Trusted Infrastructure Cloud

Norbert Schirmer (Sirrix AG)

Trustworthy Cloud Workshop

ESORICS 2013, London

Trust in Clouds

- Outsourcing of ressources (computing, network, storage) to cloud provider
- Pay-per-use
- Scalability

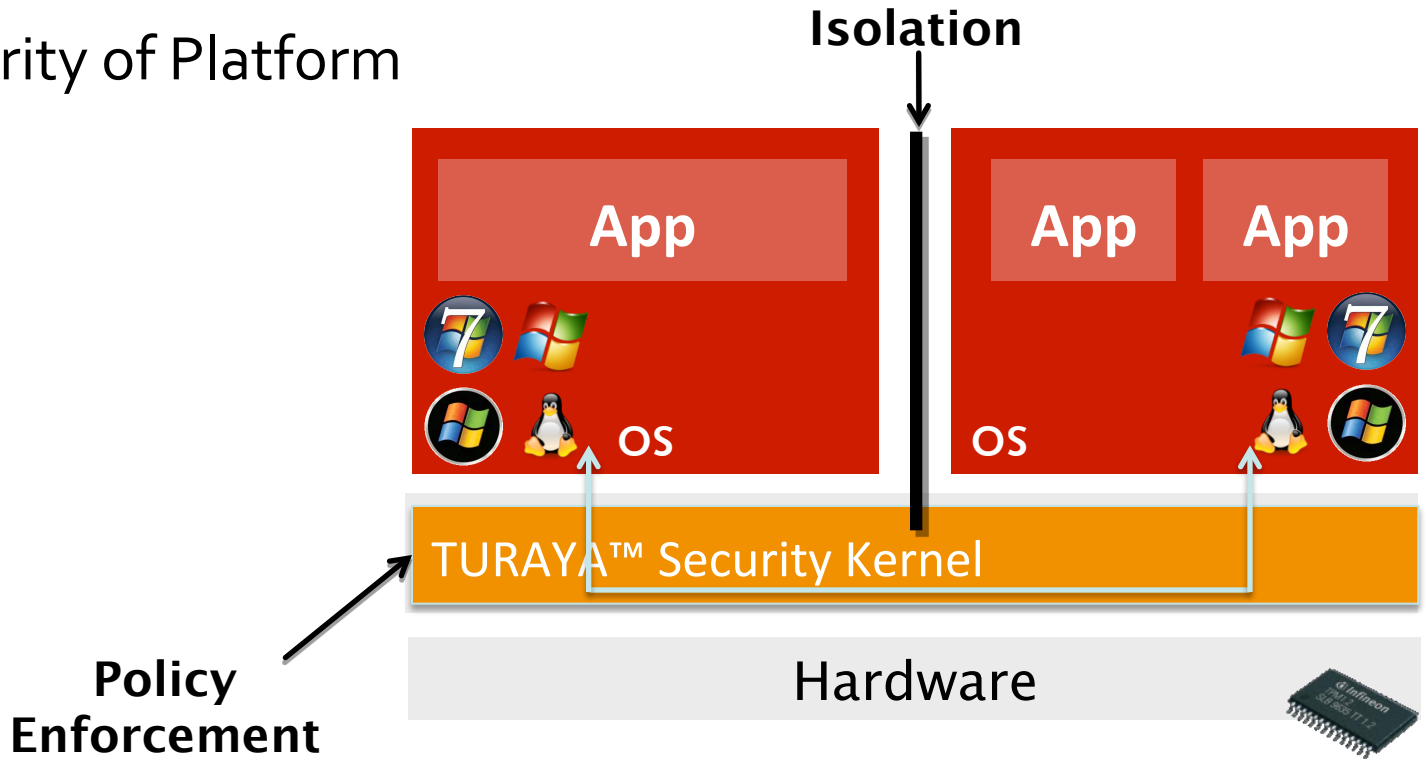
- ***Shared responsibility*** between cloud customer and cloud provider
- How to gain trust in cloud ressources?

