



# REGULATORY COMPLIANT CLOUD COMPUTING (RC3)

Arshad Noor  
November, 2011

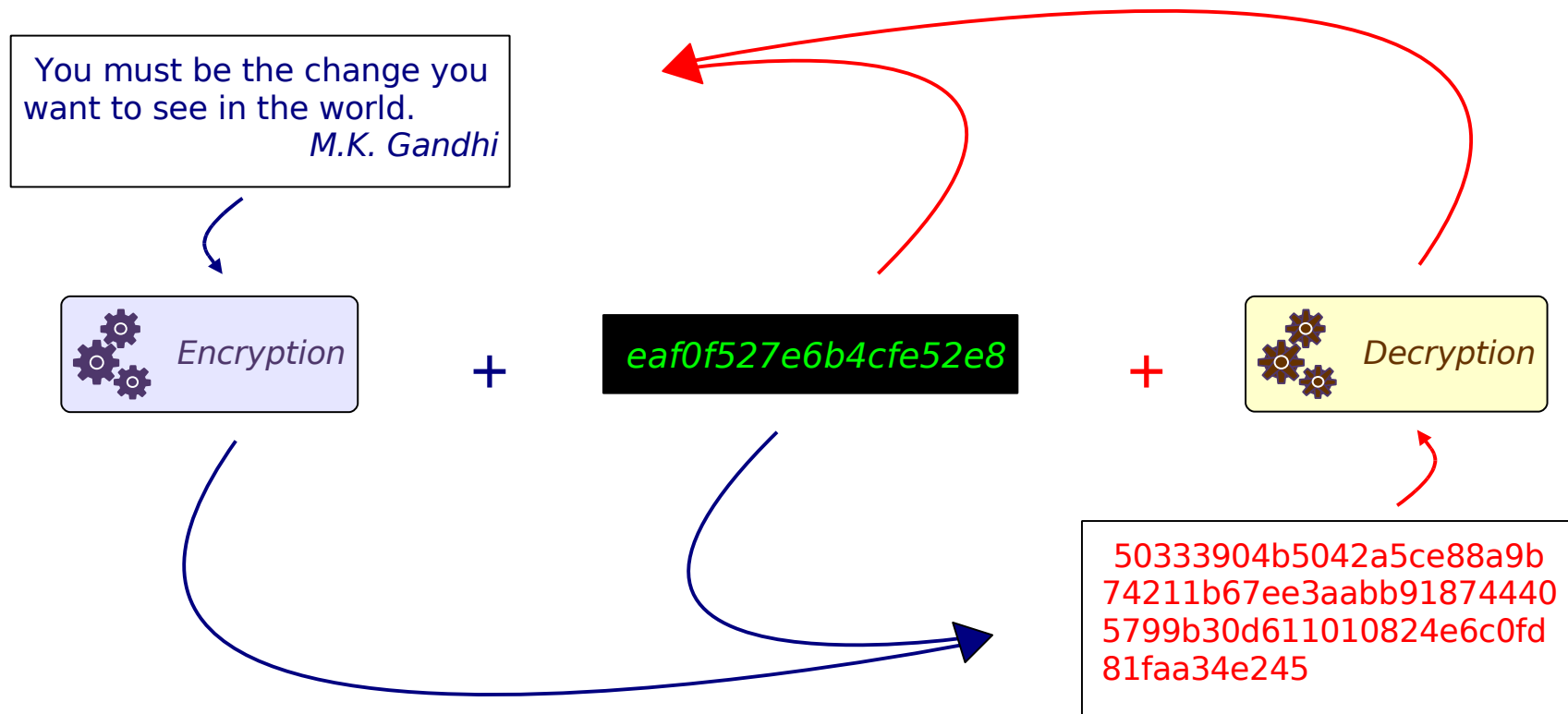
Provable regulatory compliance!

- Silicon Valley-based private company
- Founded in 2001
- Focused on Architecture, Design, Development & Support of:
  - Enterprise Key Management
    - Public Key Infrastructure (PKI)
    - Symmetric Key Management System (SKMS)
- Customers in many sectors
  - Finance, Telecom, Pharmaceutical, Medical Devices, e-Commerce, Entertainment, Retail, BPO Services, Manufacturing, Government, Military

- 32+ years of work-experience
  - 7 years on the Business side; 25+ in Information Technology (**12+ in Cryptographic Key Management**)
- Creator of **CSRTool** – an open-source key-generation tool for RSA and ECC keys (2005)
- Designer, lead-developer of **StrongKey** – industry's first, open-source, Symmetric Key Management System (2006)
- Designer, lead-developer of the **StrongAuth KeyAppliance** – industry's lowest cost encryption, tokenization & Key Management appliance (2010)
- Designer, core developer of the **StrongKey CryptoEngine** – an open-source library to secure data in the cloud (2011)

