

# *Practical Applications of Trusted Computing in the Cloud*

Jesus Molina

Fujitsu Laboratories of America

# Introduction

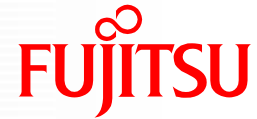
- Trusted Computing and Cloud
- Overview of Trusted Computing
- CSA guidelines and TCG standards
- Practical Application
  - Encrypted Drives
  - Trusted Network Connect
  - Metadata Access Policies
  - Trusted virtual Multitenancy

So what is the root problem of cloud security?

TRUST

- In cloud you cant verify directly the Trusted Computing Base

# TCG standards and cloud



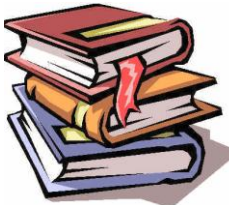
In the cloud you can

VERIFY THEN TRUST

OR

JUST TRUST

Standards



Technology



Certification

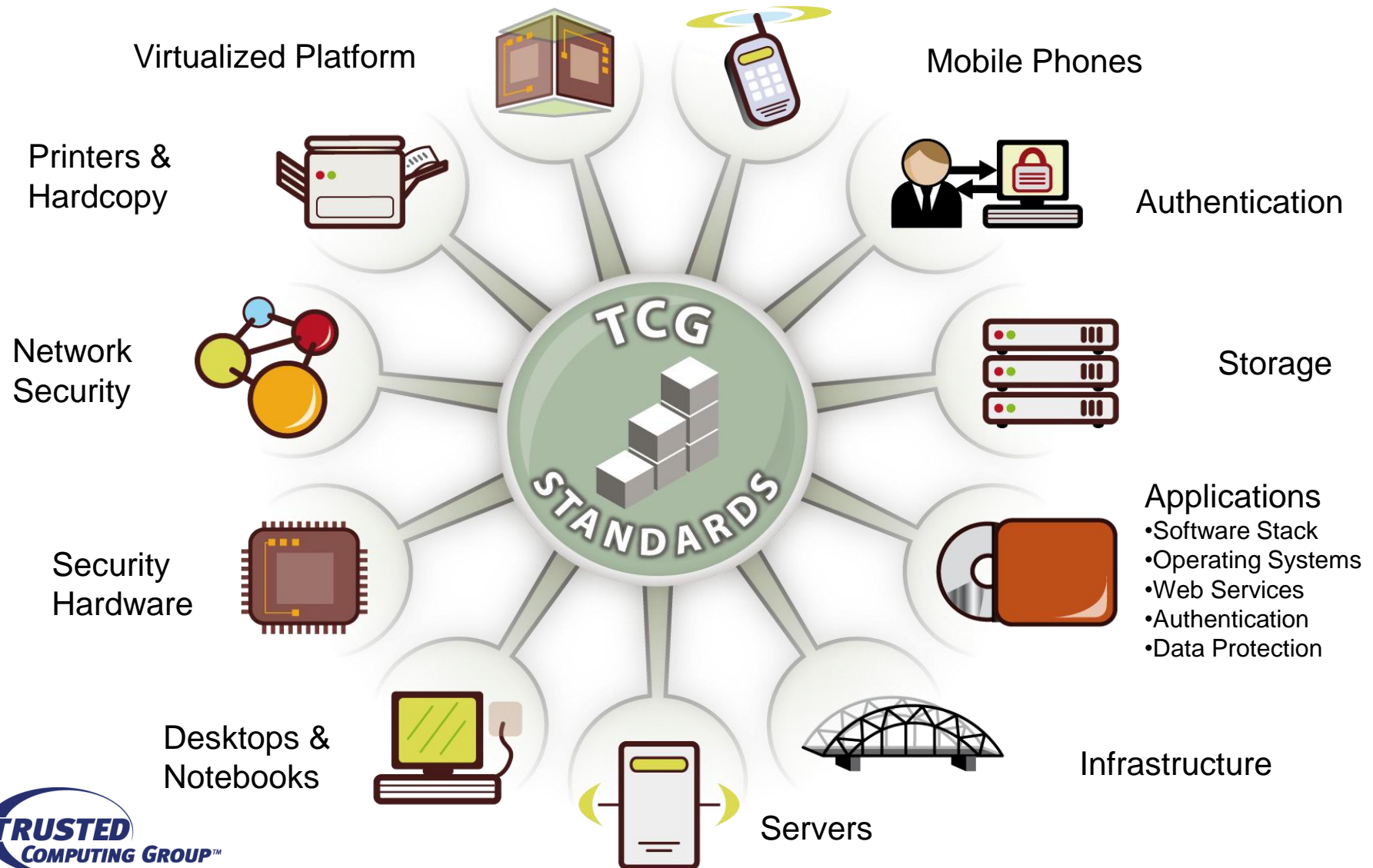
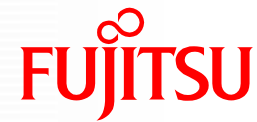


