Sirrix AG
security technologies

Trusted Clouds: Chances for Security, Resilience and Scalability

Since Successful Business needs Trustworthy Solutions.

Ammar Alkassar

RSA VIP Session on Cloud Security
February, 16th 2011 | RSA Conference, San Francisco

Who we are

Background:

- Roots in Cryptography and Operating Systems Security Research
- One of the technology leaders in Trusted Computing
- Based on substantial amount of own IP

Mission

Still applied approaches

- „Airbag approach":
  If it happens, it should hurt less.

Adequate approach :

- „ESP strategy": Avoid skidding,
  before it happens.

Who we are

Background:

- Roots in Cryptography and Operating Systems Security Research
- One of the technology leaders in Trusted Computing
- Based on substantial amount of own IP

Mission:

- Providing comprehensive Information Flow Control
- Seamless for the user, easy to manage and auditable

Customers:

- Strong business in Europe and Germany
- Focus on Midsize-companies, also organizations like NATO SACT, DoD and Defense Ministries of more than a dozen countries.
- OEMs: TCG, Raytheon, EADS, Wincor Nixdorf, …

Sirrix AG
security technologies

The Cloud

Thesis:

"The Cloud is a chance for improving companies' security."

- Looking at: Small and midsize companies (200-10,000 employees)
- IT-Security is an infrastructure topic, compliance nearly absent
- Information Flow control rather than traditional access control policies

