

# **RSA<sup>®</sup>CONFERENCE C H I N A 2012**

**RSA信息安全大会2012**

**THE GREAT CIPHER**

**MIGHTIER THAN THE SWORD**

**伟大的密码胜于利剑**



**Keys and Clouds:**

# **Strategies for Key Management in the Hybrid Cloud**

**Dr. Robert W. Griffin**  
RSA, The Security Division of EMC



**RSACONFERENCE**  
**C H I N A 2012**

# Agenda

- Issues in managing keys in the cloud
- Key management models for private, public and hybrid clouds
- Key management protocols for the cloud
- What problems need to be addressed

# Key management has a role in all cloud models

RSA CONFERENCE  
C H I N A 2012

<p>Cloud Applications Software-as-a-Service</p>	  
<p>Cloud Software Development Platform-as-a-Service</p>	  
<p>Cloud-based Infrastructure Infrastructure-as-a-Service</p>	      

# Common Key Management Issues

RSA CONFERENCE  
C H I N A 2012

- Ownership of the keys
- Protection of keys in transit
- Protection of keys at rest
- Trust establishment
- Managing access to keys
- Defining and propagating key policy
- Managing key life-cycle
- Visibility of services



RSA信息安全大会2012

# What is there to worry about in the cloud?

## Use of encryption is rare:

- Who can see your information?

## Virtual volumes and servers are mobile:

- Your data is mobile — has it moved?

## Rogue servers might access data:

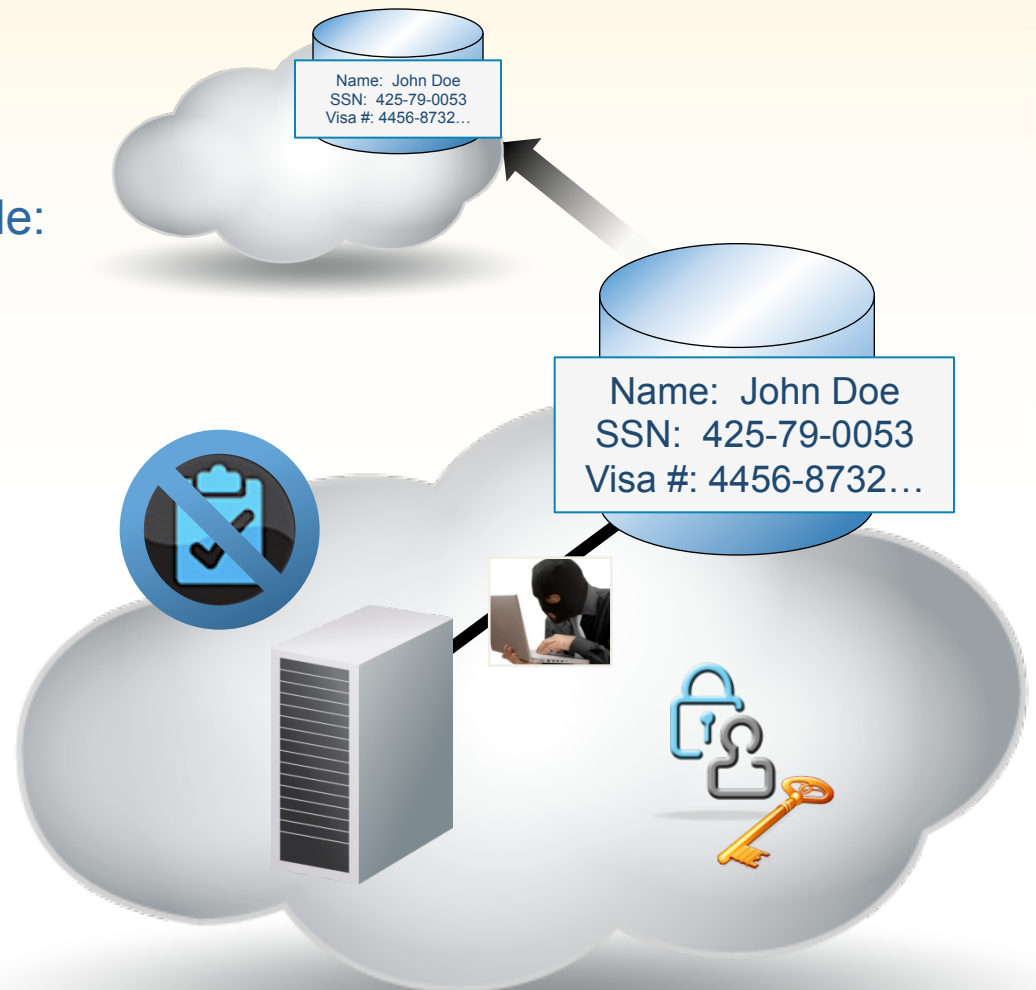
- Who is attaching to your volumes?

## Rich audit and alerting modules lacking:

- What happened when you weren't looking?

## Virtual volumes contain residual data:

- Are your storage devices recycled securely?



# CSA Top Threats

- **Threat #1:** Abuse and Nefarious Use of Cloud Computing
- **Threat #2:** Insecure Interfaces and APIs
- **Threat #3:** Malicious Insiders
- **Threat #4:** Shared Technology Issues
- **Threat #5:** Data Loss or Leakage
- **Threat #6:** Account or Service Hijacking
- **Threat #7:** Unknown Risk Profile

<http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>



# Threat #1: Abuse and Nefarious Use of Cloud Computing

RSA CONFERENCE  
C H I N A 2012

## The problem:

Cloud Computing providers (IaaS) are actively being targeted, partially because their relatively weak registration, systems facilitate anonymity, and providers' fraud detection capabilities are limited.

## What has happened (so far):

- IaaS offerings have hosted the Zeus botnet, InfoStealer trojan horses, and downloads for Microsoft Office and Adobe PDF exploits.
- Botnets have used IaaS servers for command and control functions.
- Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklisted.



RSA信息安全大会2012



## Threat #2: Insecure Interfaces and APIs

### The problem:

Reliance on a **weak set of interfaces and APIs** exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