TrustedInfrastructure Cloud

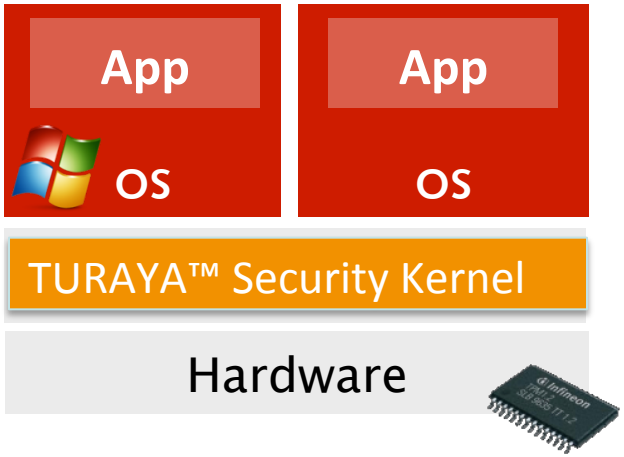
- **Trust in remote resources:** built on top of Trusted Computing technologies
  - Integrity ensured by hardware anchor, trusted boot, security kernel, remote attestation
- **Protection against insider attacks:** administration is controlled by infrastructure
  - No administrators with elevated privileges
- **Separation of tenants:** Trusted Virtual Domains (TVD)
  - Trustworthy isolation of computing / storage / networking

