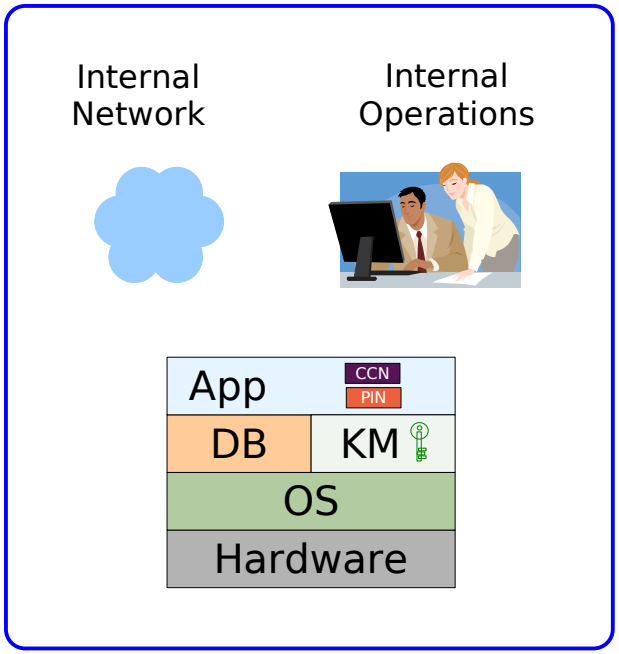
StrongAuth
Securing the Core

# A web-application architecture for Secure Cloud Computing

Provable regulatory compliance!

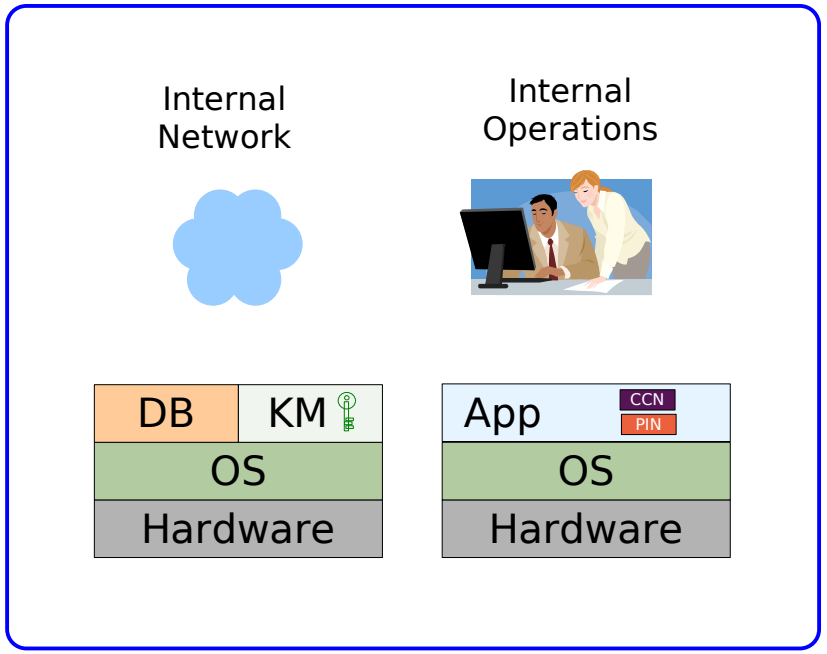
# In the beginning...




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

Provable regulatory compliance!

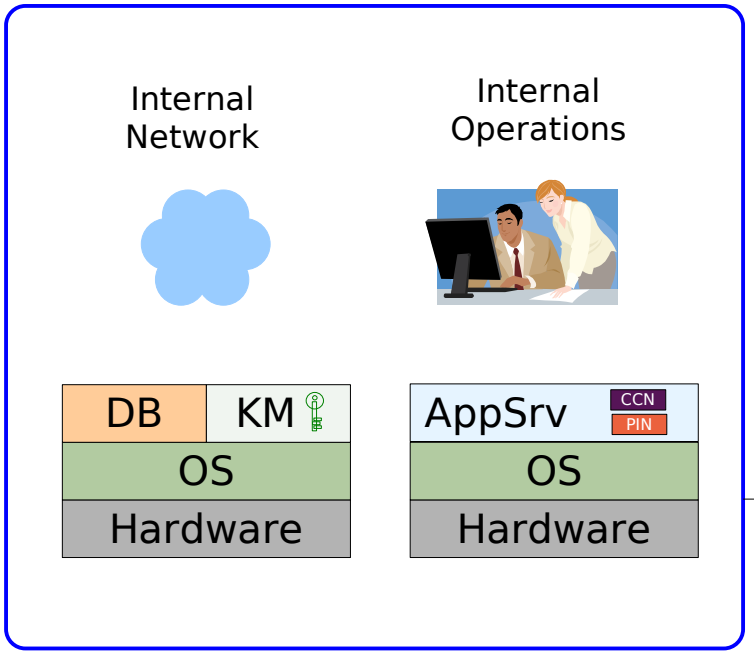
# The PC-LAN




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

Provable regulatory compliance!

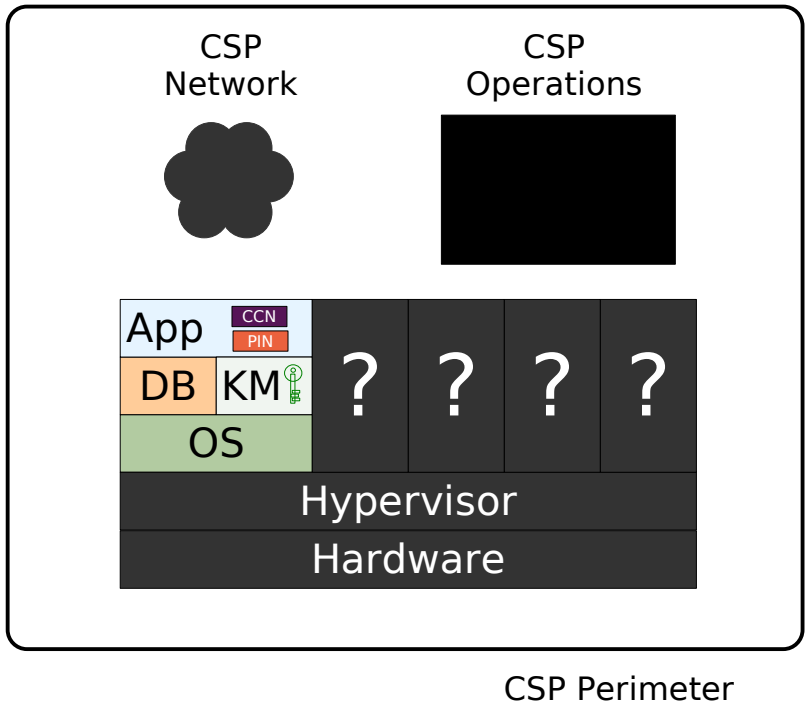
# The WWW


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

Provable regulatory compliance!

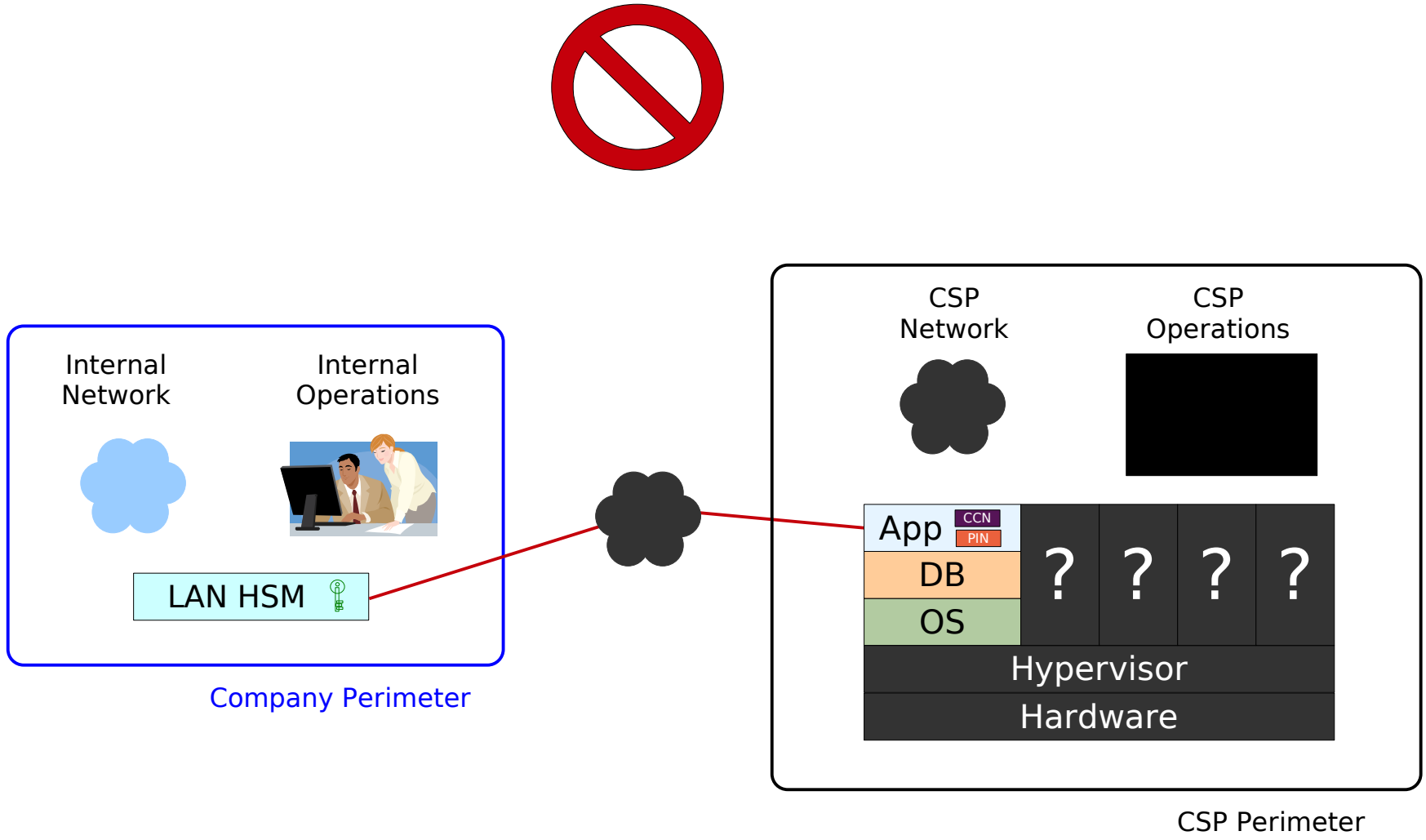
# The Public Cloud




- 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?

