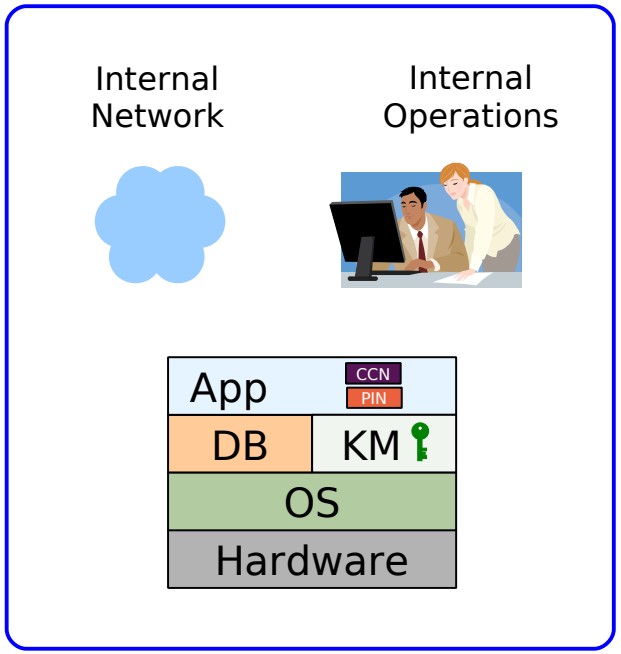
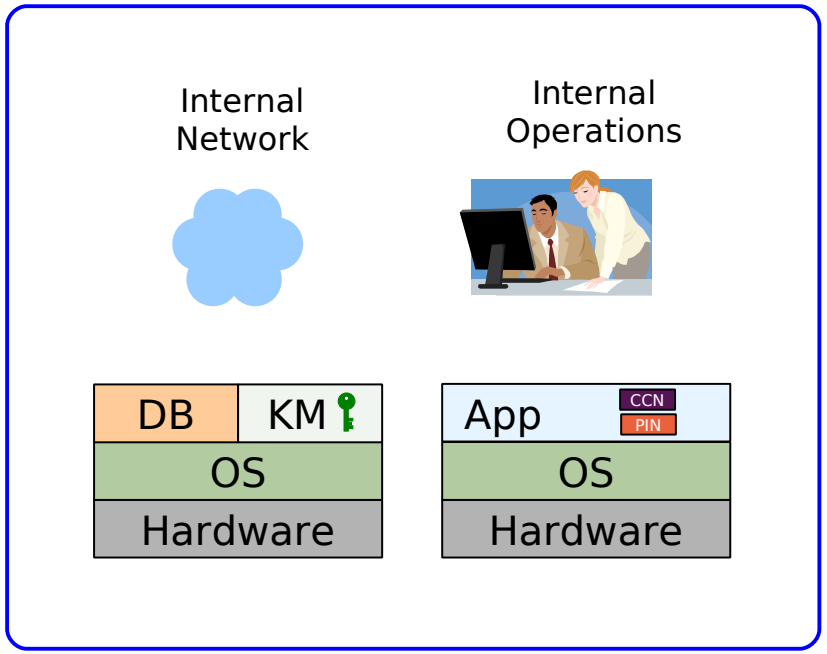
A web-application architecture for Secure Cloud Computing

In the beginning...



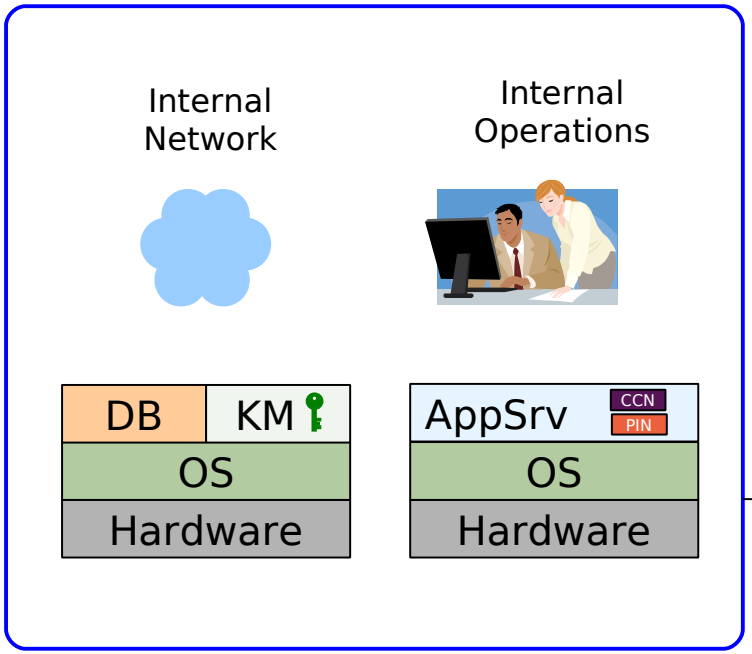
- Your data-center
- Your mainframe or mini-computer
- Your network
- Your Operations staff
- Your **single-tiered, monolithic** applications

The PC-LAN



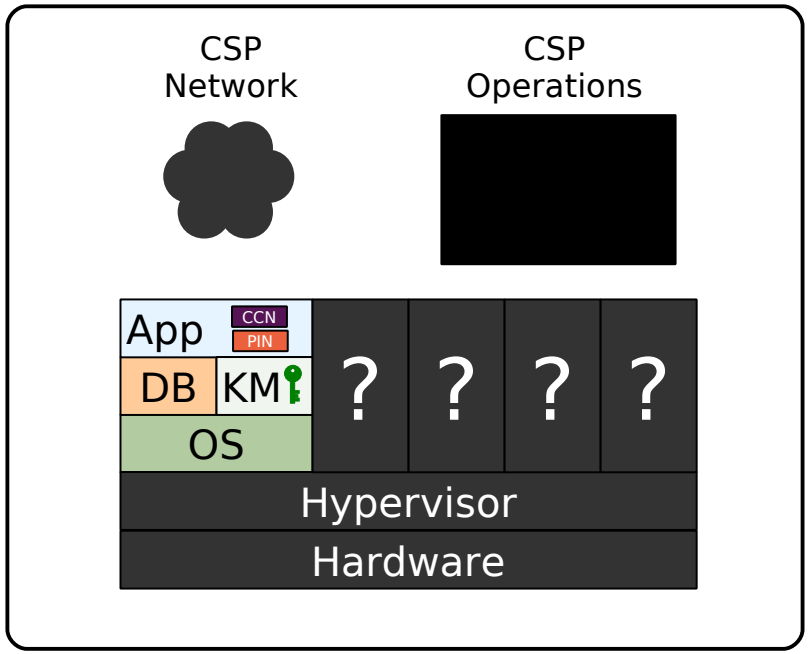
- Your data-center
- Your PC server
- Your PC client
- Your network
- Your firewall
- Your Operations staff
- Your **two-tiered, client-server** applications