TrustedServer: Security Kernel

- Isolation and Virtualisation
- Trusted Virtual Domains
- Integrity of Platform

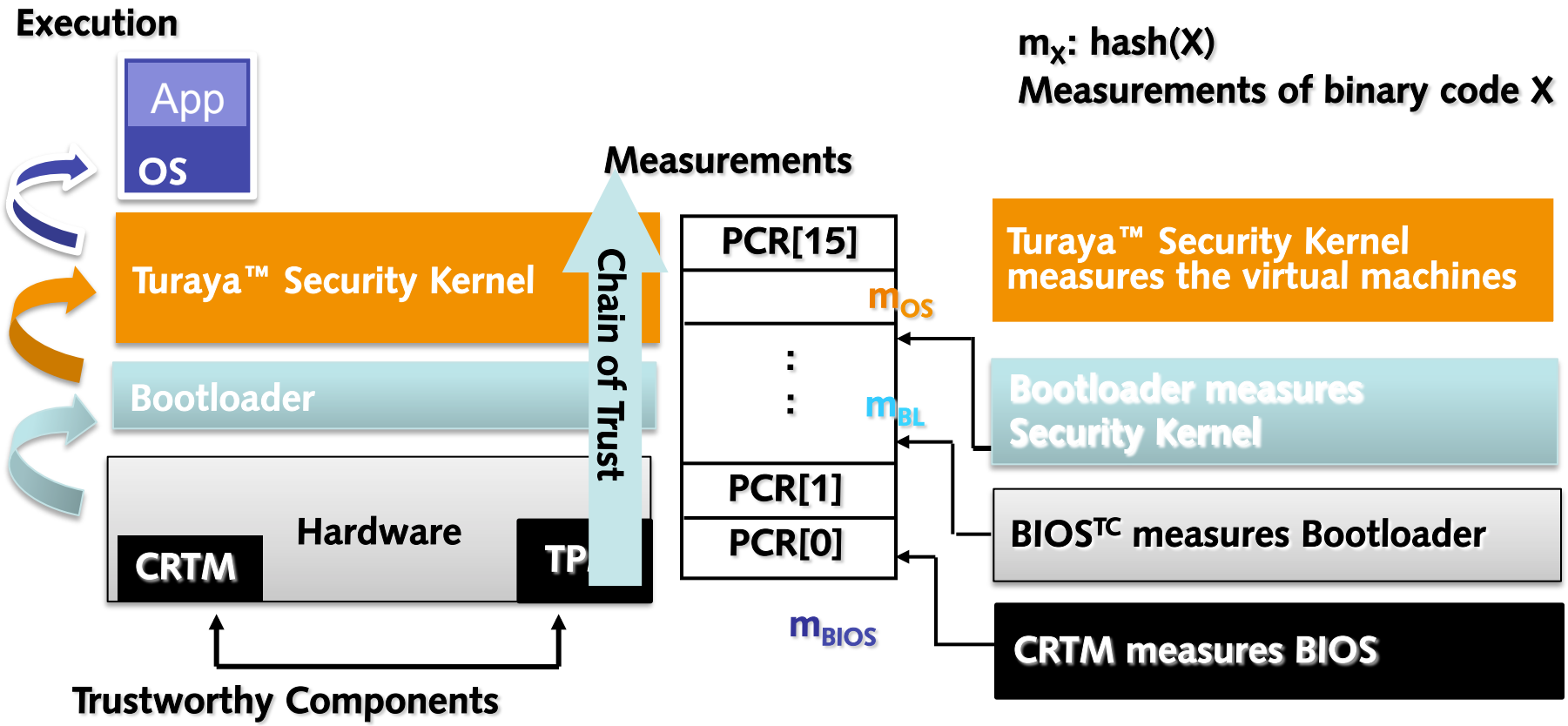


Ensuring Integrity



- Essential Preconditions
  - Tamper Proof Hardwaremodule
  - Integrity during boot
- Integration into Infrastructure
  - Remote Attestation
    - Trustworthy integrity for remote ressources
    - Communication only between trustwortyh systems
    - Isolation of faulty / malicious systems
  - Secure Binding
    - Binding of boot process to trusted configuration
    - Only untampered security kernel is booted

Chain of Trust

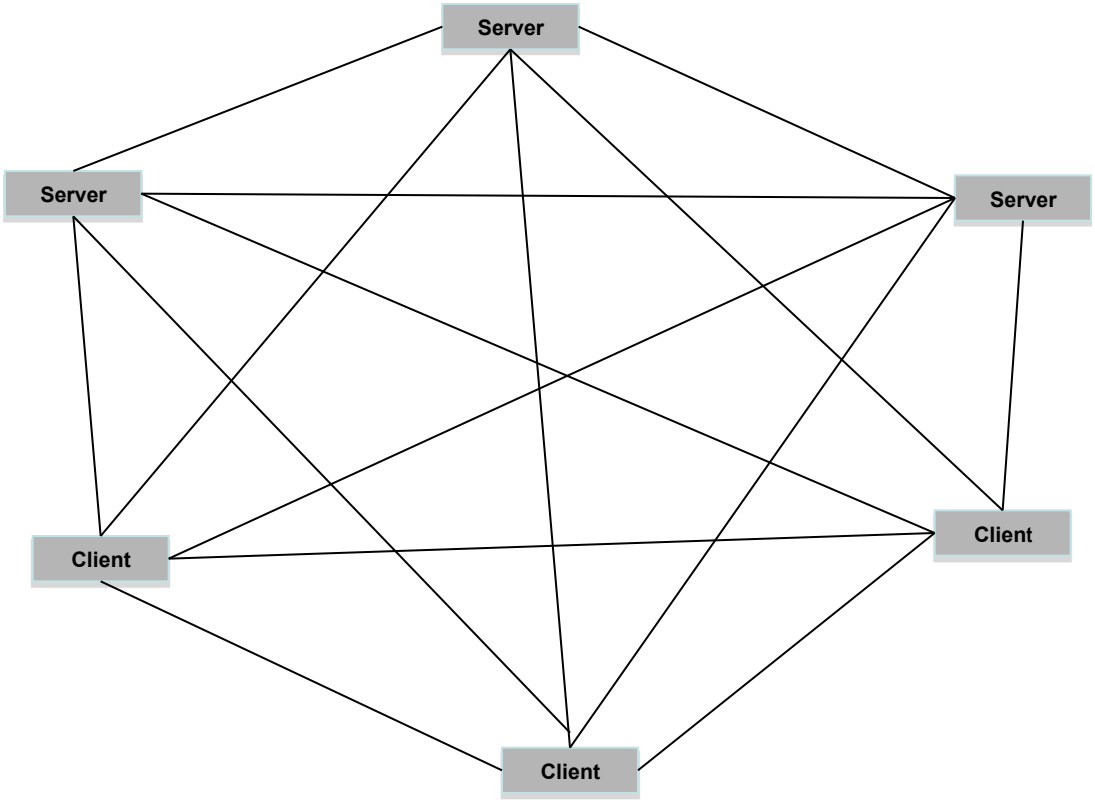


Core Root of Trust for Measurement (CRTM)
Trusted Platform Module (TPM)