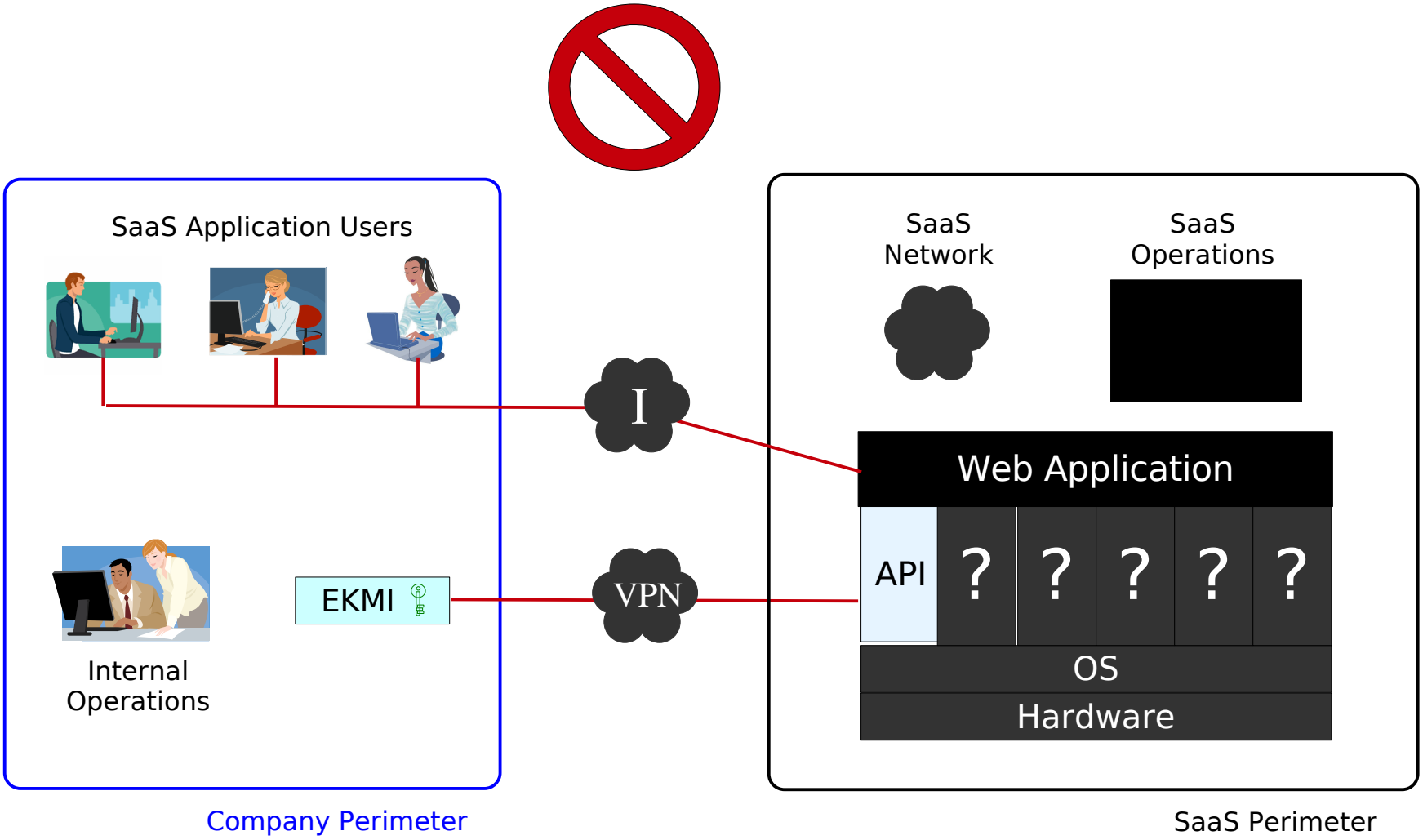
Provable regulatory compliance!

# EKM in the Public Cloud?




Provable regulatory compliance!

# EKM with SaaS?




Provable regulatory compliance!

# What's missing?

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

Provable regulatory compliance!

# The Paradigm Shift


## Regulatory Compliant Cloud Computing (RC3)

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

Provable regulatory compliance!

# RC3 Characteristics

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

Provable regulatory compliance!

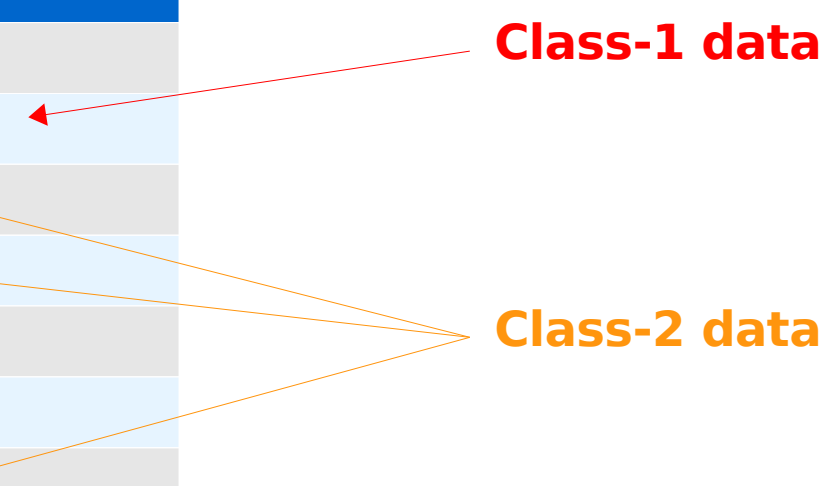
# RC3 Data Classification

- **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

Provable regulatory compliance!

# Data – Before RC3

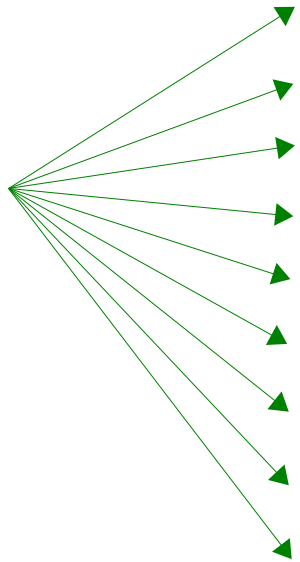
| Employee | |
|---|---|
| EID | 12345 |
| **SSN** | **111-22-3333** |
| **Firstname** | **John** |
| **Lastname** | **Doe** |
| HireDate | 01/01/2011 |
| Supervisor | 23456 |
| **Salary** | **55000** |
| Location | 123 |
| .... | |




Provable regulatory compliance!

# Data – After RC3

**Class-3 data**

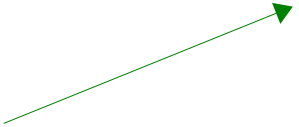


| Employee | |
|---|---|
| EID | 12345 |
| SSN | 9999000000003912 |
| Firstname | 9999000000005126 |
| Lastname | 9999000000005127 |
| HireDate | 01/01/2011 |
| Supervisor | 23456 |
| Salary | 9999000000007184 |
| Location | 123 |
| .... | |

Provable regulatory compliance!

# Another way – After RC3

```
<EmployeeRC3Data>
  <SSN>111-22-3333</SSN>
  <Firstname>John</Firstname>
  <Lastname>Doe</Lastname>
  <Salary>55000</Salary>
</EmployeeRC3Data>
```

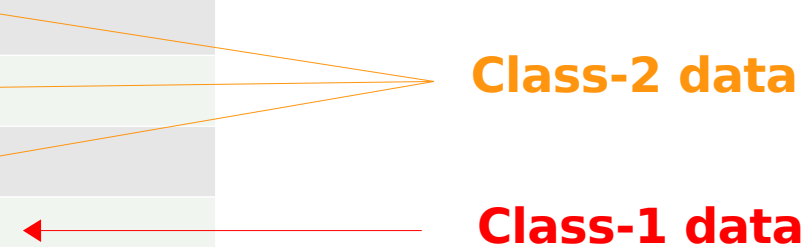


| Employee | |
|---|---|
| EID | 12345 |
| RC3Data | 9999000000001212 |
| HireDate | 01/01/2011 |
| Supervisor | 23456 |
| Location | 123 |
| ,,,, | |

Provable regulatory compliance!

# Data – Before RC3

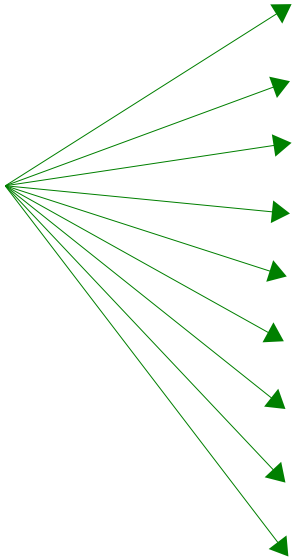
| Bank Account | |
|---|---|
| **AID** | **12345678** |
| **Firstname** | **Jane** |
| **Lastname** | **Smith** |
| **SSN** | **111-22-4444** |
| BranchID | 123 |
| AccountType | 1 |
| DateOpened | 02/02/2012 |
| Balance | 794.25 |
| .... | |




Provable regulatory compliance!