### What has happened (so far):

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

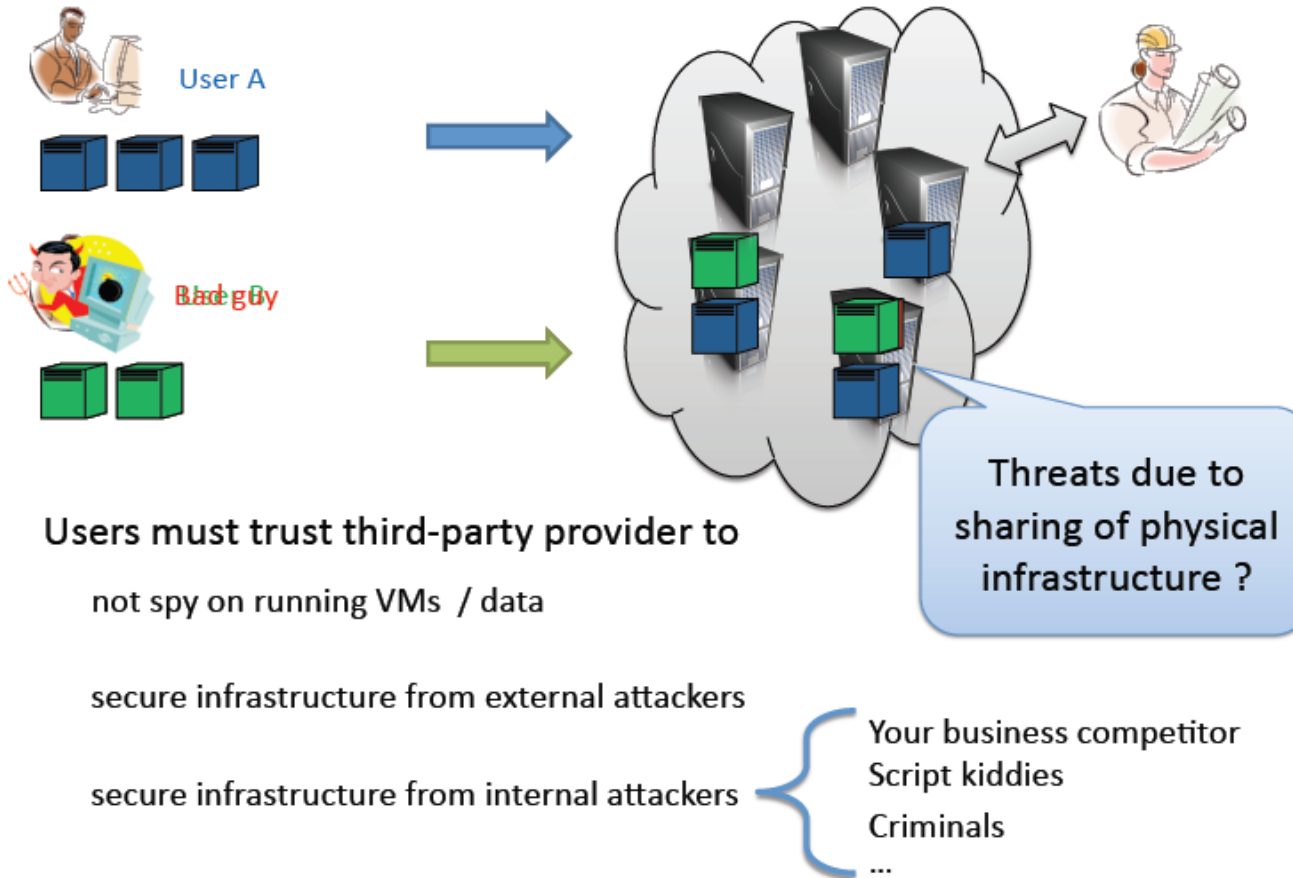


## Threat #3: Malicious Insiders

" If you work with a company long enough, eventually you will have access to everything, and no one will know it. "

# Threat #4: Shared Technology

## Trust models in cloud computing



Users must trust third-party provider to  
not spy on running VMs / data

secure infrastructure from external attackers

secure infrastructure from internal attackers

Tom Ristenpart: [ristenpart-invited-csc2011.pdf](#)

## Threat # 5: Data loss

- The Microsoft data loss of 2009 resulted in an estimated 800,000 smartphone users in the United States temporarily losing personal data, such as emails, address books and photos from their mobile handsets.
- The computer servers holding the data were run by Microsoft.
- At the time, it was described as the biggest disaster to affect the concept of cloud computing.

# Threat #6: Account or Service Hijacking

InfoWorld Home / Cloud Computing / News / Hackers find a home in Amazon's EC2 cloud

DECEMBER 10, 2009

## Hackers find a home in Amazon's EC2 cloud

Security researchers discover the Zeus password-stealing botnet running on Amazon's EC2 cloud computing servers

By Robert McMillan | IDG News Service

Share or Email | Print | 5 comments | 24 Records

Security researchers have spotted the Zeus botnet running an and control center on Amazon's EC2 cloud computing infrastr

## Virtual Machine Sniffer on ESX Hosts

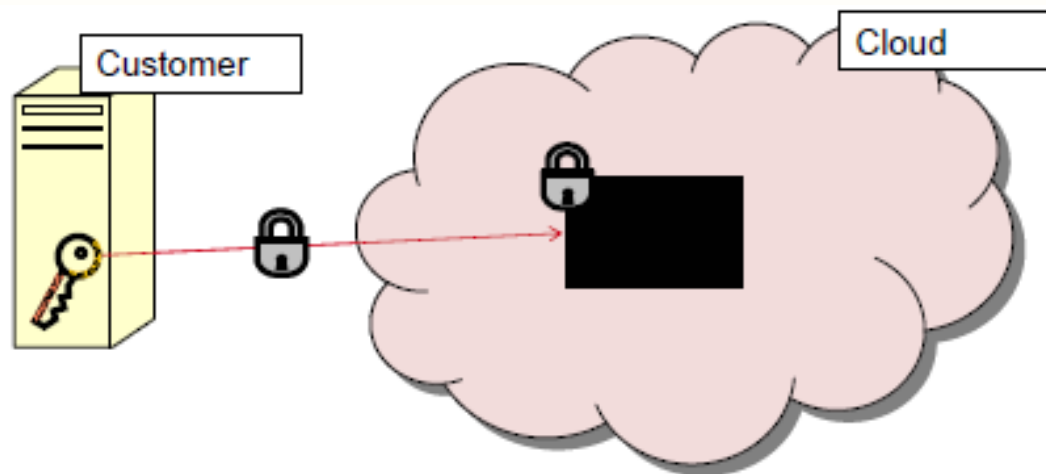
March 12th, 2009 | Author: Rich Brambley

If you thought that because all ESX virtual machines (VM) share a virtual portgroup on a virtual switch (vSwitch) inside an ESX host you could easily sniff all VM traffic with a protocol analyzer like ethereal or wireshark, when you tried it you found out you were wrong. If I am not mistaken, ESX vSwitches are considered layer 2 devices and come with all the expected security and isolation. However, you can make some relatively simple vSwitch design and setting changes to turn a VM into a virtual sniffer and monitor all other VMs on that same host. Another option is a free virtual appliance that can allow you to use your physical monitoring tools to watch your VMs. This post explores both of these free VM sniffer alternatives.

## Threat #7: Unknown Risk Profile

Trust the Provider?

=> If you want to do anything useful with cloud computing, you have to trust the provider.