The WWW



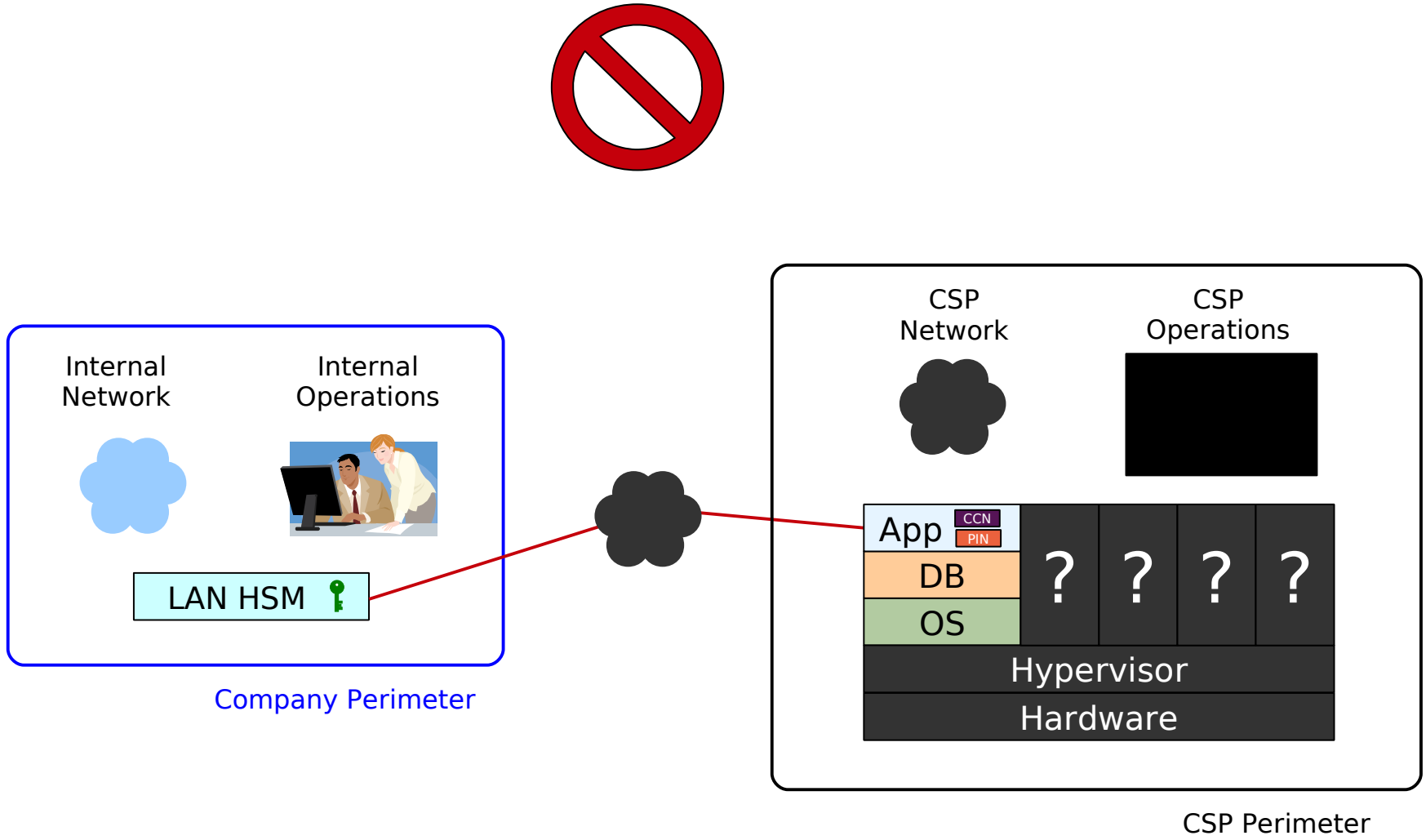
- Your data-center
- Your PC servers
- Your network
- Your firewall
- Your Operations staff
- Your **three-tiered, web** applications

The Public Cloud

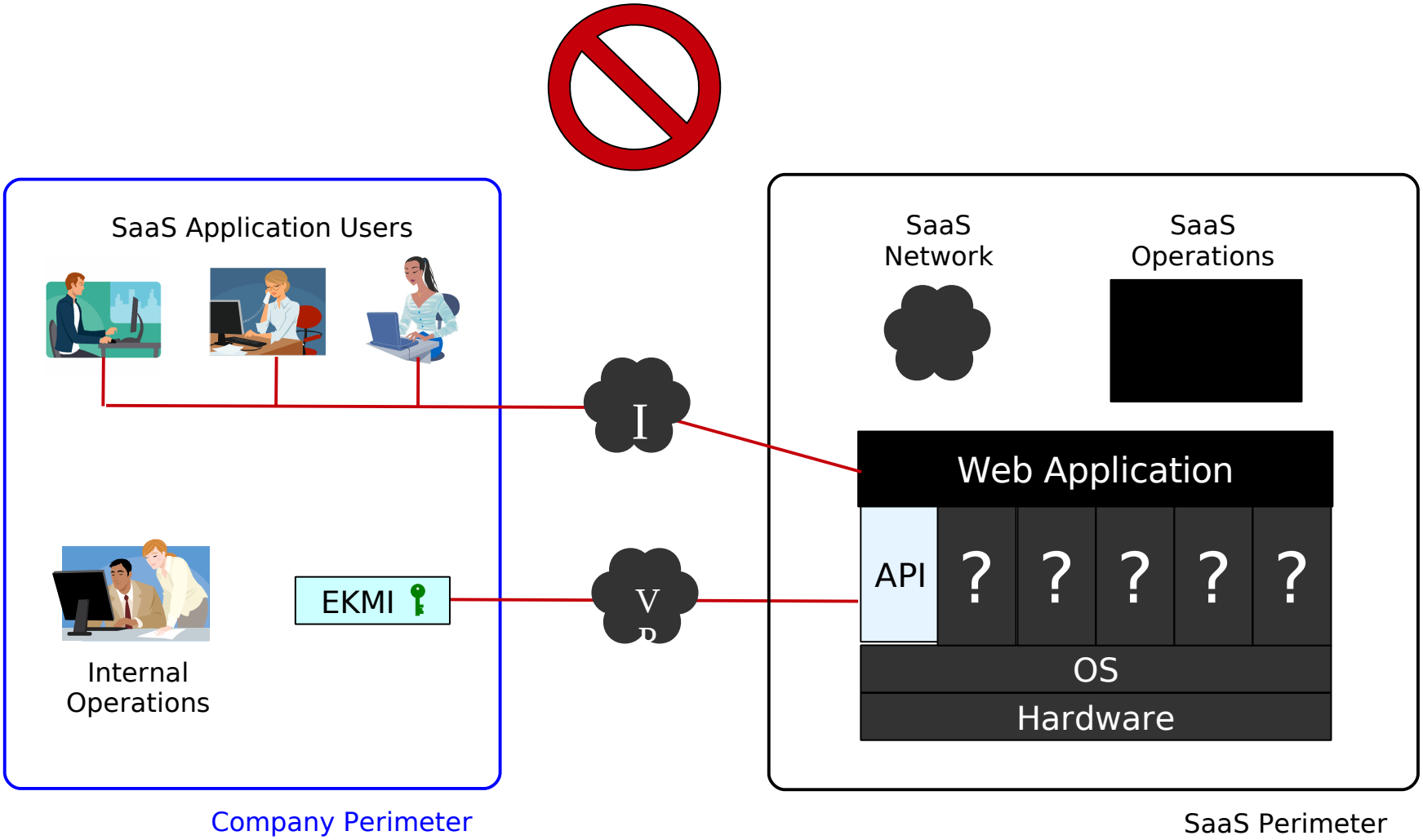


- Cloud Service Provider's (CSP) data-center
- CSP's hardware
- CSP's Hypervisor
- CSP's Network
- CSP's Operations staff
- Unknown guests in VMs
- Your applications and data?

EKM in the Public Cloud?



EKM with SaaS?



What's missing?

- Methodology to use the Cloud without being vulnerable
- Controls to ensure that neither CSP nor attacker can compromise your data

The Paradigm Shift

Regulatory Compliant Cloud Computing (RC3)

Architecture to secure data in the Cloud with proof of compliance.

RC3 Characteristics

1) Data-classification
2) Separate processing zones
3) Encryption Key Management Infrastructure

RC3 Data Classification

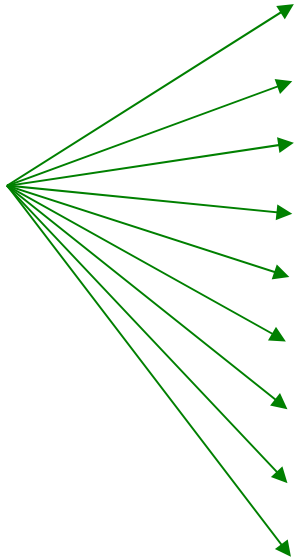
- **Class-1**
  - Sensitive and **regulated** data
  - SSN, CCN, ACH, Medical, etc.
- **Class-2**
  - Sensitive but **unregulated** data
  - Application Credentials, Salaries, Sales figures, etc.
- **Class-3**
  - Non-sensitive data