Lawyers



# Introduction to TCG

# TCG: Standards for Trusted Systems





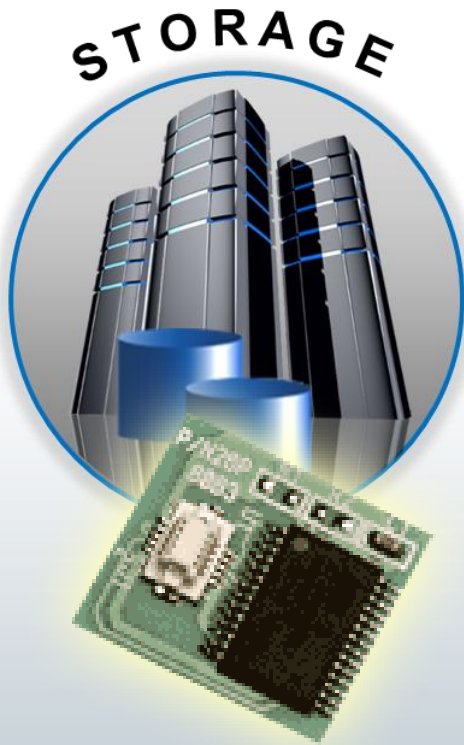
- Security Built In
  - Trusted Platform Module (TPM)
  - Mobile Trusted Module (MTM)
- Features
  - Authentication
  - Encryption
  - Attestation



- Security Built In
  - Trusted Platform Module (TPM)
  - Secure Virtualization
  - Secure Cloud
- Features
  - Authentication
  - Encryption
  - Attestation



# Trusted Storage



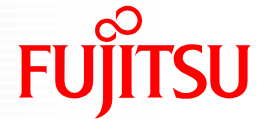
- Security Built In
  - Self Encrypting Drive (SED)
- Features
  - Encryption
  - Authentication



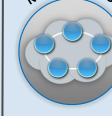















# Trusted Networks



- Security Built In & Coordinated
  - Trusted Network Connect (TNC)
- Features
  - Authenticate
  - Health Check
  - Behavior Monitor
  - Enforce

# CSA Guidelines and TCG



CSA Domain (Number) Type	STORAGE 	SERVERS 	NETWORKS 	CLIENTS 	Examples
(2) Governance/Risk Management					Decrease risk exposure
(3) Legal and Electronic Discovery					Data Recovery and Encryption
(4) Compliance and Audit					Server Attestation
(5) Information Lifecycle Management					Safe Data Retirement
(6) Portability and Interoperability					Metadata Access Policy
(7) Traditional Security					Network Access Control
(8) Incident Response					Coordinated Security
(11) Encryption / Key Management					SED, Hardware Key storage
(12) Identity/ Access Management					Hardware Token Authentication
(13) Virtualization					Trusted Multitenancy

