RSA CONFERENCE ASIA PACIFIC 2013

RETHINKING WEB-APPLICATION ARCHITECTURE FOR THE CLOUD

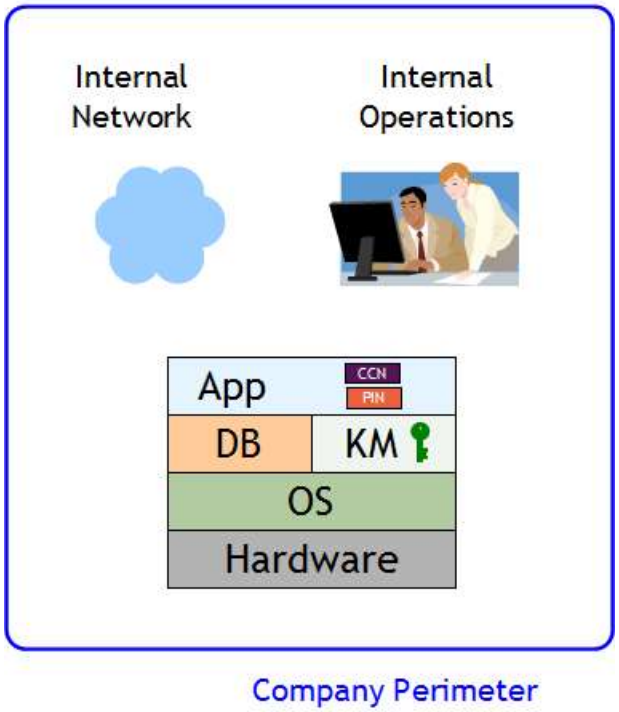
Arshad Noor
StrongAuth, iNc.

Session ID: CLD-W05

Session Classification: Intermediate

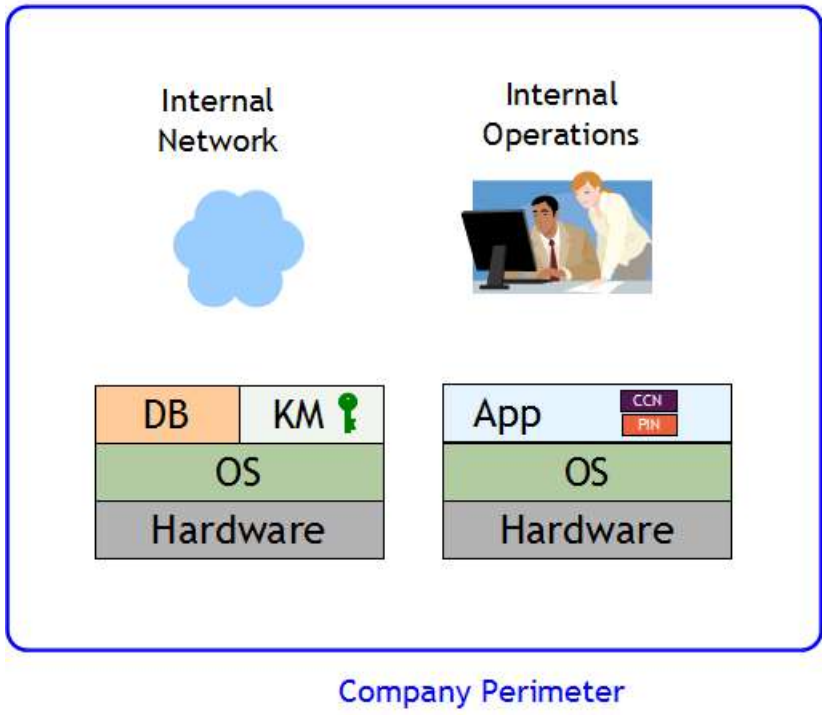
In the beginning…

- Your data-center
- Your mainframe or mini-computer
- Your network
- Your Operations staff
- Your **single-tiered, monolithic** applications



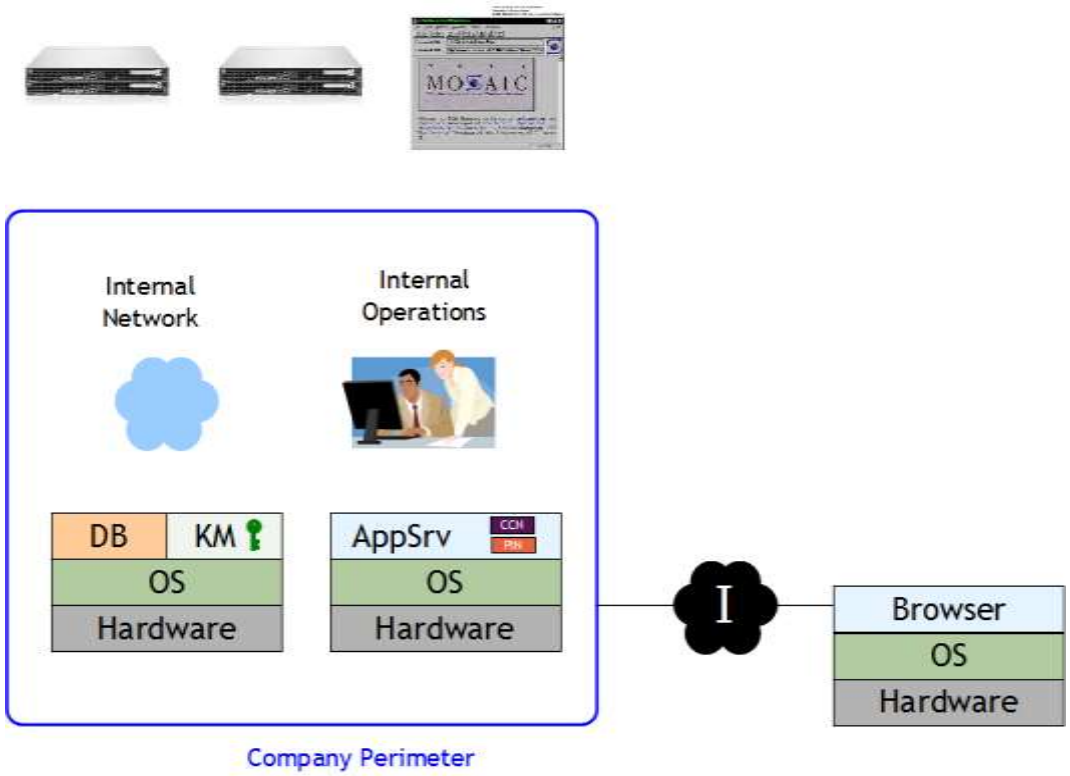
The PC-LAN

- Your data-center
- Your PC Server
- Your PC Client
- Your network
- Your firewall
- Your Operations staff
- Your **two-tiered client-server** applications



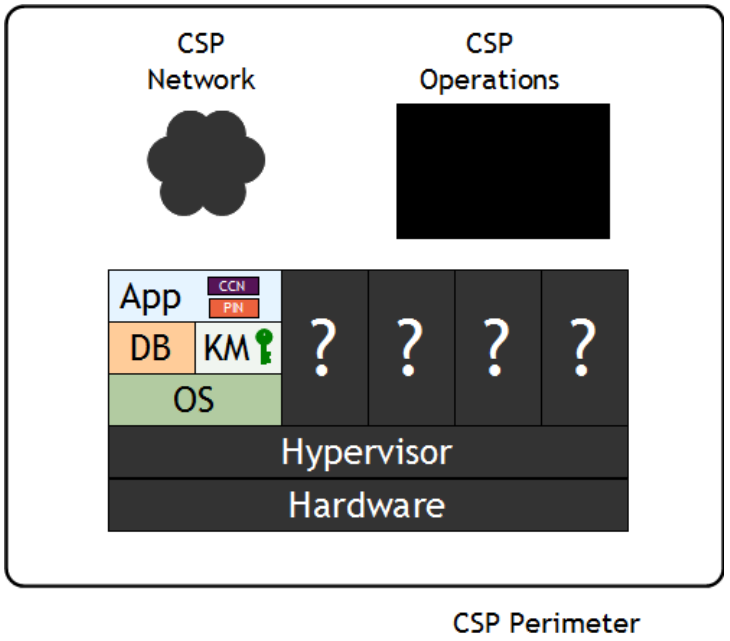
The WWW

- Your data-center
- Your Servers
- Your network
- Your firewall
- Your Operations
- Your **three-tiered web-applications**

