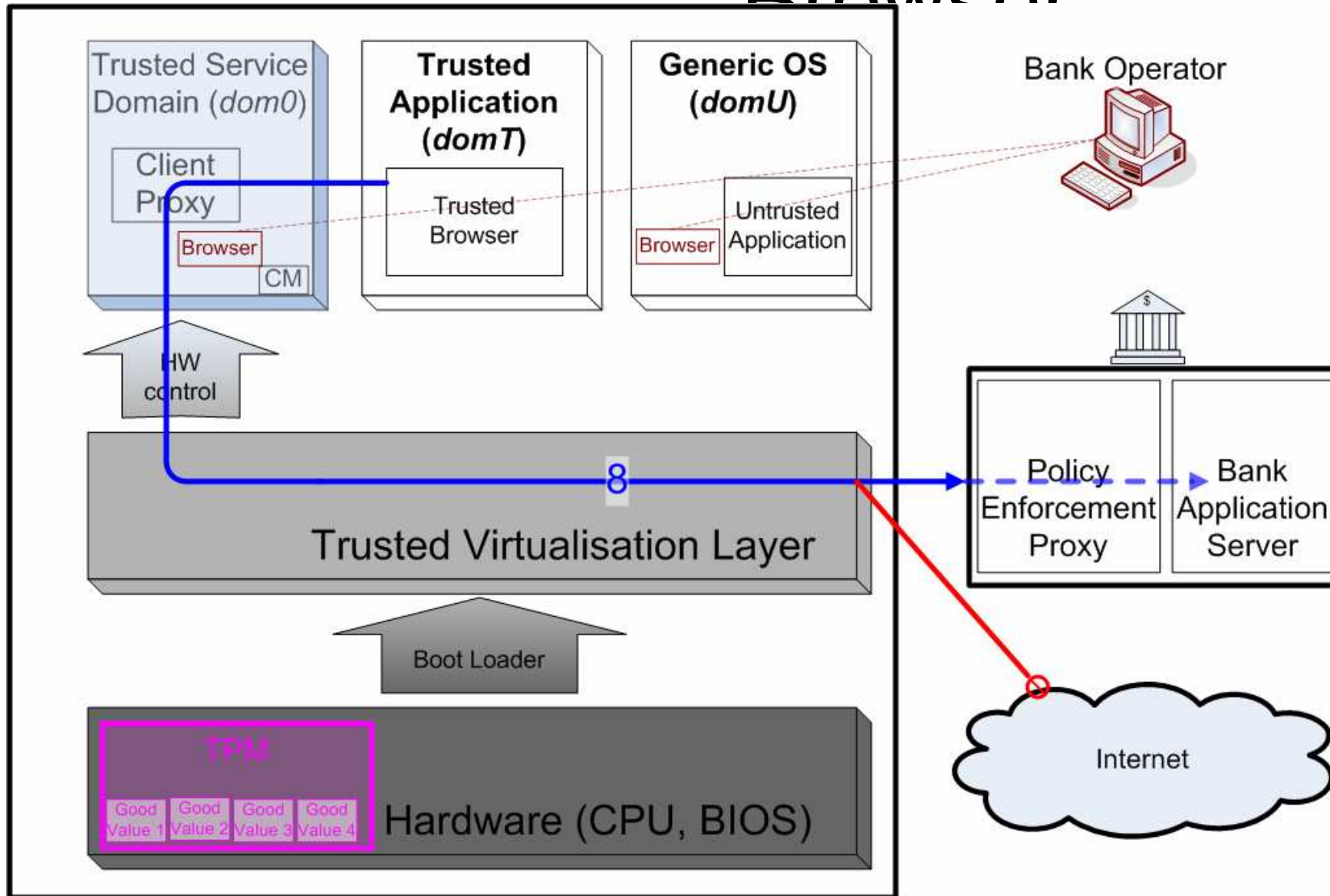
- Correttezza dell'hardware e del VMM sono requisiti essenziali per la virtualizzazione trusted
- Estensioni per Xen
 - OS Library: libreria per macchine virtuali minimali
- Microkernel (famiglia L4)
 - seL4: formalmente verificato

Private Electronic Transactions (PET)