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

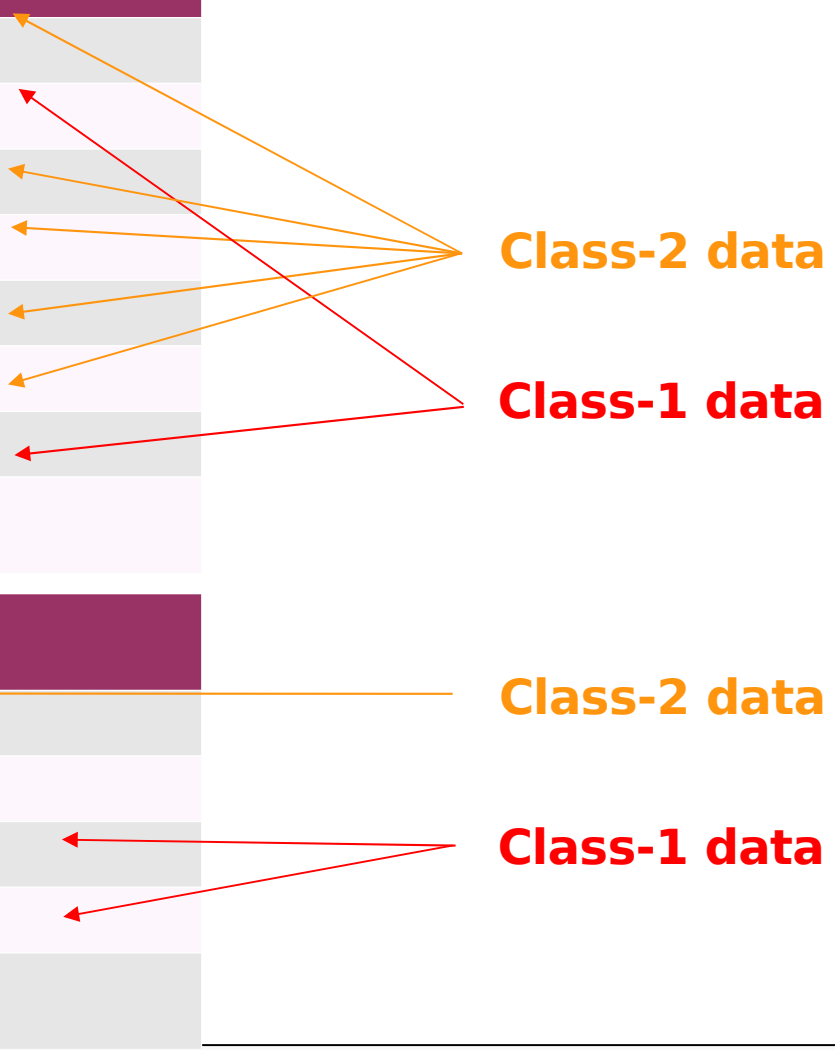


Bank Account	
AID	9999000000023745
Firstname	9999000000071847
Lastname	9999000000071849
SSN	9999000000088764
BranchID	123
AccountType	1
DateOpened	02/02/2012
Balance	794.25
....	

Data – Before RC3

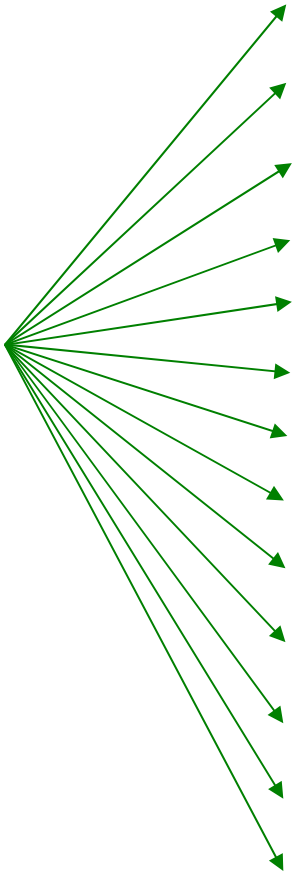
Patient	
PID	**1234567**
SSN	**111-222-5555**
Firstname	**John**
Lastname	**Smith**
Gender	**M**
DateOfBirth	**03/03/1953**
BloodType	**O+**
….	

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+
....	

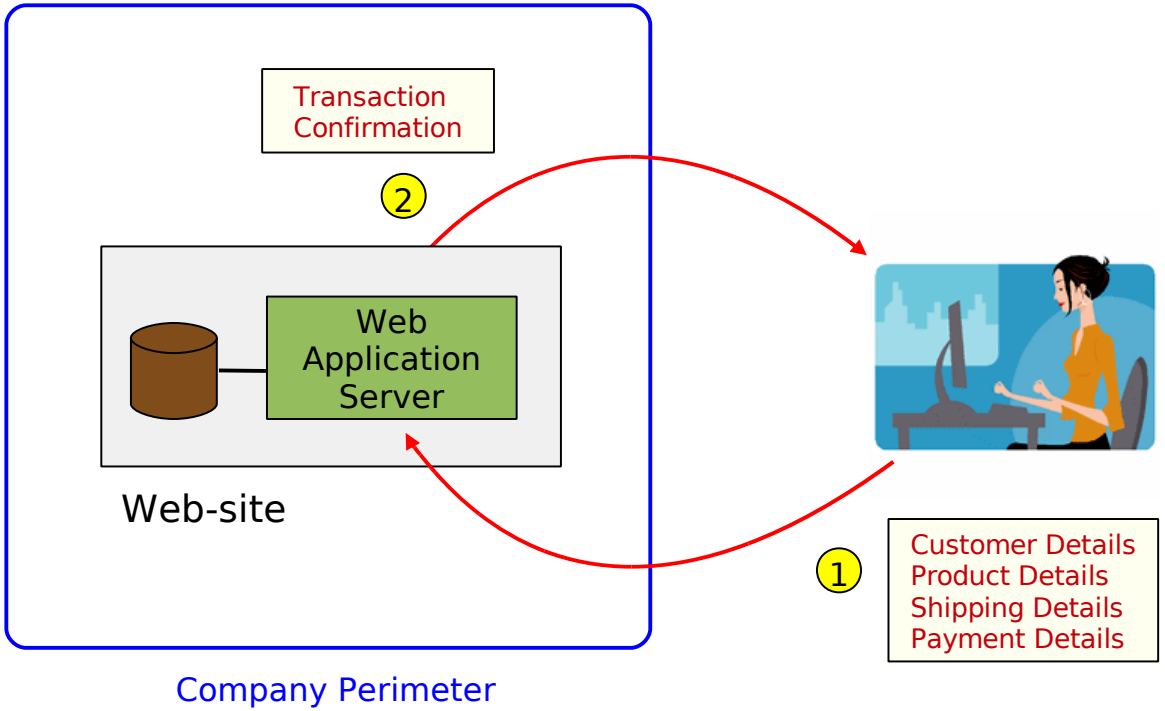
Blood Report	
PID	9999000000023745
ReportDate	04/04/2012
RBC	5.1
WBC	7.5
....	

RC3 Zones

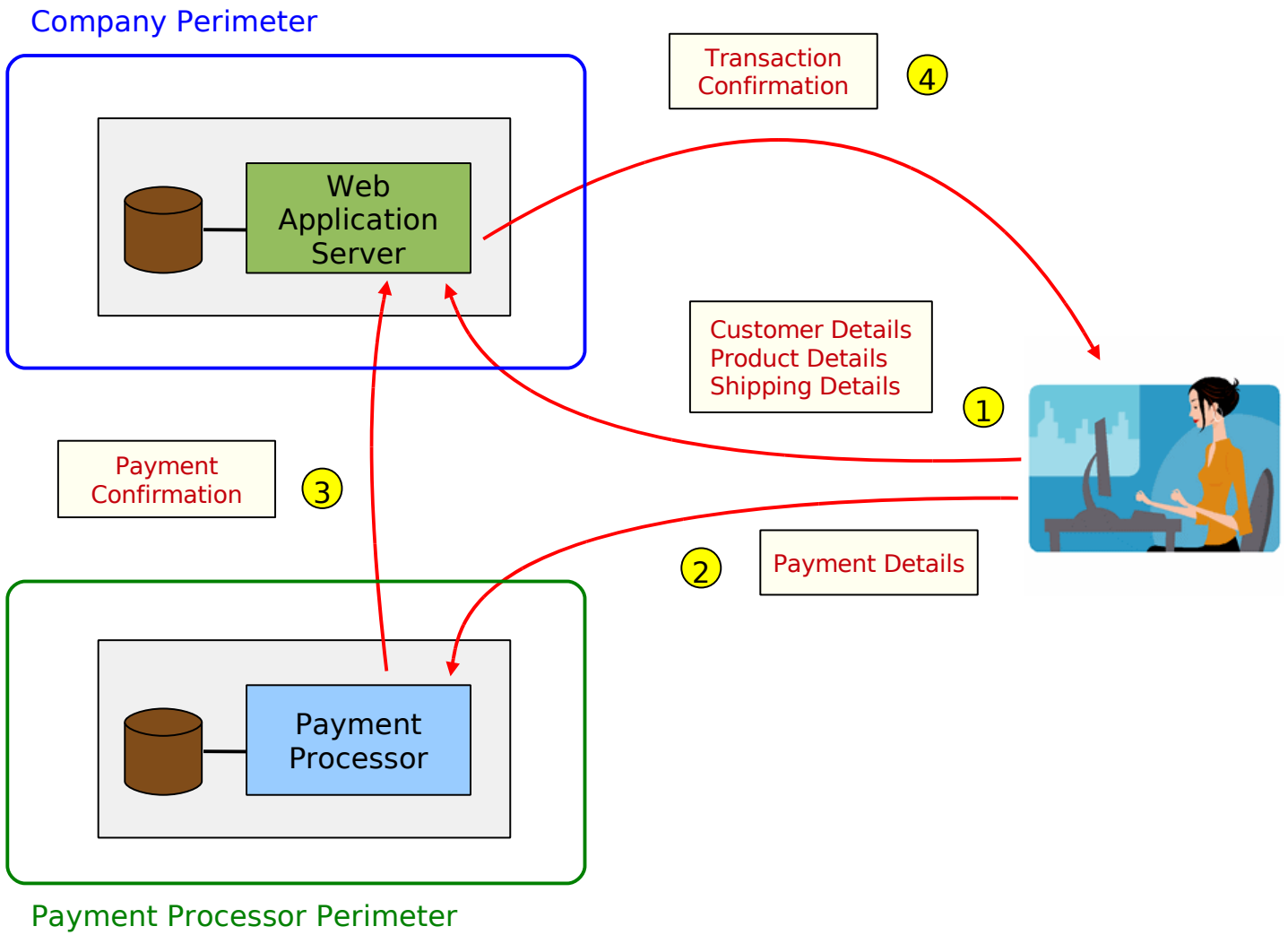
- Regulated Zone (Secure Zone)
  - Class-1 and Class-2 data-processing & storage
  - Enterprise Key Management Infrastructure (EKMI)
- Cloud Zone (Public Zone)
  - Class-3 data-processing & storage
  - Can, optionally, store C1/C2 tokens (C3-equivalent)
  - **NO CRYPTOGRAPHY**
  - **NO IDENTITY MANAGEMENT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