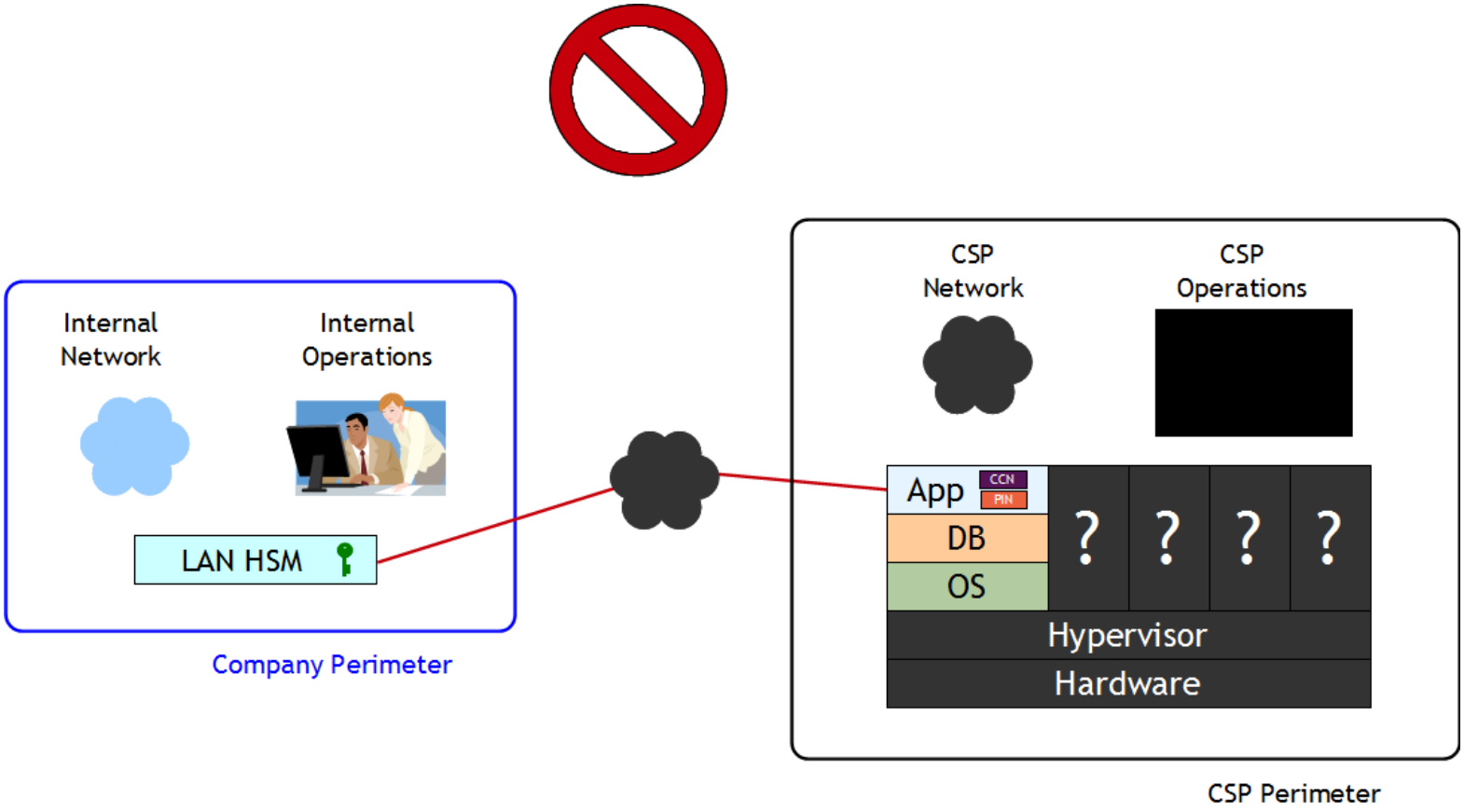


The Public Cloud

- Cloud Service Provider's (CSP) data-center
- CSP's hardware
- CSP's hypervisor
- CSP's network
- CSP's Operations
- Unknown guests in VMs
- **Your** applications and data?



EKM in the Cloud?



What's missing?

- A methodology to take your applications and data to the Cloud without taking your vulnerabilities along
- Security controls to guarantee that neither the CSP nor attackers can compromise your sensitive data in the Cloud

The paradigm shift

- **Regulatory Compliant Cloud Computing (RC3)**
- An architecture that secures your data in Public Clouds while proving compliance to data-security regulations

RC3 Characteristics

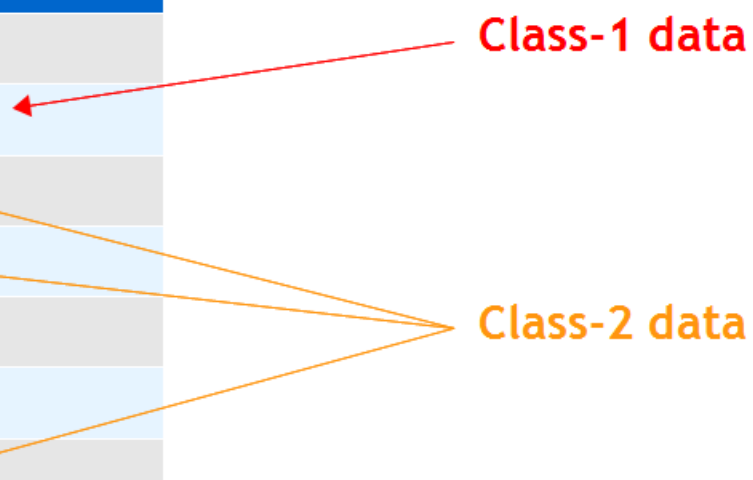
- Data Classification
- Distinct processing/storage zones
- Enterprise Key Management Infrastructure

RC3 Data Classification

- **Class-1**
  - Sensitive and **regulated** data
  - Examples: PII, PHI, etc.
- **Class-2**
  - Sensitive, but unregulated data
  - Examples: Application credentials, salaries, etc.
- **Class-3**
  - Non-sensitive (public) data

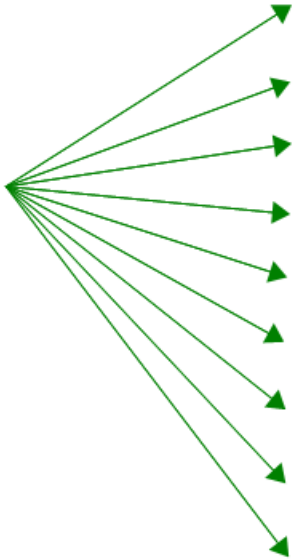
Data – Before RC3

Employee	
EID	12345
SSN	**111-22-3333**
Firstname	**John**
Lastname	**Doe**
HireDate	01/01/2011
Supervisor	23456
Salary	**55000**
Location	123
....	



Data – After RC3

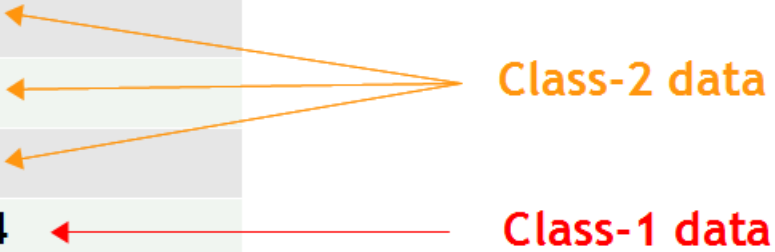
Class-3 data



Employee	
EID	12345
SSN	9999000000003912
Firstname	9999000000005126
Lastname	9999000000005127
HireDate	01/01/2011
Supervisor	23456
Salary	9999000000007184
Location	123
....	

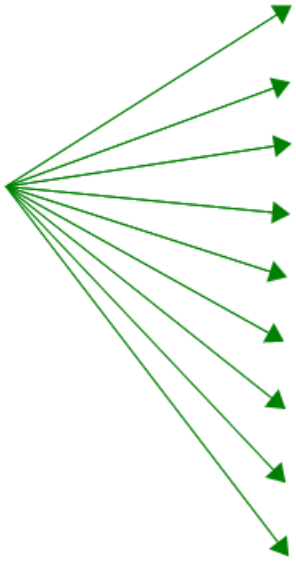
Data – Before RC3

Bank Account	
AID	**12345678**
Firstname	**Jane**
Lastname	**Smith**
SSN	**111-22-4444**
BranchID	123
AccountType	1
DateOpened	02/02/2012
Balance	794.25
....	