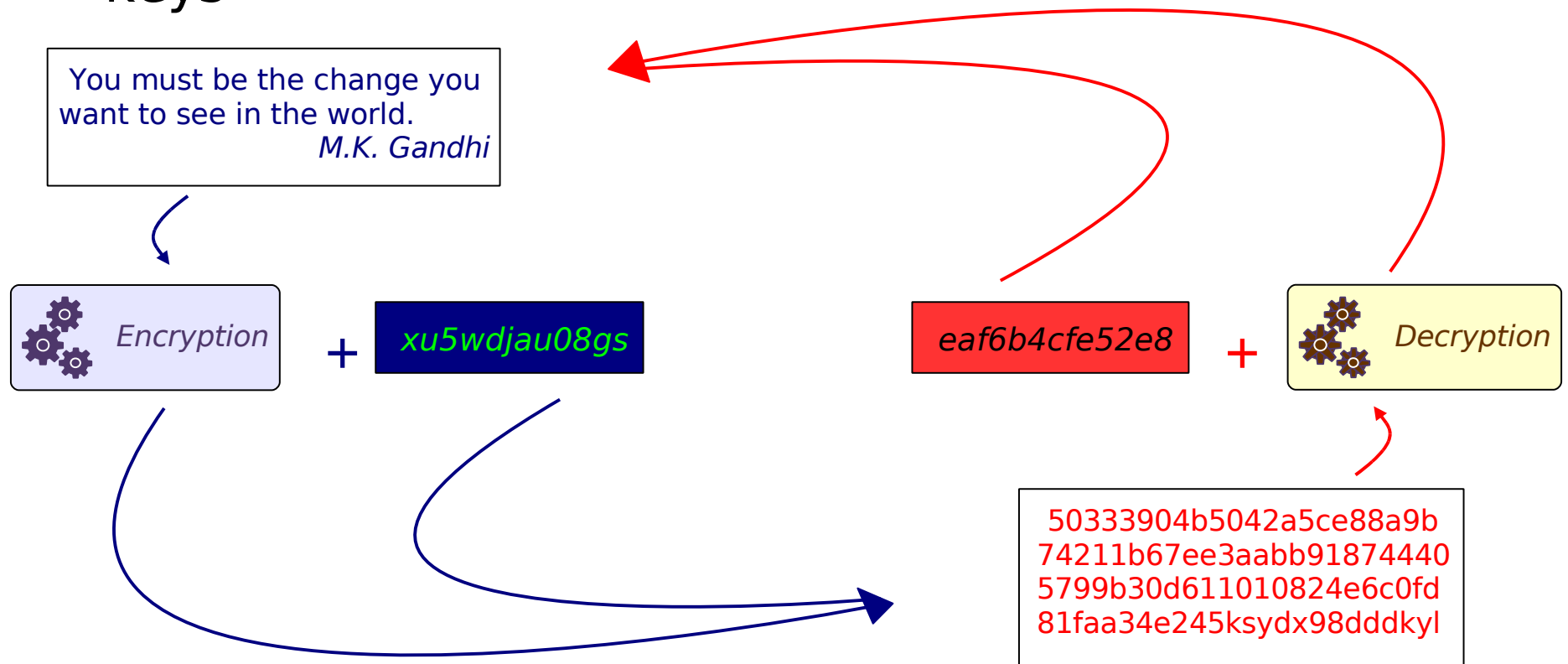
- **ENCRYPTION:** A *reversible* cryptographic operation that *transforms* meaningful “plaintext” to illegible “ciphertext”
- **TOKENIZATION:** A *reversible* operation that *substitutes* meaningful “plaintext” to meaningless “plaintext”
- **HASHING:** An *irreversible* cryptographic operation that *transforms* meaningful “plaintext” to an illegible message-digest (hash)
- **KEY MANAGEMENT:** The life-cycle operations associated with the secure creation, use, management, distribution and destruction of cryptographic keys

- The process of transforming **plaintext** to **ciphertext**, and vice-versa, using the same encryption/decryption key



- **Shared key** for encryption and decryption
- Faster
- Unlimited size for plaintext
  - Typically used to encrypt bulk data
- **Data Encryption Standard (DES) – 56-bit**
- Triple-Data Encryption Standard (3DES)
  - 112 and 168-bit
- Advanced Encryption System (AES)
  - 128, 192 and 256-bit

- The process of transforming **plaintext** to **ciphertext**, and vice-versa, using **two different keys**



- **Different** keys for encryption & decryption
- Slower
- Limited size for plaintext
  - Less than the size of the key
  - Used to encrypt symmetric keys & hashes
- Rivest-Shamir-Adelman (RSA)
  - 512 to 8192-bits
  - 2048-bits recommended for 2010 deployments

- The object created by the process of transforming data to a **fixed-size** cryptographic value using a **one-way** transformation process

You must be the change you  
want to see in the world.  
*M.K. Gandhi*



5033904b5042a5c0e88a9b

- No key is involved – just an algorithm
- Unlimited size data
- Typically used to verify the integrity of a file
- **Message Digest 5 (MD5) – Broken!!**
  - 128-bit fixed size
- Secure Hashing Algorithm – (SHA)
  - SHA1: 160-bit (Avoid, if possible)
  - SHA-256, SHA-384 and SHA-512

- The process of **substituting** a like-value for plaintext without the use of cryptography

1234 5678 9012 3456

 9999 0000 0000 5678

123-45-6789

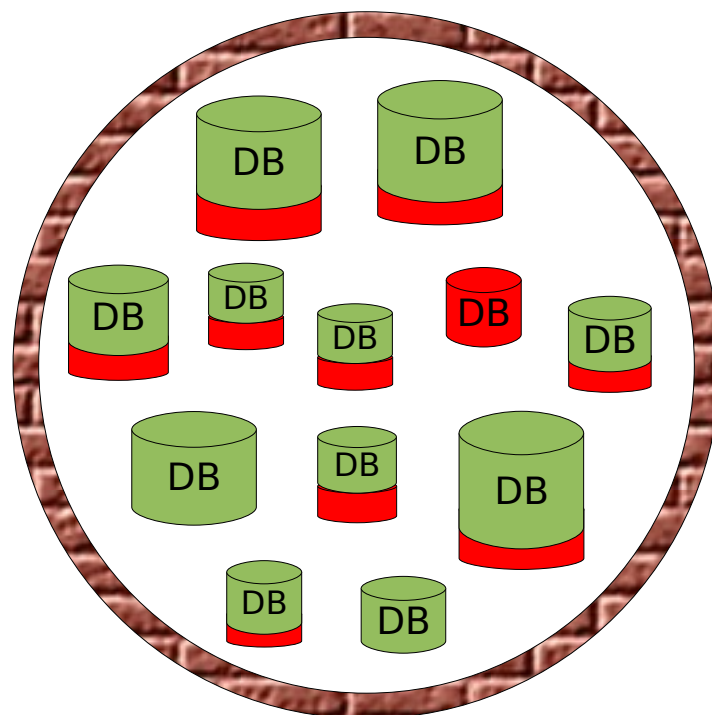
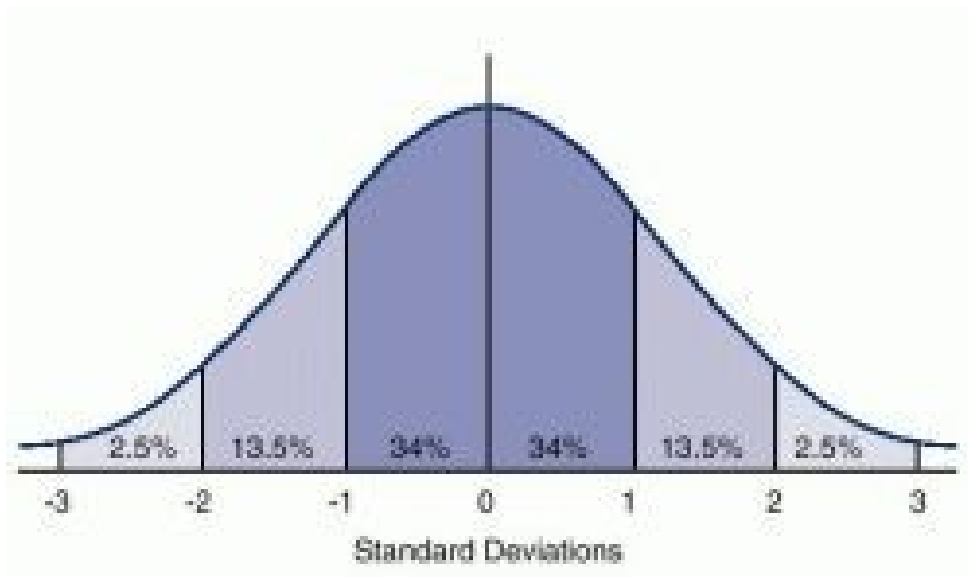
 800-00-0123