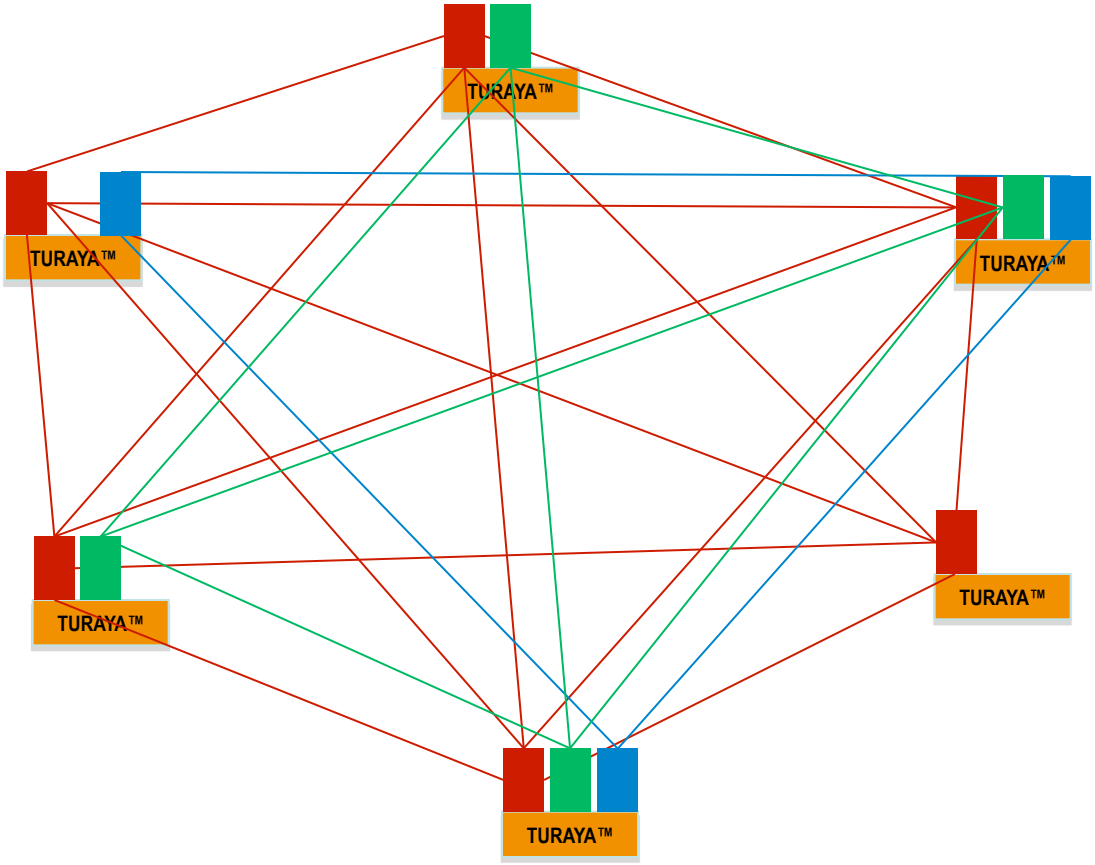
Trusted Virtual Domains (TVD)