- Infrastructure security as part of the service

Sirrix AG
security technologies

Requirements for Trusted Clouds

1) **Trustworthy Virtualization**
   - Strong isolation

2) **Strong Authentication**
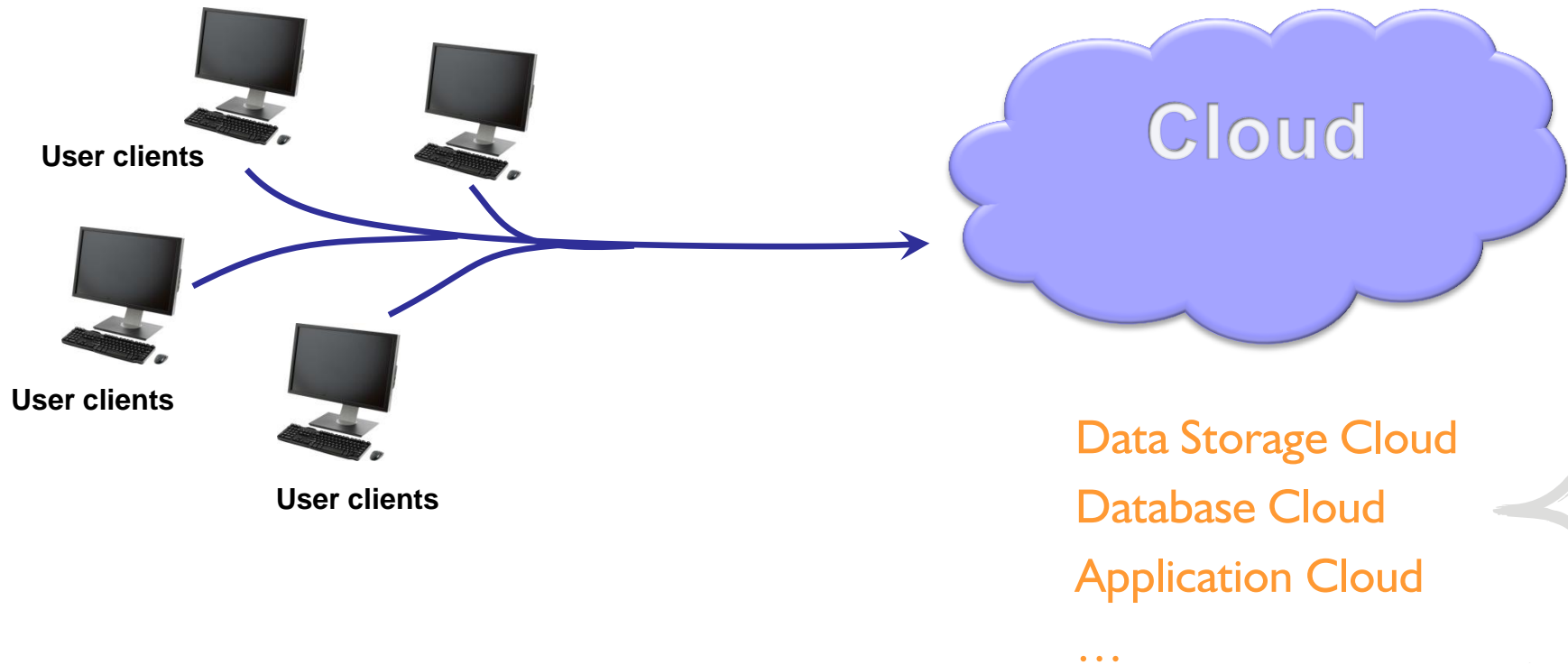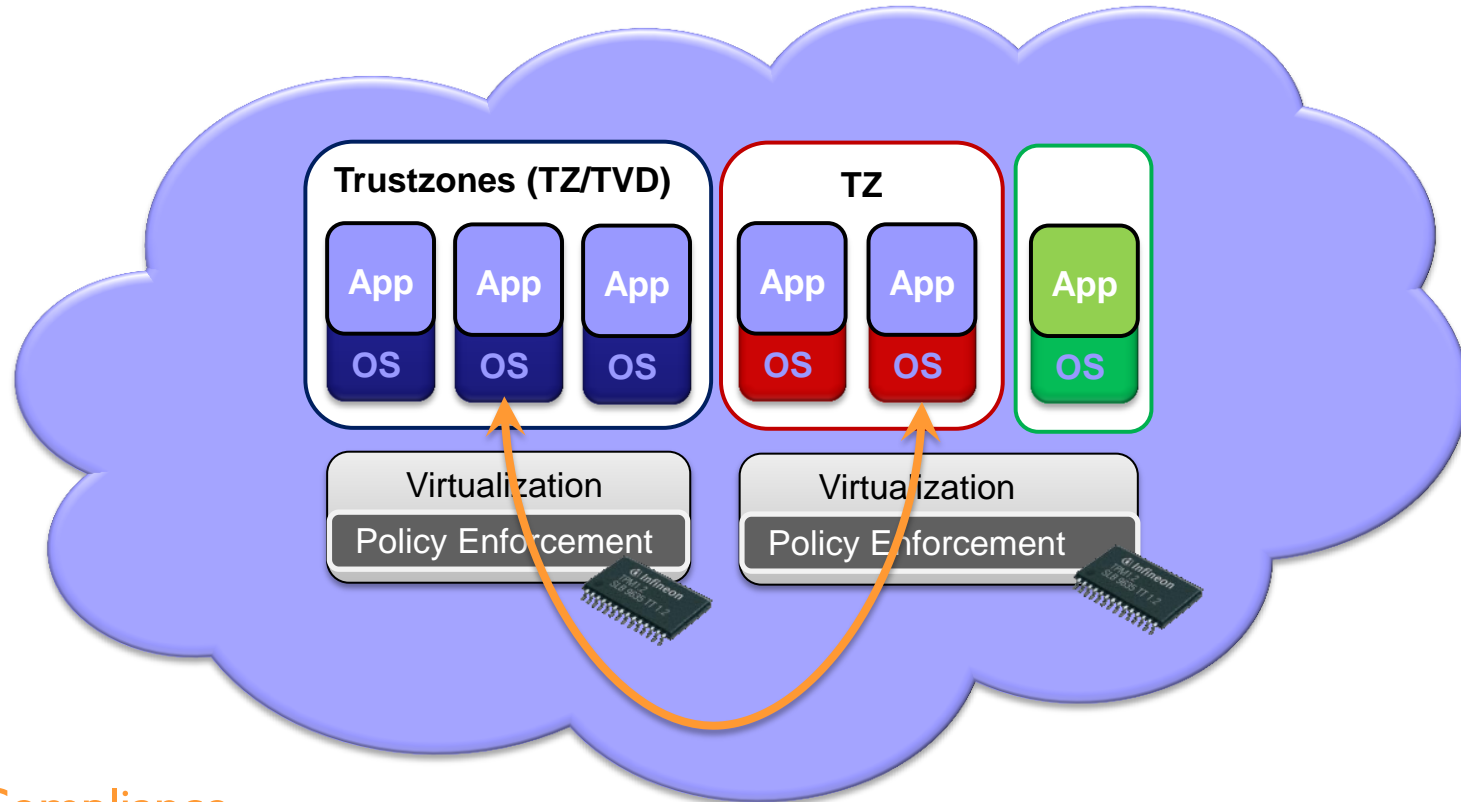   - Multi-factor, cryptographic authentication