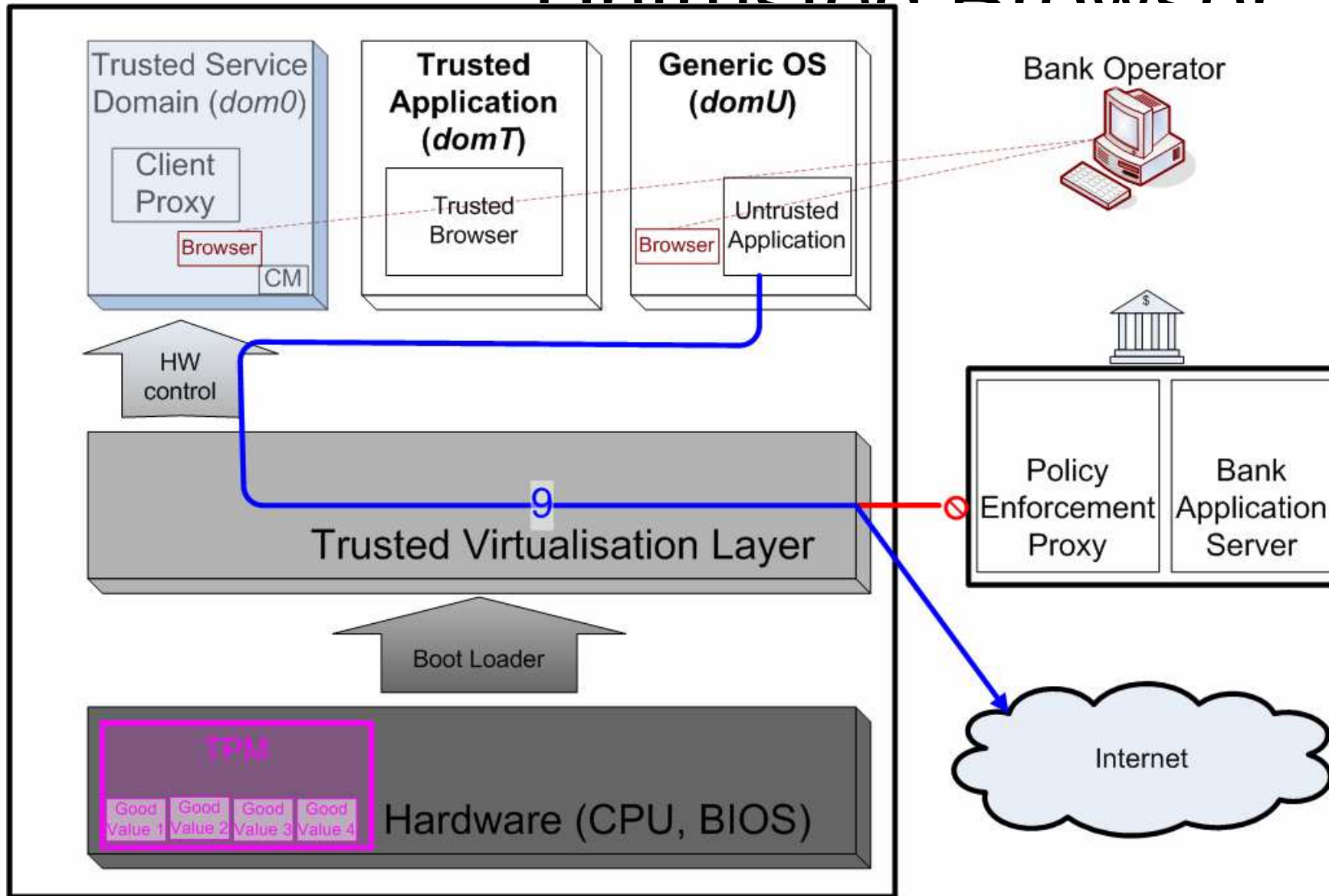


Transactions (PET) - Trusted

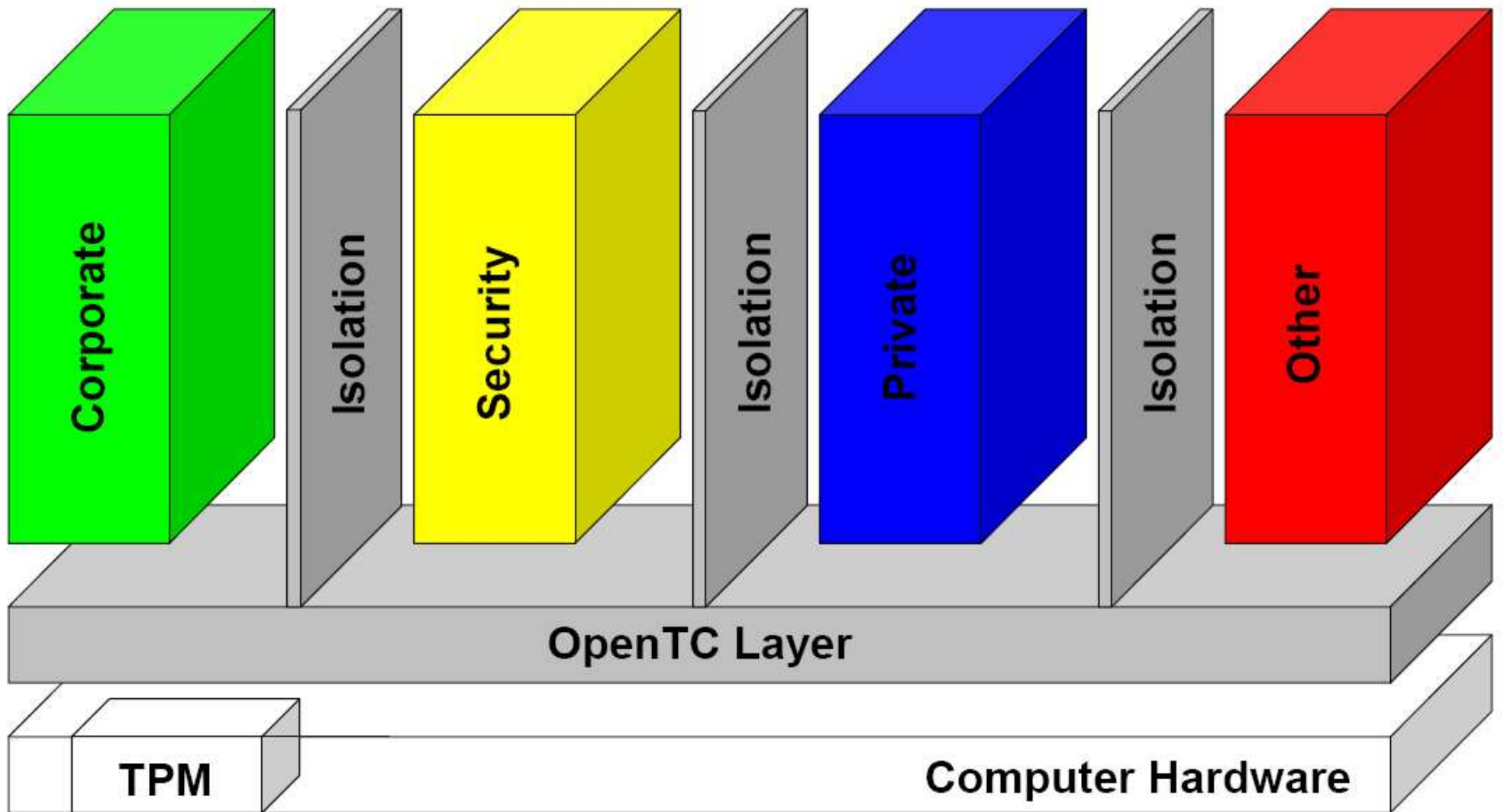