# Data – After RC3

**Class-3 data**

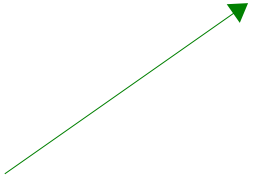


| Bank Account | |
|---|---|
| AID | 9999000000023745 |
| Firstname | 9999000000071847 |
| Lastname | 9999000000071849 |
| SSN | 9999000000088764 |
| BranchID | 123 |
| AccountType | 1 |
| DateOpened | 02/02/2012 |
| Balance | 794.25 |
| .... | |

Provable regulatory compliance!

# Another way – After RC3

```
<BankAccountRC3Data>
  <SSN>111-22-4444</SSN>
  <Firstname>Jane</Firstname>
  <Lastname>Smith</Lastname>
</BankAccountRC3Data>
```



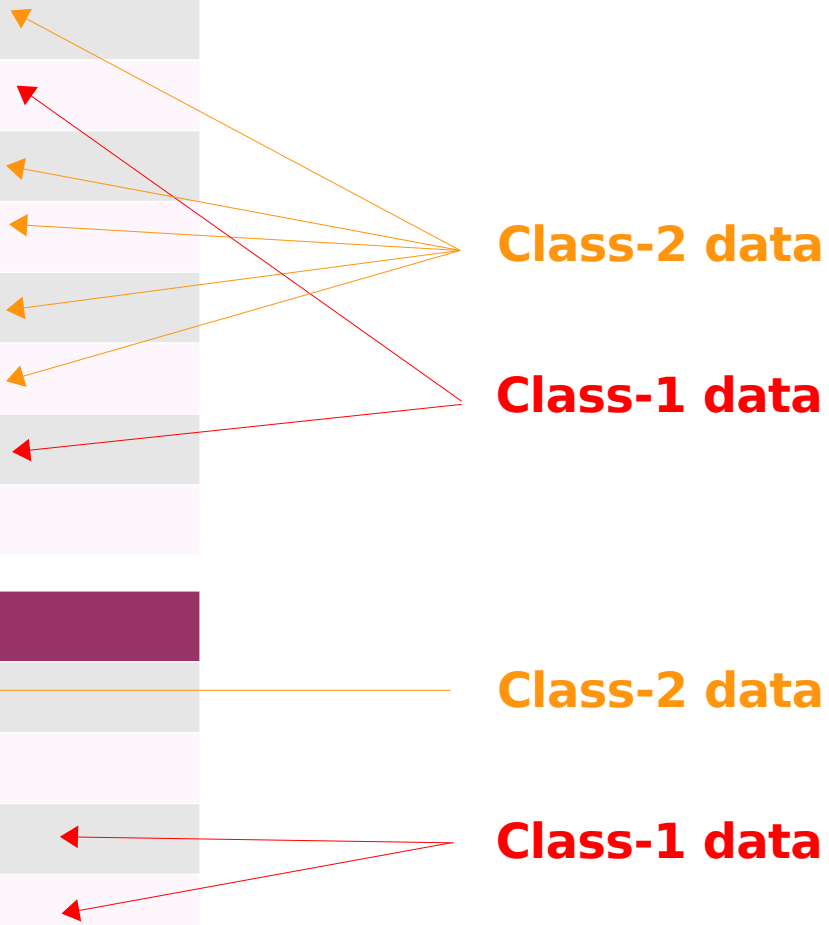
| Bank Account | |
|---|---|
| AID | 9999000000023745 |
| RC3Data | 9999000000026458 |
| BranchID | 123 |
| AccountType | 1 |
| DateOpened | 02/02/2012 |
| Balance | 794.25 |
| .... | |

Provable regulatory compliance!

# Data – Before RC3

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

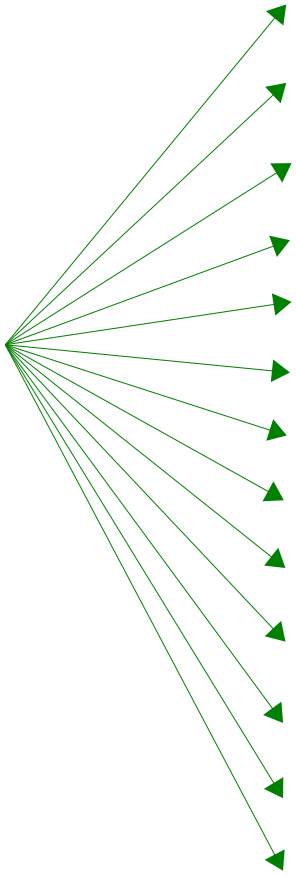
| Blood Report | |
|---|---|
| **PID** | **1234567** |
| ReportDate | 04/04/2012 |
| **RBC** | **5.1** |
| **WBC** | **7.5** |
| …. | |




Provable regulatory compliance!

# Data – After RC3

**Class-3 data**



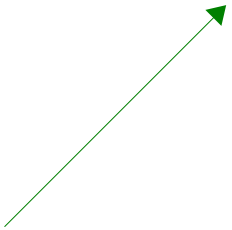
| Patient | |
|---|---|
| PID | 9999000000023745 |
| SSN | 9999000000057599 |
| Firstname | 9999000000045910 |
| Lastname | 9999000000045911 |
| Gender | M |
| DateOfBirth | 03/03/1953 |
| BloodType | O+ |
| .... | |

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

Provable regulatory compliance!

# Another way – After RC3

```
<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 |
| .... | |

Provable regulatory compliance!

# Yet another way – After RC3

```
<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 |
| .... | |

Provable regulatory compliance!

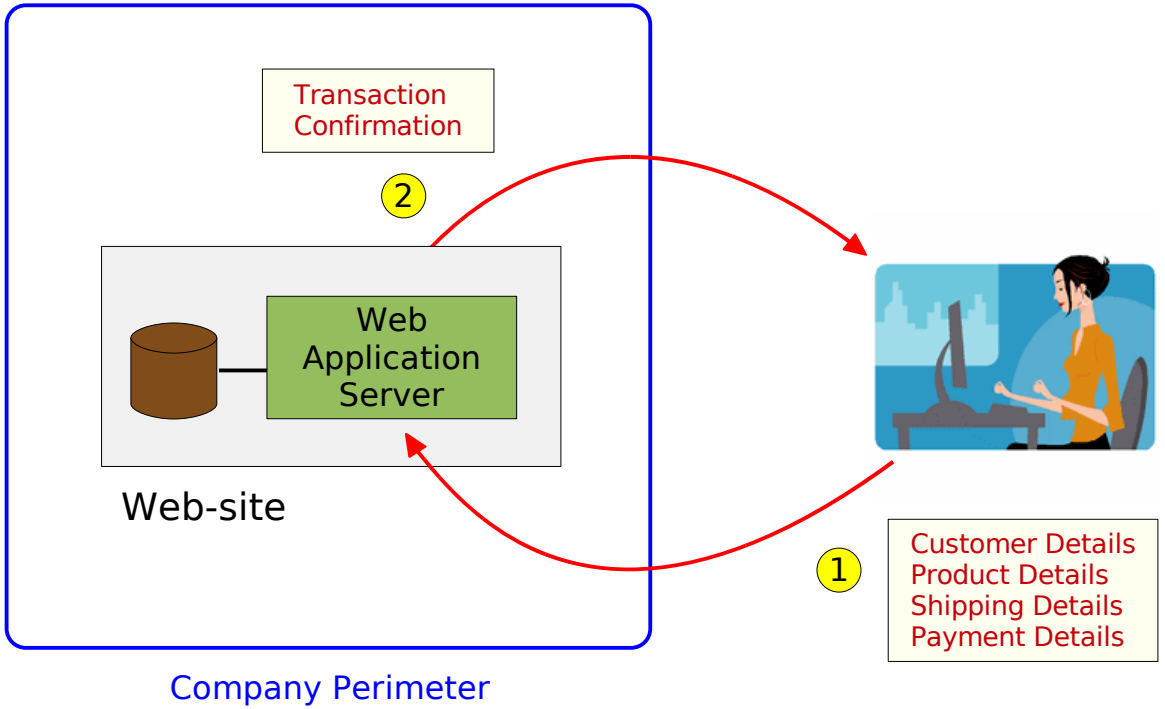
# RC3 Zones

- 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**

Provable regulatory compliance!