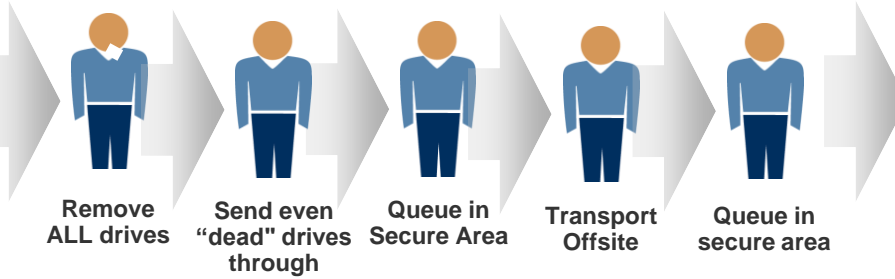
# Practical Applications

# How the Drive Retirement Process Works



Retire Drive

- Replace
- Repair
- Repurpose



## People make mistakes

“Because of the volume of information we handle and **the fact people are involved, we have occasionally made mistakes.**”



*which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007<sup>1</sup>*

## Retirement Options



Overwriting takes days and there is no notification of completion from drive



Hard to ensure degauss strength matched drive type



Shredding is environmentally hazardous



Not always as secure as shredding, but more fun

SECURE?

**99% of Shuttle Columbia's hard drive data recovered from crash site**

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

- May 7, 2008 (Computerworld)

1. <http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach>

## Retirement Options



### Retire Drive

- Replace
- Repair
- Repurpose

Drive Retirement is:

*Expensive*

*Time-consuming*

*Error-prone*

Overwriting takes  
is no  
n drive

gth  
type

y

dding,

hard drive data

SECURE?



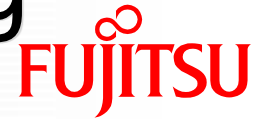
which lost a tape with 150,000 Social Security numbers  
stored at an Iron Mountain warehouse, October 2007<sup>1</sup>

Data recovery specialists at Kroll Ontrack Inc. retrieved  
99% of the information stored on the charred Seagate hard  
drive's platters over a two day period.

- May 7, 2008 (Computerworld)