Data – After RC3

Class-3 data

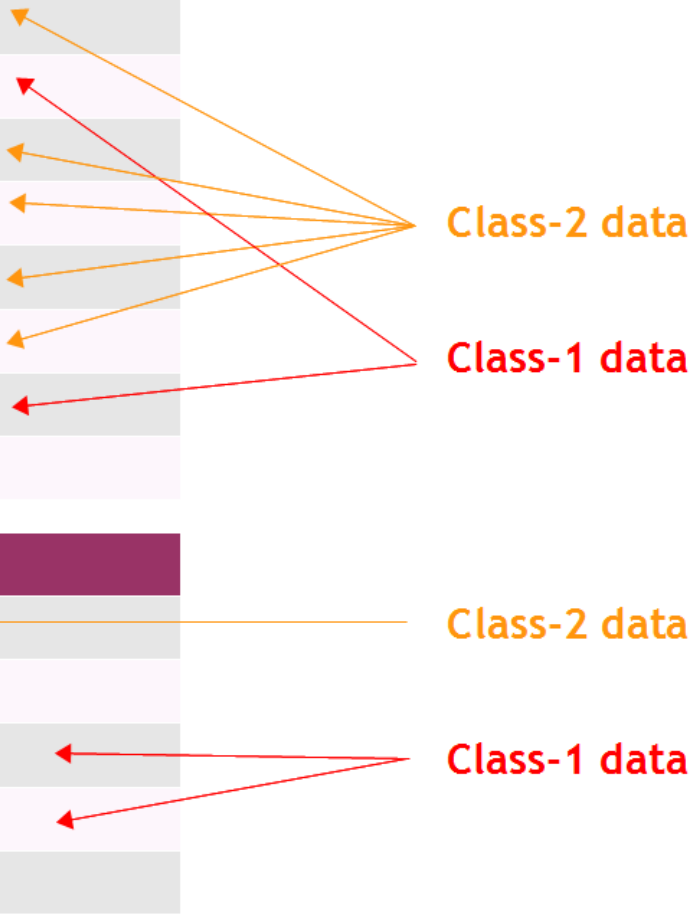


Bank Account	
AID	9999000000023745
Firstname	9999000000071847
Lastname	9999000000071849
SSN	9999000000088764
BranchID	123
AccountType	1
DateOpened	02/02/2012
Balance	794.25
....	

Data – Before RC3

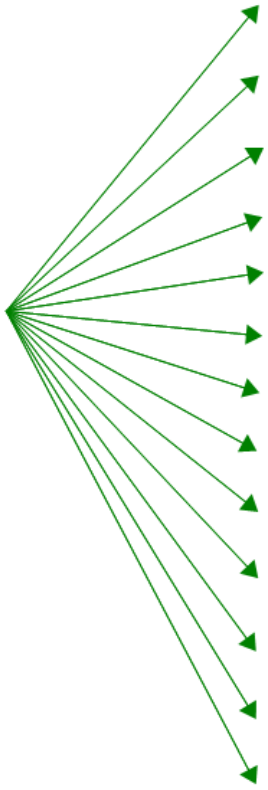
Patient	
PID	**1234567**
SSN	**111-222-5555**
Firstname	**John**
Lastname	**Smith**
Gender	**M**
DateOfBirth	**03/03/1953**
BloodType	**O+**
….	

Blood Report	
PID	**1234567**
ReportDate	04/04/2012
RBC	**5.1**
WBC	**7.5**
….	



Data – After RC3

Class-3 data

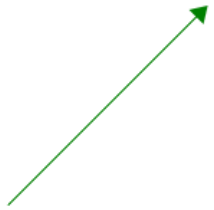


Patient	
PID	9999000000023745
SSN	9999000000057599
Firstname	9999000000045910
Lastname	9999000000045911
Gender	M
DateOfBirth	03/03/1953
BloodType	O+
....	

Blood Report	
PID	9999000000023745
ReportDate	04/04/2012
RBC	5.1
WBC	7.5
....	

Data – After RC3 – Alternative

```
<PatientRC3Data>
  <SSN>111-22-5555</SSN>
  <Firstname>John</Firstname>
  <Lastname>Smith</Lastname>
</PatientRC3Data>
```

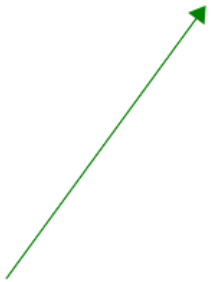


Patient	
PID	9999000000023745
RC3Data	9999000000079921
Gender	M
DateOfBirth	03/03/1953
BloodType	O+
....	

Blood Report	
PID	9999000000023745
ReportDate	04/04/2012
RBC	5.1
WBC	7.5
....	

Data – After RC3 – Alternative

```
<PatientRC3Data>
  <SSN>111-22-5555</SSN>
  <Firstname>John</Firstname>
  <Lastname>Smith</Lastname>
  <Gender>M</Gender>
  <DOB>03/03/1953</DOB>
</PatientRC3Data>
```



Patient	
PID	9999000000023745
RC3Data	9999000000079921
BloodType	O+
....	

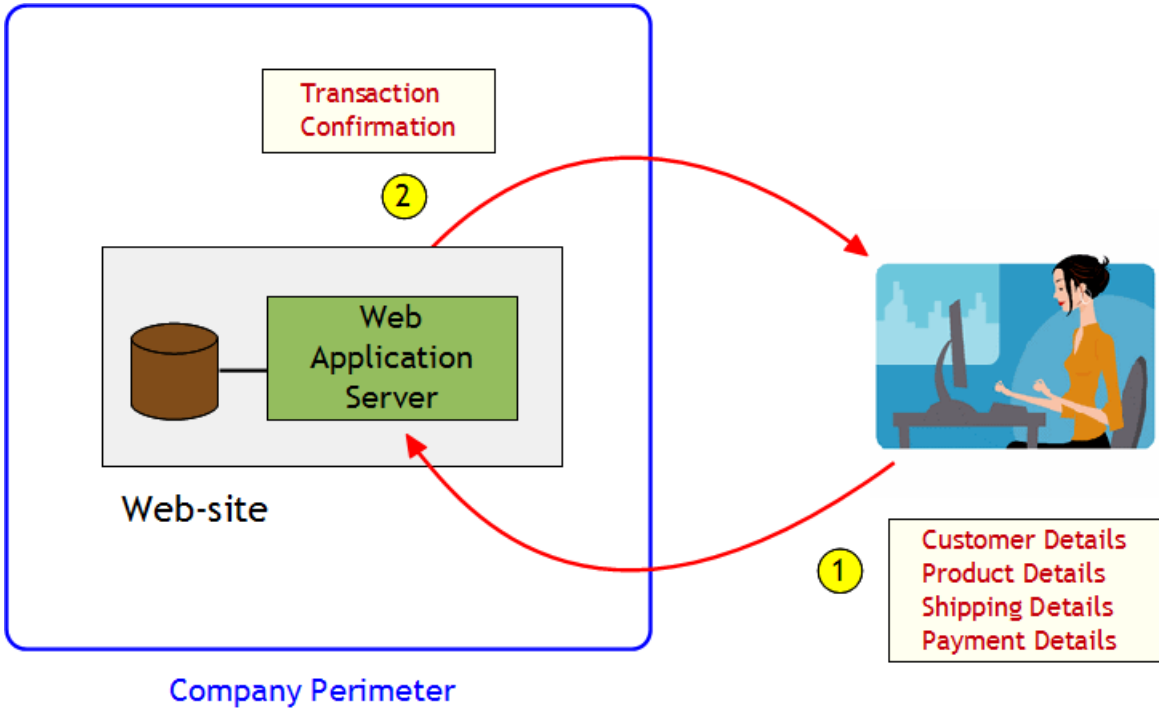
Blood Report	
PID	9999000000023745
ReportDate	04/04/2012
RBC	5.1
WBC	7.5
....	