Browser



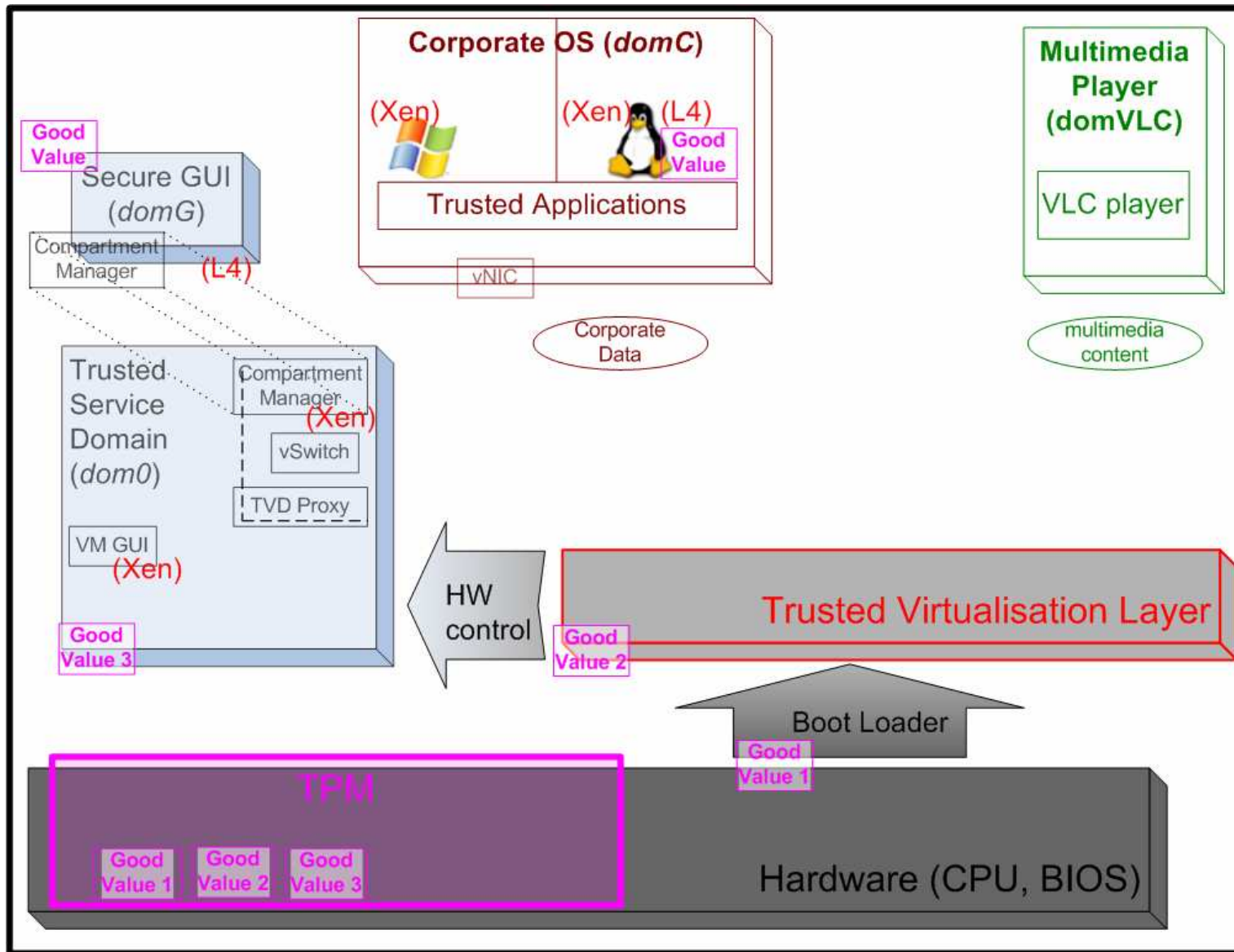
Private Electronic Transactions (PET) - Trusted Browser



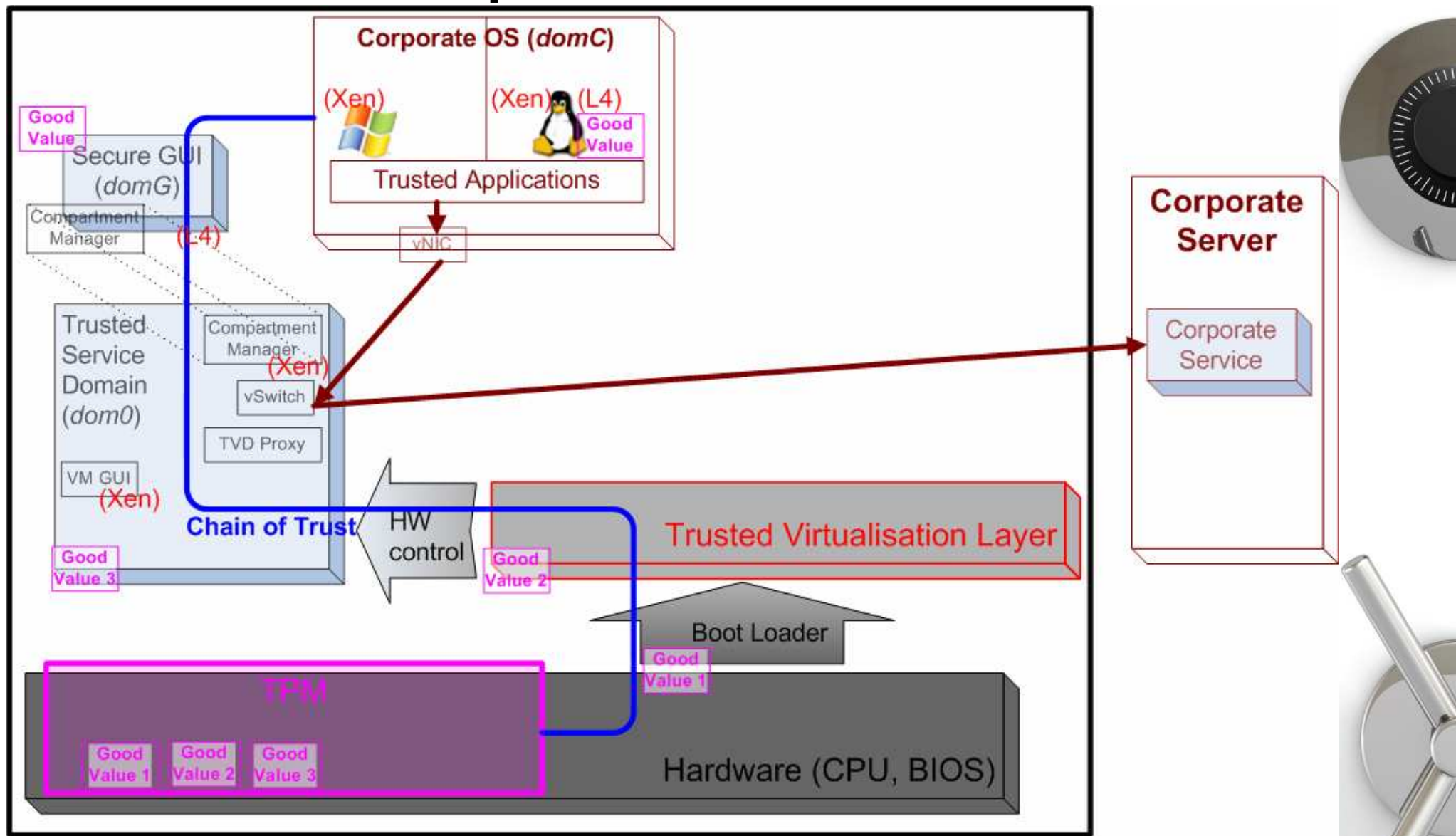
Corporate Computing at Home (CC@H)