1. <http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach>

# Drive Retirement: Self-Encrypting Drives

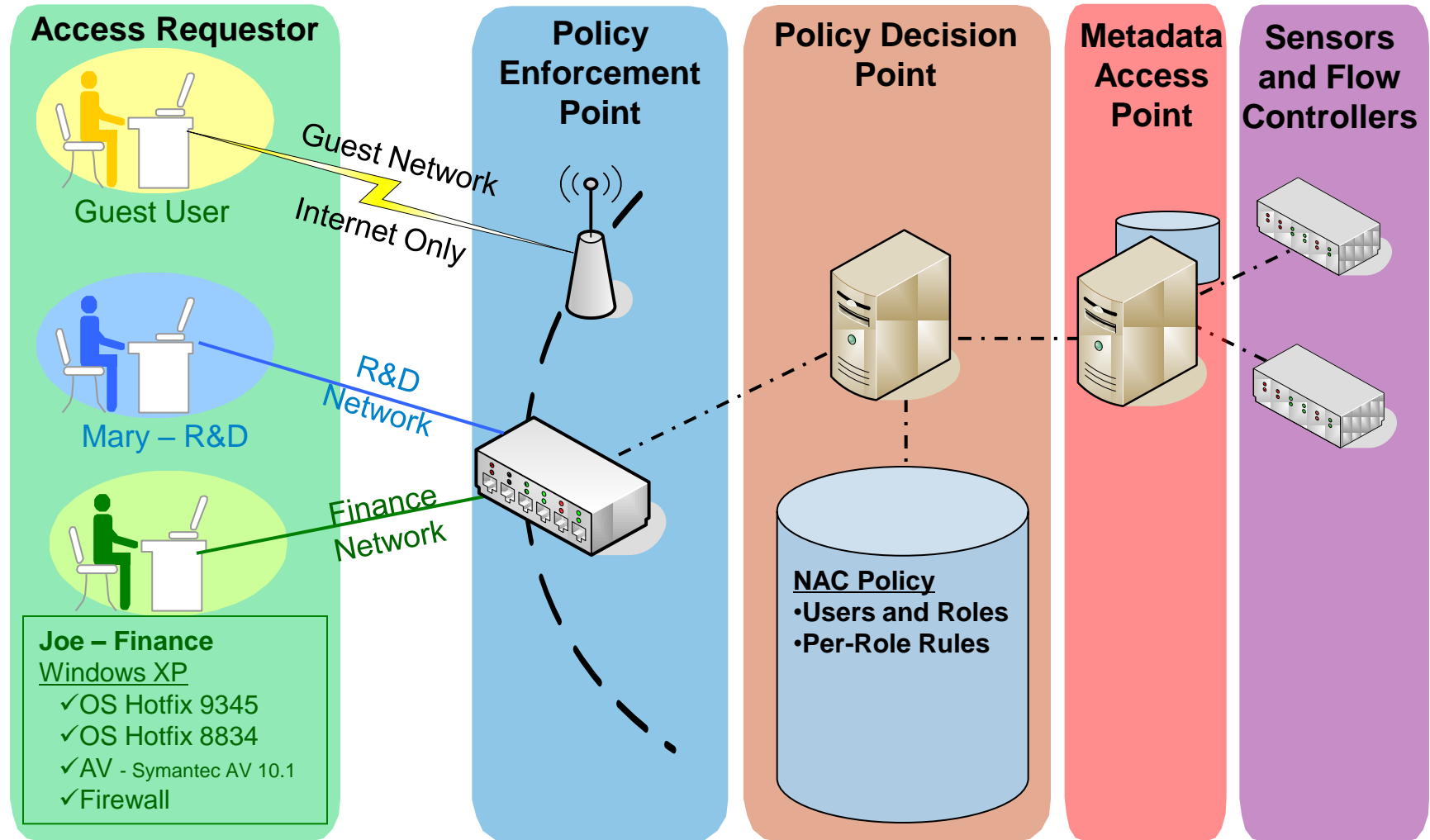


## ■ Reduces IT operating expense

- Eliminates the need to overwrite or destroy drive