RC3 Zones

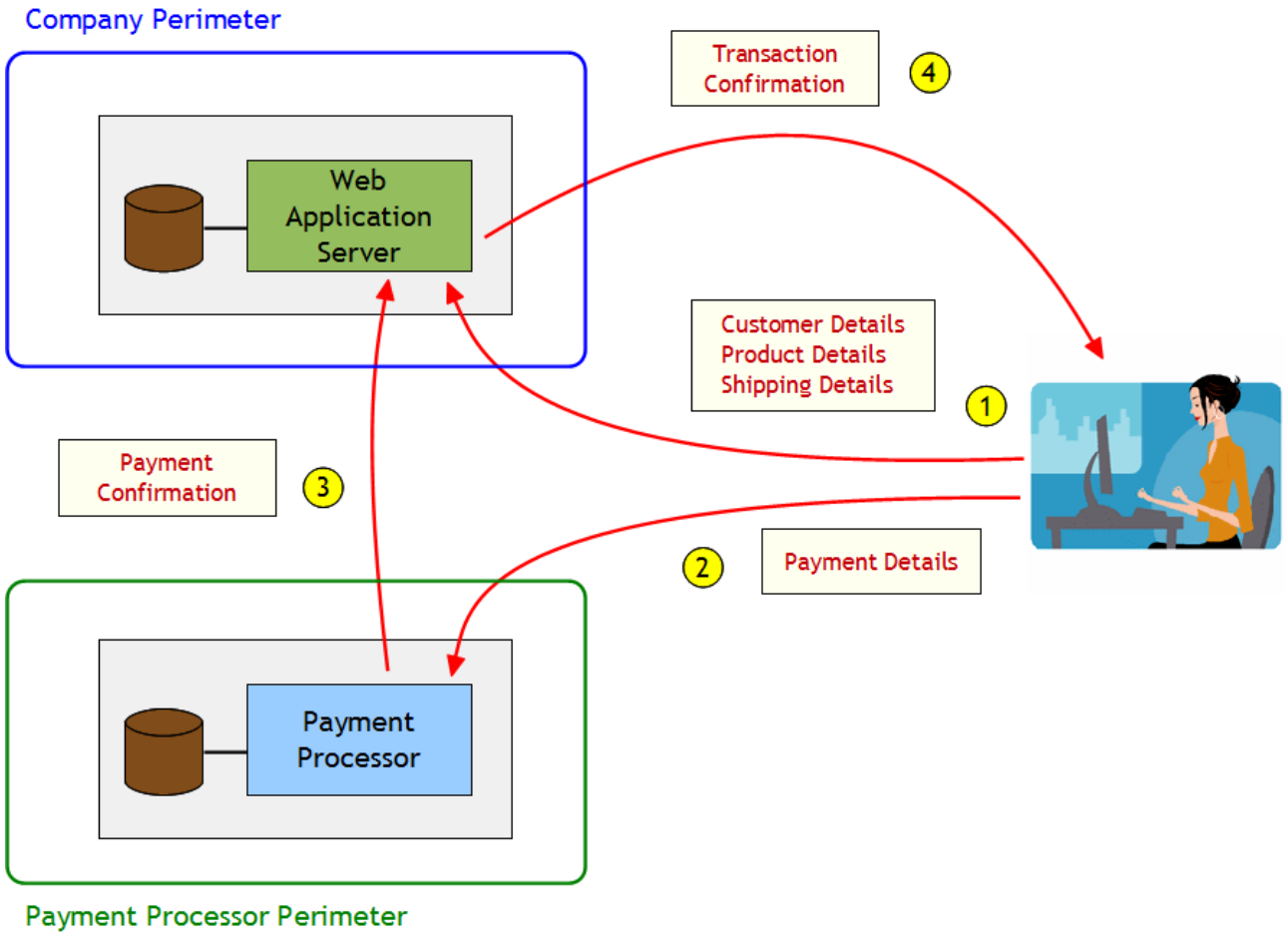
- Regulated (Secure) Zone
  - **Class-1** and **Class-2** data-processing and storage
  - Enterprise Key Management Infrastructure
- Cloud (Public) Zone
  - **Class-3** data-processing and storage
  - Can, optionally, store **C1**/**C2** tokens (**C3**-equivalent)
  - **NO CRYPTOGRAPHY**
  - **NO IDENTITY MANAGEMENT SYSTEM**
  - **NO INBOUND CONNECTION TO REGULATED ZONE FROM CLOUD ZONE**