3) **Trusted Platforms**
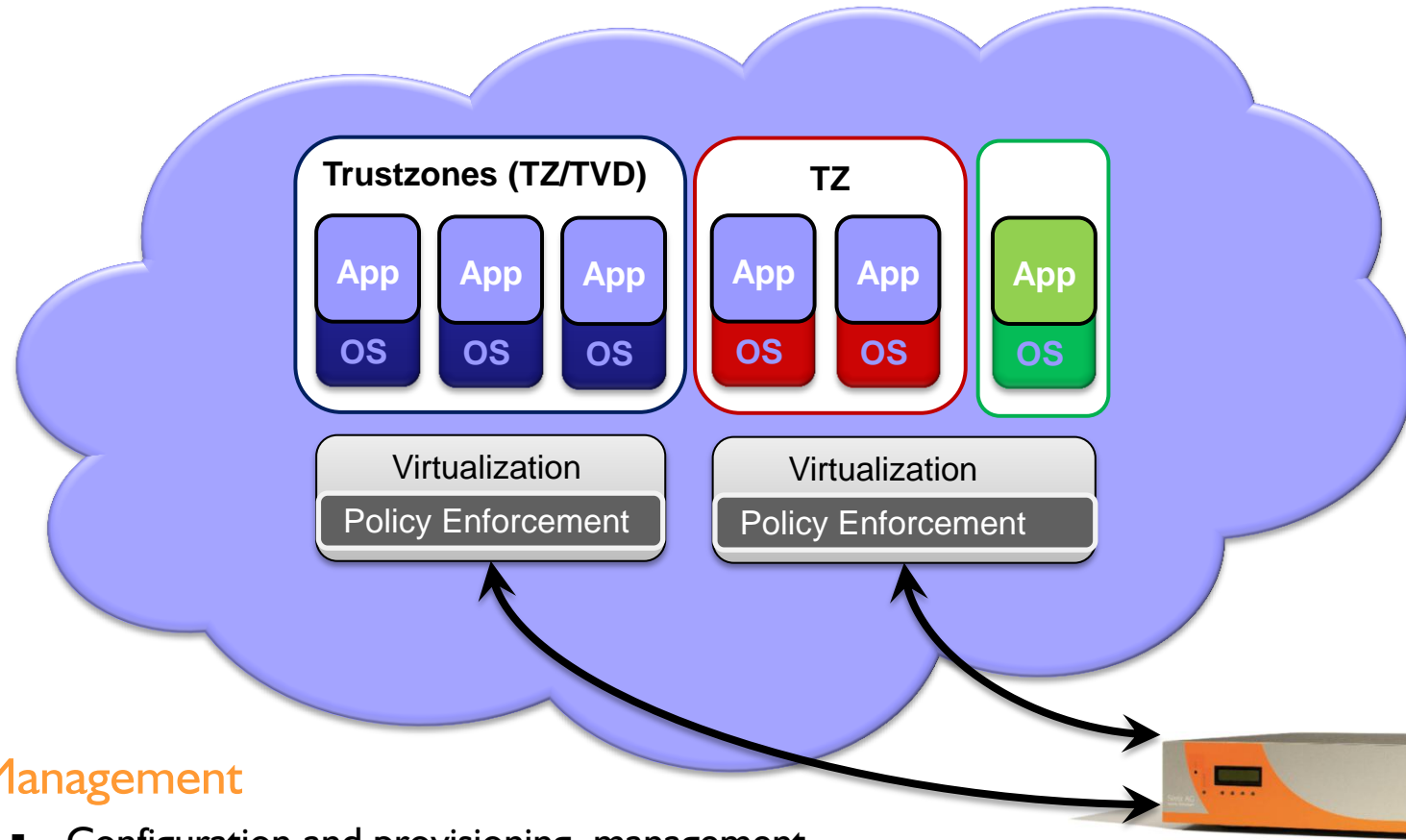   - Reliable integrity verification