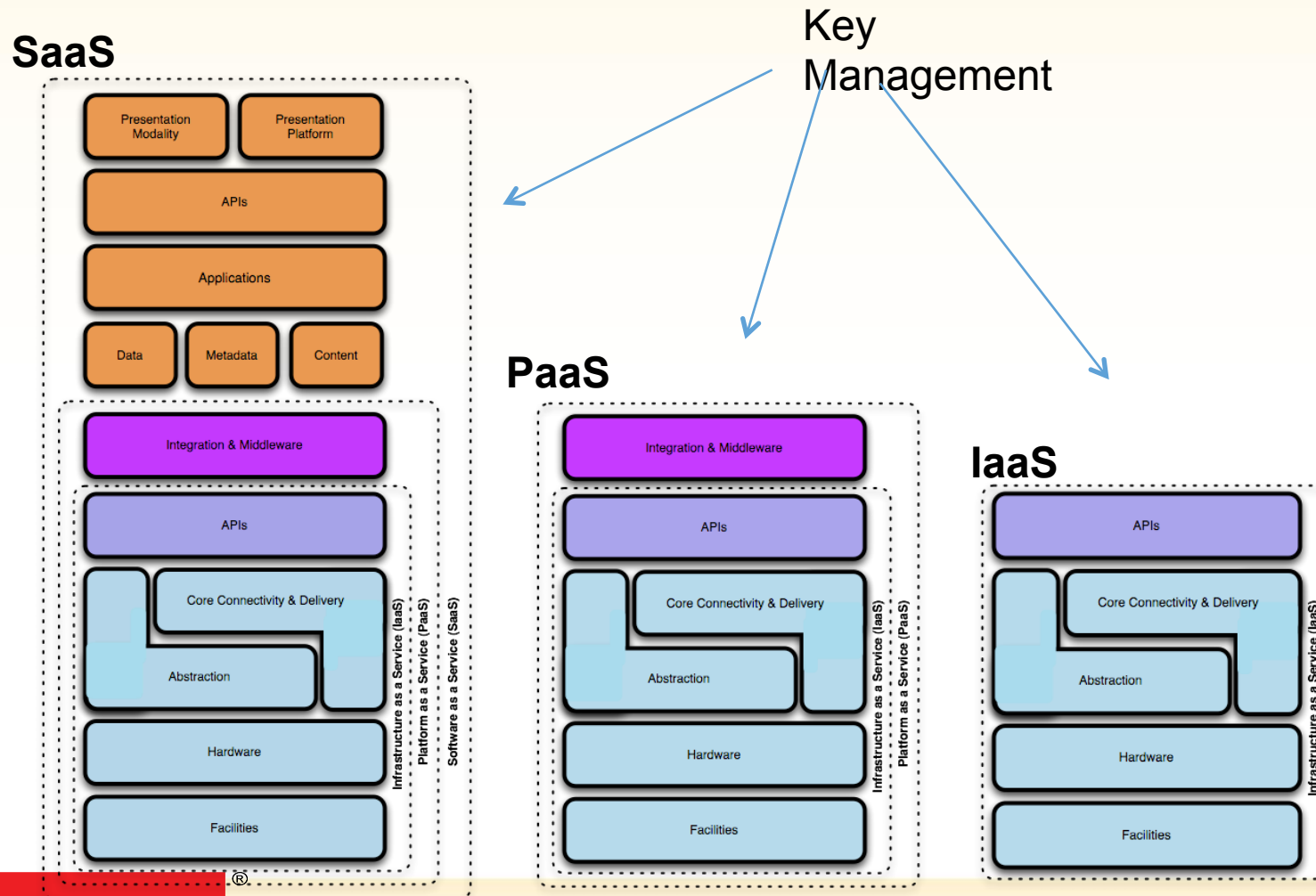


# Agenda

- Issues in managing keys in the cloud
- Key management models for private, public and hybrid clouds
- Key management protocols for the cloud
- What problems need to be addressed

# Key management has a role in each cloud model - but where?


RSA CONFERENCE  
C H I N A 2012





# CSA Security Guidance

RSA CONFERENCE  
C H I N A 2012

- **Section I. Cloud Architecture**
- Domain 1: Cloud Computing Architectural Framework
- **Section II. Governing in the Cloud**
- Domain 2: Governance and Enterprise Risk Management
- Domain 3: Legal and Electronic Discovery
- Domain 4: Compliance and Audit
- Domain 5: Information Lifecycle Management
- Domain 6: Portability and Interoperability
- **Section III. Operating in the Cloud**
- Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
- Domain 8: Data Center Operations
- Domain 9: Incident Response, Notification, and Remediation
- Domain 10: Application Security
- Domain 11: Encryption and Key Management 
- Domain 12: Identity and Access Management

<http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>



RSA信息安全大会2012

# CSA Guidance for Encryption

RSA CONFERENCE  
C H I N A 2012

Cloud customers and providers need to guard against data loss and theft. Today, encryption of personal and enterprise data is strongly recommended, and in some cases mandated by laws and regulations around the world. Cloud customers want their providers to encrypt their data to ensure that it is protected no matter where the data is physically located. Likewise, the cloud provider needs to protect its customers' sensitive data.

Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data. While encryption itself doesn't necessarily prevent data loss, safe harbor provisions in laws and regulations treat lost encrypted data as not lost at all. The encryption provides resource protection while key management enables access to protected resources.

- ✓ Use encryption to separate data holding from data usage.
- ✓ When stipulating encryption in contract language, assure that the encryption adheres to existing industry and government standards, as applicable.
- ✓ Assure regulated and/or sensitive customer data is encrypted in transit over the cloud provider's internal network, in addition to being encrypted at rest.
- ✓ In IaaS environments, understand how sensitive information and key material otherwise protected by traditional encryption may be exposed during usage.

<http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>



RSA信息安全大会2012

# CSA Guidance for Key Management

RSA CONFERENCE  
C H I N A 2012

- ✓ Segregate the key management from the cloud provider hosting the data, creating a chain of separation. This protects both the cloud provider and customer from conflicts when compelled to provide data due to a legal mandate.
- ✓ Understand whether and how cloud provider facilities provide role management and separation of duties.
- ✓ In cases where the cloud provider must perform key management, understand whether the provider has defined processes for a key management lifecycle: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Further, understand whether the same key is used for every customer or if each customer has its own key set.

<http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>



# Defining Cloud Key Management Models

RSA CONFERENCE  
C H I N A 2012

- Where are keys created?
- Where are keys used?
- Where are keys stored?
- Where are key policies managed?