WEB-APPLICATION MODEL

Basic web application



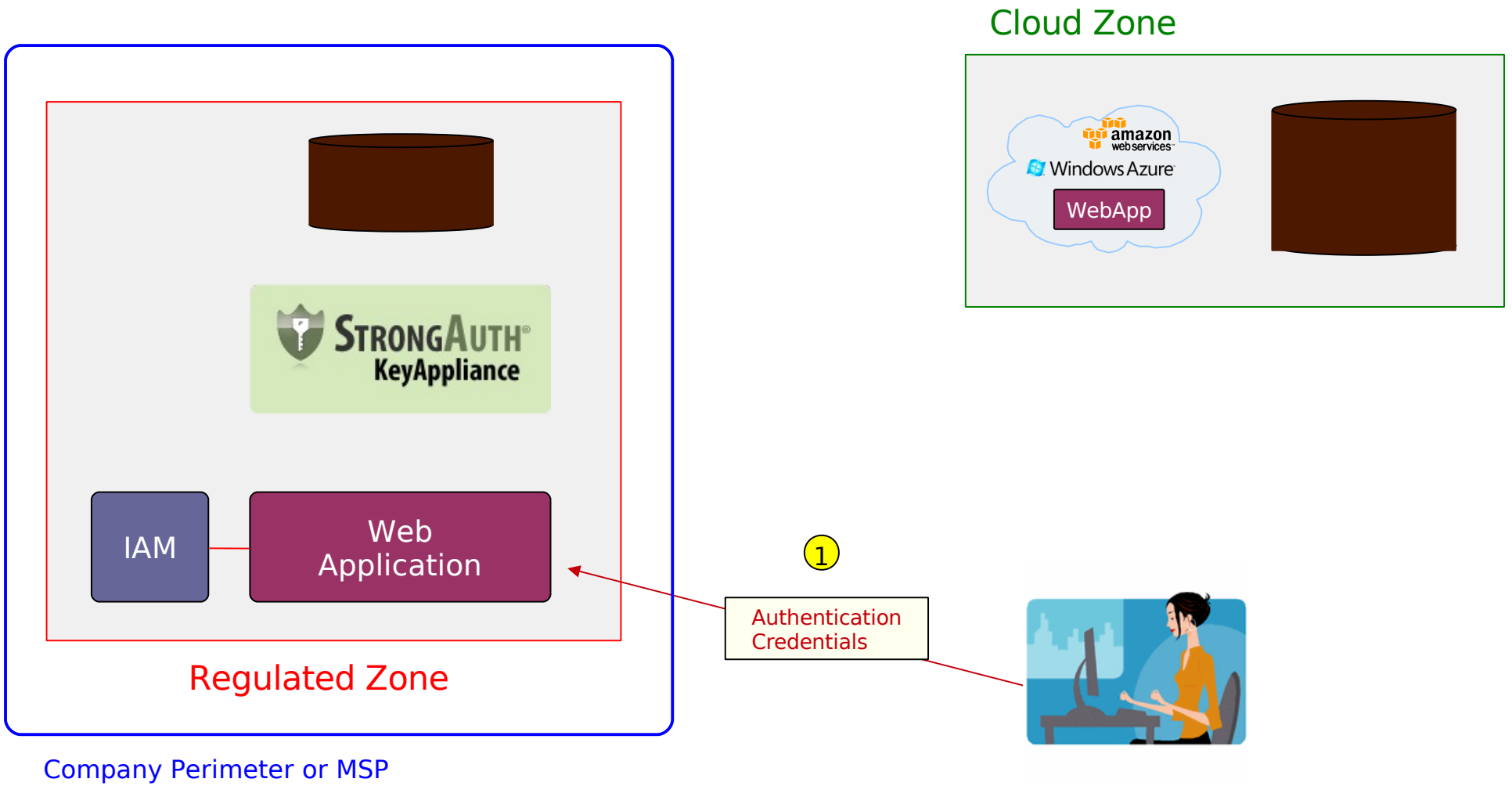
With Redirection



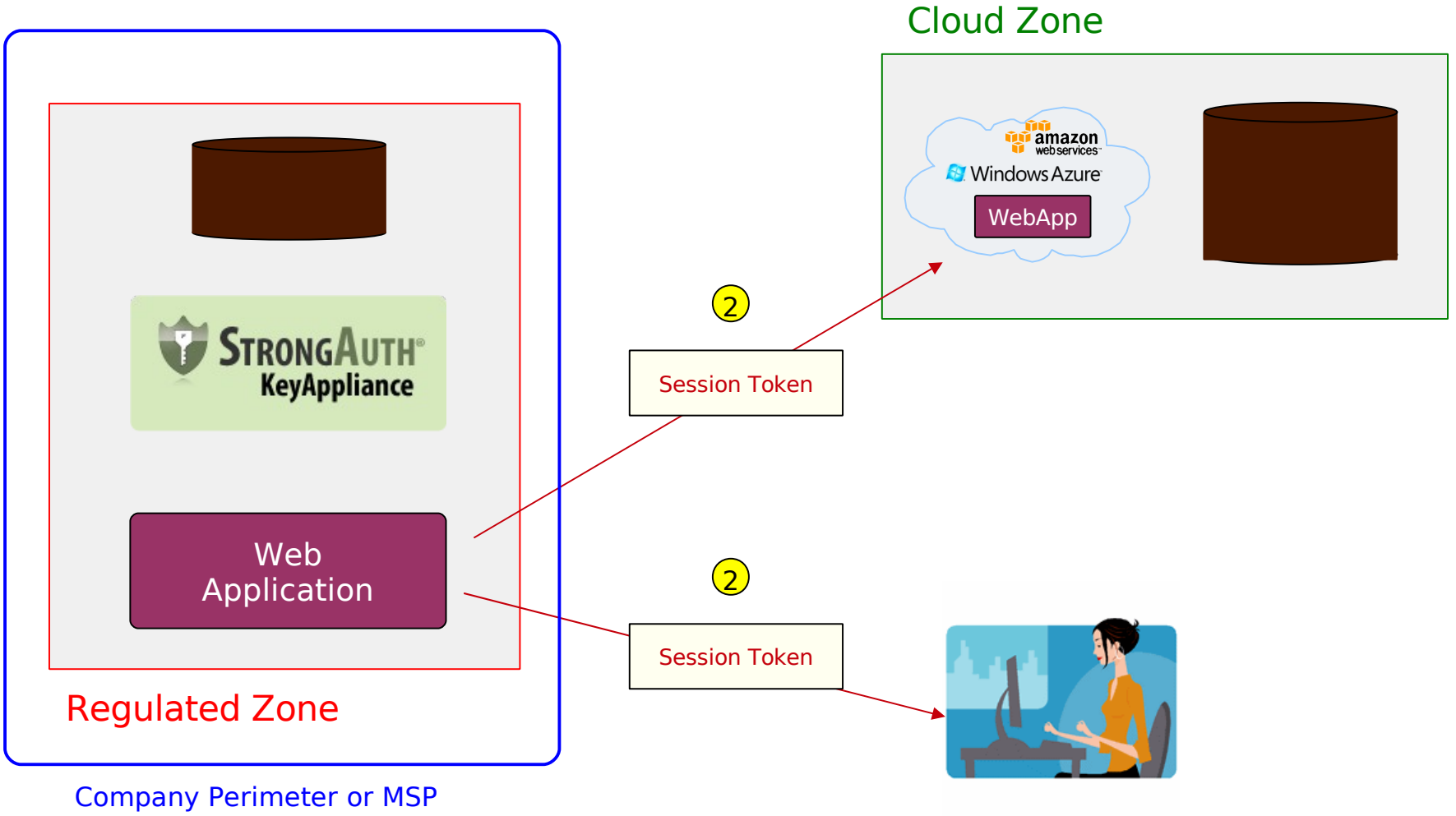
SECURE CLOUD COMPUTING FOR E-COMMERCE

RC3 MODEL

E-COMMERCE - 1

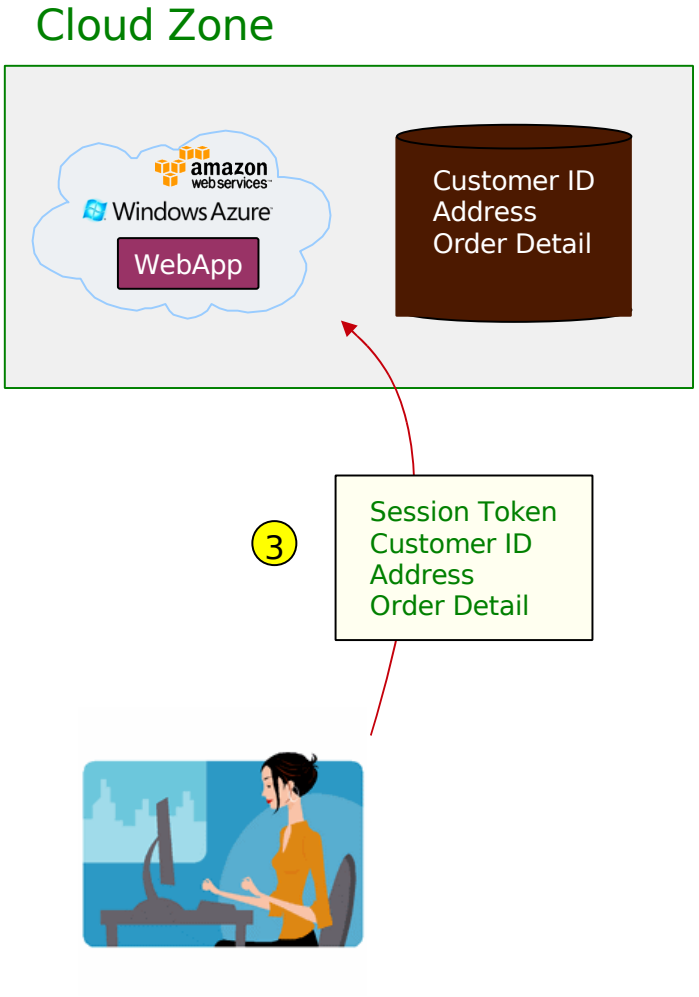

Cloud Zone
amazon web services
Windows Azure
WebApp
StrongAuth