Example Scenario

User clients

User clients

User clients

Cloud

Data Storage Cloud

Database Cloud

Application Cloud

…

Sirrix AG
security technologies

Trusted Cloud

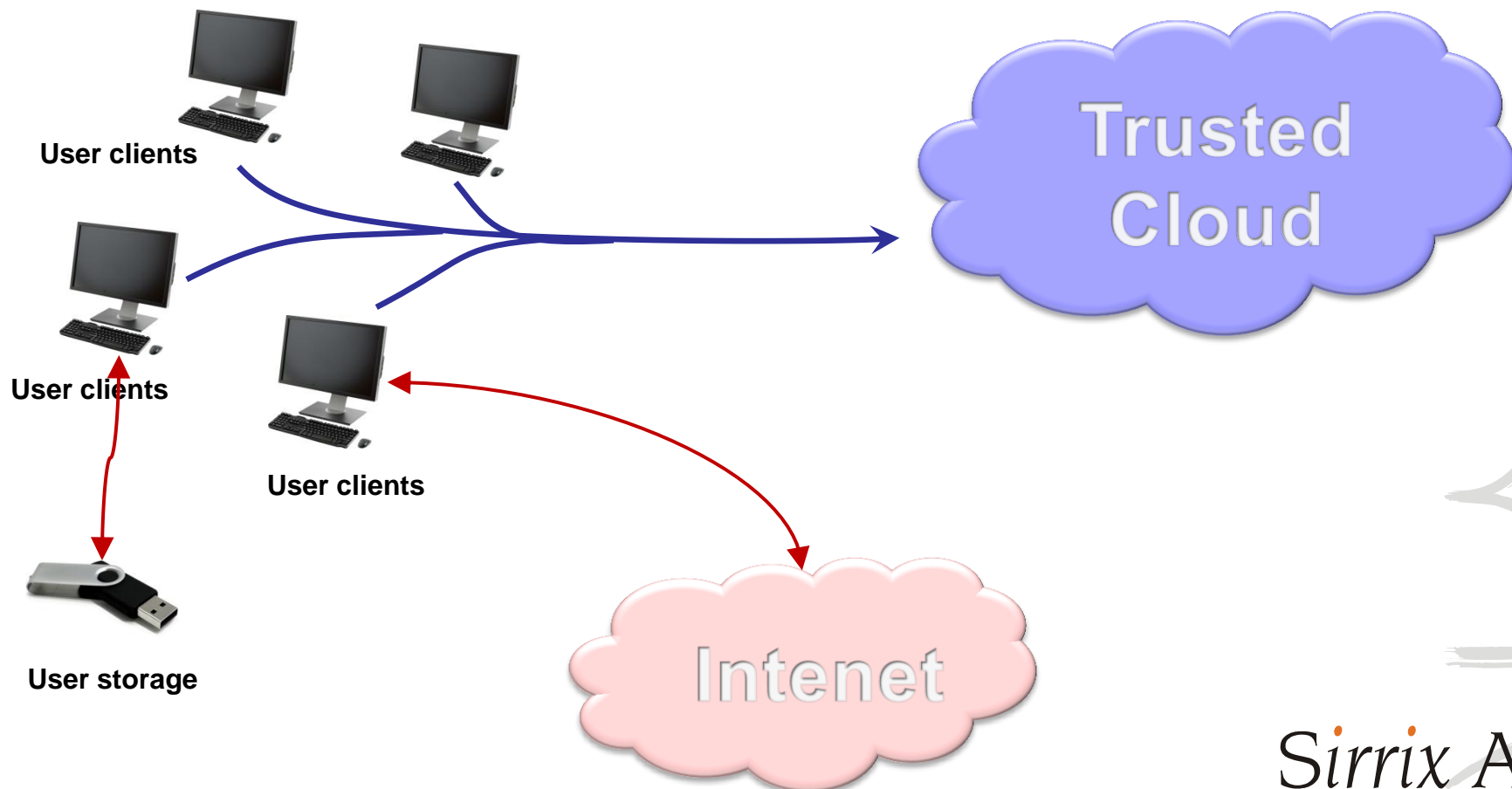## Compliance

- By audit
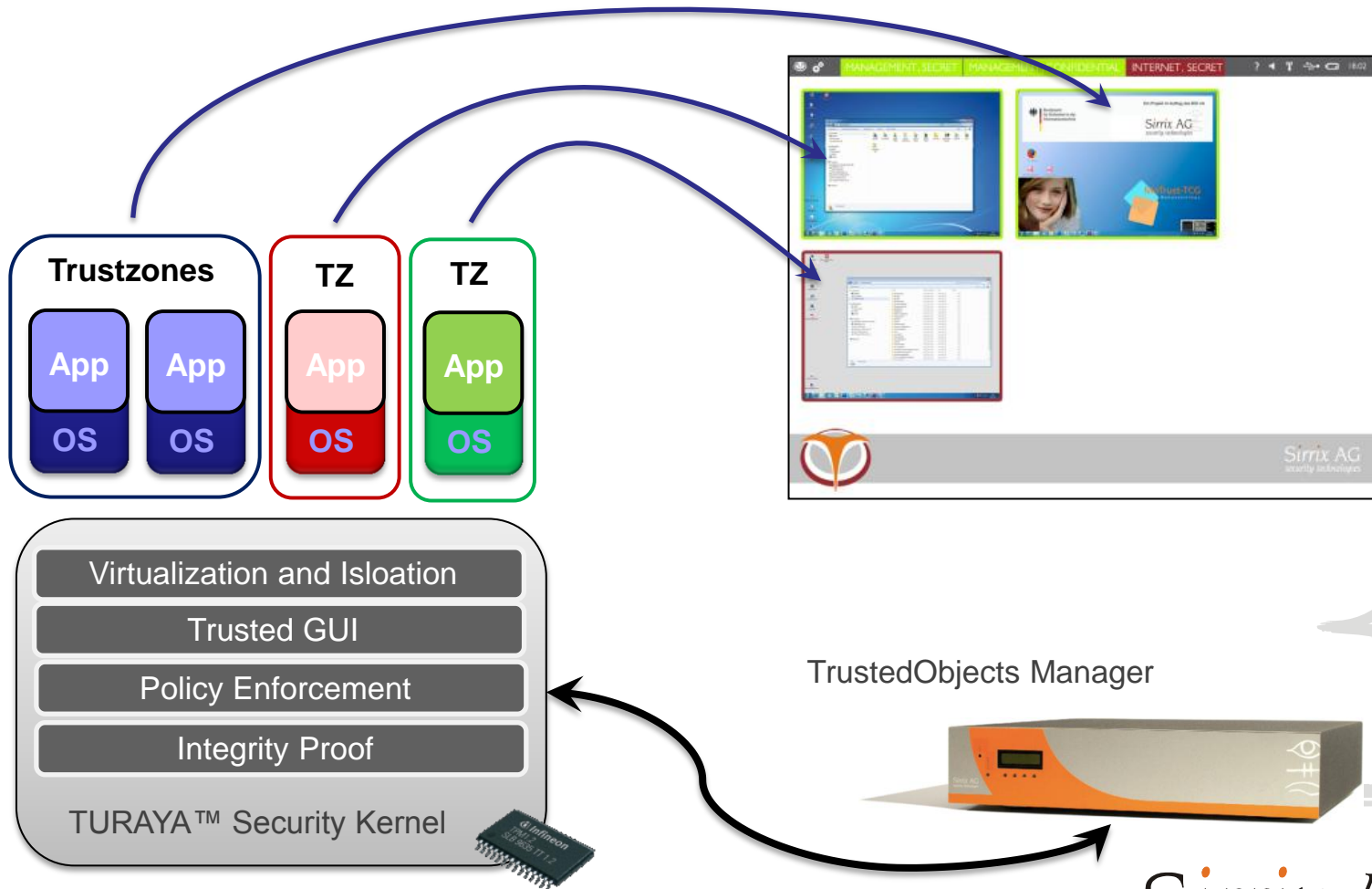- By attestation (technically)