RSA信息安全大会2012

# Cloud Key Management Models

RSA CONFERENCE  
C H I N A 2012

## Enterprise

- Keys created, used, stored and managed by enterprise

## Hybrid

- Keys created, stored and managed by enterprise, but used by CSP

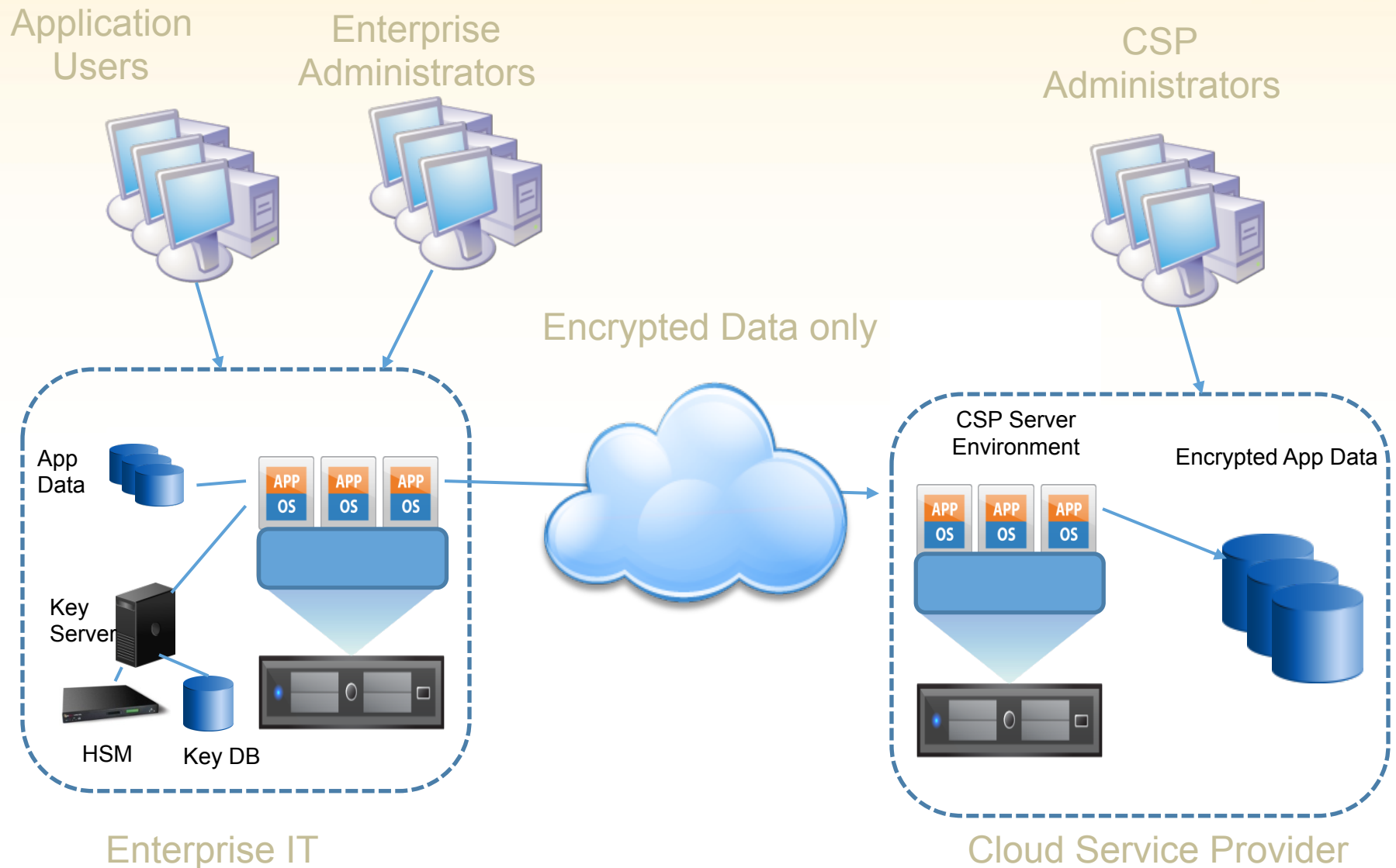
## CSP

- Keys created, used, stored and managed by CSP



# Model 1: Enterprise Key Management

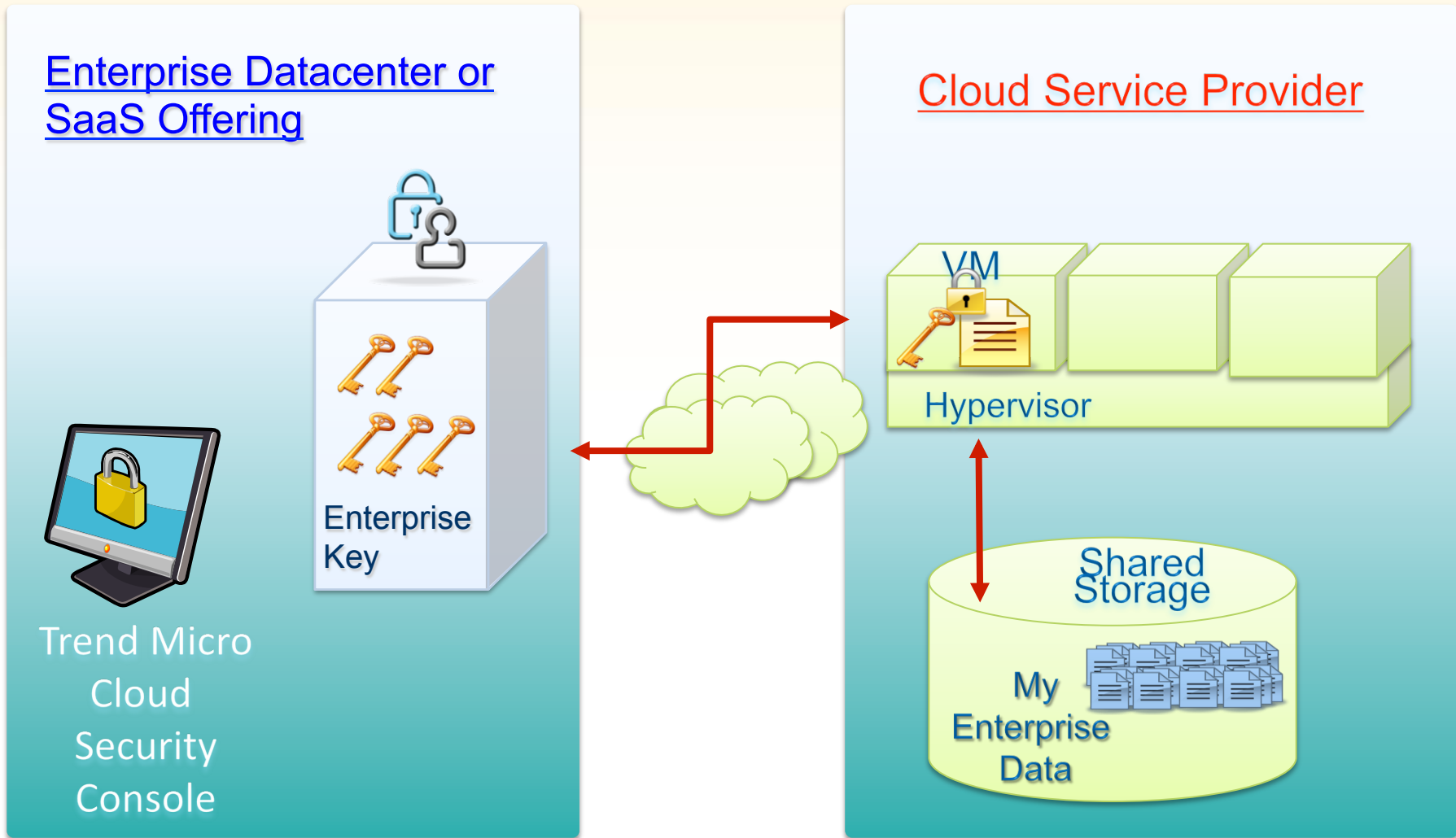
RSA CONFERENCE  
C H I N A 2012