KeyAppliance
IAM
Web Application
1
Authentication Credentials
Regulated Zone
Company Perimeter or MSP

E-COMMERCE - 2

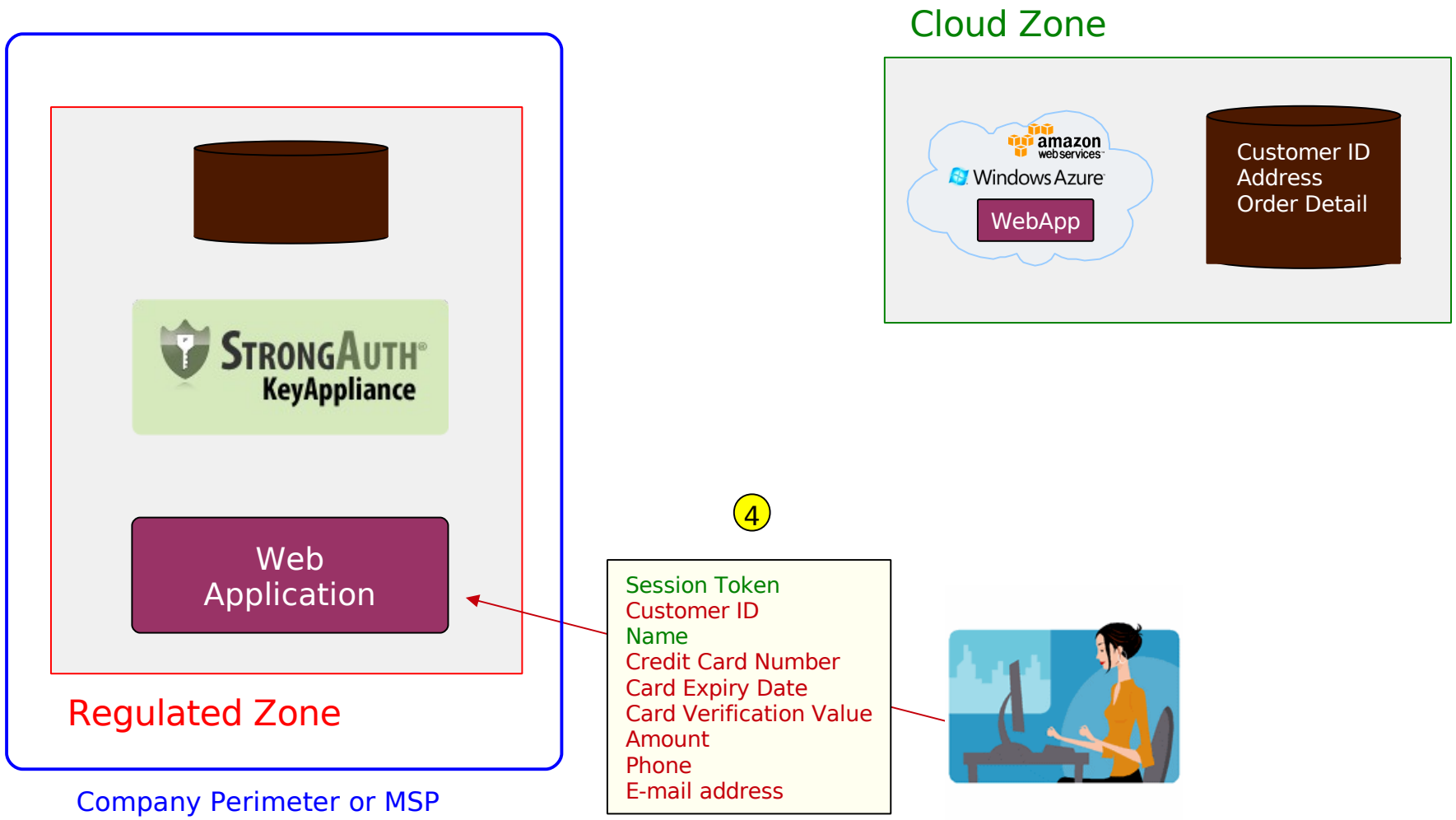

Cloud Zone
amazon web services
Windows Azure
WebApp
StrongAuth
KeyAppliance
Web Application
2
Session Token
2
Session Token
Regulated Zone
Company Perimeter or MSP