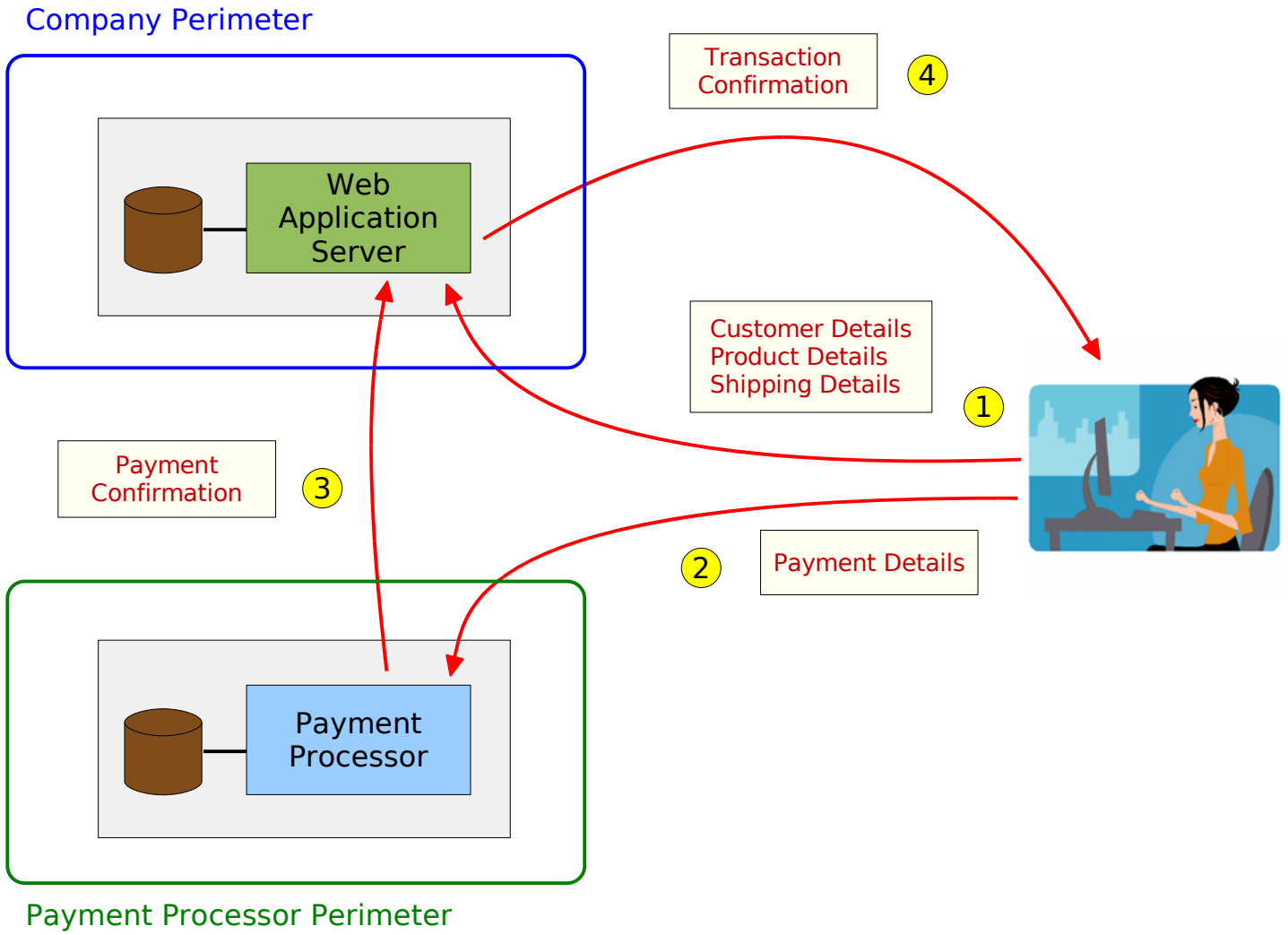
# WEB-APPLICATION MODEL

# Basic web application




Provable regulatory compliance!

# With Redirection



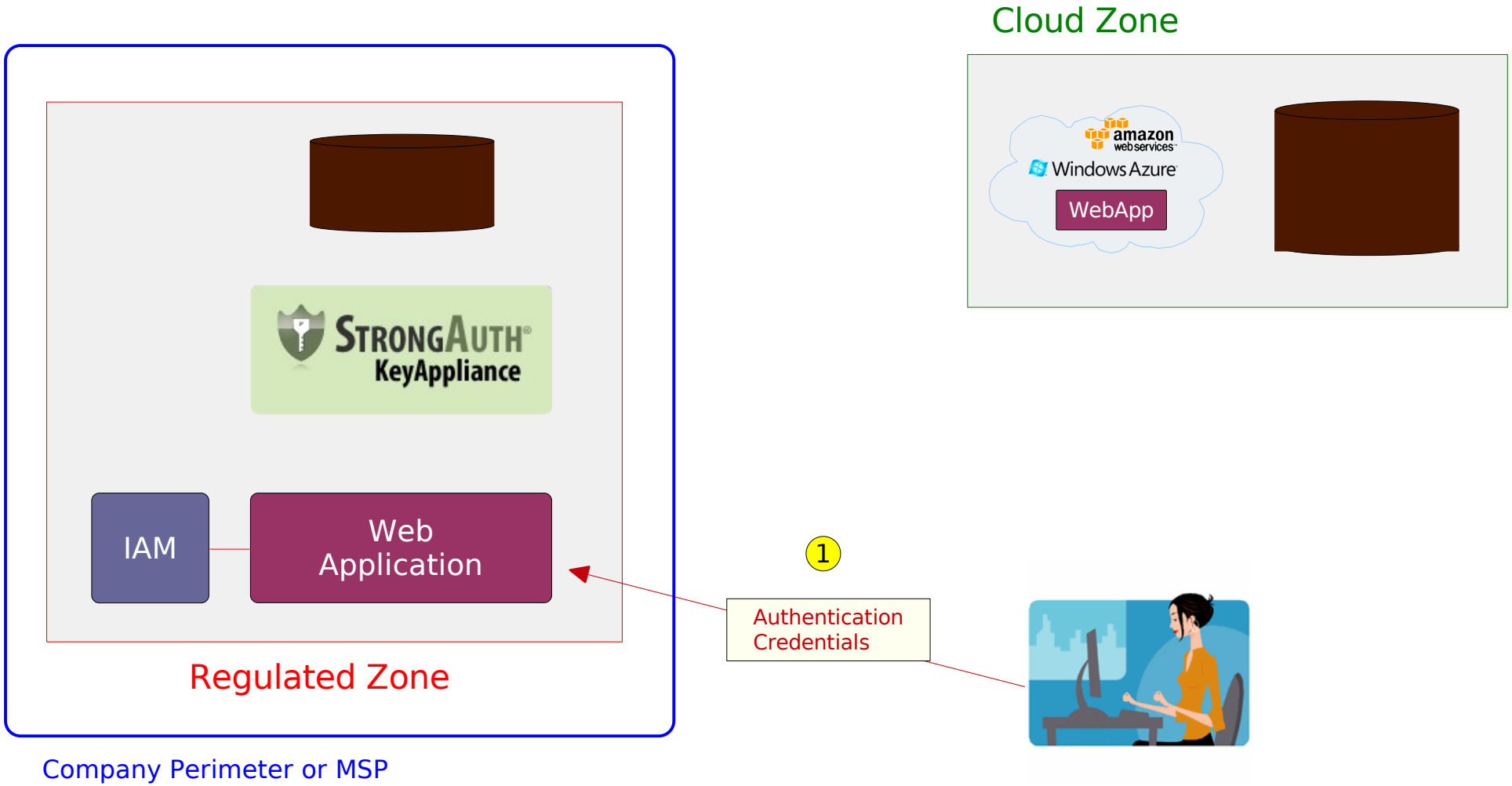

Provable regulatory compliance!

# SECURE CLOUD COMPUTING FOR E-COMMERCE

# RC3 MODEL

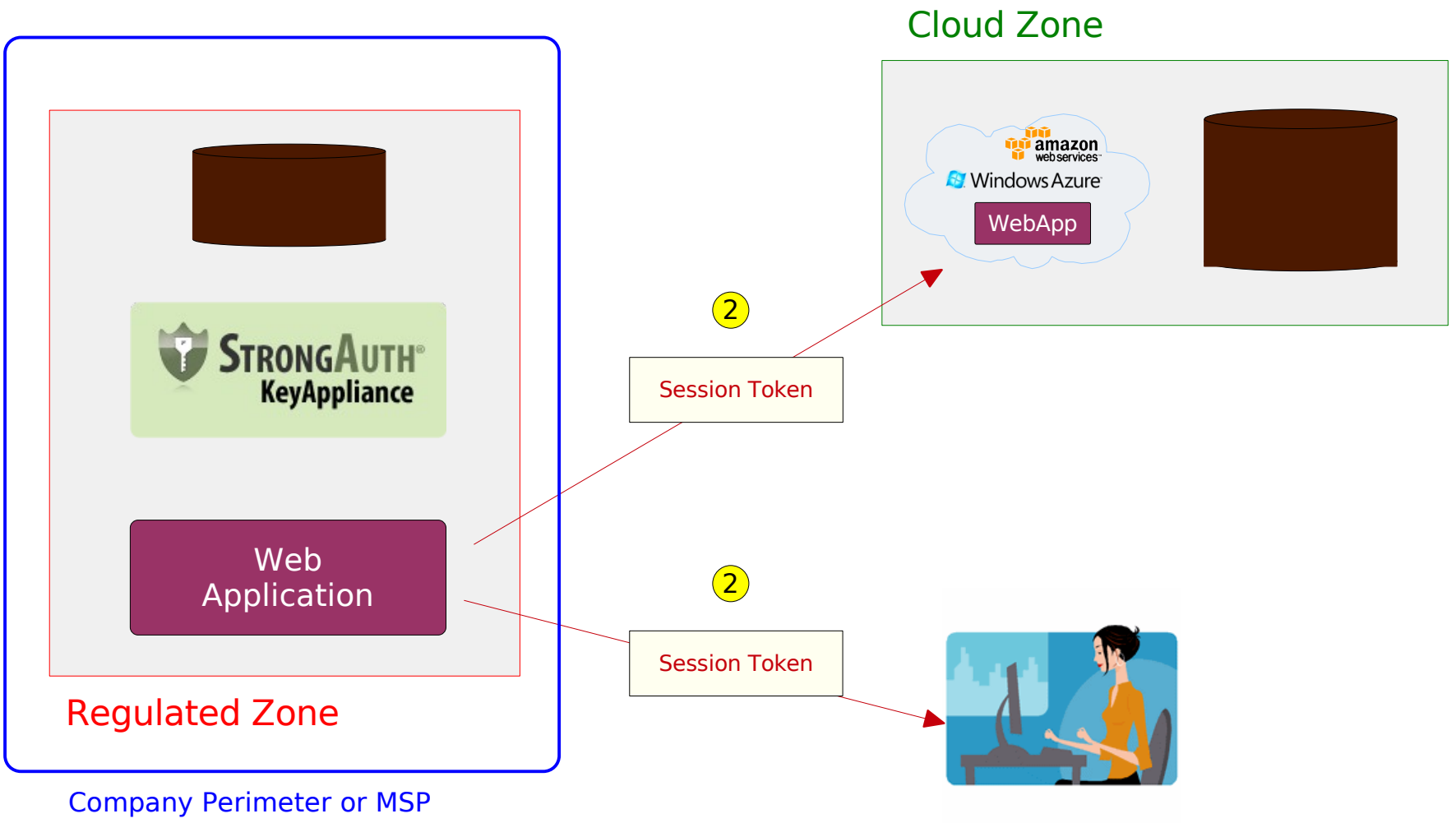
Provable regulatory compliance!