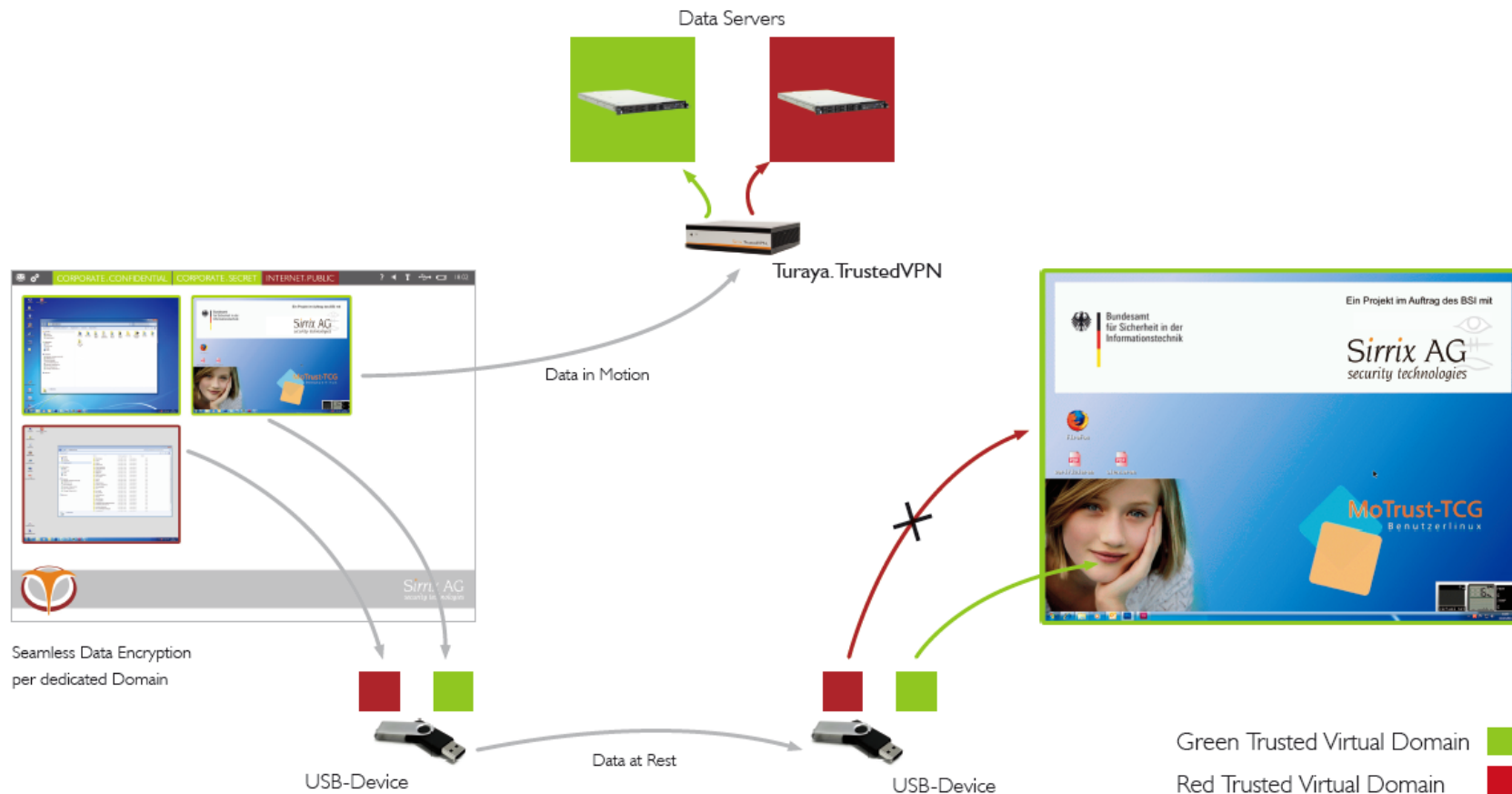# Trusted Cloud: Management

Management

- Configuration and provisioning management