E-COMMERCE - 3

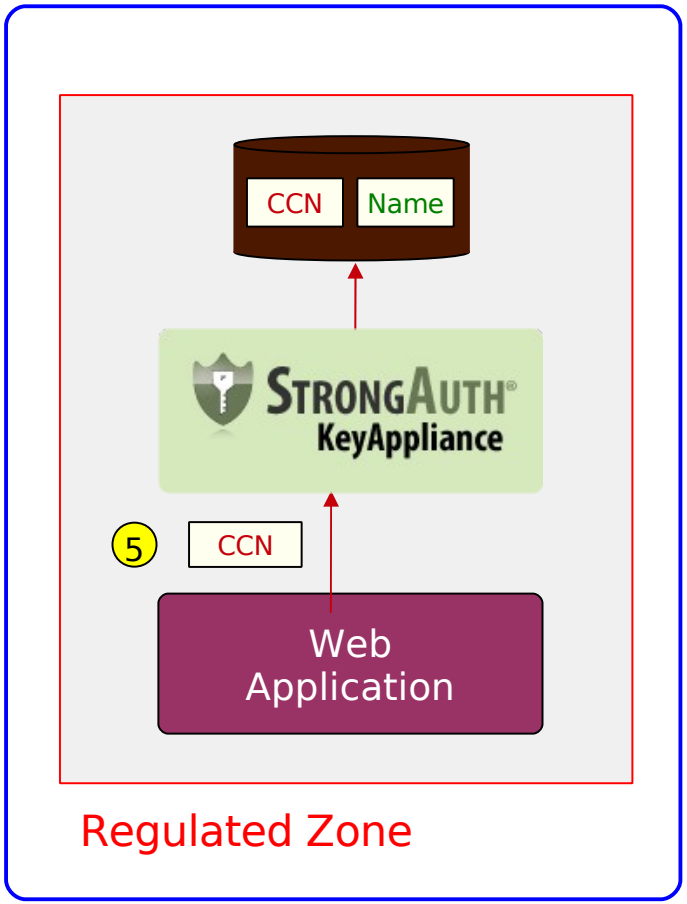

StrongAuth
KeyAppliance
Web Application
Regulated Zone
Company Perimeter or MSP


Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail
3
Session Token
Customer ID
Address
Order Detail

E-COMMERCE - 4

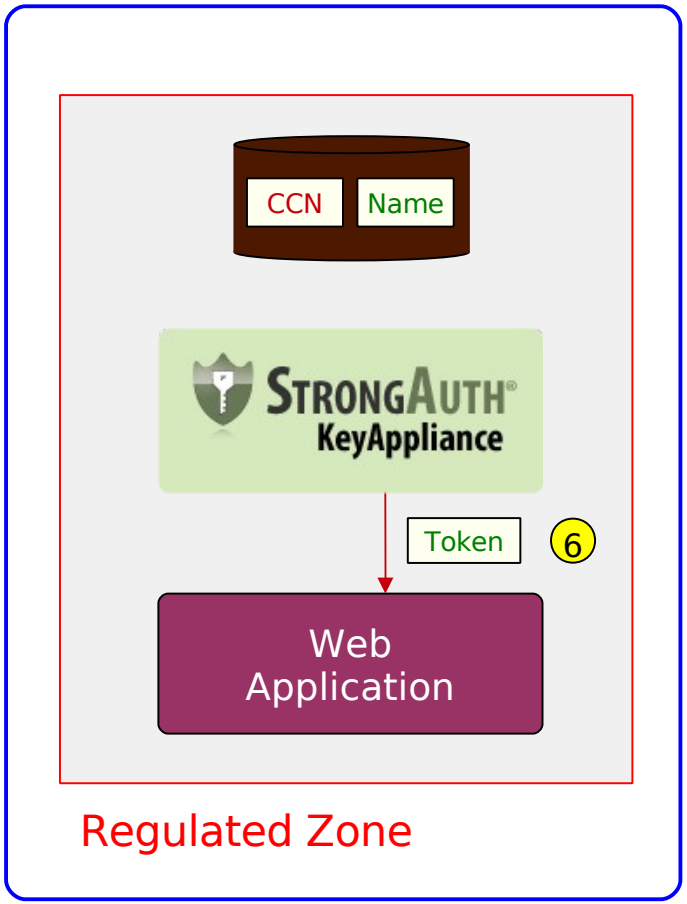

Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail
StrongAuth
KeyAppliance
Web Application
Regulated Zone
Company Perimeter or MSP
4
Session Token
Customer ID
Name
Credit Card Number
Card Expiry Date
Card Verification Value
Amount
Phone
E-mail address