WEB-APPLICATION MODEL

Basic web-application

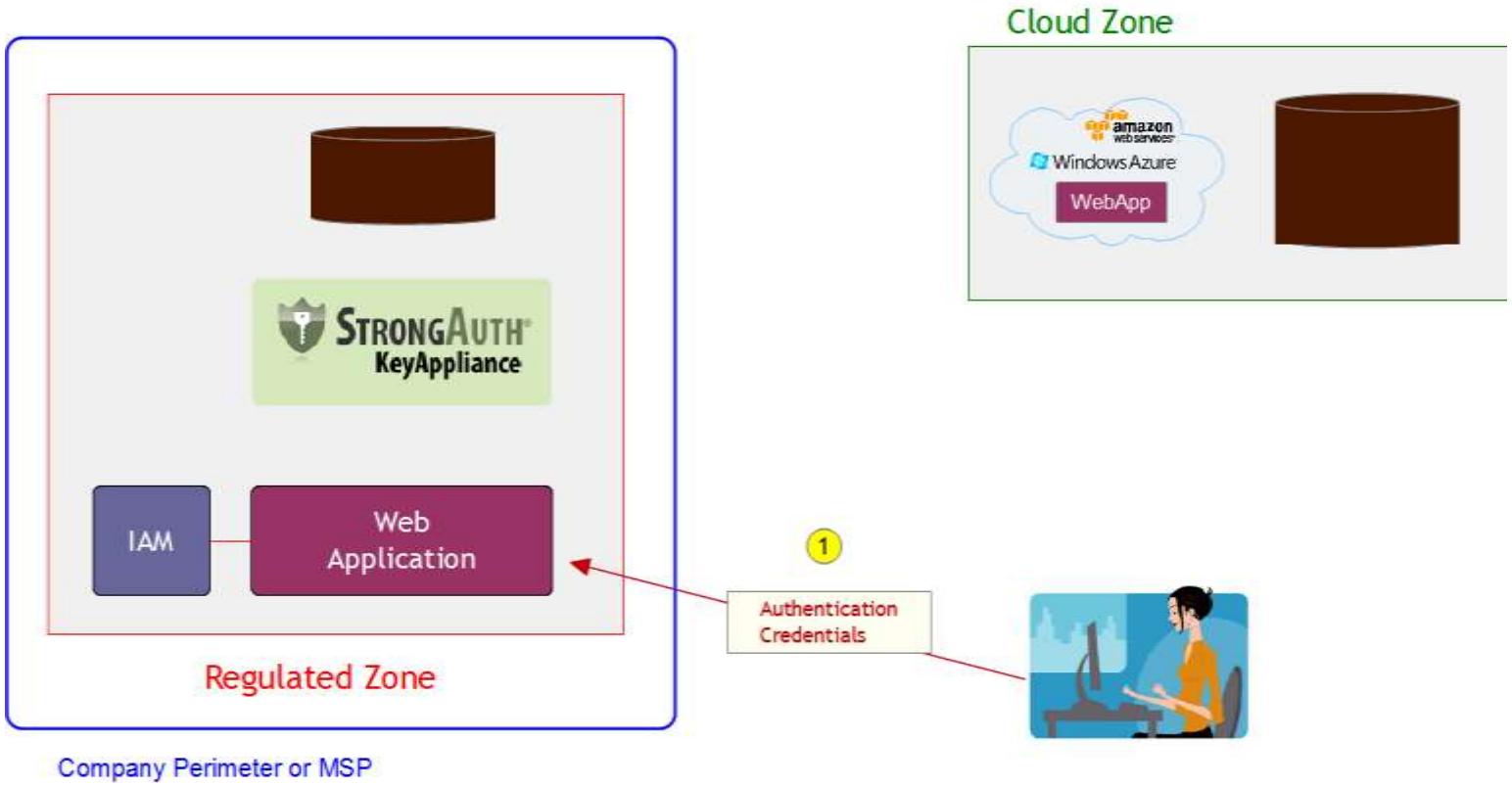


With HTTP Redirection

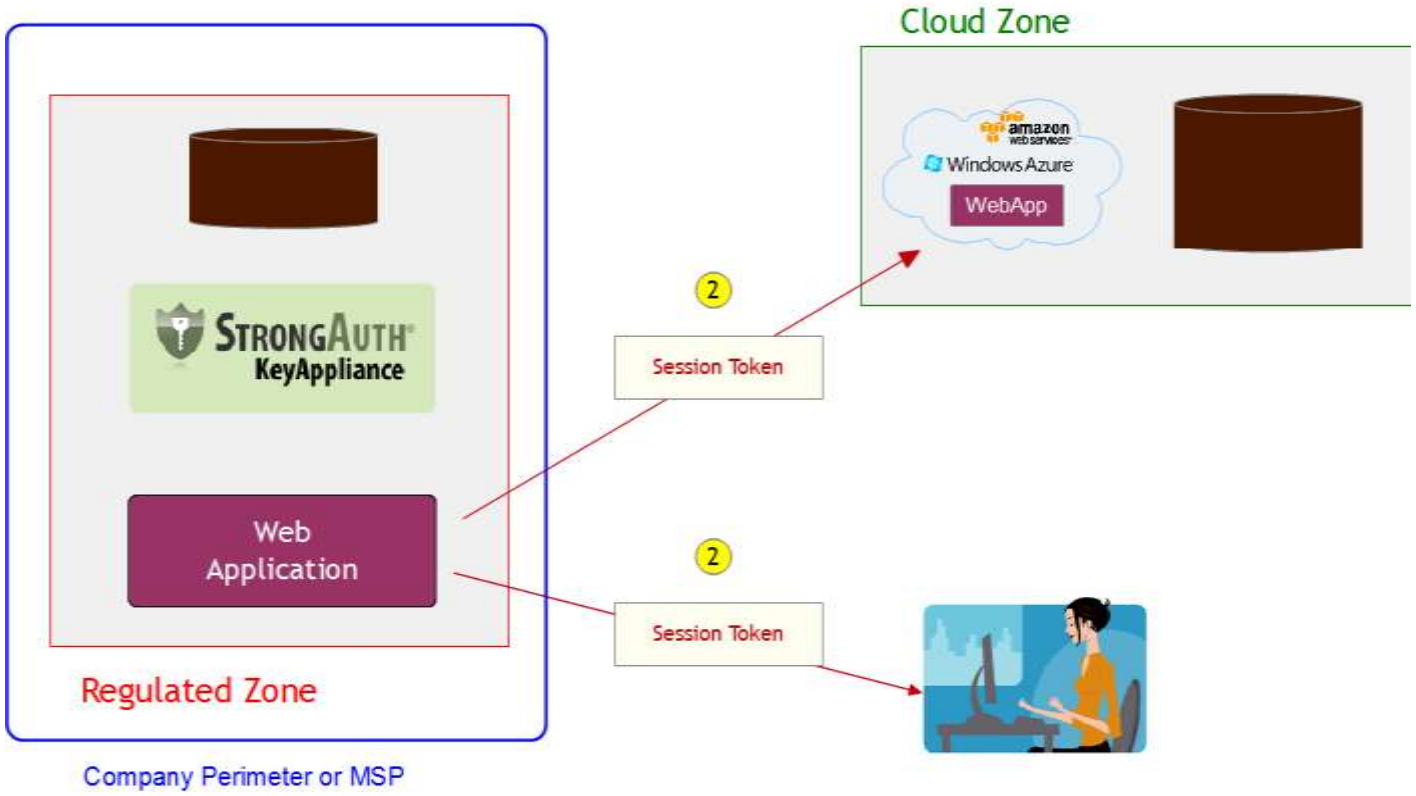


RC3 WEB-APPLICATION MODEL

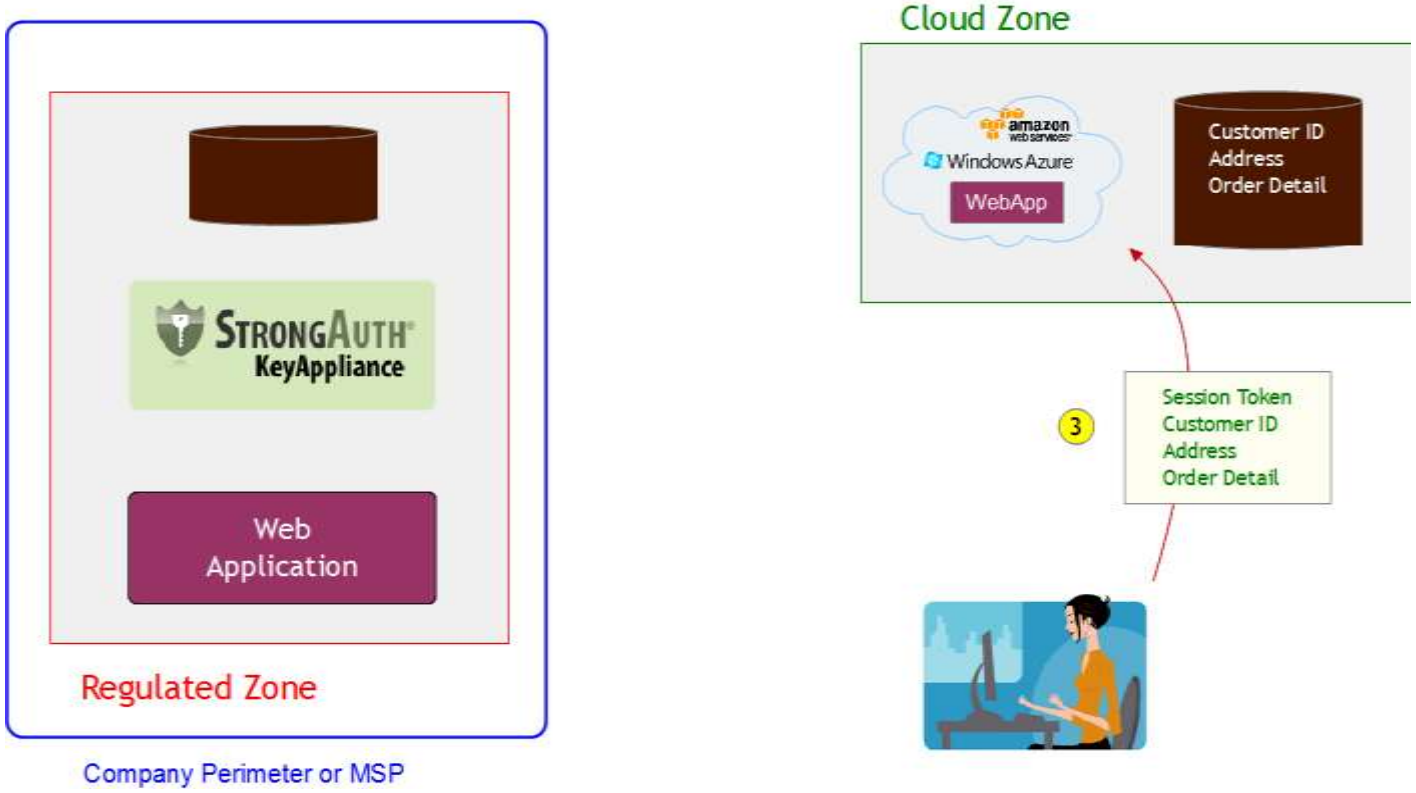
E-Commerce 1


Cloud Zone
amazon web services
Windows Azure
WebApp
StrongAuth
KeyAppliance
IAM
Web Application
1
Authentication Credentials
Regulated Zone
Company Perimeter or MSP