RSA信息安全大会2012

# Example: TrendMicro SecureCloud

RSA CONFERENCE  
C H I N A 2012



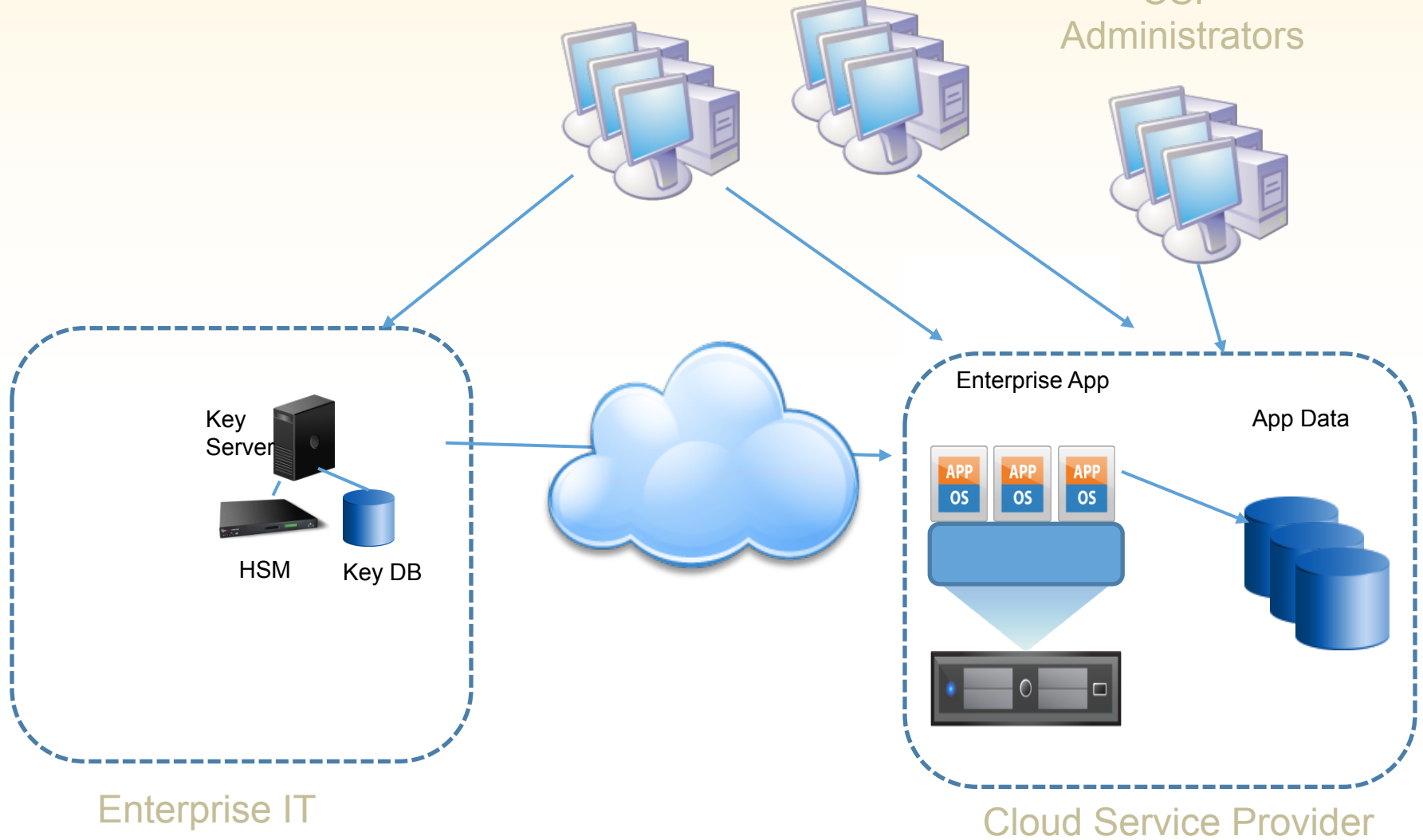
# Model 2: Hybrid Key Management

RSA CONFERENCE  
C H I N A 2012

Enterprise  
Administrators

Application  
Users

CSP  
Administrators



Enterprise IT

Cloud Service Provider

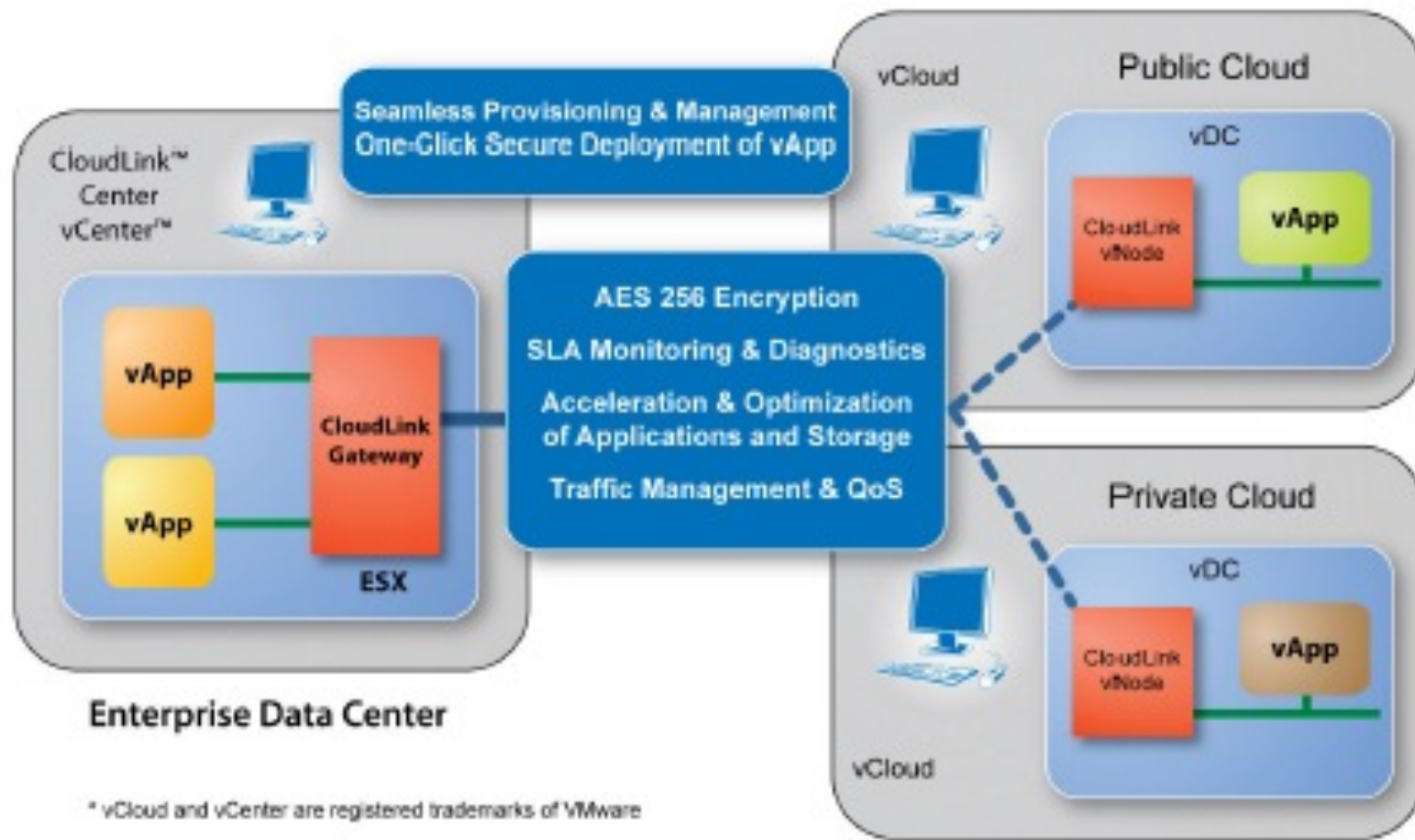


RSA信息安全大会2012



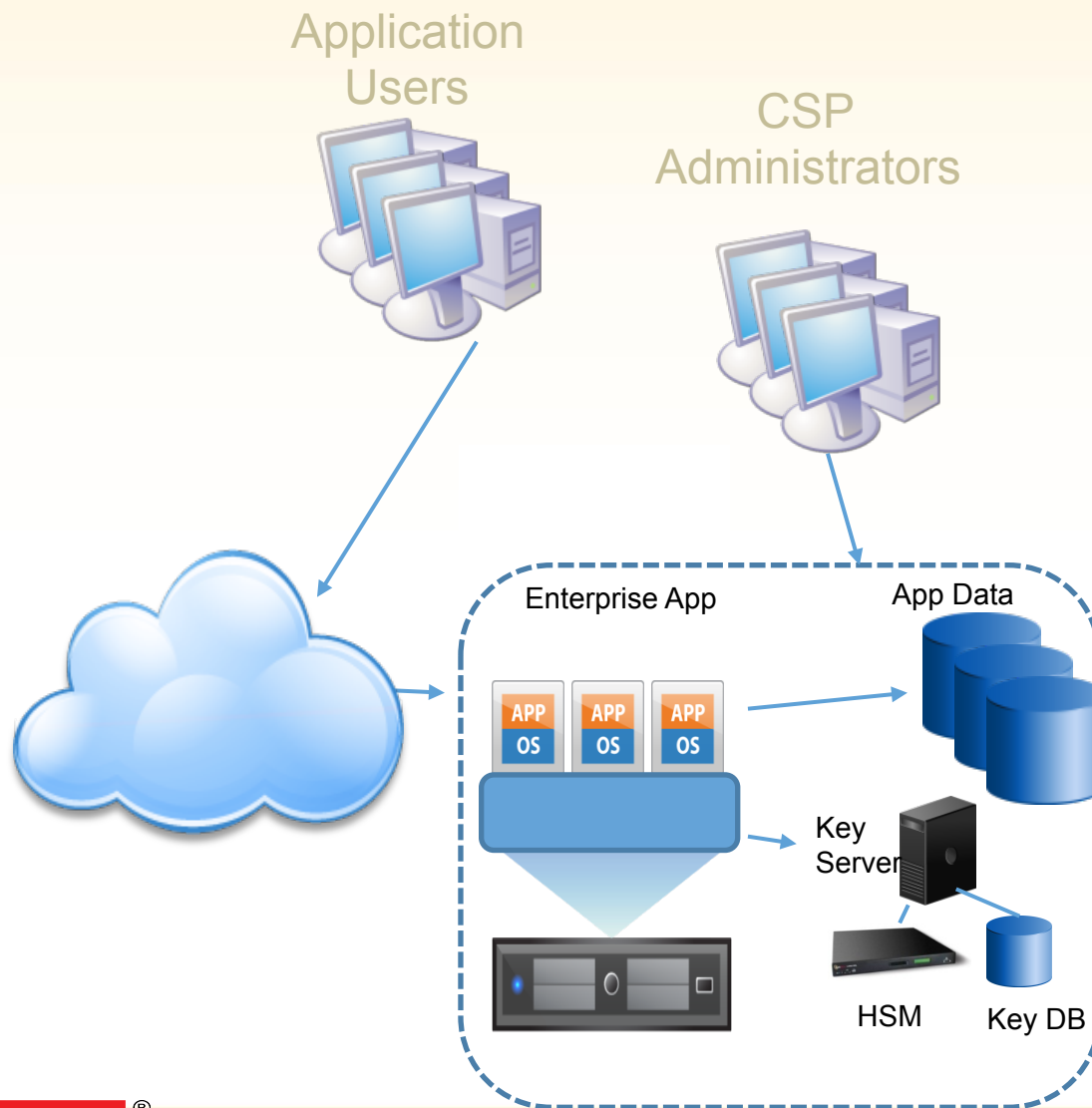
# Example: Afore CloudLink

RSA CONFERENCE  