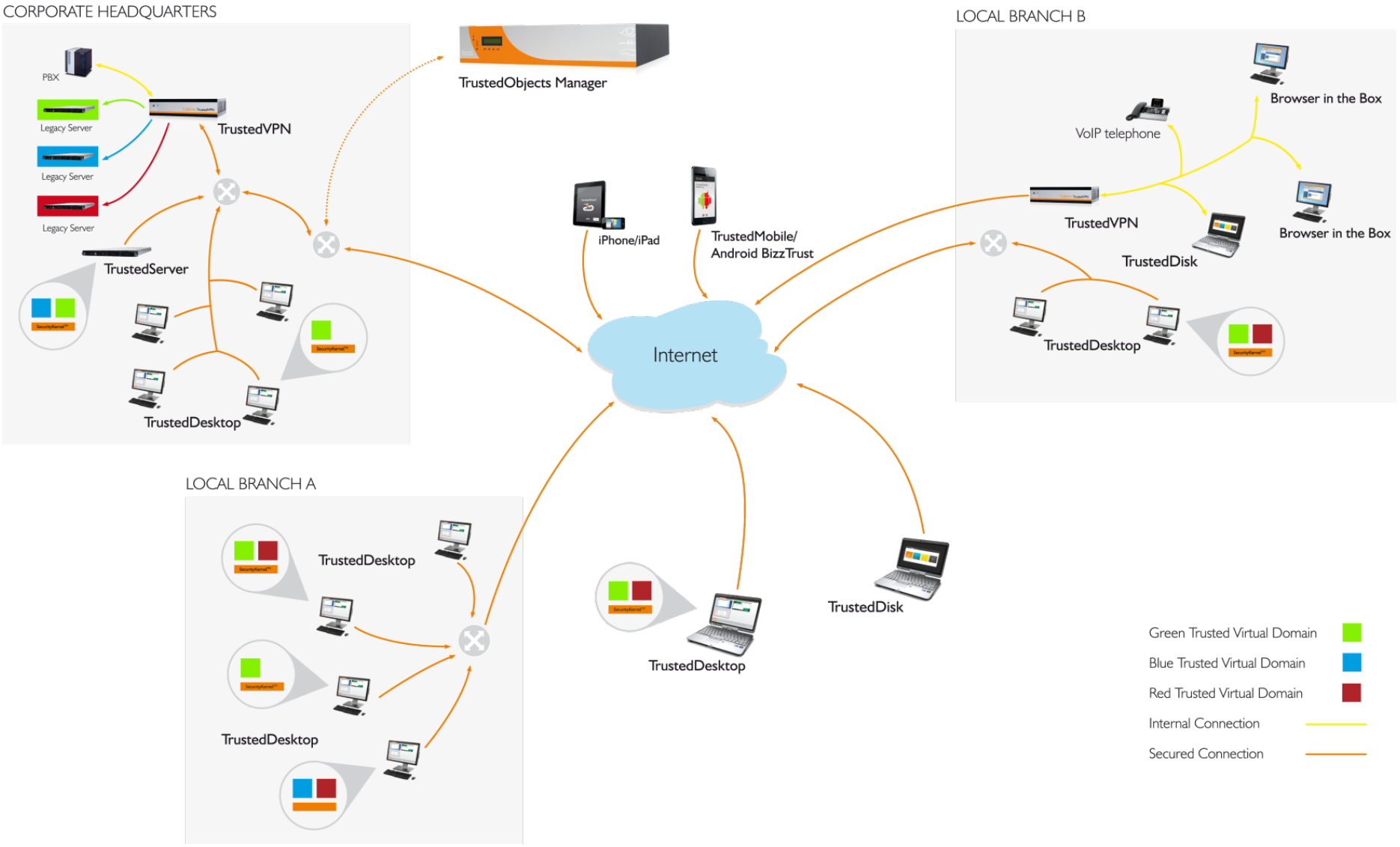
- Core concept for
  - Simple but pervasive **information flow control**
  - Trustworthy isolation of shared computing / storage / networking resources
- Association of compartments (VMs) with security domains
  - Direct information flow only within same TVD
  - Control of all interfaces between TVDs
  - Used to separate tenants, but can also be used to separate security domains of a single tenant