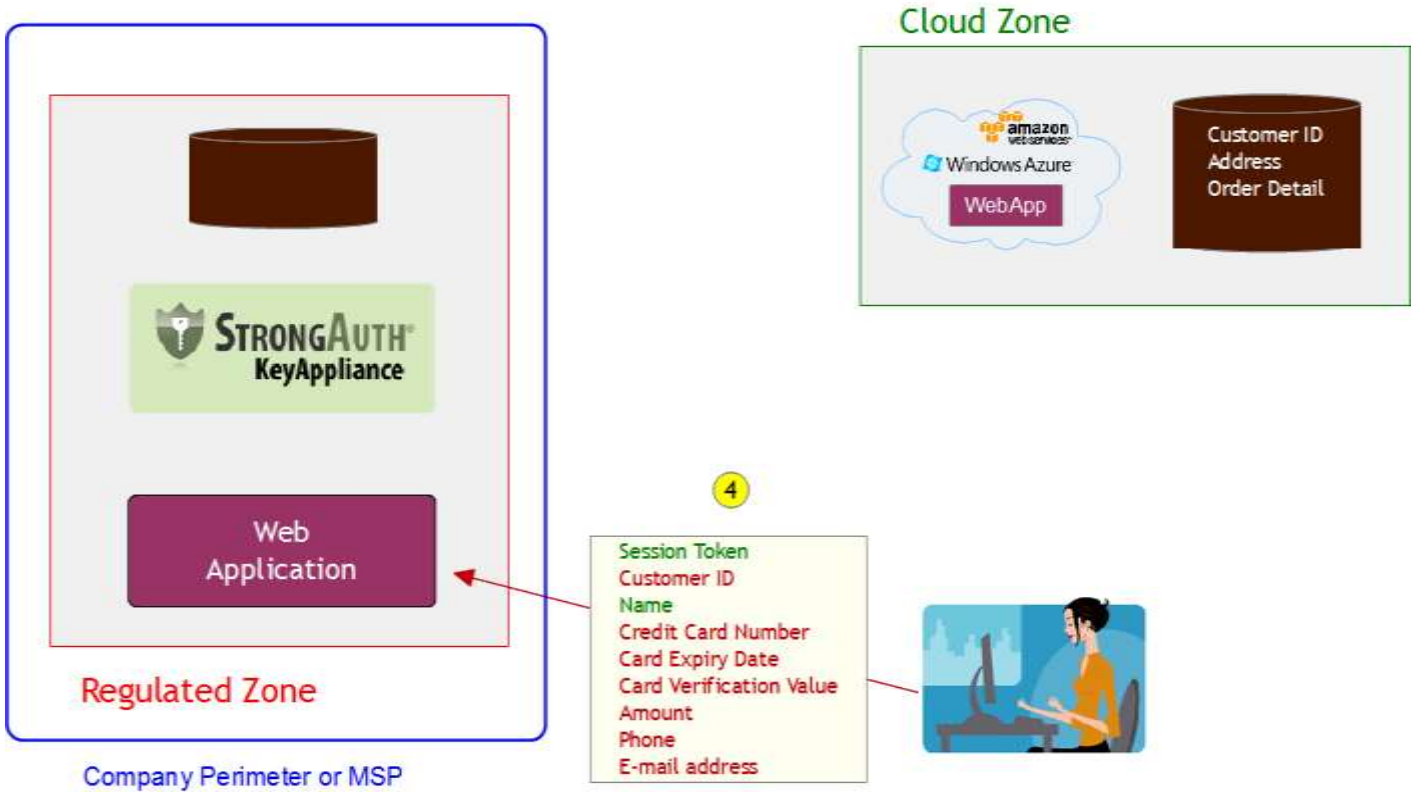
E-Commerce 2


Cloud Zone
amazon web services
Windows Azure
WebApp
StrongAuth
KeyAppliance
Web Application
2
Session Token
2
Session Token
Regulated Zone
Company Perimeter or MSP

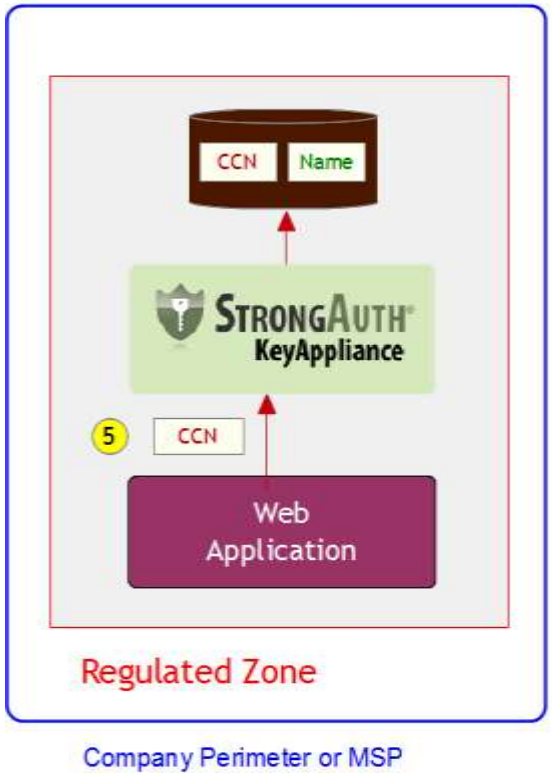
E-Commerce 3


StrongAuth
KeyAppliance
Web Application
Regulated Zone
Company Perimeter or MSP
Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail
3
Session Token
Customer ID
Address
Order Detail

E-Commerce 4

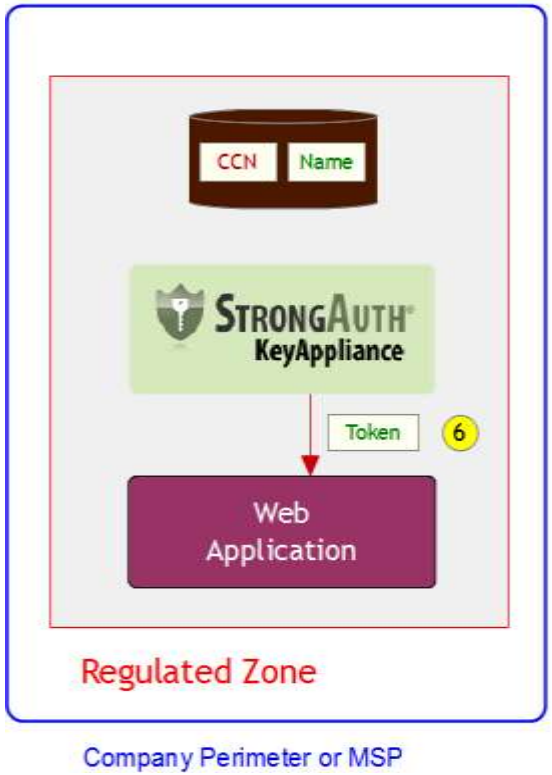

Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail
StrongAuth
KeyAppliance
Web
Application
Regulated Zone
Company Perimeter or MSP
4
Session Token
Customer ID
Name
Credit Card Number
Card Expiry Date
Card Verification Value
Amount
Phone
E-mail address

E-Commerce 5


CCN
Name
StrongAuth
KeyAppliance
5
CCN
Web
Application
Regulated Zone
Company Perimeter or MSP