123456789 98765432

 100000000 00001234

# What is the problem?

- Not all your data is sensitive, so why are you using scarce security resources protecting all of it?



- Cloud Computing presents many opportunities:
  - Fast time-to-market
  - Low cost-of-entry
  - Low cost-of-migration amongst clouds
  - Immense scalability with just-in-time costs
- Yet...
  - Legislation around securing data is getting stricter
  - Cost of dealing with the consequences of a breach are increasing (TJX, HPS, RockYou, ....)
- So, how does one take advantage of the opportunity while proving compliance?

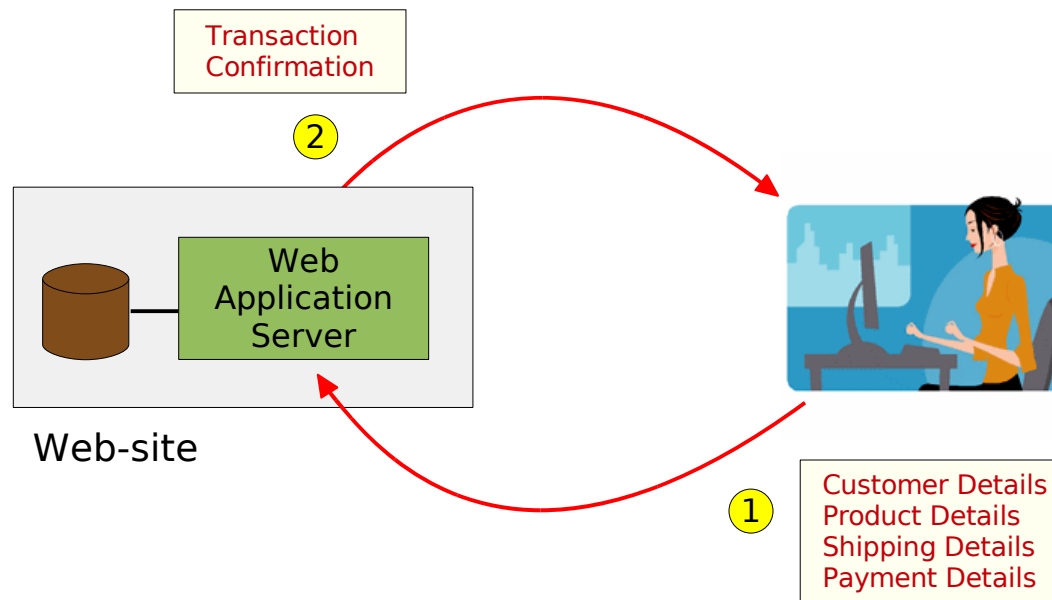
Regulatory Compliant Cloud Computing (RC3) is the term given to the model of cloud computing, where business transactions span:

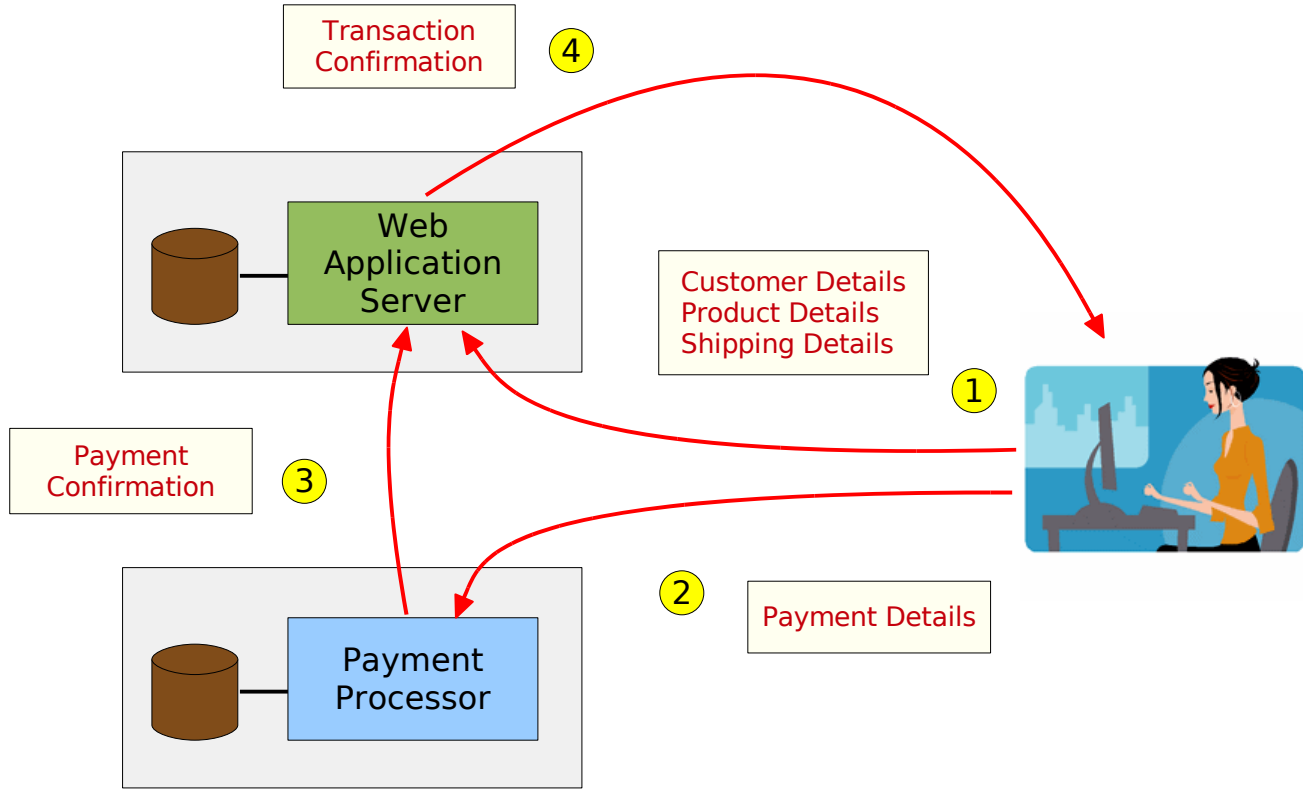
- **Regulated - or Controlled - zones** containing sensitive data; and
- **Public - or Cloud - zones** containing all other data

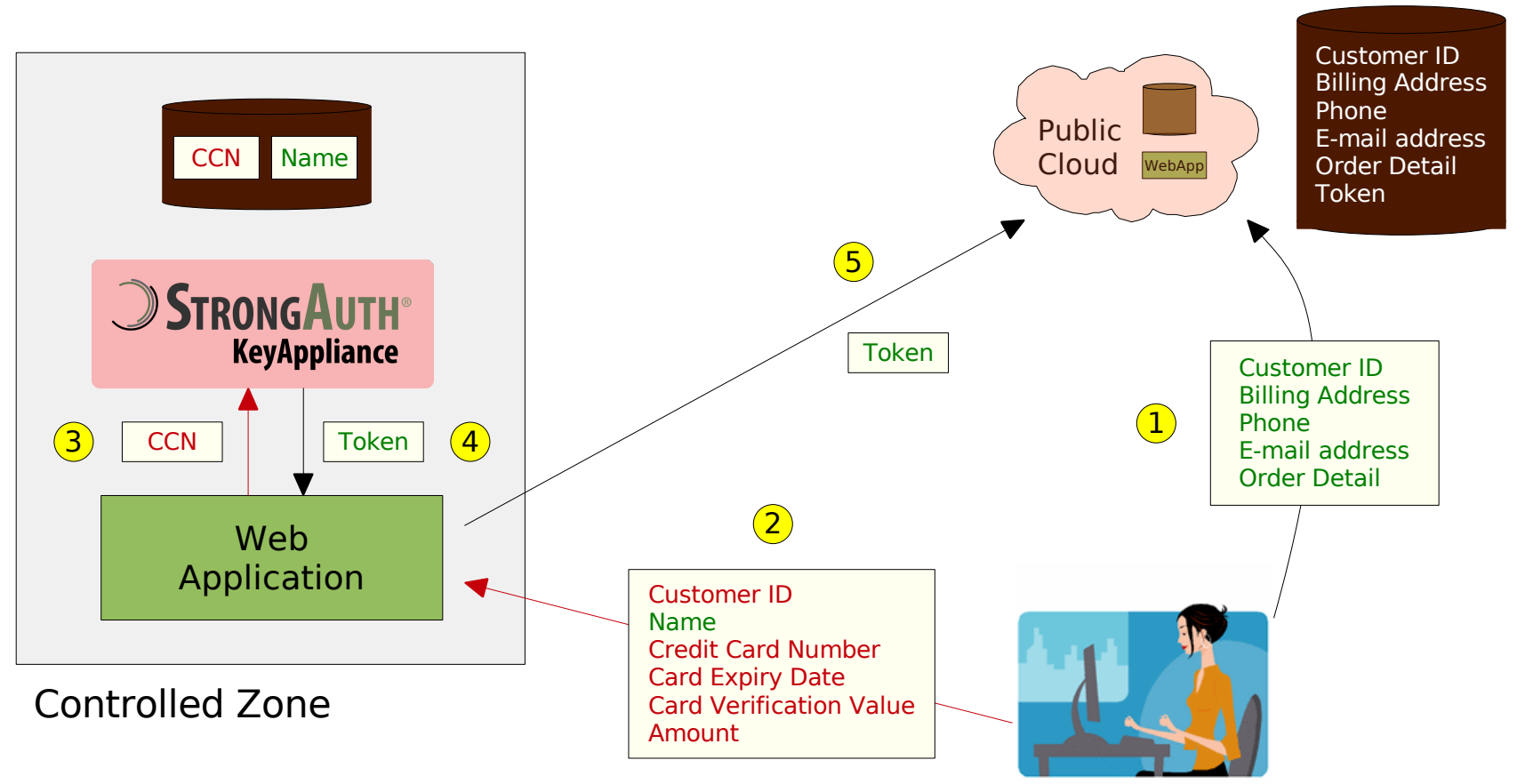
- Works with existing web-application architecture with a slight modification
- Use security resources appropriately by securing only what needs to be secured
- Prove regulatory compliance to data-security regulations
- Leverage public clouds to reduce costs, increase flexibility, scalability, etc.
  - Also works with private clouds and existing IT infrastructure for those who do not want to dive into public clouds just yet

<b>Class 1 (C1)</b>	Sensitive and regulated data	Data whose disclosure to the public would result in fines, potential lawsuits, and loss of goodwill to the breached entity. Examples are: credit card numbers, social security numbers, bank account numbers, medical data, etc.
<b>Class 2 (C2)</b>	Sensitive but non-regulated data	Data which is not regulated, but whose disclosure to the public would be detrimental to a company and/or result in some loss of goodwill to the breached entity. Examples are: an employee's salary, sales figures for specific product-lines, name, gender and age of a customer, etc.
<b>Class 3 (C3)</b>	All other data	It should be noted, that when sensitive data is tokenized in a well-designed encryption and key-management (EKM) system, it is effectively rendered non-sensitive. Thus, even C1/C2 data can be classified as C3 after it has undergone encryption and tokenization.