CC@H: high-level architecture



CC@H: Trusted Access to the Corporate Service



CC@H: OpenTC taskbar

- Icona di controllo
 - Conosciuta solo dall'utente legittimo
 - Non fornita con la distribuzione
 - sealed (cioè cifrata) in relazione ad una buona configurazione di sistema "good"
 - Se l'operazione di unsealing fallisce al boot, questo significa che la configurazione del sistema è cambiata



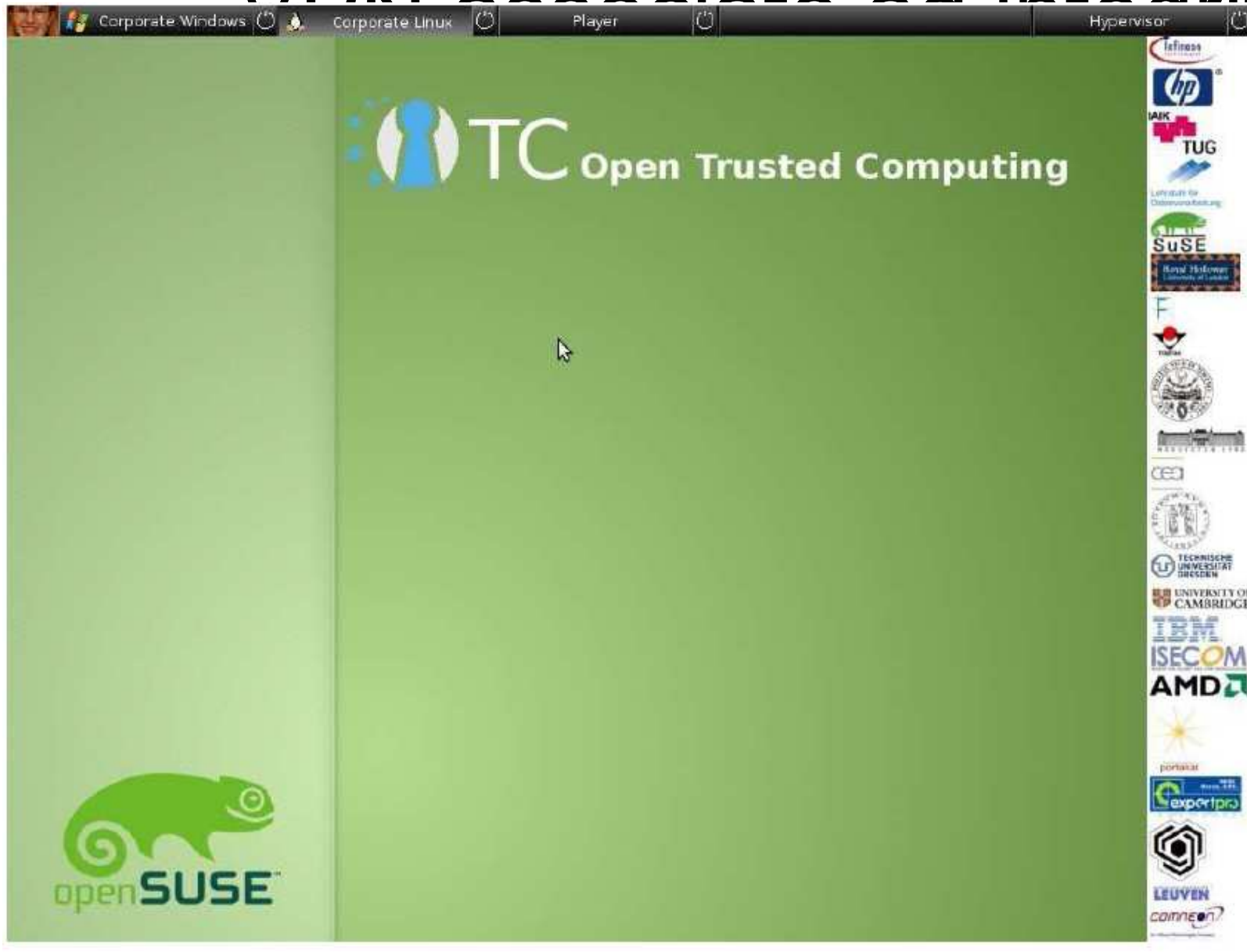