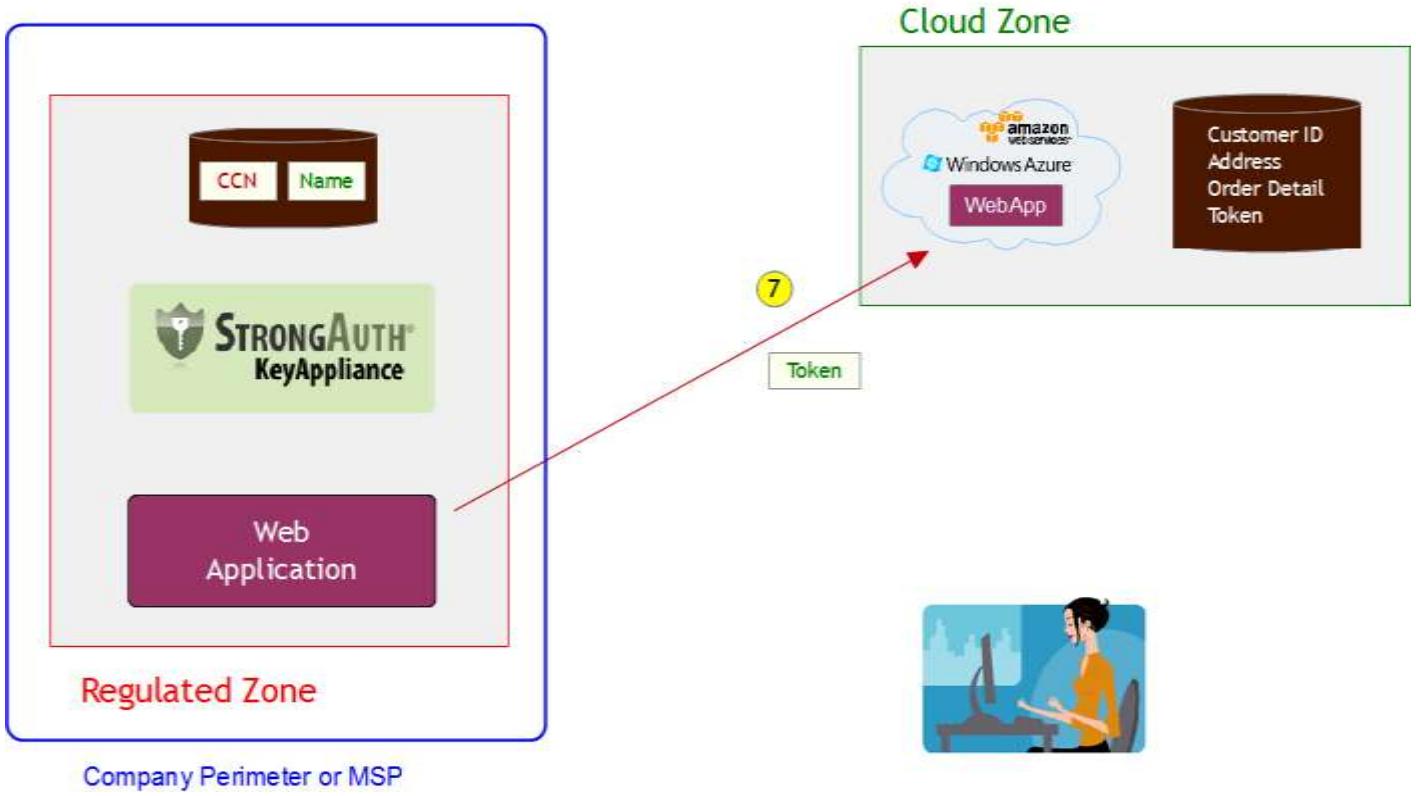

Cloud Zone
amazon
Windows Azure
WebApp
Customer ID
Address
Order Detail

E-Commerce 6

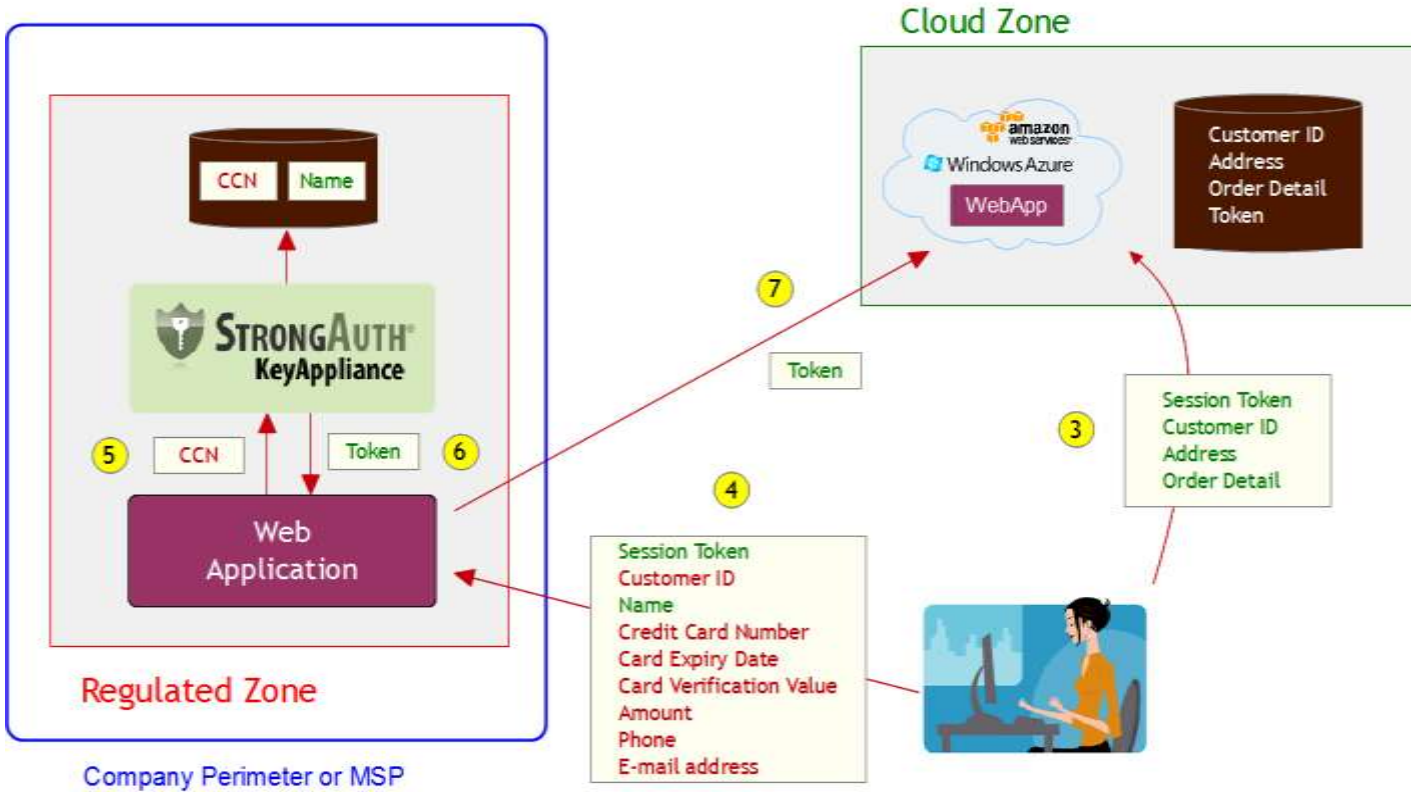

CCN
Name
StrongAuth
KeyAppliance
Token
6
Web
Application
Regulated Zone
Company Perimeter or MSP


Cloud Zone
amazon
Windows Azure
WebApp
Customer ID
Address
Order Detail

E-Commerce 7

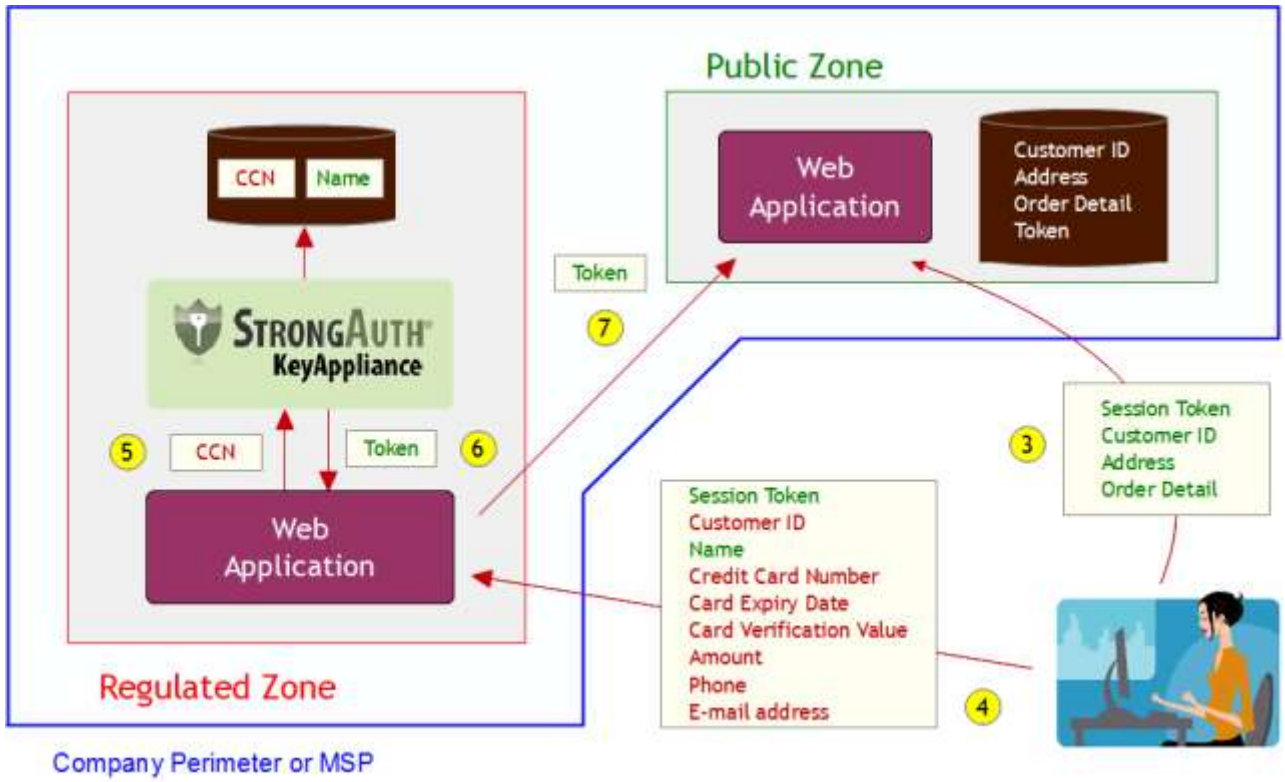

Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail
Token
7
Token
CCN
Name
StrongAuth
KeyAppliance
Web
Application
Regulated Zone
Company Perimeter or MSP