# E-COMMERCE - 1



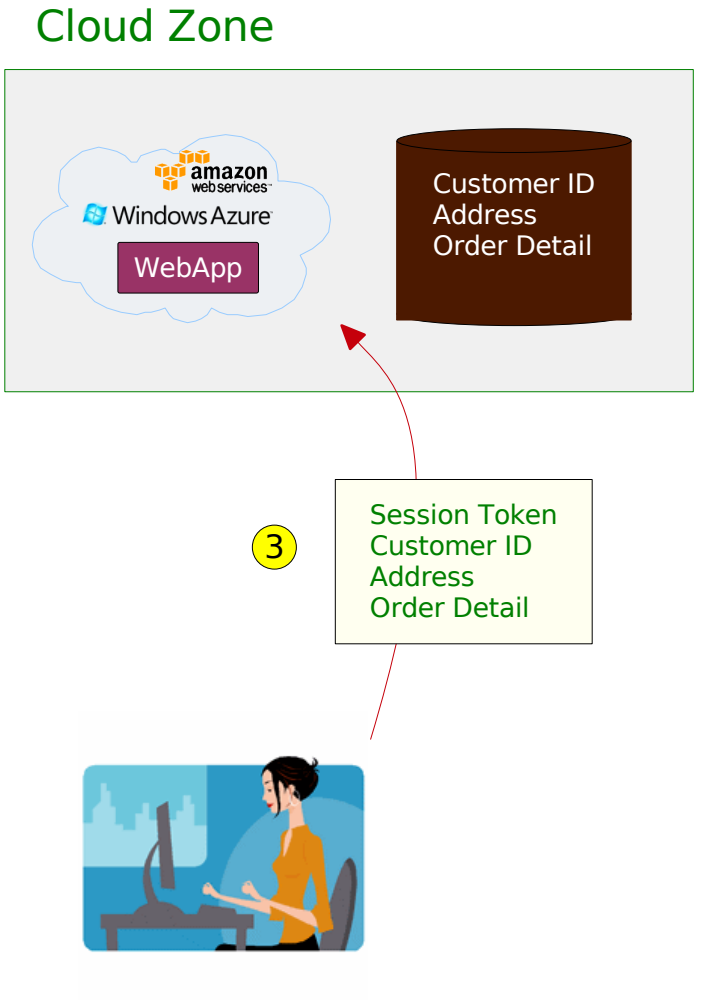

Provable regulatory compliance!

# E-COMMERCE - 2



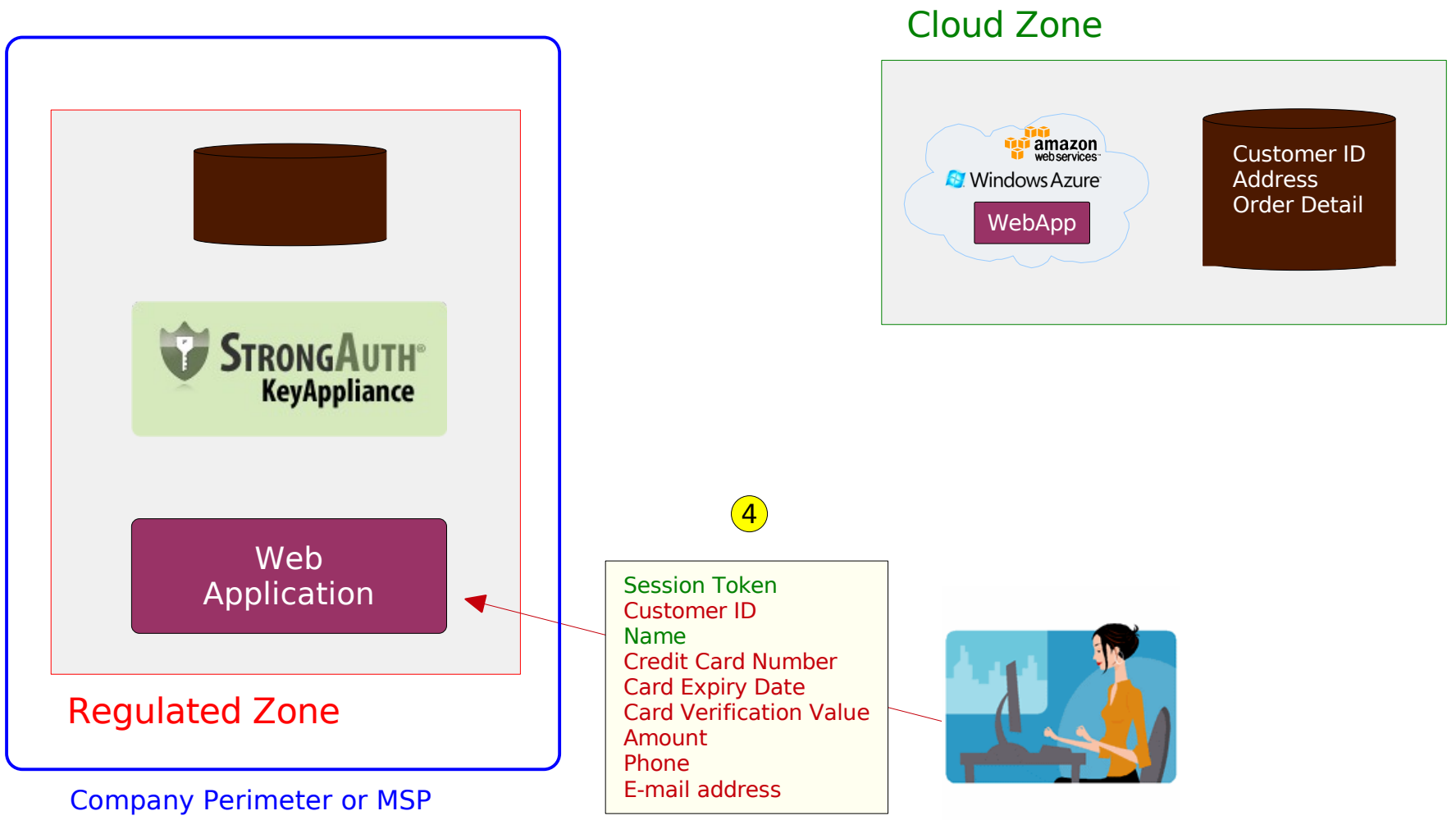

Provable regulatory compliance!

# E-COMMERCE - 3

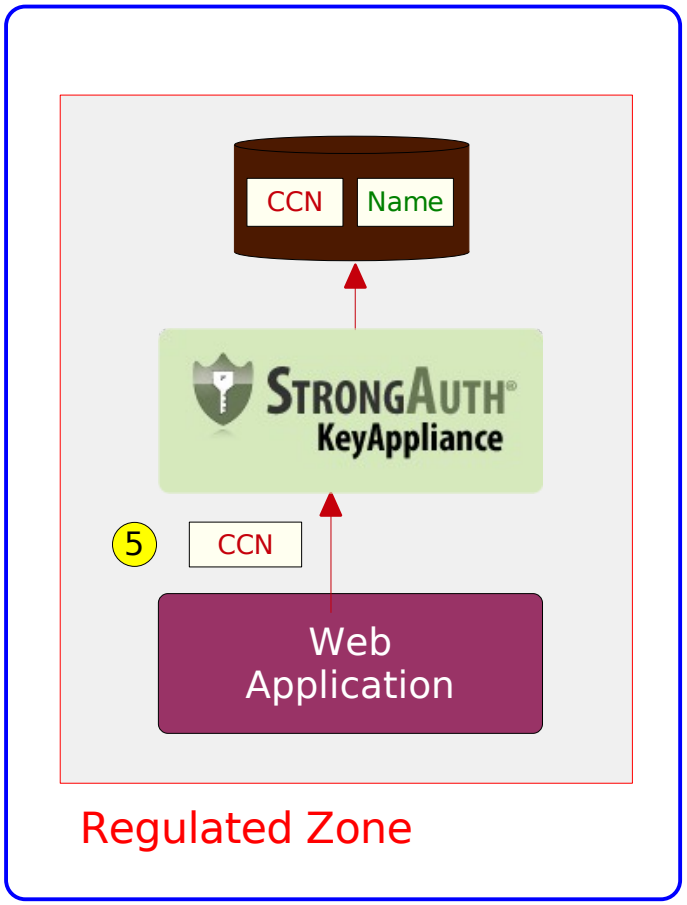

Provable regulatory compliance!

# E-COMMERCE - 4




Provable regulatory compliance!