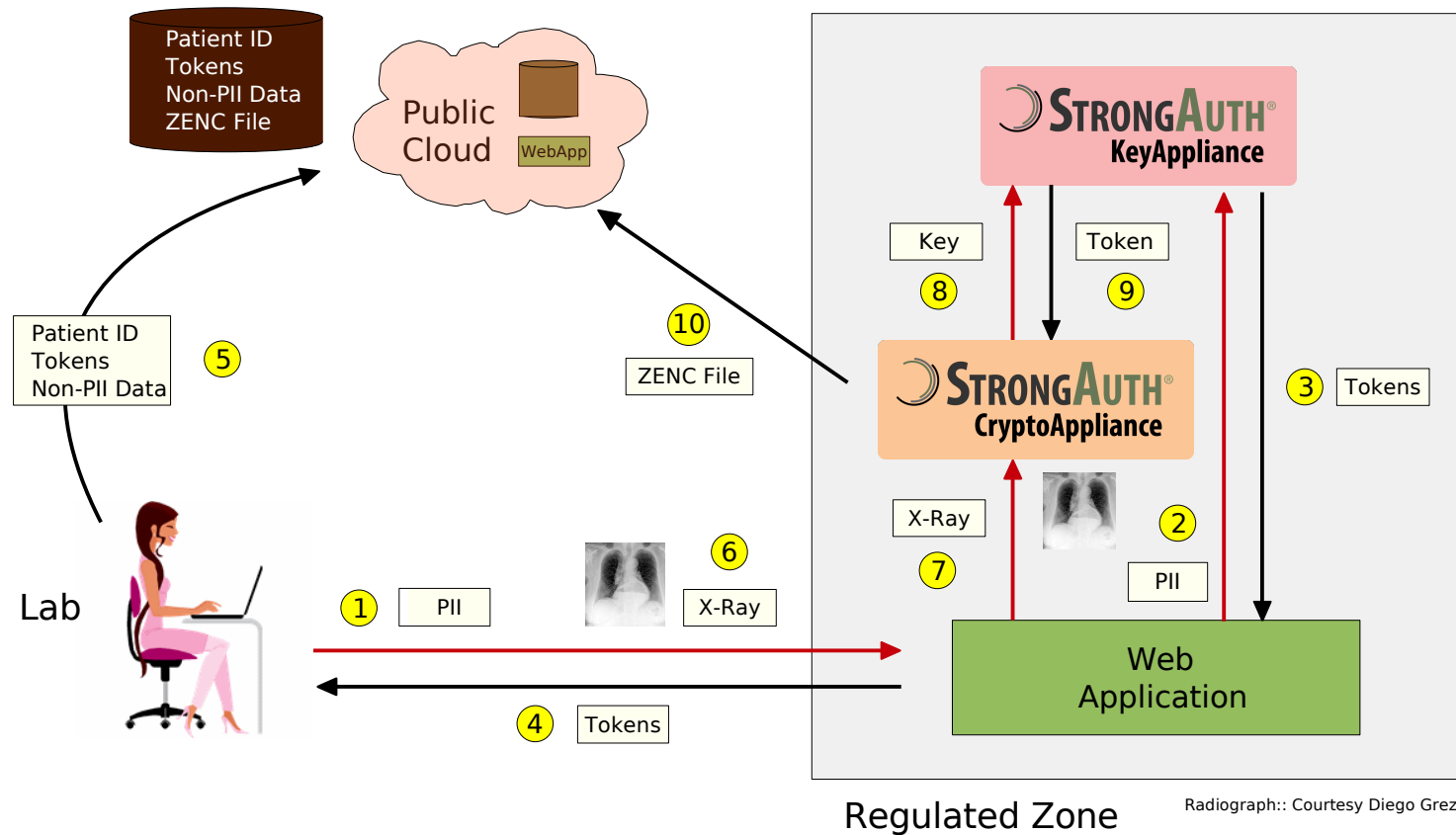
<b>Class 1 (C1)</b>	Processed only in Controlled Zones. Tokens may be stored in Clouds.
<b>Class 2 (C2)</b>	Processed in secure, but not necessarily Controlled Zones. Tokens may be stored in Clouds.
<b>Class 3 (C3)</b>	Processed and stored in Clouds.