- Secures warranty and expired lease returns
- Enables drives to be repurposed securely

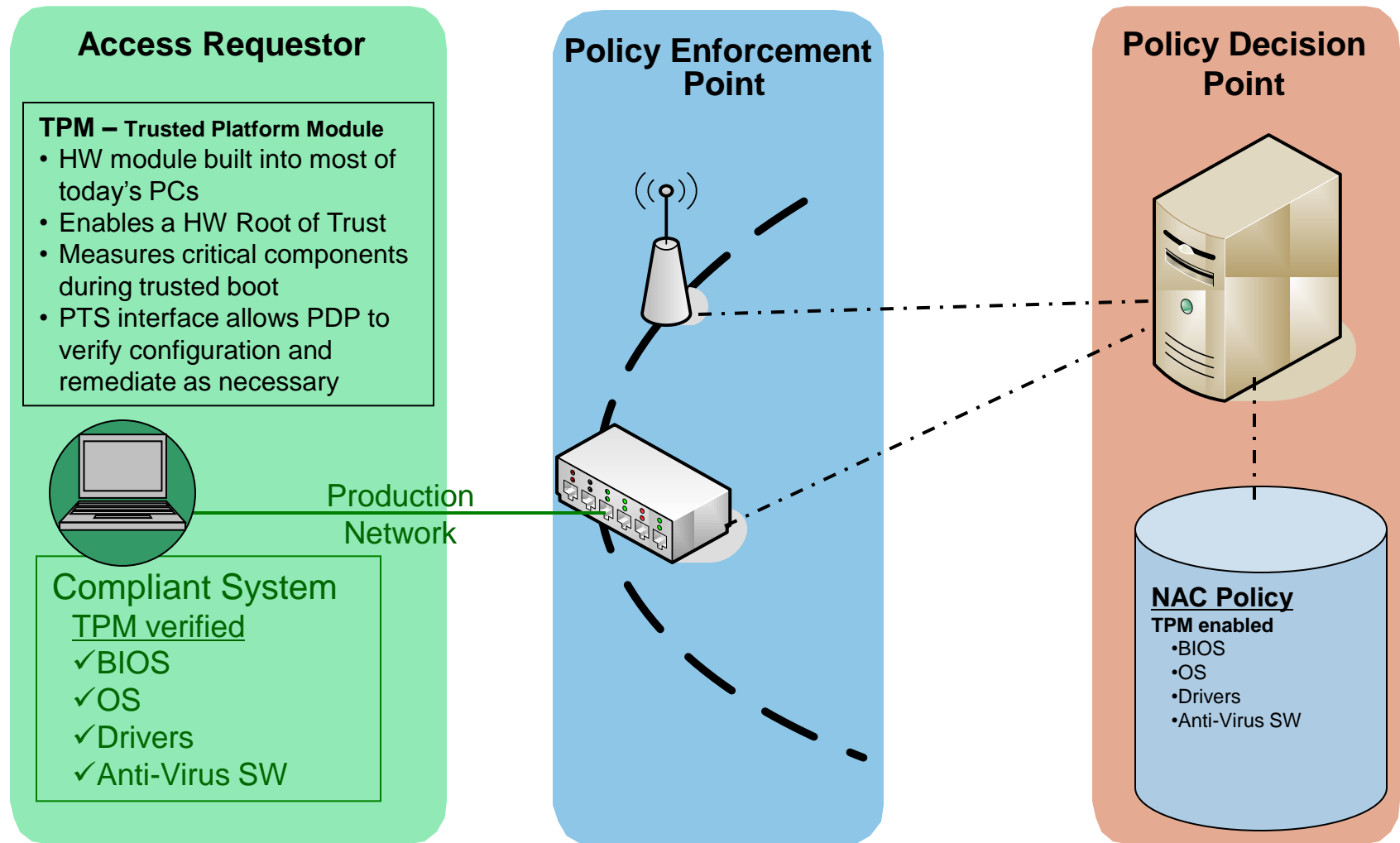
## ■ Provides safe harbor for most data privacy laws