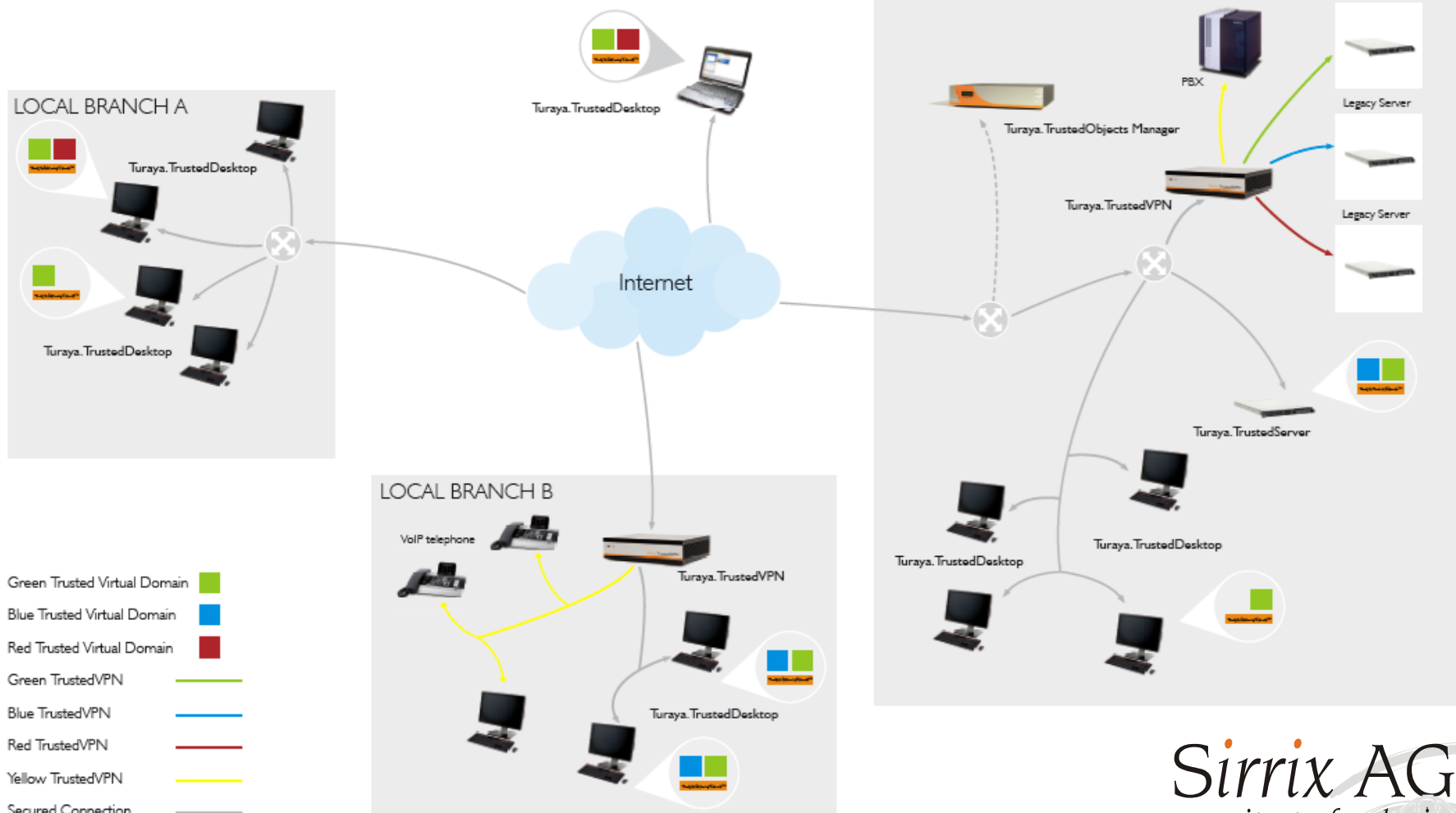- Security policy management
- Tools, e.g., RSA Archer