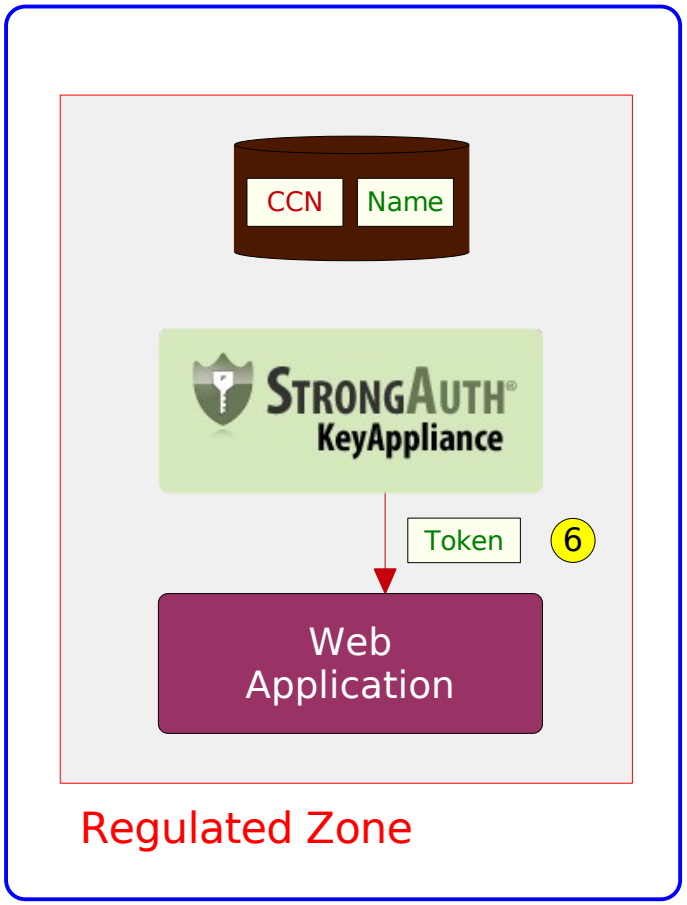
# E-COMMERCE - 5





Provable regulatory compliance!

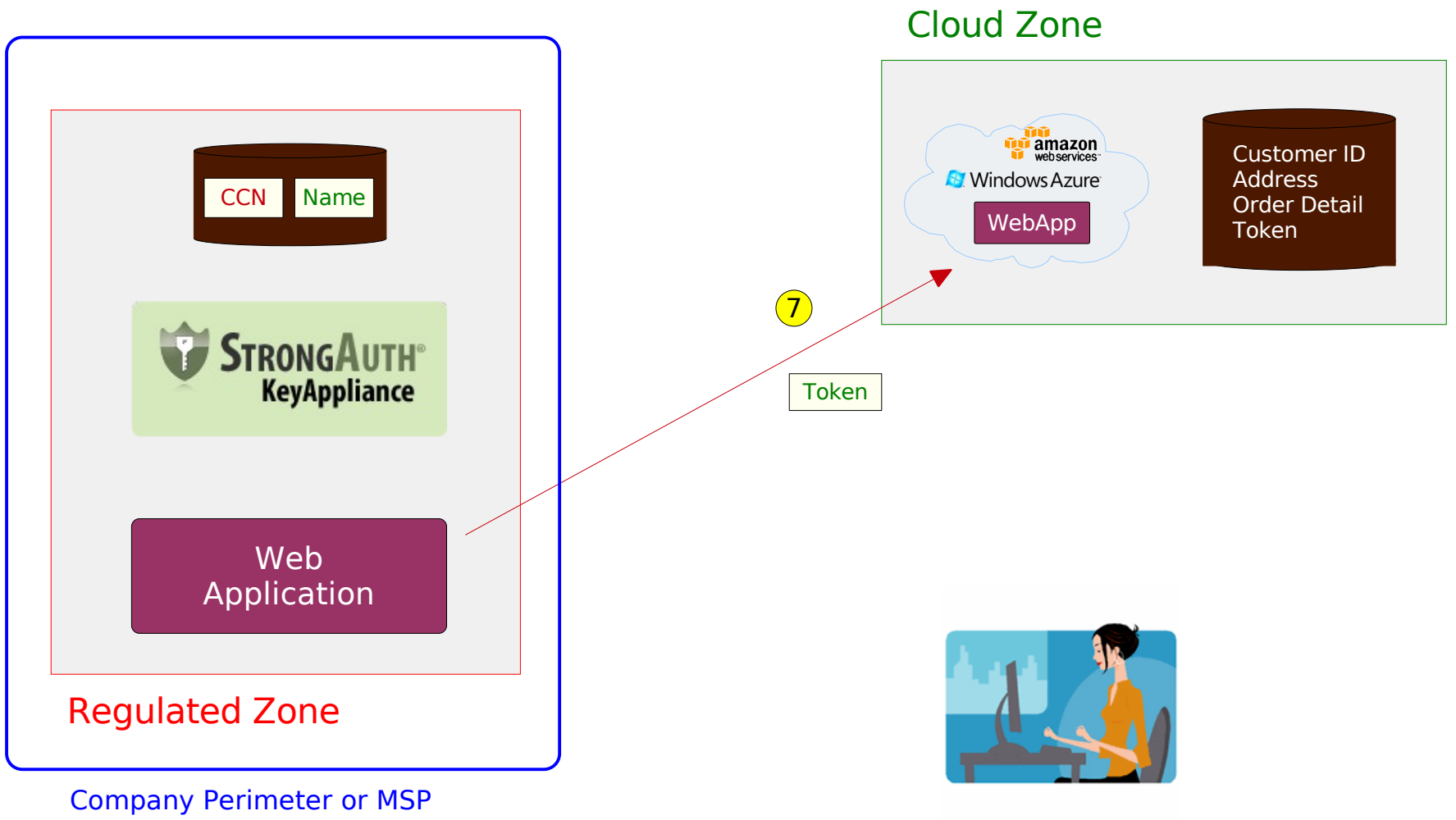
# E-COMMERCE - 6





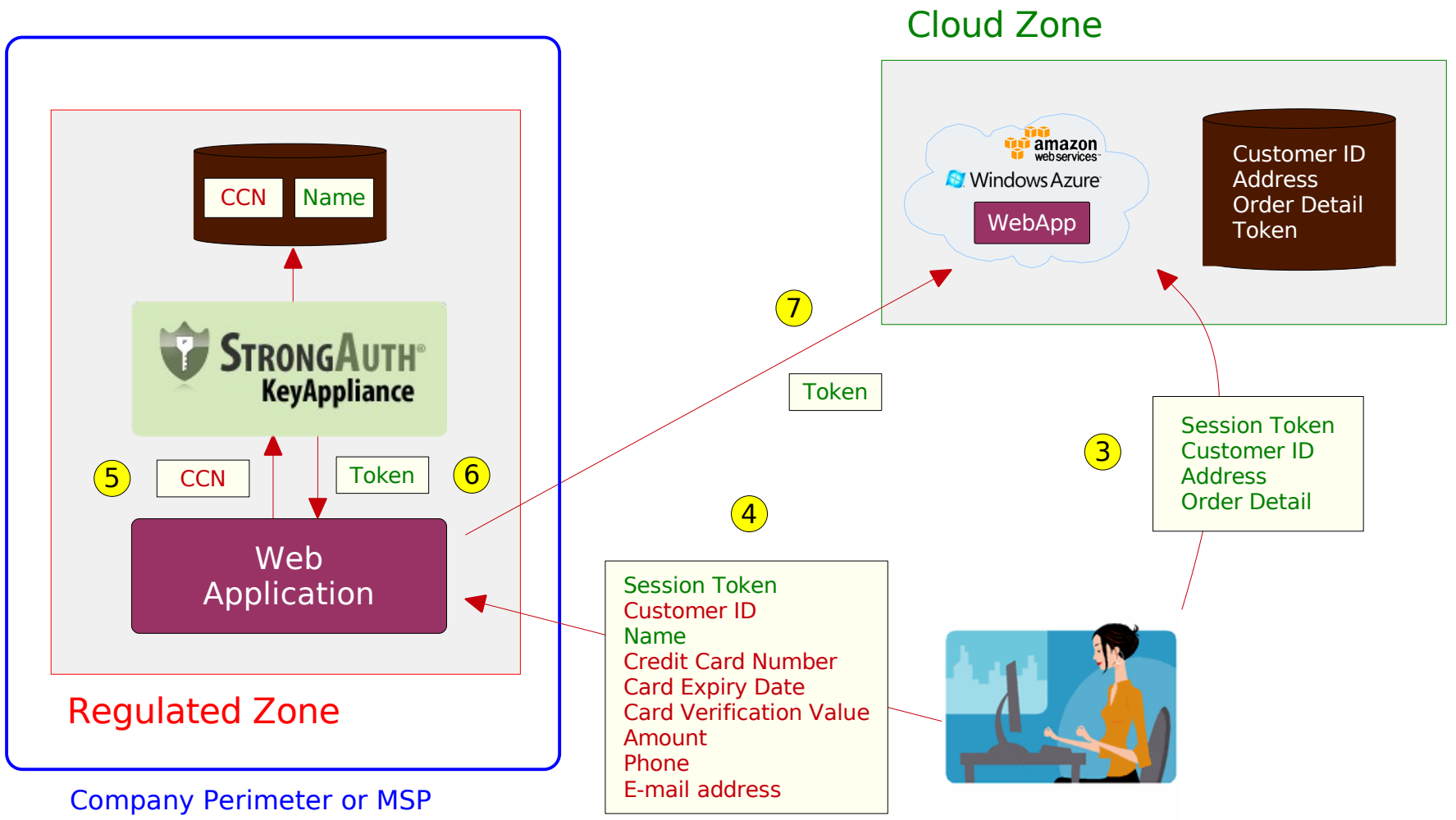
Provable regulatory compliance!

# E-COMMERCE - 7




Provable regulatory compliance!