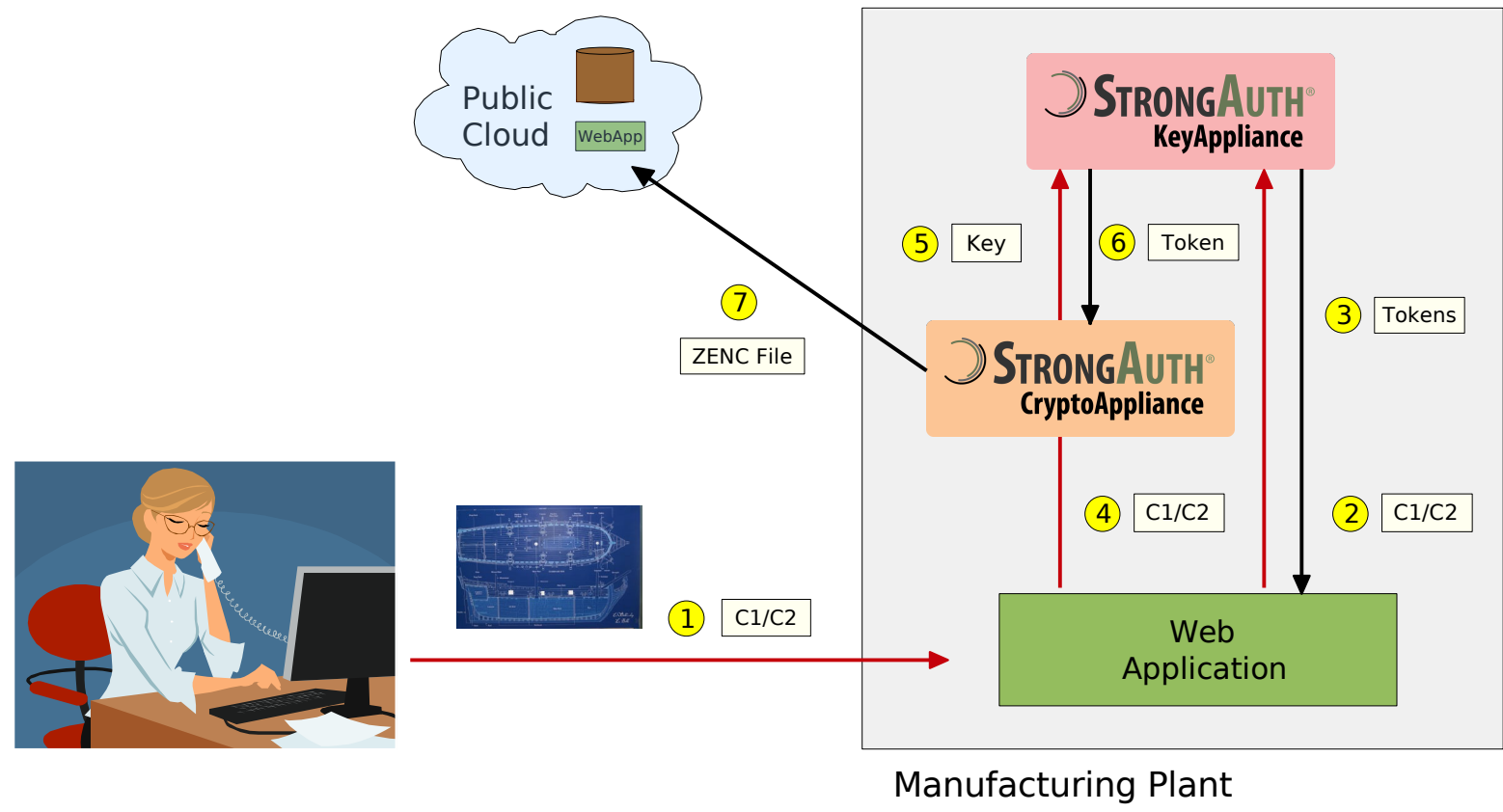






Provable regulatory compliance!



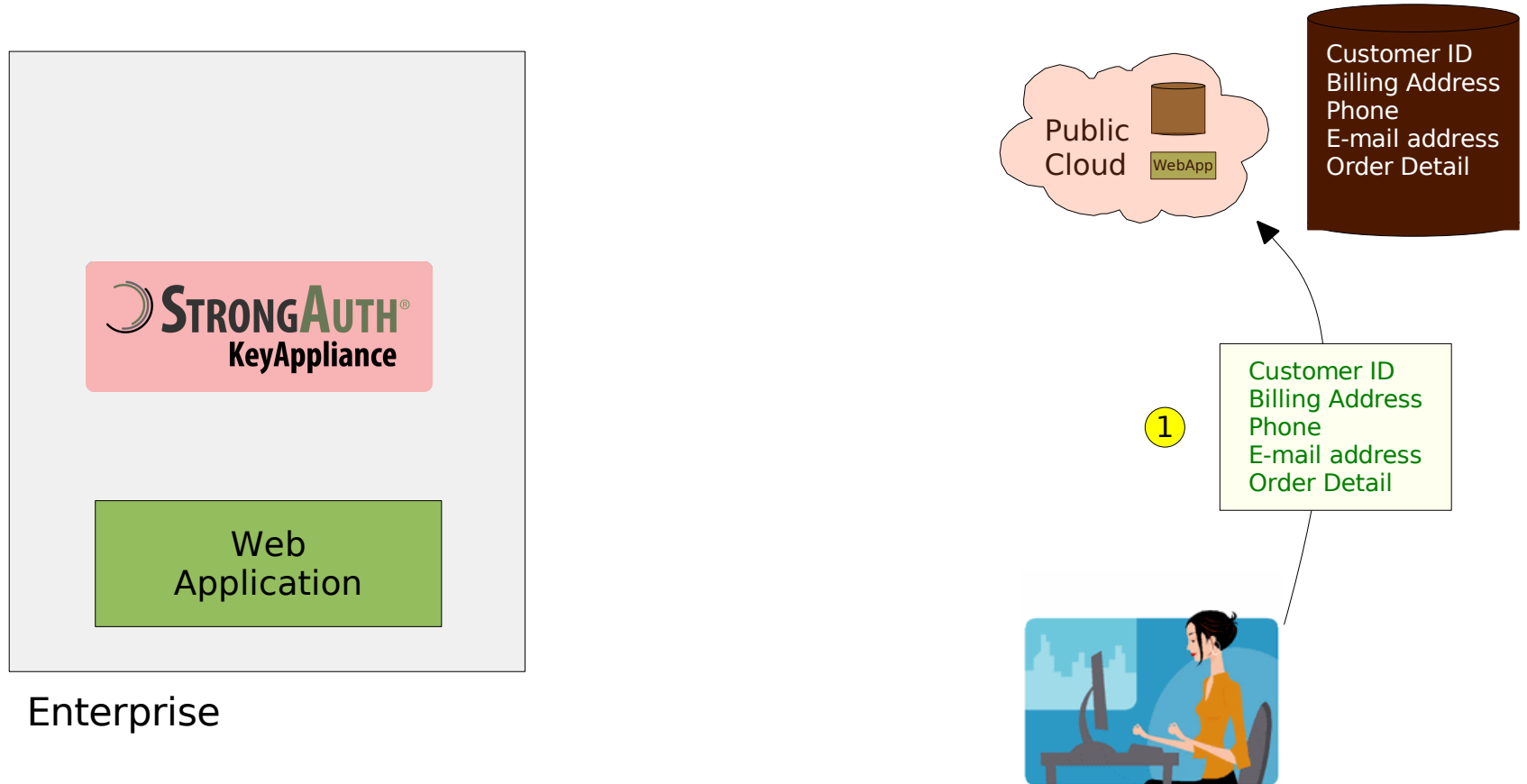


Provable regulatory compliance!