Compartment con standard

VPN software

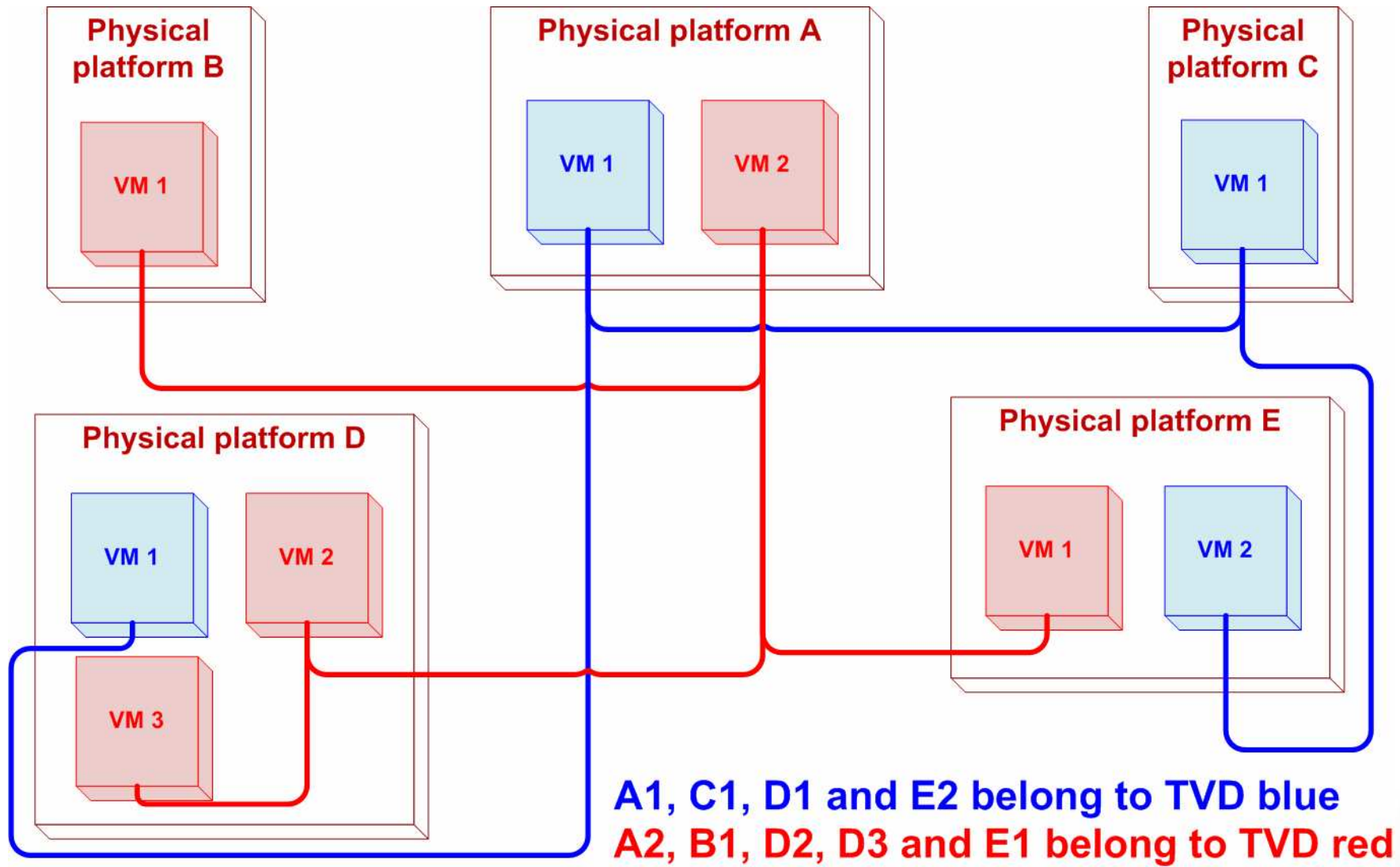


Corporate Compartment con OpenTC

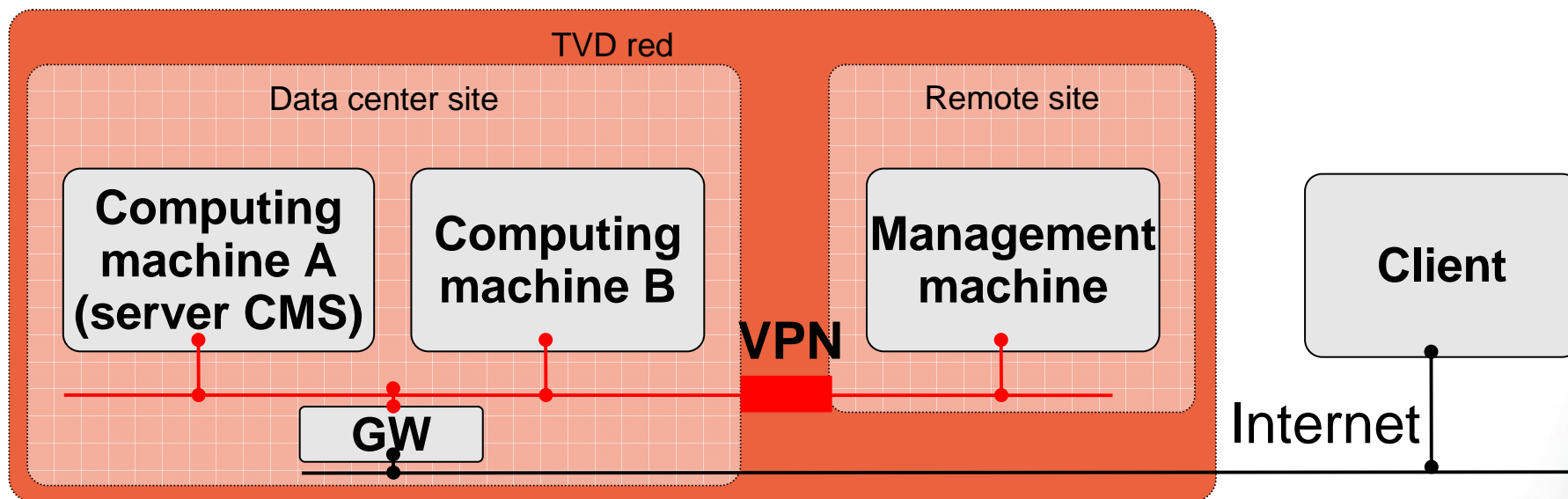
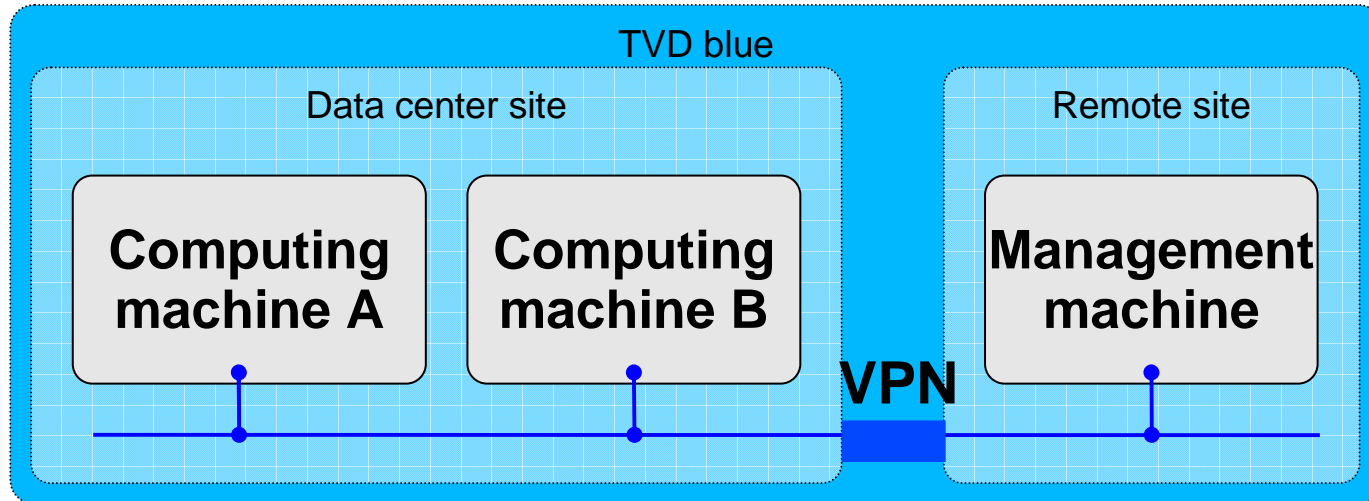
VPN associata ed integrità