FULL TRANSACTION

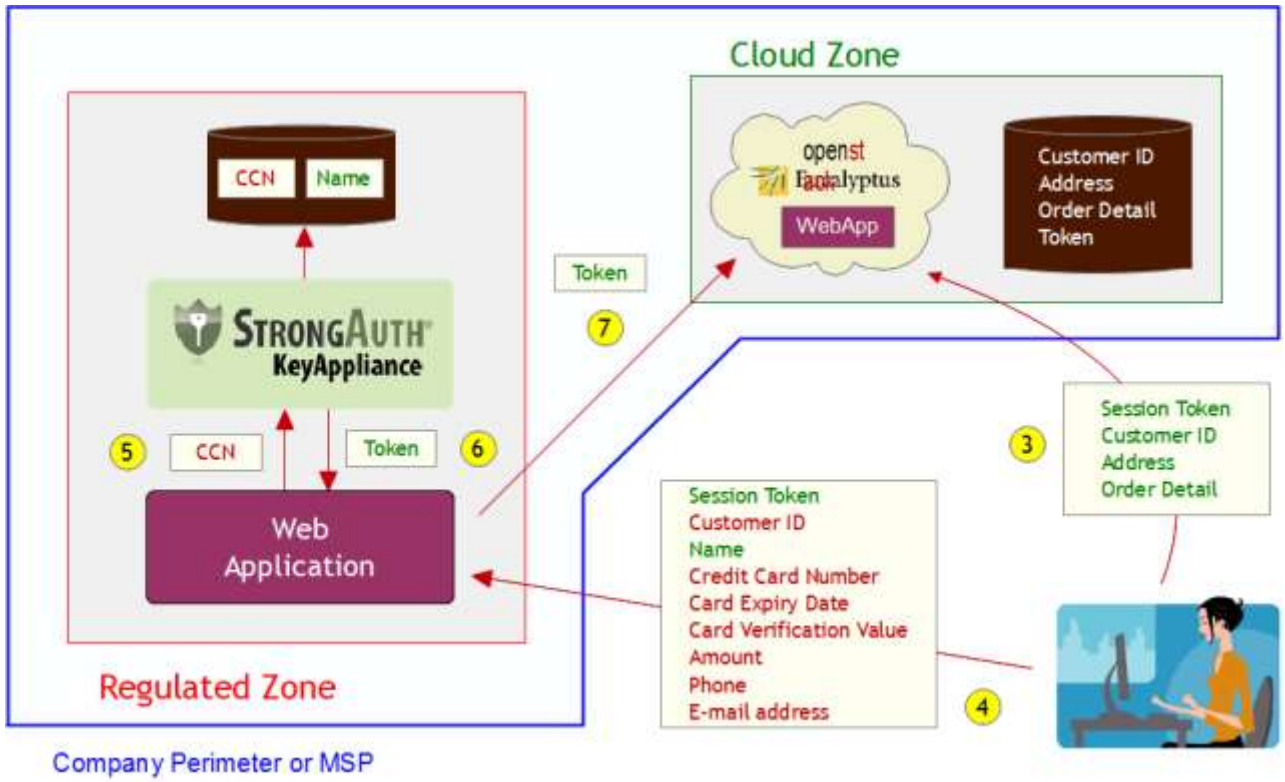


HOW DO YOU TRANSITION TO RC3?

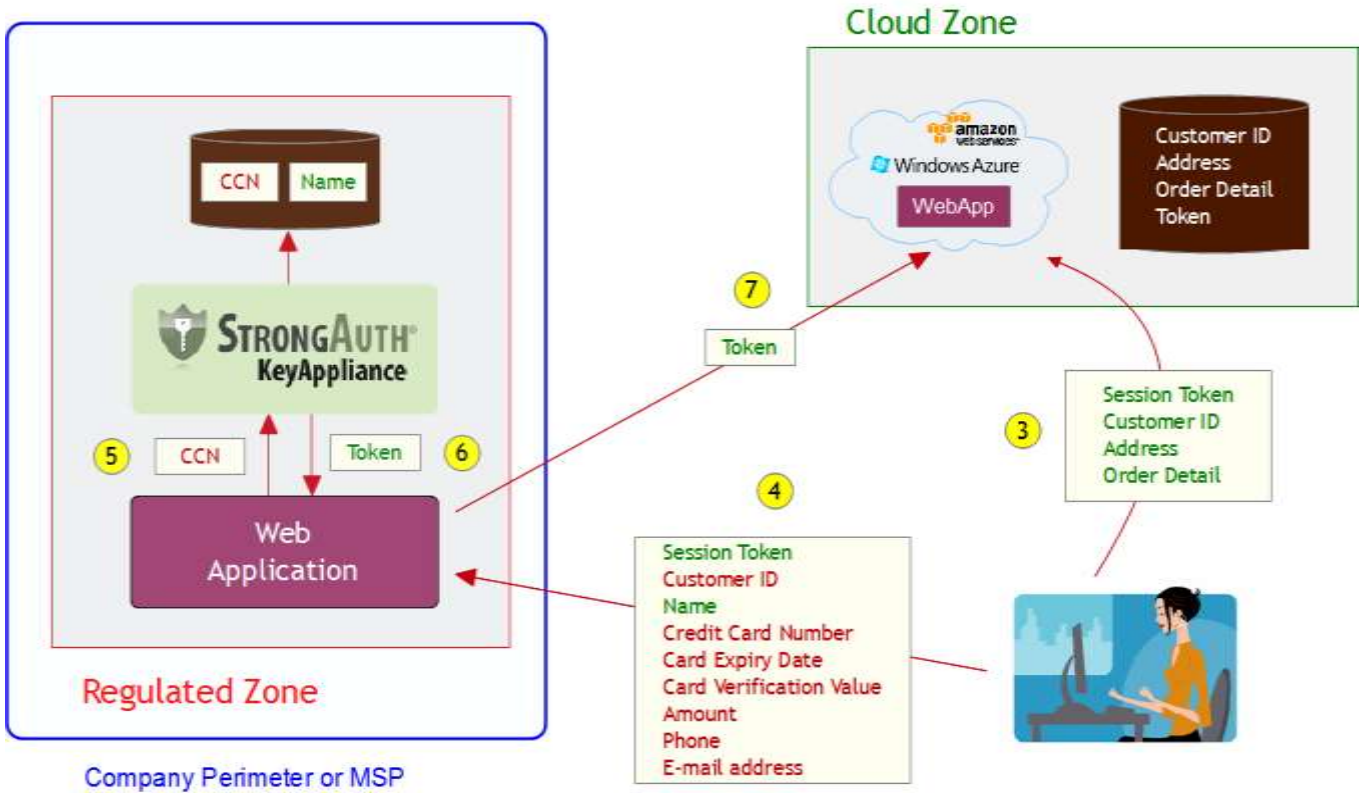
RC3 in the Enterprise



RC3 in the Private Cloud



RC3 in the Public Cloud



RC3 rules for the Cloud

- Do **NOT** store/use cryptographic keys in the Cloud
- Do **NOT** store/use plaintext sensitive data in the Cloud
- Do **NOT** store/use credentials to anything in the Cloud
- Do **NOT** use CSP-supplied cryptographic keys
- **DO** change your SSL key-pair frequently
- **DO** consider digitally signing/verifying Cloud data in the Regulated Zone
- Assume the worst – that your applications and data are on the open internet – and design/code for it

RC3 Resources

- While paper
  - http://www.ibm.com/developerworks/cloud/library/cl-regcloud/index.html
  - http://www.infoq.com/articles/regulatory-compliant-cloud-computing
- Cryptographic engine that enables RC3 applications (FOSS)
  - http:/www.cryptoengine.org
- CryptoCabinet (Sample RC3 web-application) (FOSS)
  - http://www.cryptocabinet.org

RSA CONFERENCE ASIA PACIFIC 2013

Thank You!