TVD: Physical Network Layer



TVD: VPN-based Virtual Network Layers




CORPORATE HEADQUARTERS
PBX
Legacy Server
Legacy Server
Legacy Server
TrustedVPN
TrustedServer
TrustedDesktop
TrustedObjects Manager
iPhone/iPad
TrustedMobile/
Android BizzTrust
Internet
LOCAL BRANCH B
Browser in the Box
VoIP telephone
TrustedVPN
Browser in the Box
TrustedDisk
TrustedDesktop
LOCAL BRANCH A
TrustedDesktop
TrustedDesktop
TrustedDesktop
TrustedDisk
Green Trusted Virtual Domain
Blue Trusted Virtual Domain
Red Trusted Virtual Domain
Internal Connection
Secured Connection

Workflow Illustration

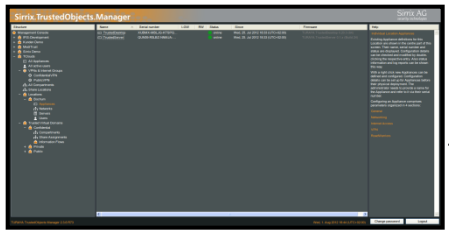
Step 1: Trusted Boot

TURAYA™ Security Kernel

TrustedServer

TURAYA™ Security Kernel

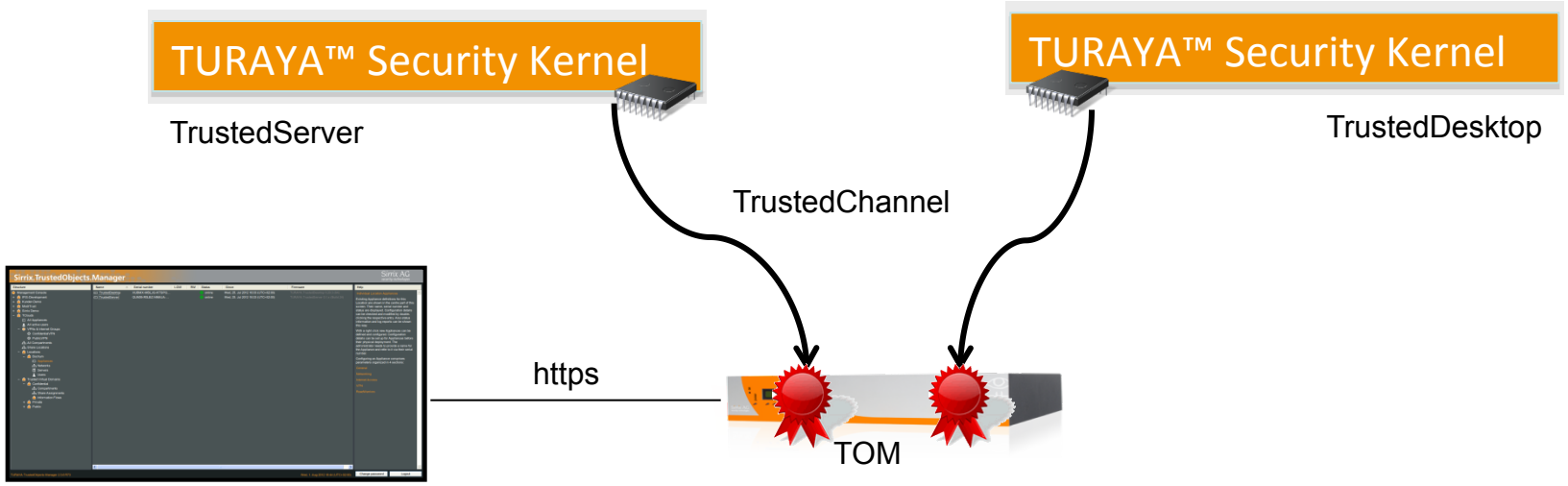
TrustedDesktop



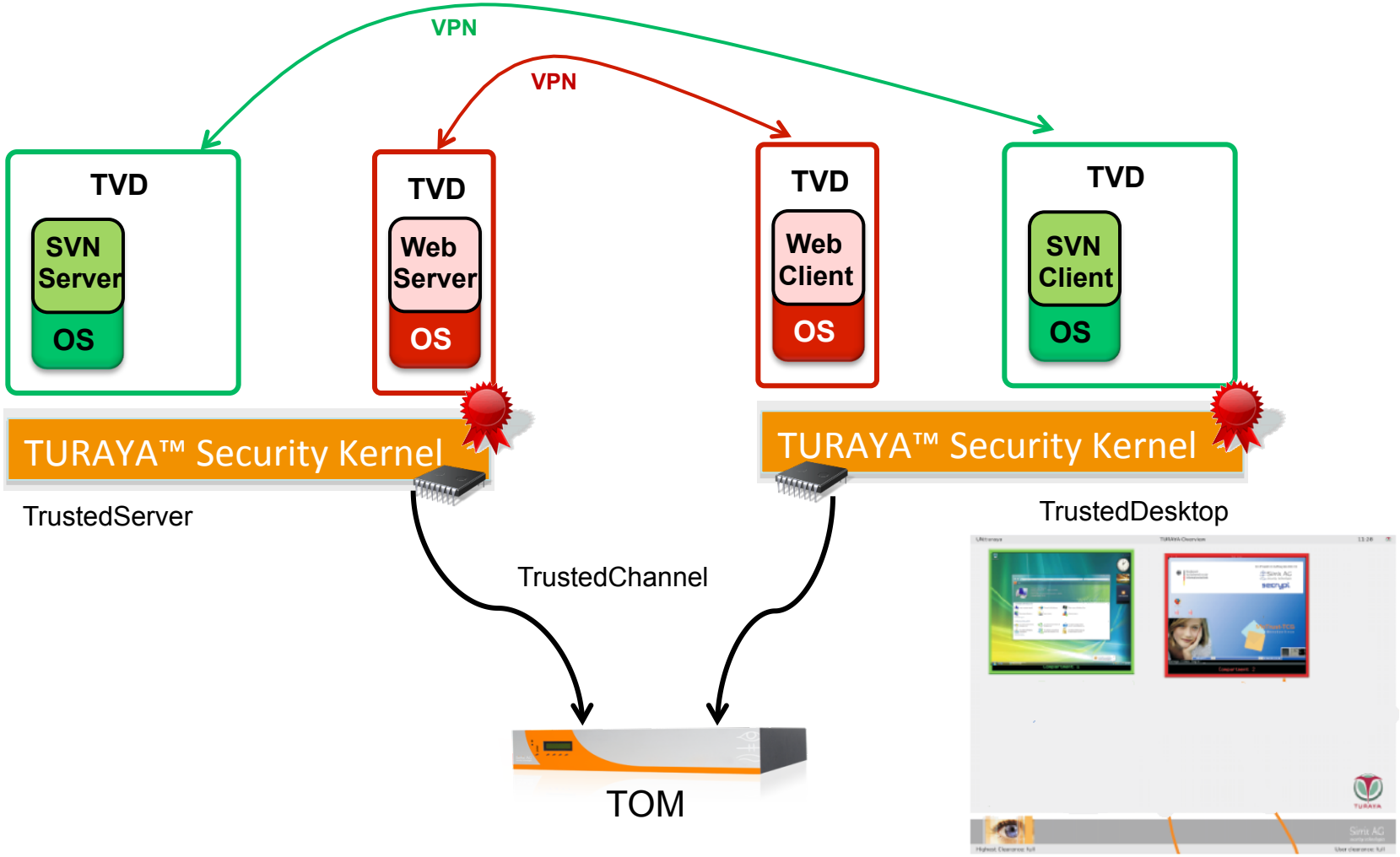
https

TOM

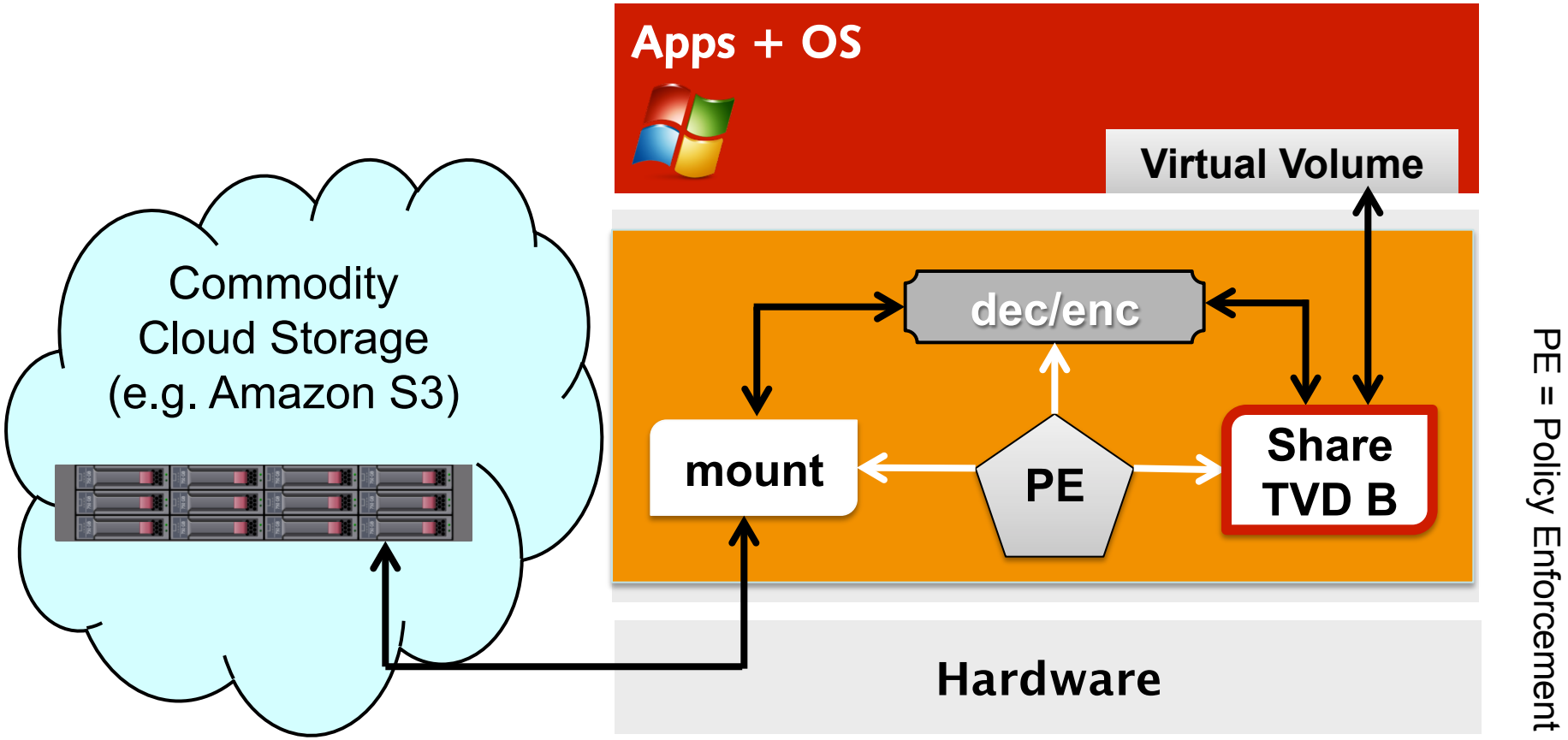
Step 2: TrustedChannel & Remote Attestation



Step 3: Start Compartments



Integration of Commodity Cloud Storage



Conclusion

- Establish trust in remote resources by Trusted Computing technologies
  - Hardware trust anchor
  - Trusted boot ensures integrity
  - Security kernel
- Protection against insider attacks
  - Automated management / maintenance via controlled remote interfaces
  - No administrators with elevated privileges
- Trusted Virtual Domains (TVD)
  - Trustworthy isolation of computing / storage / networking
  - Information flow control
  - Transparent encryption
  - VPN

TClouds EC CONTRACT No: 257243

"The TClouds project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-257243."

If you need further information, please contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a, 9500 Villach, AUSTRIA

Tel: +43 4242 233 55 Fax: +43 4242 233 55 77

E-Mail: coordination@tclouds-project.eu