# FULL TRANSACTION

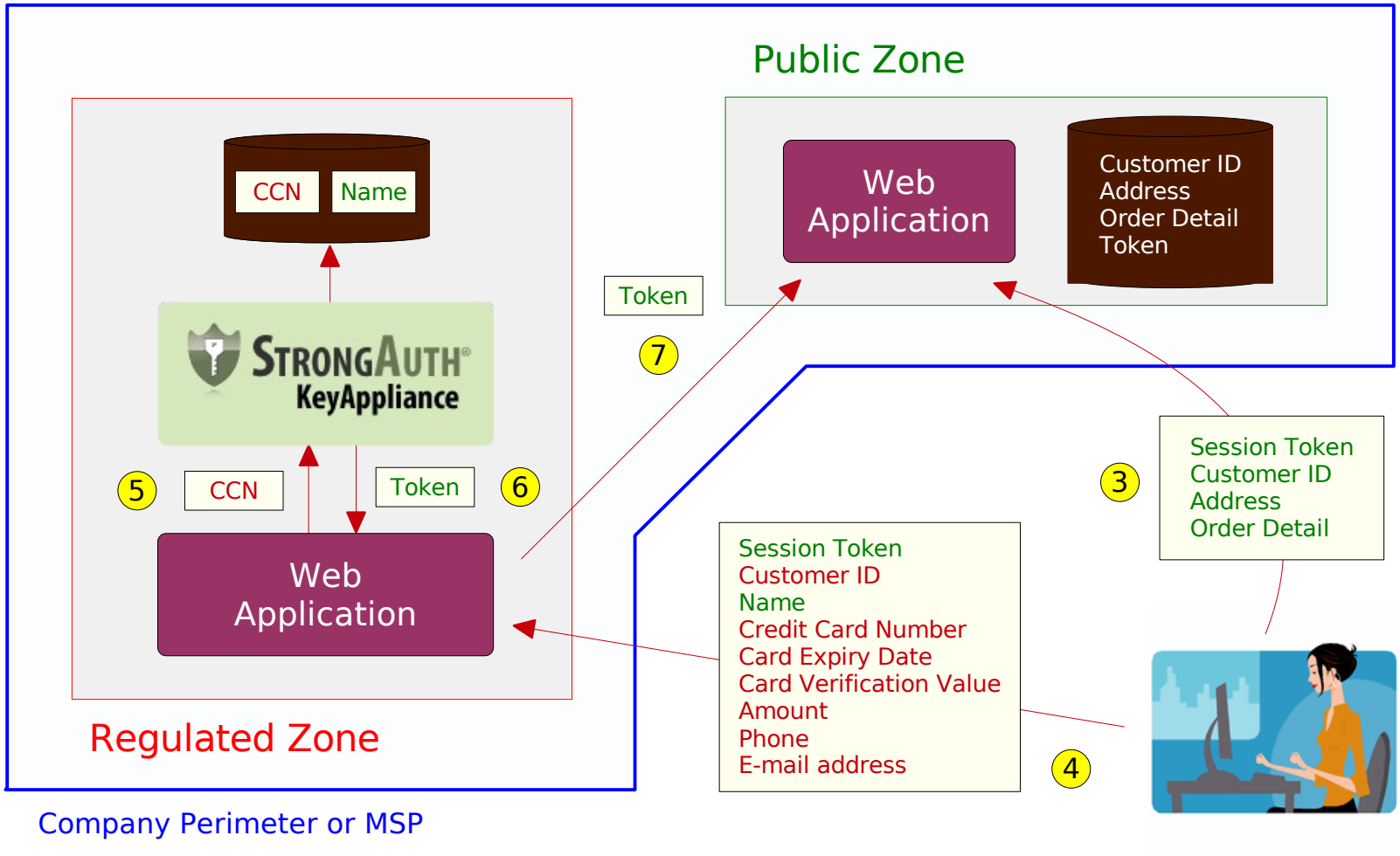



Provable regulatory compliance!

# HOW DO YOU TRANSITION TO RC3?

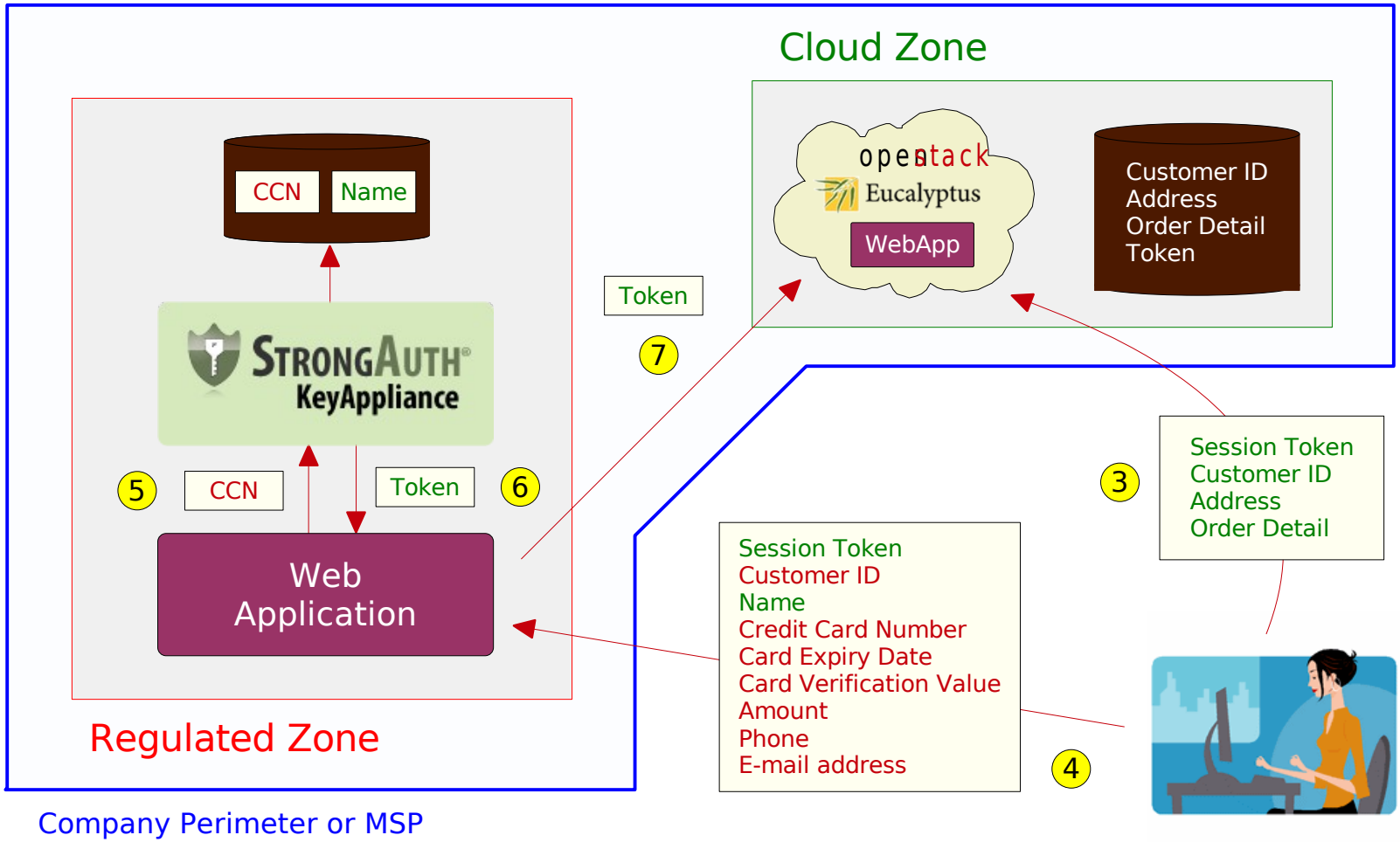
Provable regulatory compliance!

# RC3 in the Enterprise



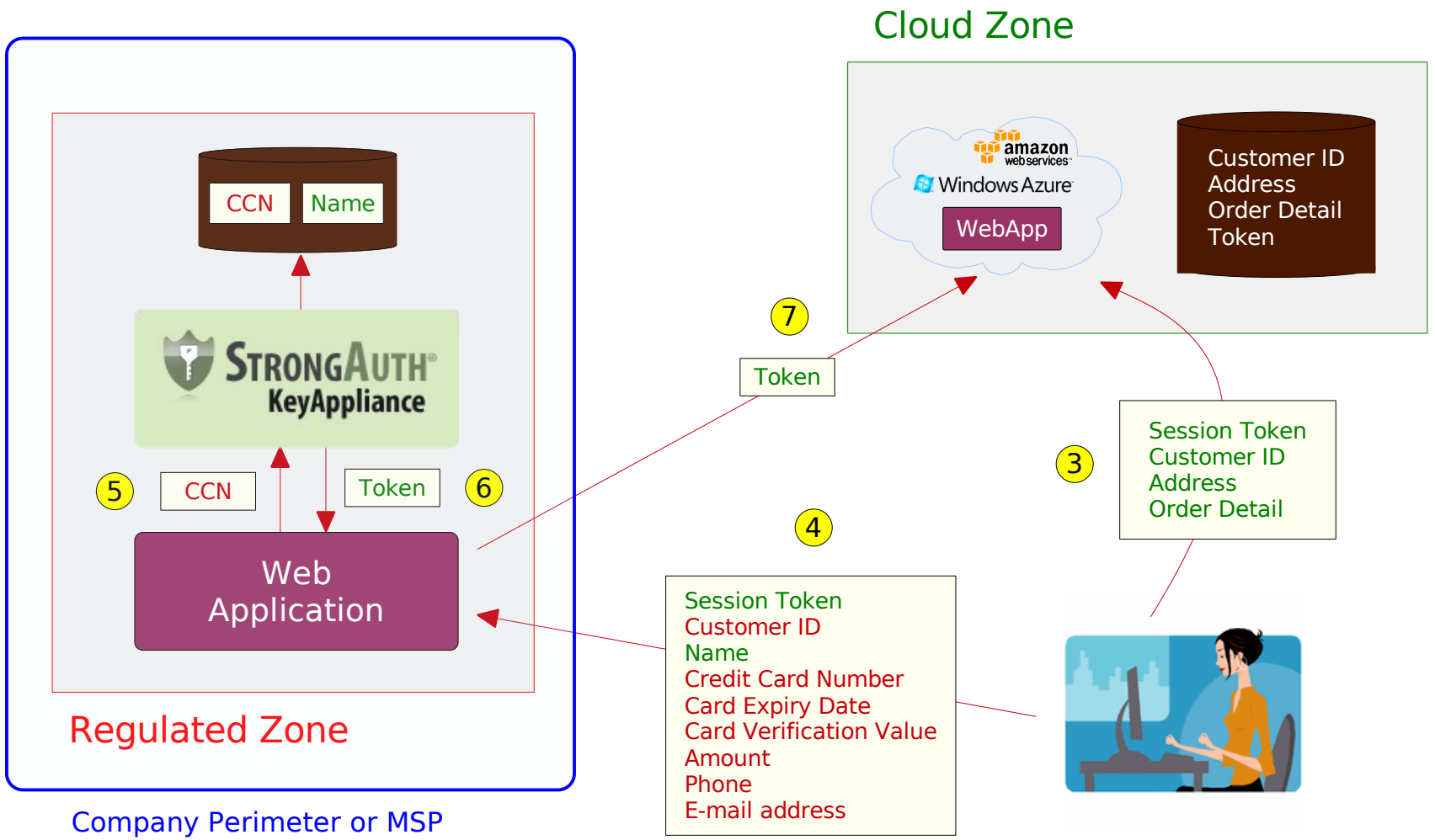

Provable regulatory compliance!