C H I N A 2012



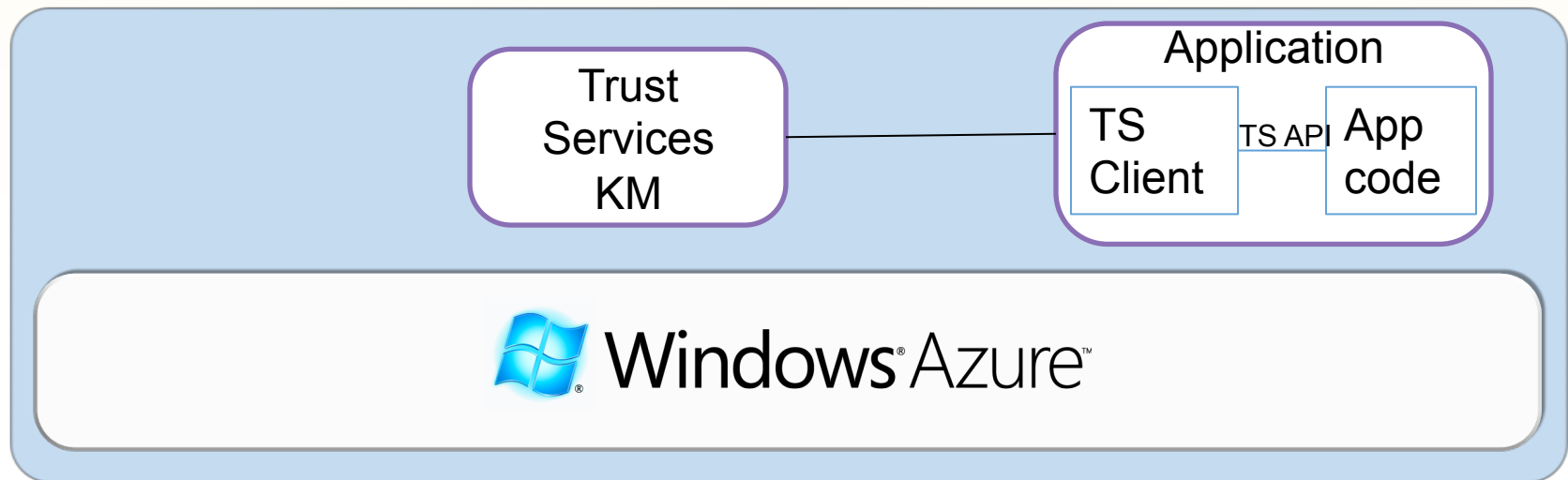
AFORE CloudLink Product Brief.pdf

# Model 3: CSP Key Management



# Example: Azure Trust Services

RSA CONFERENCE  
C H I N A 2012

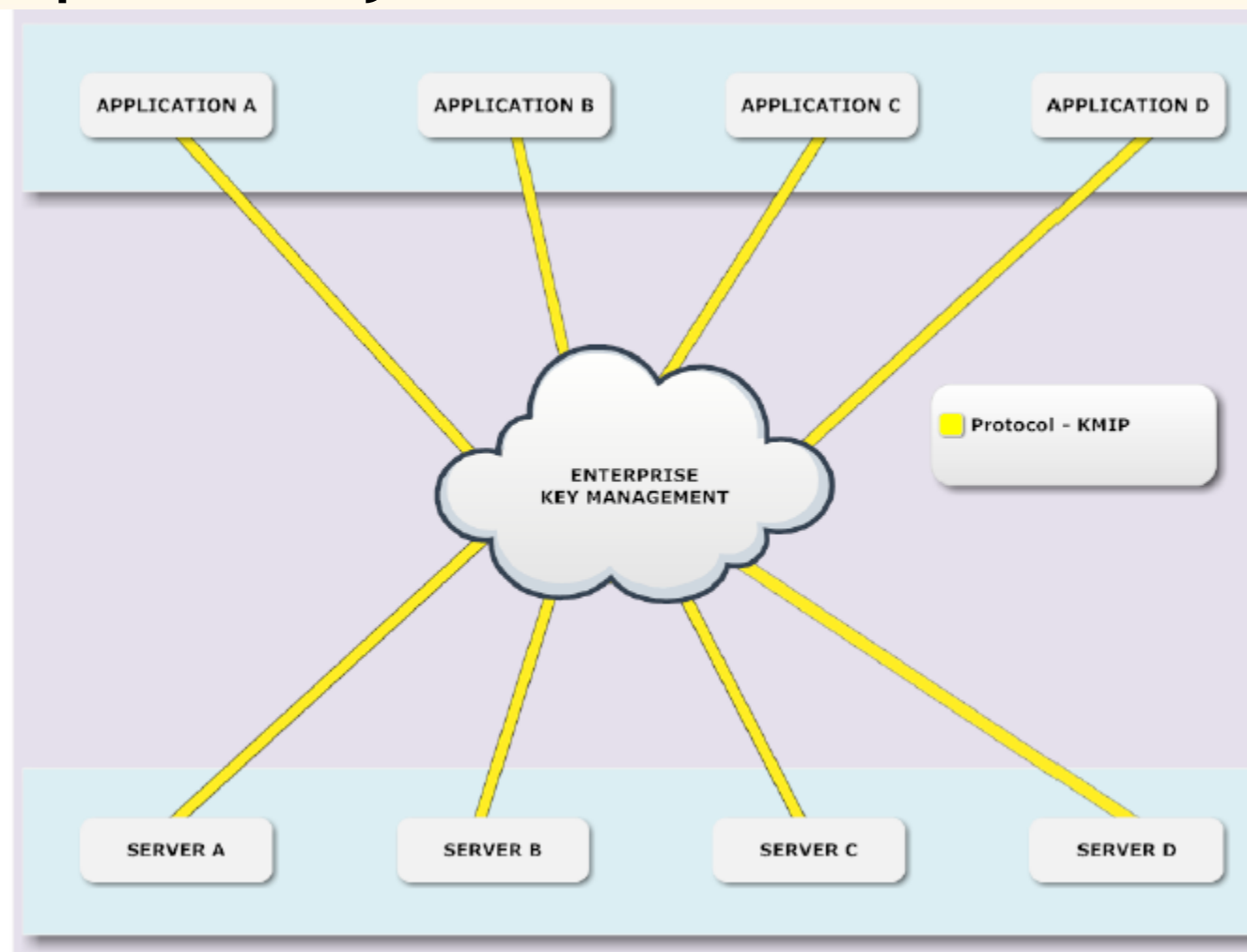


# Agenda

- Issues in managing keys in the cloud
- Key management models for private, public and hybrid clouds
- Key management protocols for the cloud
- What problems need to be addressed