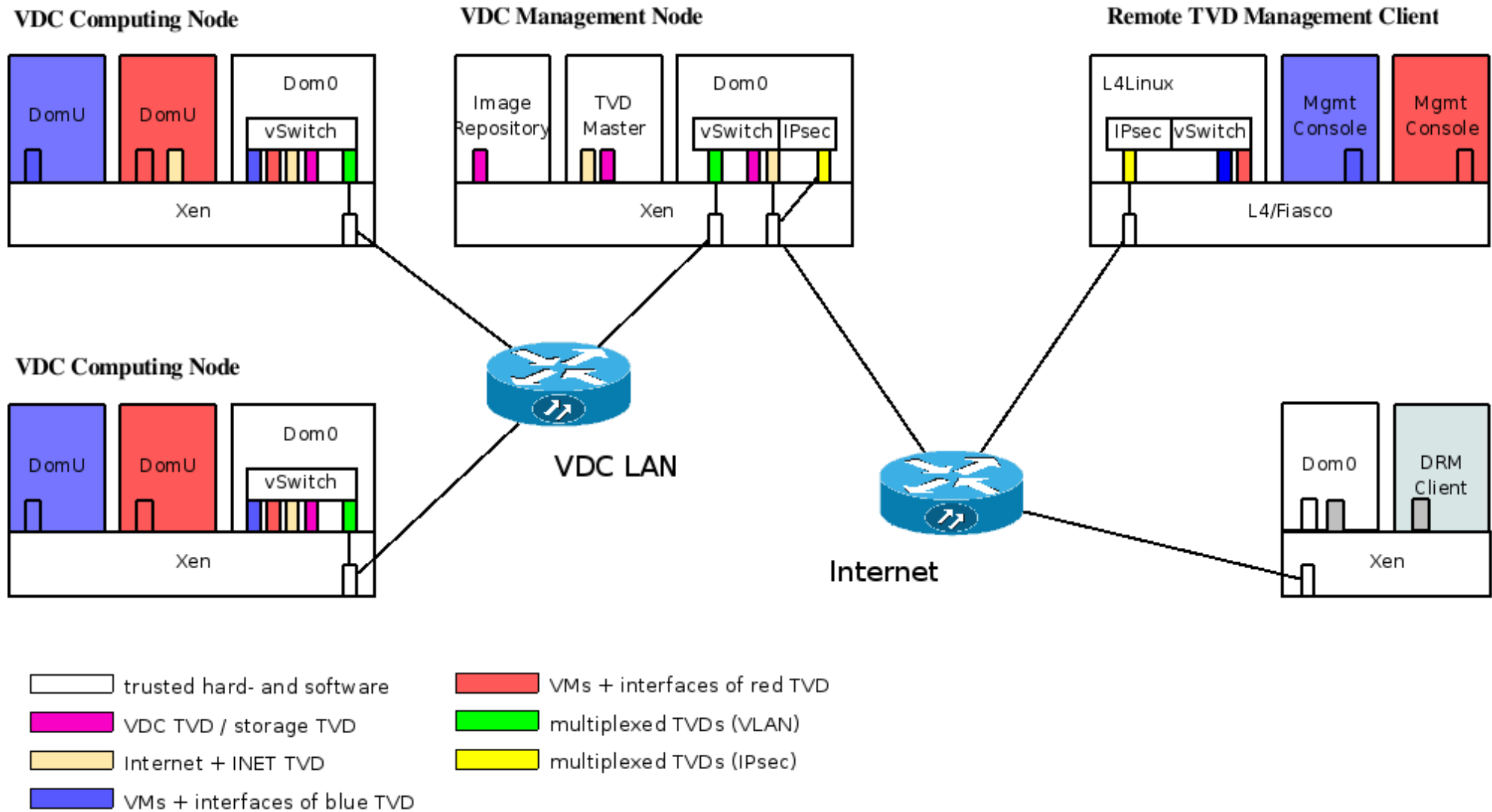
Concetto di Trusted Virtual Domain



Virtual Data Centers (VDC)



VDC: Layout Fisico del Data Center



Grazie per l'attenzione

- Domande?