# RC3 in Private Clouds




Provable regulatory compliance!

# RC3 in Public Clouds




Provable regulatory compliance!

# 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

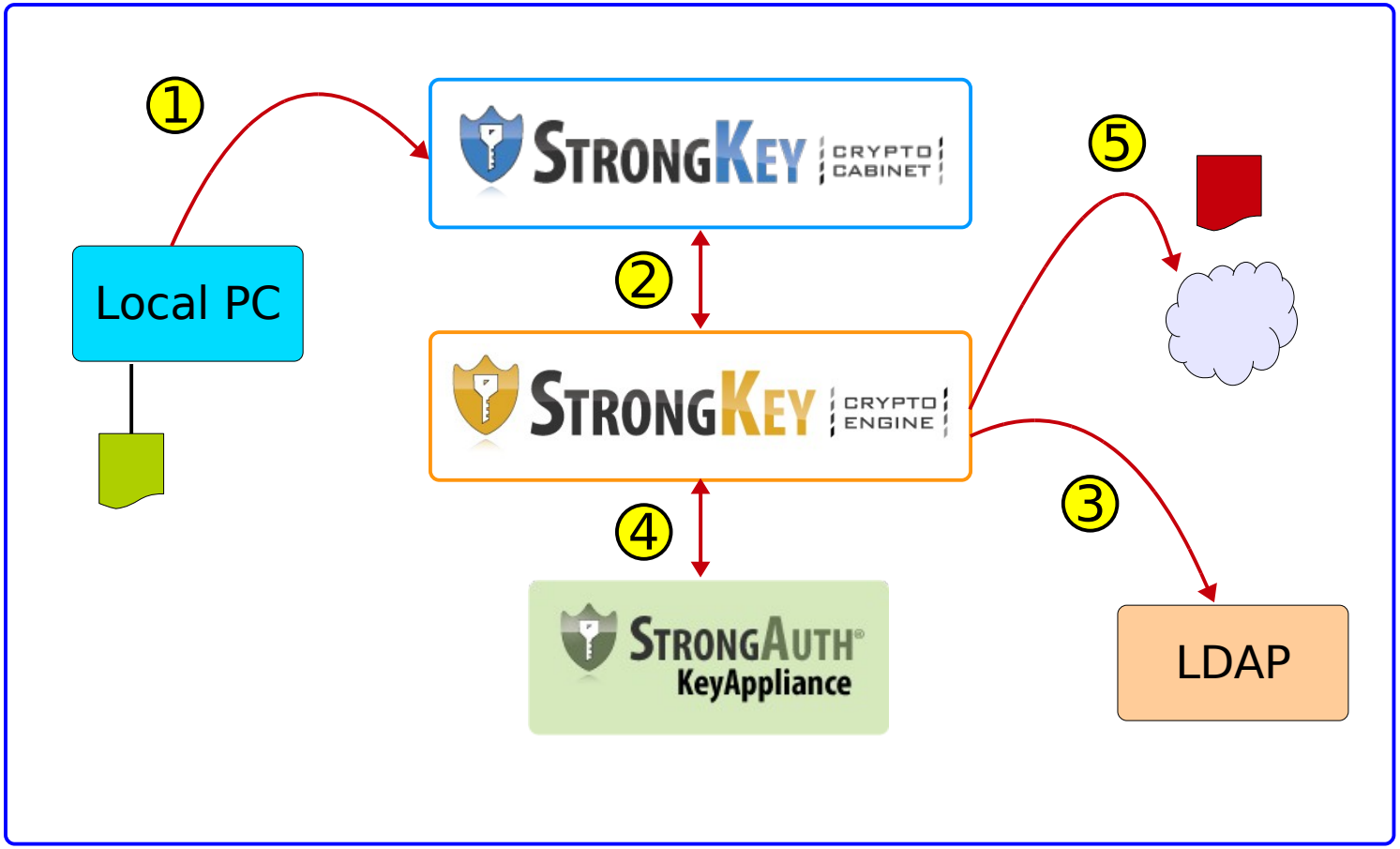
Provable regulatory compliance!

# 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

Provable regulatory compliance!

# RC3 Application Demo




amazon web services

Windows Azure

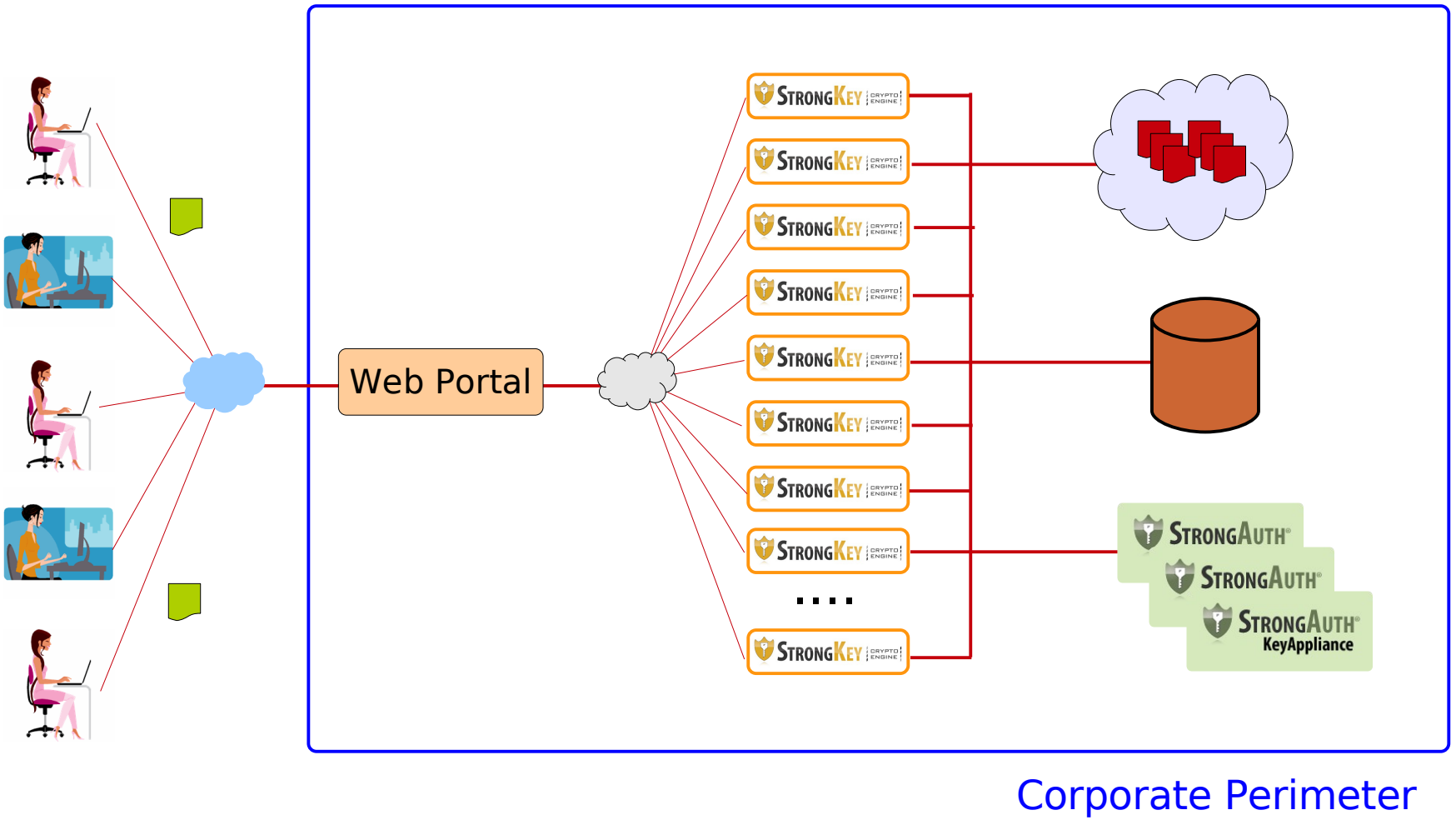
Provable regulatory compliance!

# RC3 Case Study

- Document-management e-commerce company in US
- Serving financial, health-care and legal markets
- Private Cloud
- Millions of documents
  - Sizes ranging from a few kilobytes to gigabytes
- Needed PCI-DSS level security
- Needed automatic ramp-up/ramp-down capability

Provable regulatory compliance!

# RC3 Case Study




Provable regulatory compliance!

# Questions?

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

Provable regulatory compliance!