Back to Scenario

User clients

User clients

User clients

User storage

Trusted Cloud

Intenet

Trusted Platforms at the Endpoints

Trustzones

App | App
OS | OS

TZ

App
OS

TZ

App
OS

Virtualization and Isloation

Trusted GUI

Policy Enforcement

Integrity Proof

TURAYA™ Security Kernel

TrustedObjects Manager

Sirrix AG
security technologies

Data Servers

Turaya.TrustedVPN

Data in Motion

Seamless Data Encryption
per dedicated Domain

USB-Device

Data at Rest

USB-Device

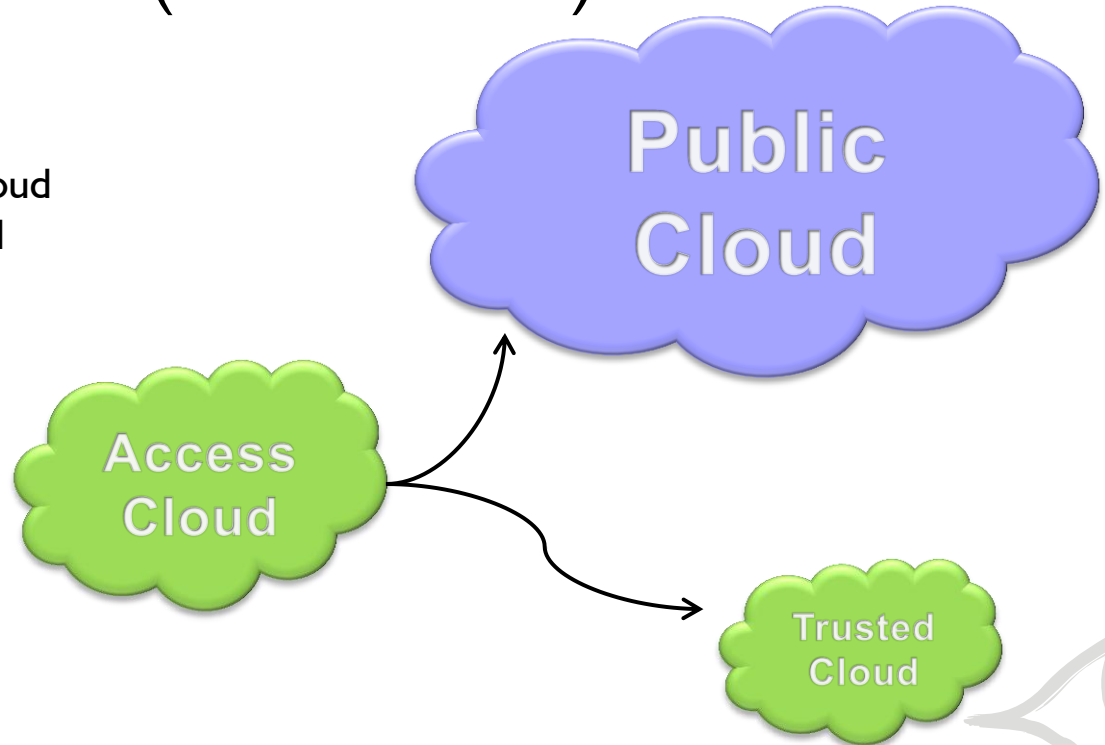Green Trusted Virtual Domain

Red Trusted Virtual Domain

Trusted Clouds – Outlook (FP7-TClouds)

Clouds of Clouds

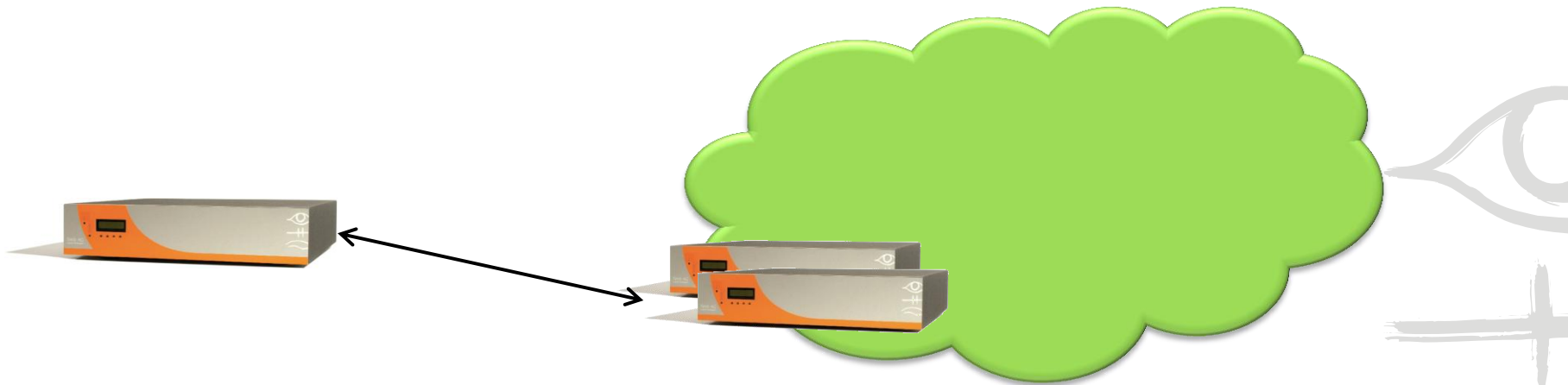- Expanding a small trusted cloud by using a larger public cloud

Trusted Clouds – Outlook

Clouds of Clouds

- Expanding a small trusted cloud
  by using a larger public cloud

Management and provisioning in the cloud

- Distributing security management to allow
  deployment inside the cloud

Trusted Clouds – Outlook

Clouds of Clouds

- Expanding a small trusted cloud
  by using a larger public cloud

Management and provisioning in the cloud

- Distributing security management to allow
  deployment inside the cloud

Mobile and autonomous entities accessing the cloud

- Concept of TZ on mobile user devices (smartphones, tablets)
- Enabling trustworthy M2M authentication
  to allow for cloud resource access

Sirrix AG
security technologies

It's your turn now . . .

Sirrix AG

Ammar Alkassar
Building D3^2
66123 Saarbrücken, Germany

Phone +49-681-95986-0
Fax +49-681-95986-500

a.alkassar@sirrix.com
http://www.sirrix.com

Sirrix AG
security technologies