# User-Specific Policies

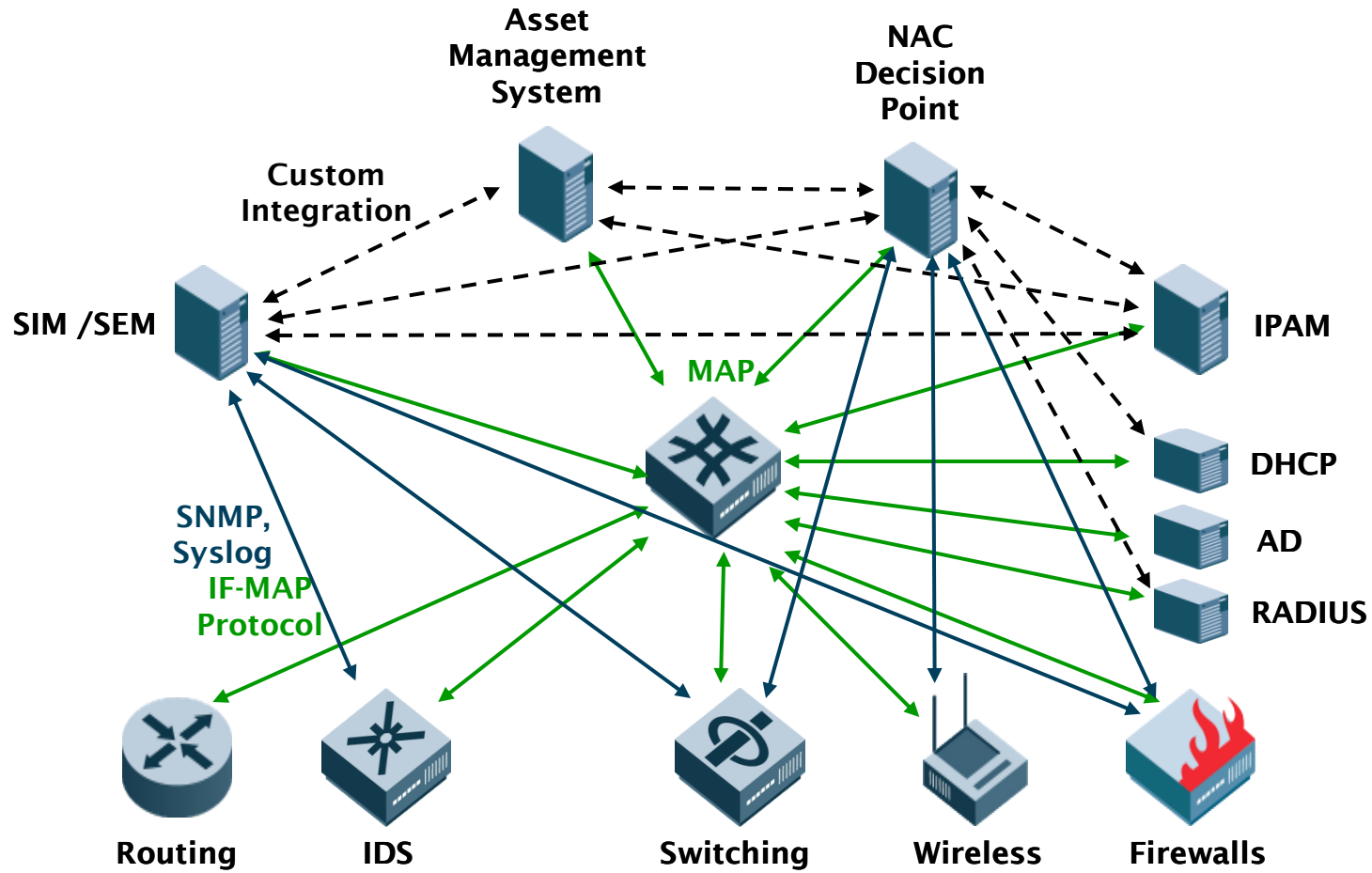




# TPM-Based Integrity Check



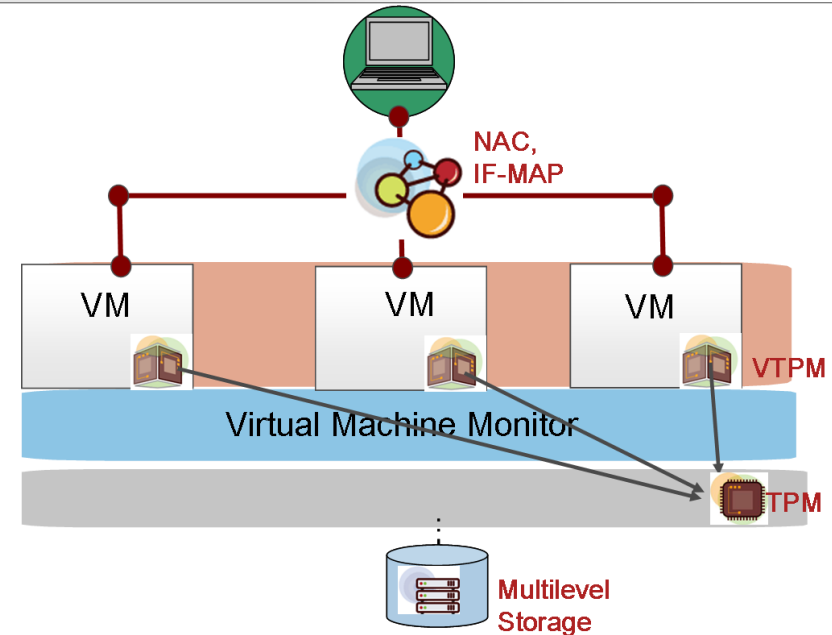
# IF-MAP



# Securing Multitenant Platforms Using TCG



- Some goals
  - Protection of processing and information in motion and at rest
  - Ability to share physical platforms among tenant domain components (shared services)
  - Visibility and auditability of actions across the enterprise
  - Management of physical resources independently of domain resources
  - Loosely coupled architecture managed using application of appropriate policy and trust
  - Ability to control the flow of information between tenant domains within policy constraints
  - Ability to address various security models to protect integrity and confidentiality of services and data exchanges within enterprise

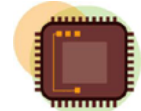


## Relevant Working Groups

Virtualization work group  
(virtual certificates, virtual TPM, migration)



TPM working Group (Server Attestation)



Storage workgroup (multilevel storage)



Trusted Network Connect  
(Policy definitions and enforcement)



# Support Slides