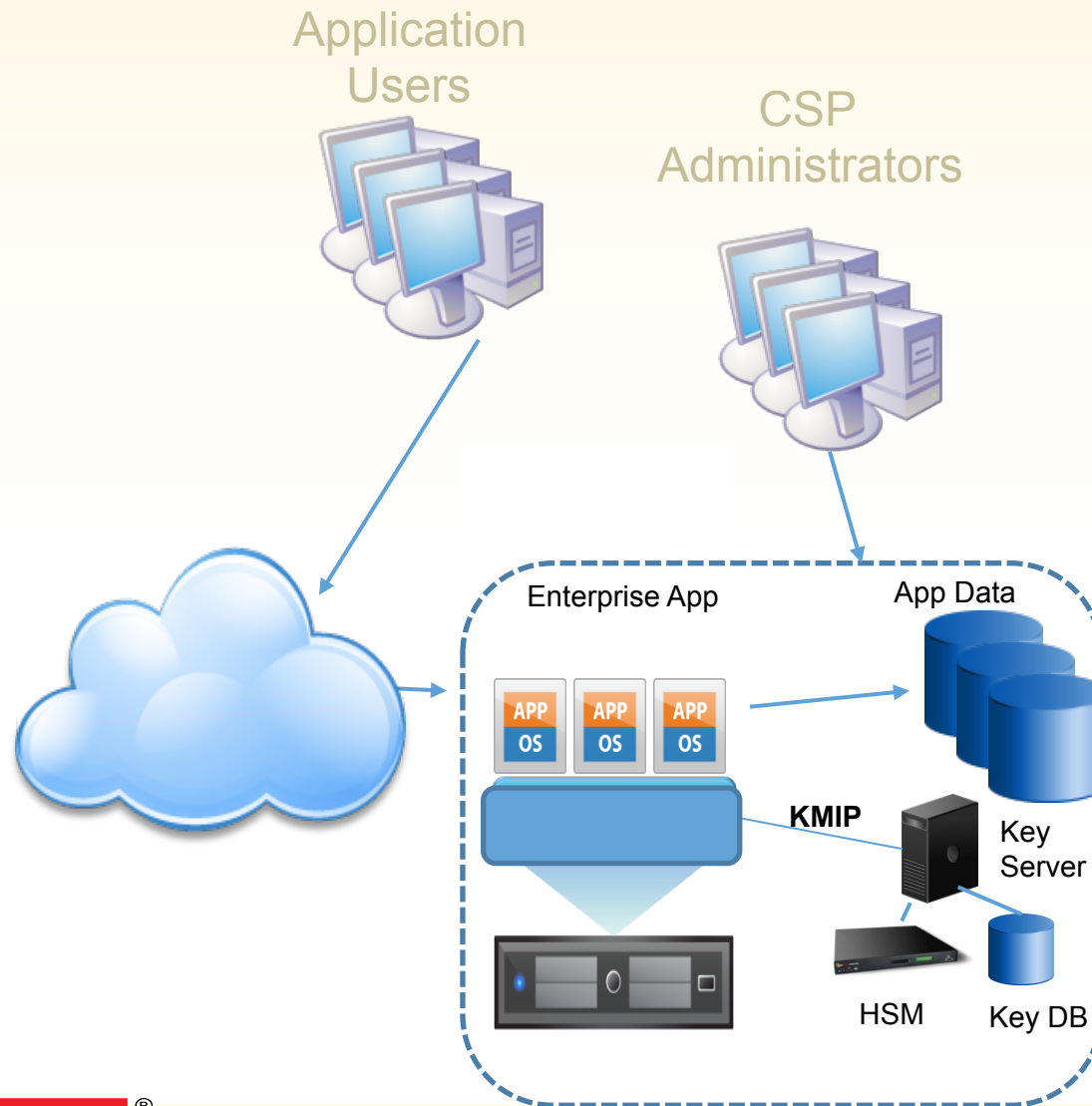
# OASIS Key Management Interoperability Protocol

RSA CONFERENCE  
C H I N A 2012



# Using KMIP in CSP Key Management

RSA CONFERENCE  
C H I N A 2012

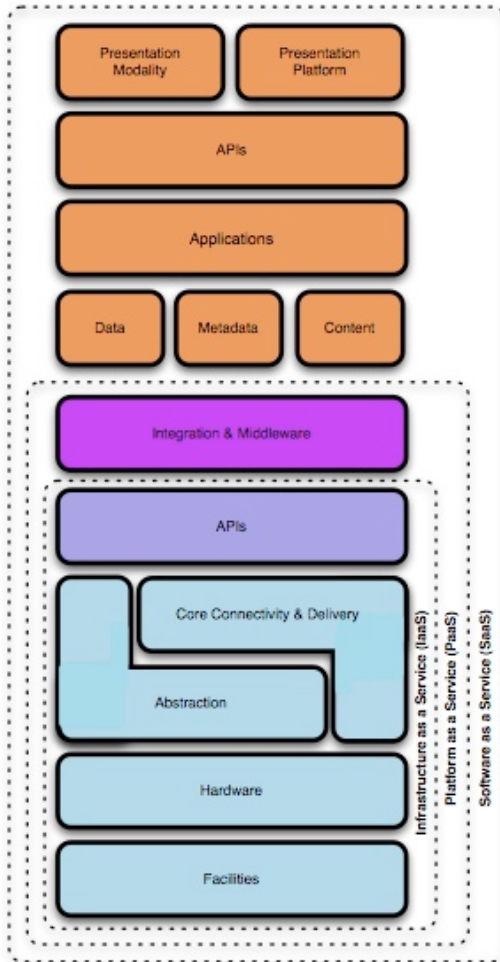


# Agenda

- Issues in managing keys in the cloud
- Key management models for private, public and hybrid clouds
- Key management protocols for the cloud
- What problems need to be addressed

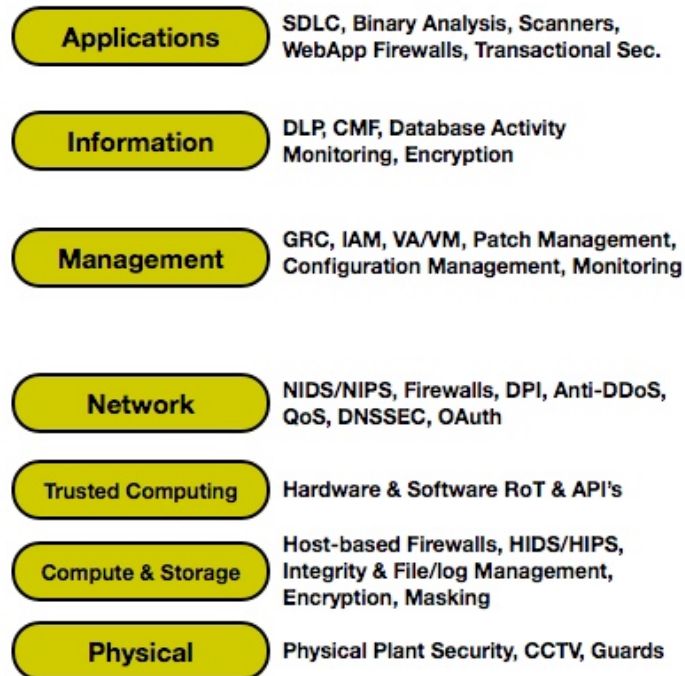
# Key Management and Compliance

## Cloud Model

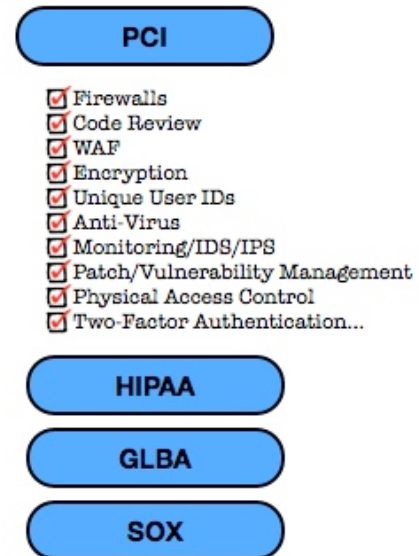


Find the Gaps!