E-COMMERCE - 5


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

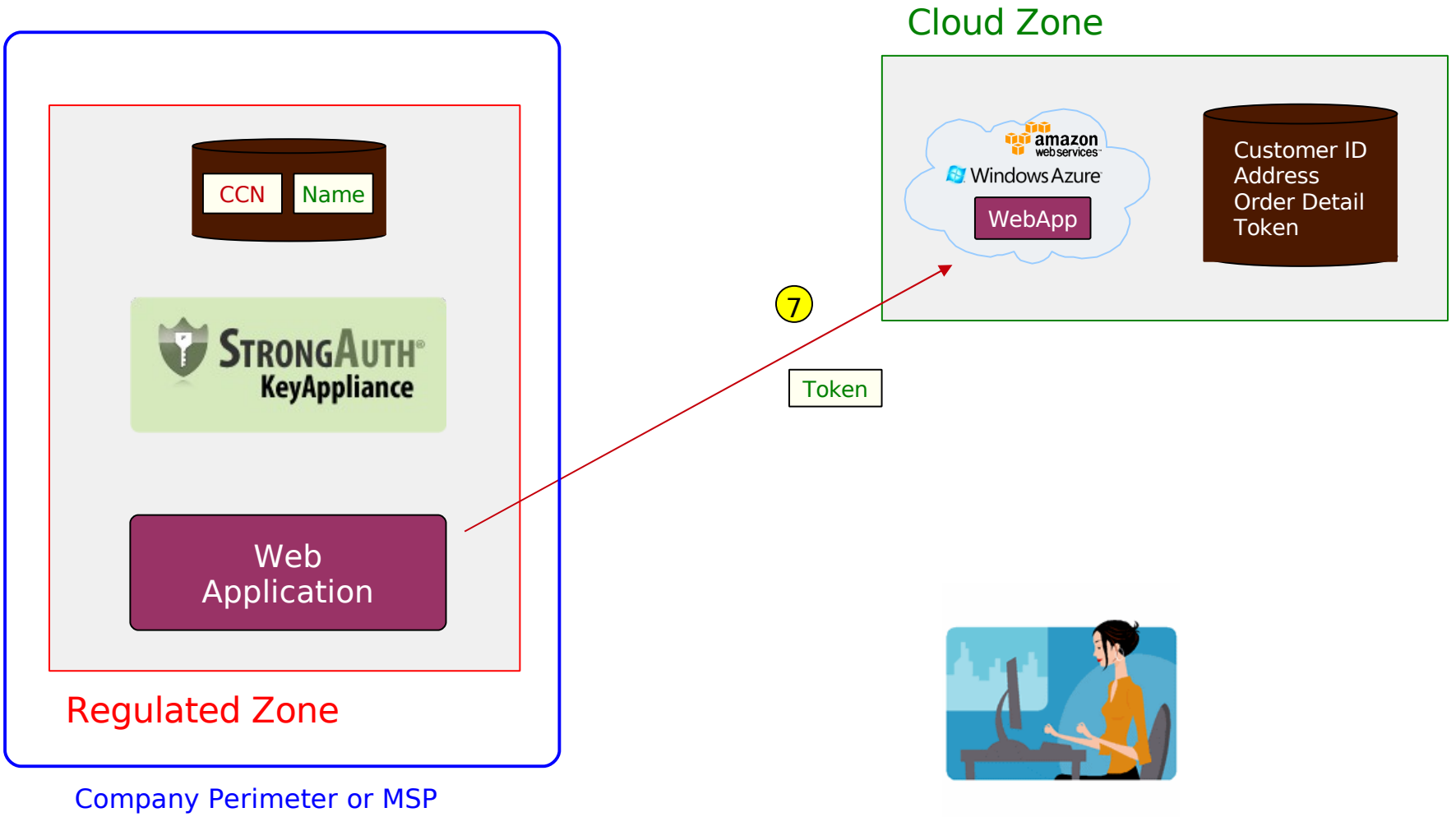

Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail

E-COMMERCE - 6

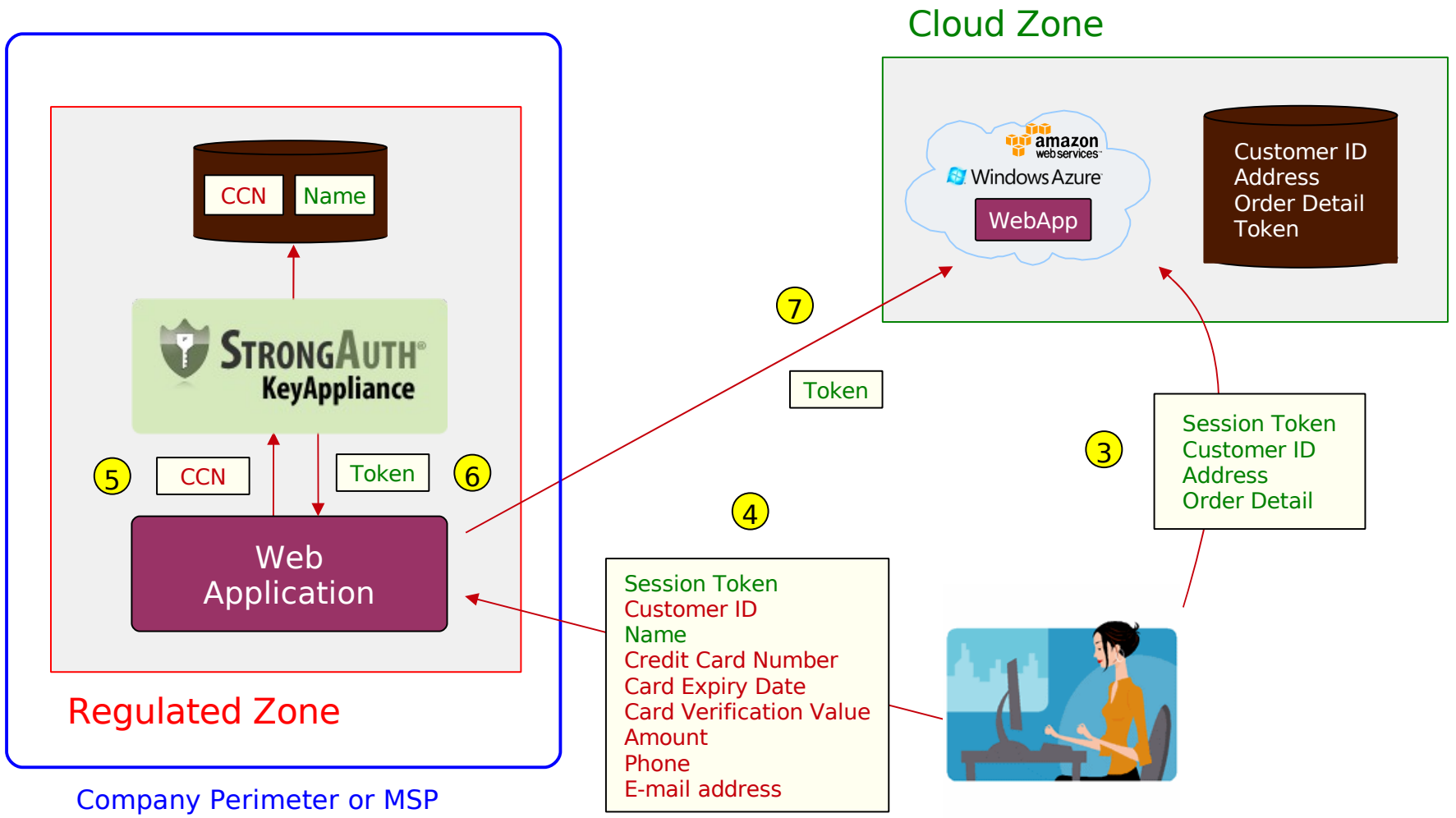

CCN
Name
StrongAuth
KeyAppliance
Token
6
Web Application
Regulated Zone
Company Perimeter or MSP


Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail

E-COMMERCE - 7

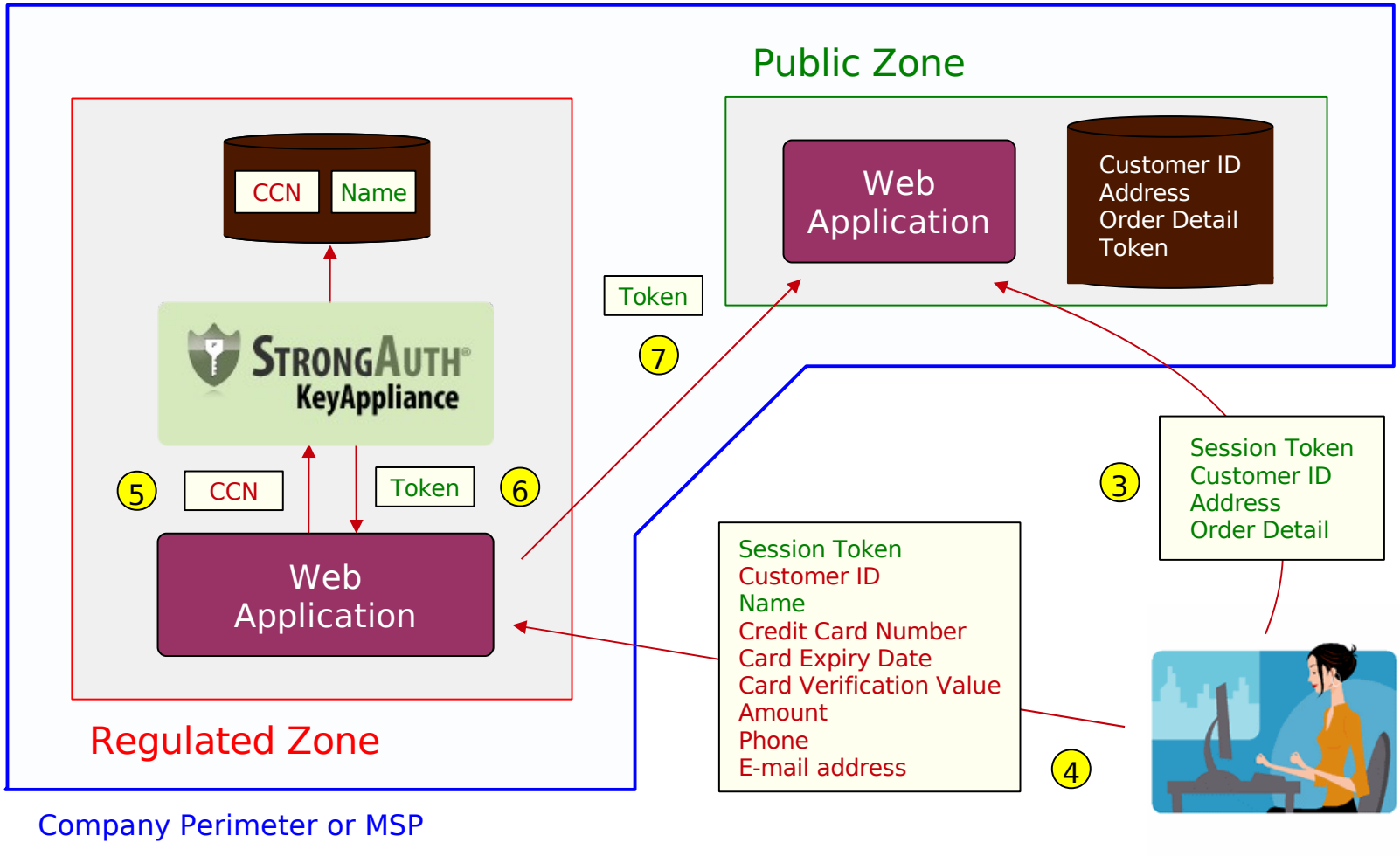

Cloud Zone
amazon web services
Windows Azure
WebApp
Customer ID
Address
Order Detail
Token
CCN
Name
StrongAuth
KeyAppliance
Web Application
7
Token
Regulated Zone
Company Perimeter or MSP