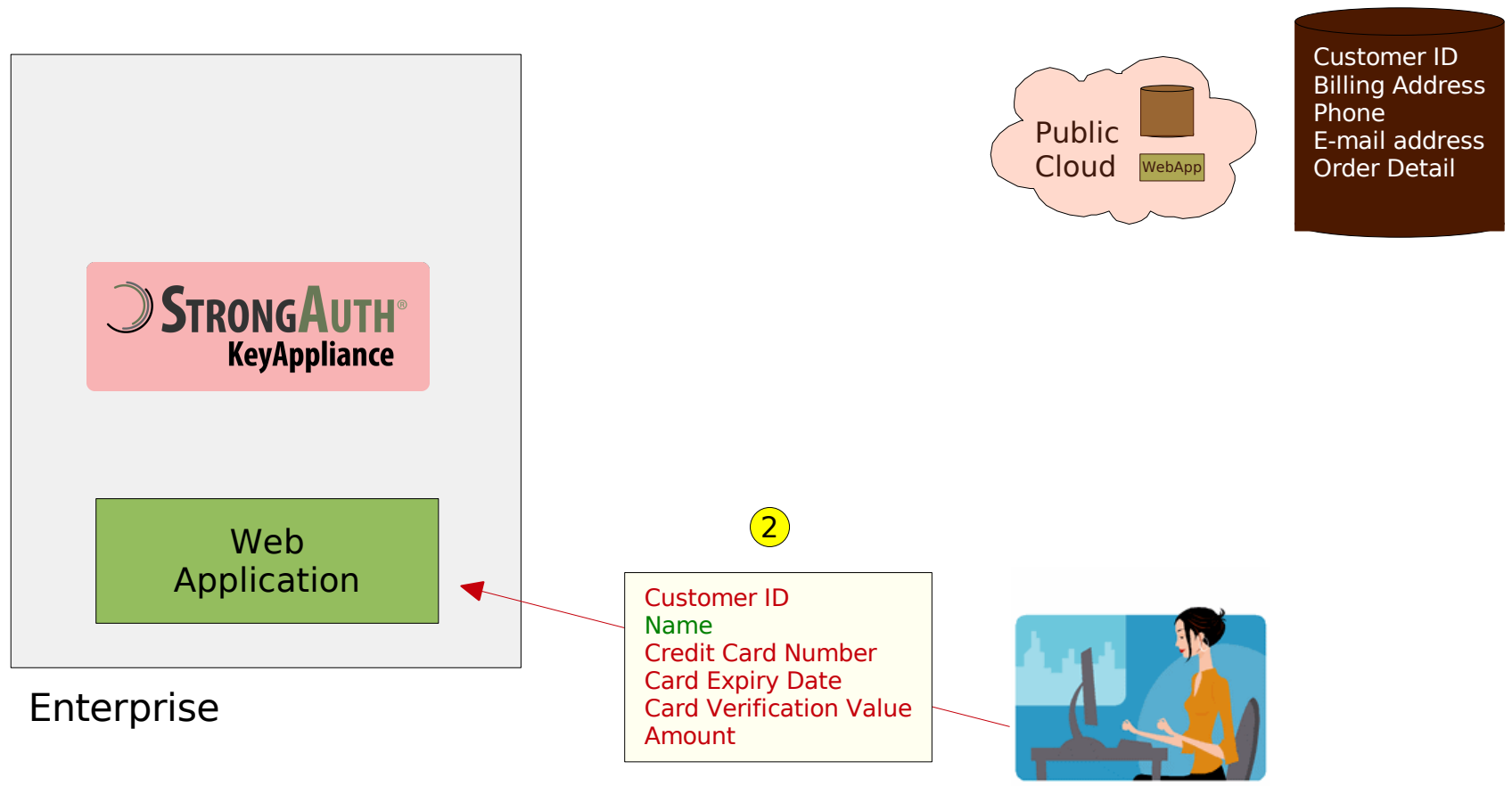


## SECURE CLOUD COMPUTING FOR E-COMMERCE

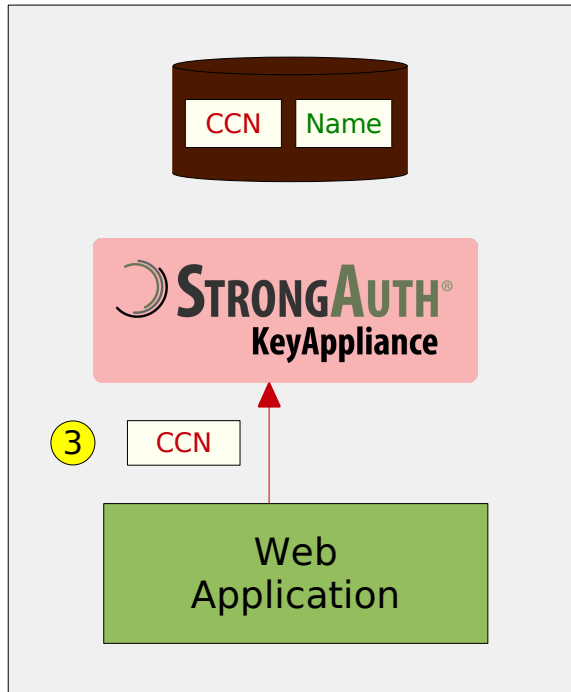
Provable regulatory compliance!