## Security Control Model

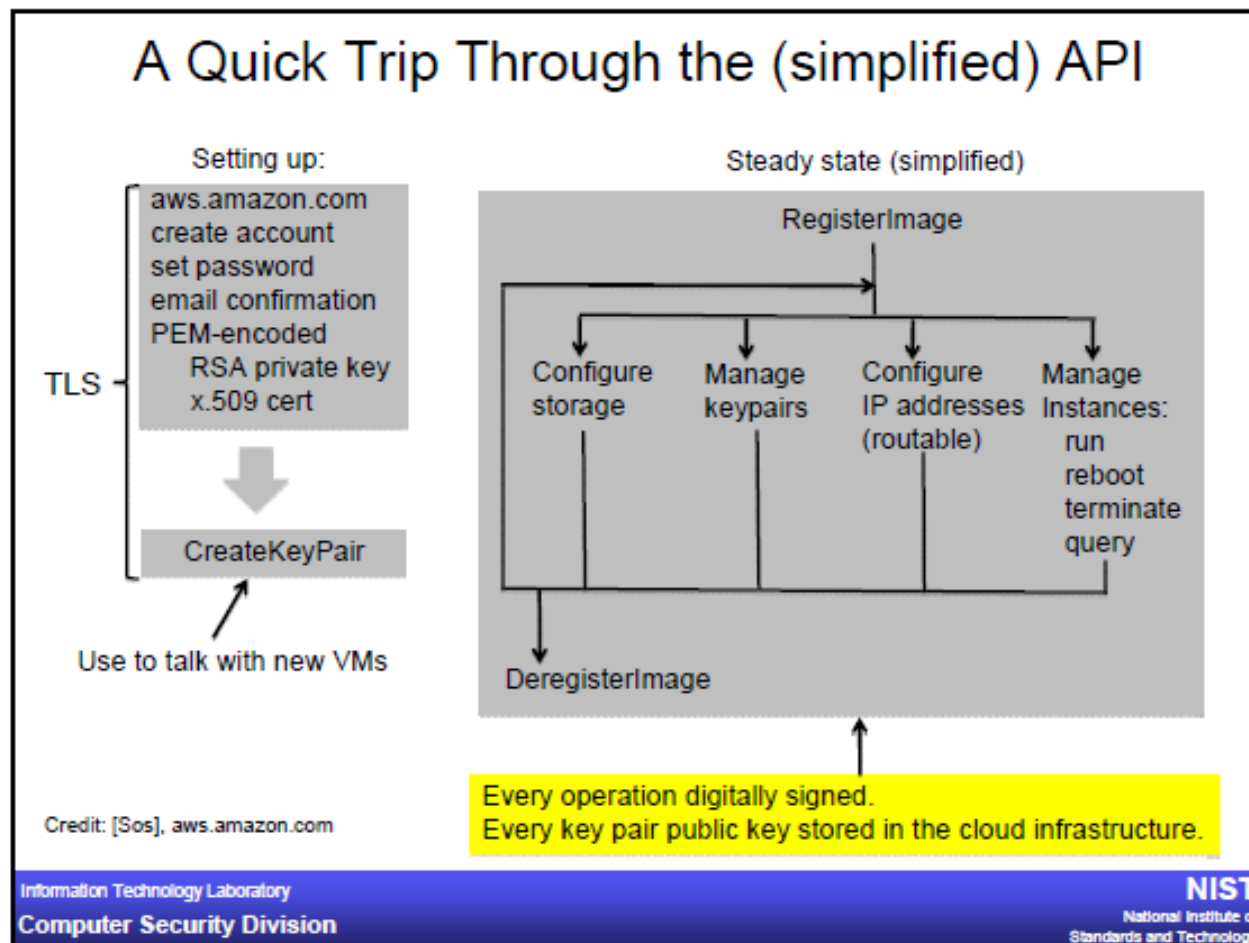


## Compliance Model



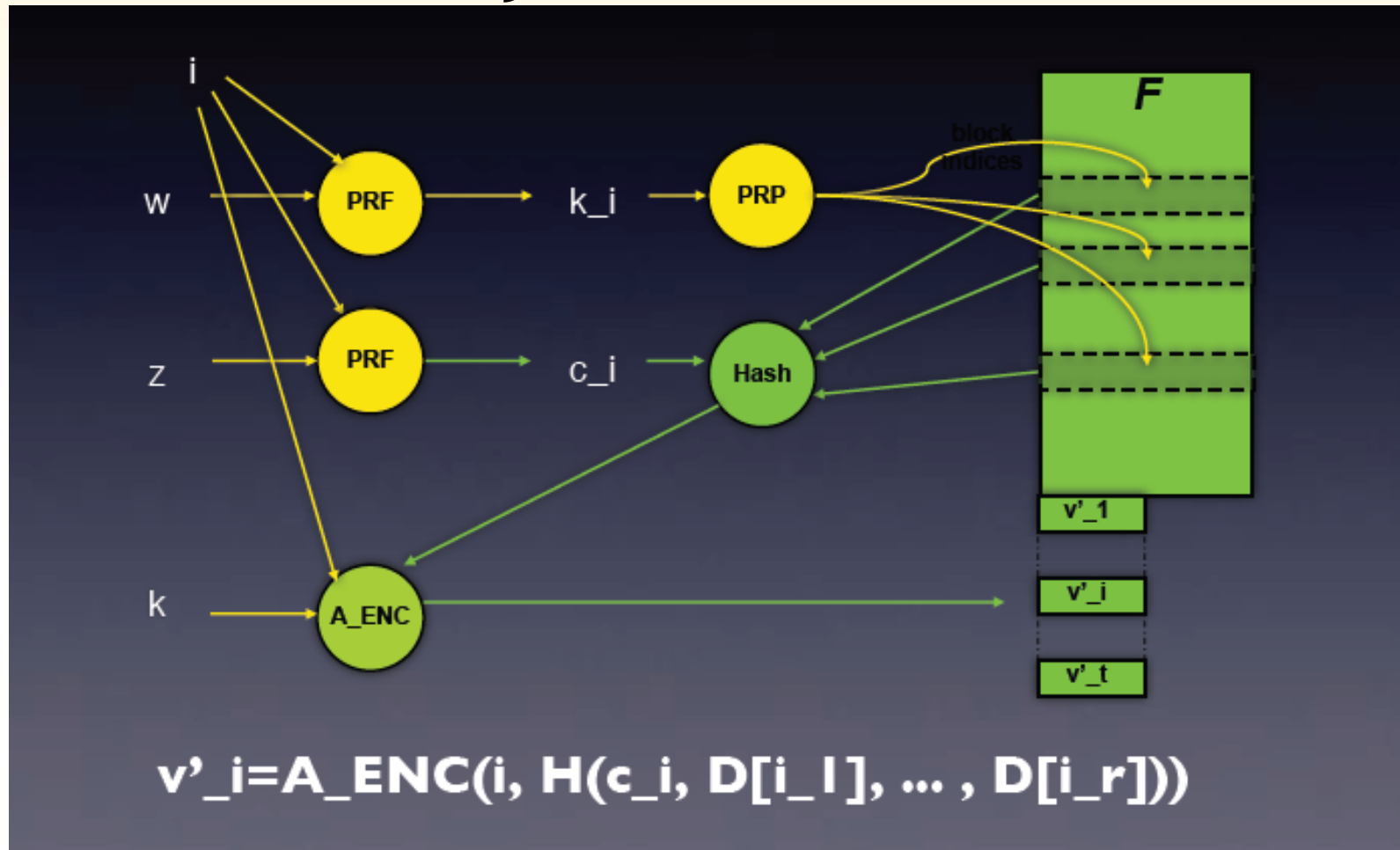


# Are new cryptographic or key management standards needed?



lee\_badger\_KMWJune09\_clouds\_keys.pdf

# Do we have to establish proof-of-possession for keys?



Giuseppe Ataniense: PDP1.pdf

# Thank You

[robert.griffin@rsa.com](mailto:robert.griffin@rsa.com)



RSACONFERENCE  
C H I N A 2012