FULL TRANSACTION

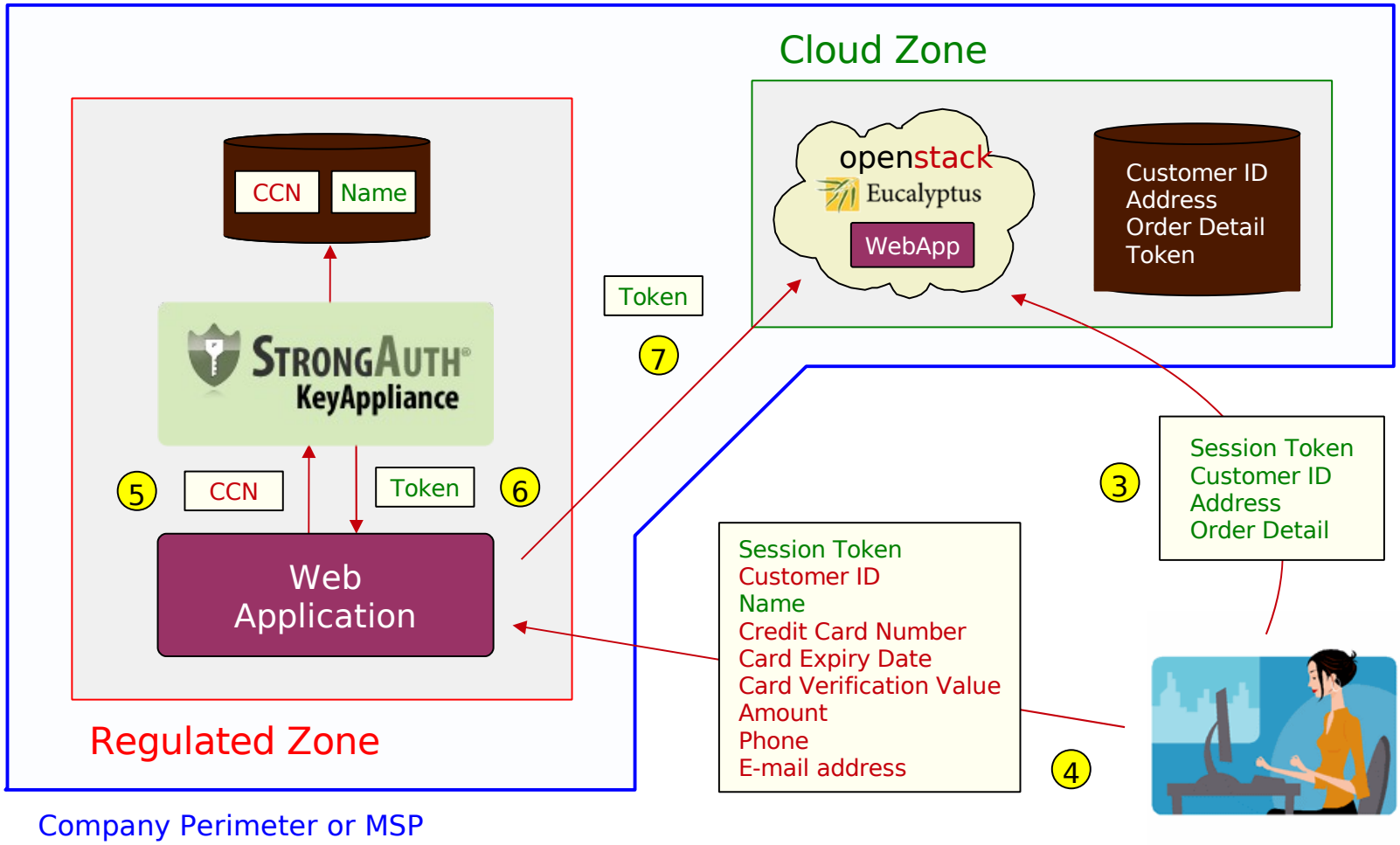


HOW DO YOU TRANSITION TO RC3?

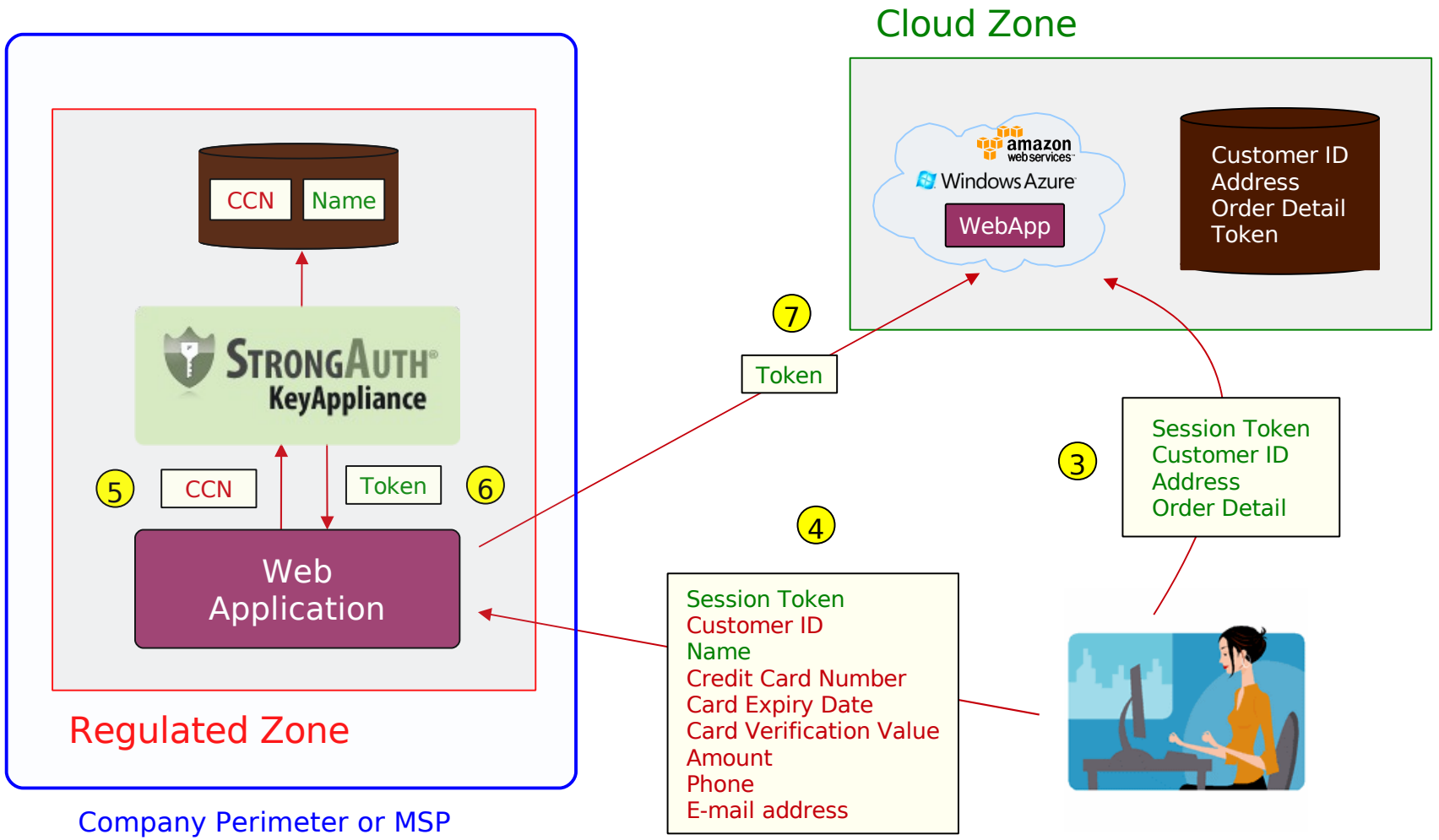
RC3 in the Enterprise



RC3 in Private Clouds



RC3 in Public Clouds



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 credentials to anything in the Cloud
- Do NOT use CSP-supplied cryptographic keys
- DO change your Server SSL keys very frequently
- DO consider digitally signing/verifying Cloud data in the Regulated Zone
- Assume the worst (that your applications and data are operating on the open internet) and design for it

RC3 Case Study

- e-commerce company in US (ticket marketplace)
- Private Cloud
- Millions of documents
  - Sizes ranging from a few kilobytes to megabytes
- Needed automatic ramp-up/ramp-down capability

http://www.infoq.com/articles/cloud-data-encryption-infrastructure

Resources

- Regulatory Compliant Cloud Computing (RC3)
  - http://www.ibm.com/developerworks/cloud/library/cl-regcloud/index.html
  - http://www.infoq.com/articles/regulatory-compliant-cloud-computing
  - http://bit.ly/rc3issa
- Cryptographic engine (enables RC3 applications)
  - http://www.cryptoengine.org
- CryptoCabinet (RC3 sample application)
  - http://www.cryptocabinet.org

Questions?

- Contact Information
  - Arshad Noor
  - arshad.noor@strongauth.com
  - +1 (408) 331-2001