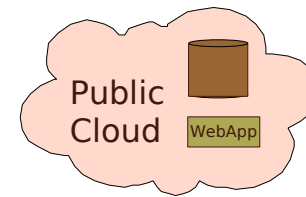
Provable regulatory compliance!



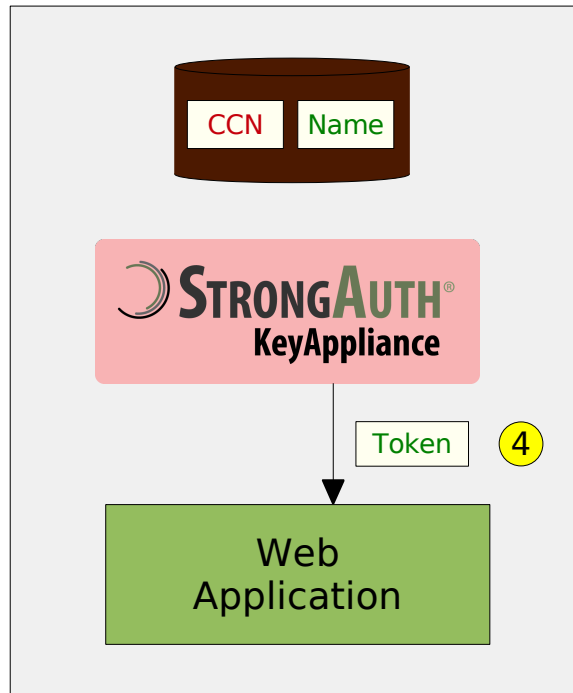
Provable regulatory compliance!



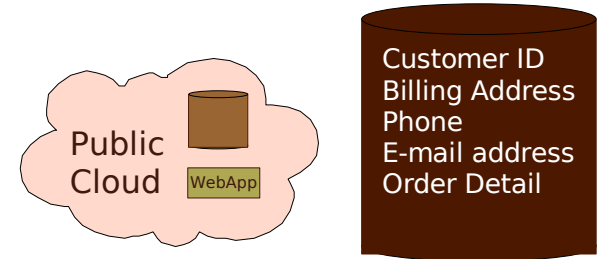
Enterprise

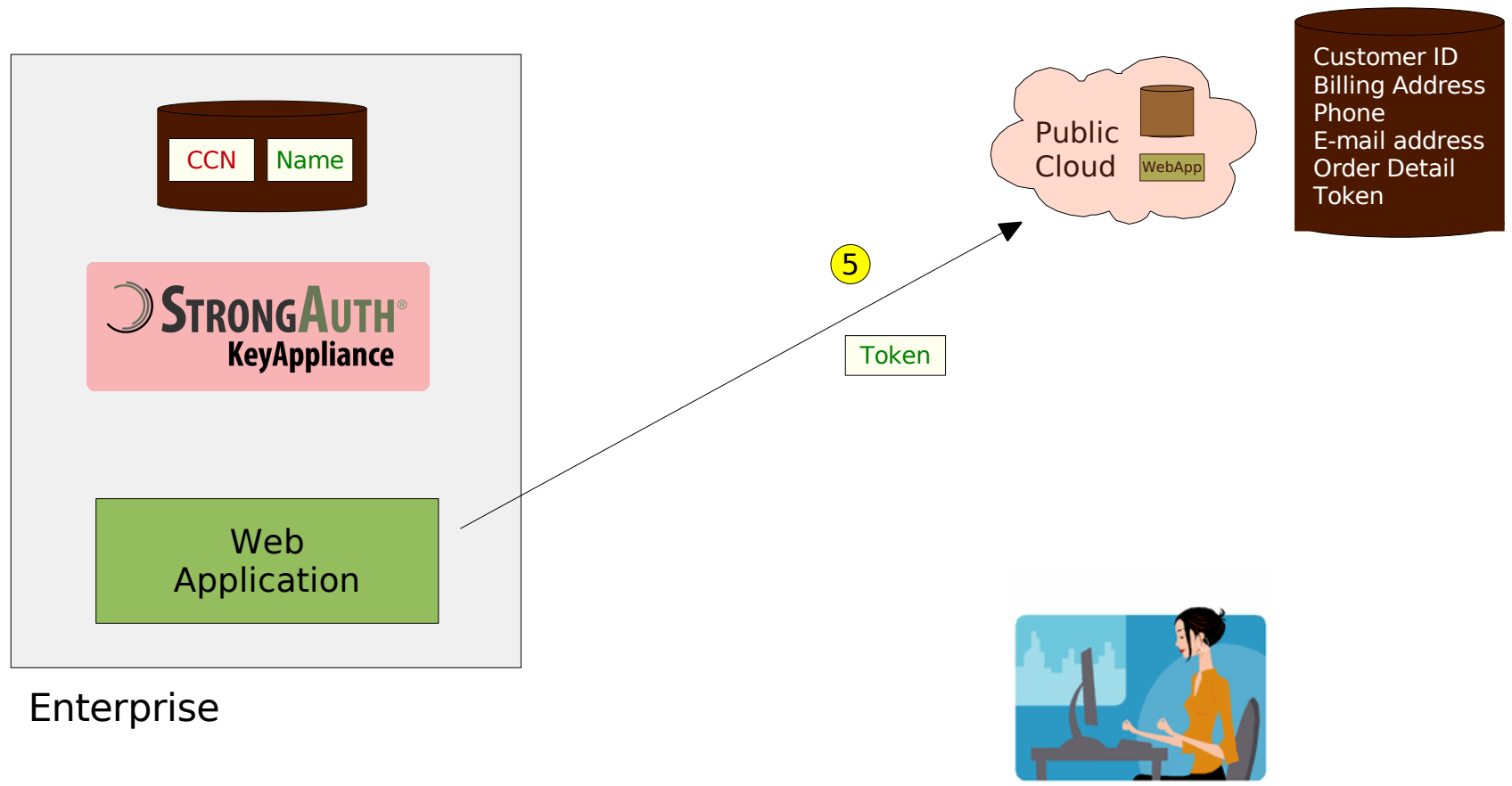


Provable regulatory compliance!



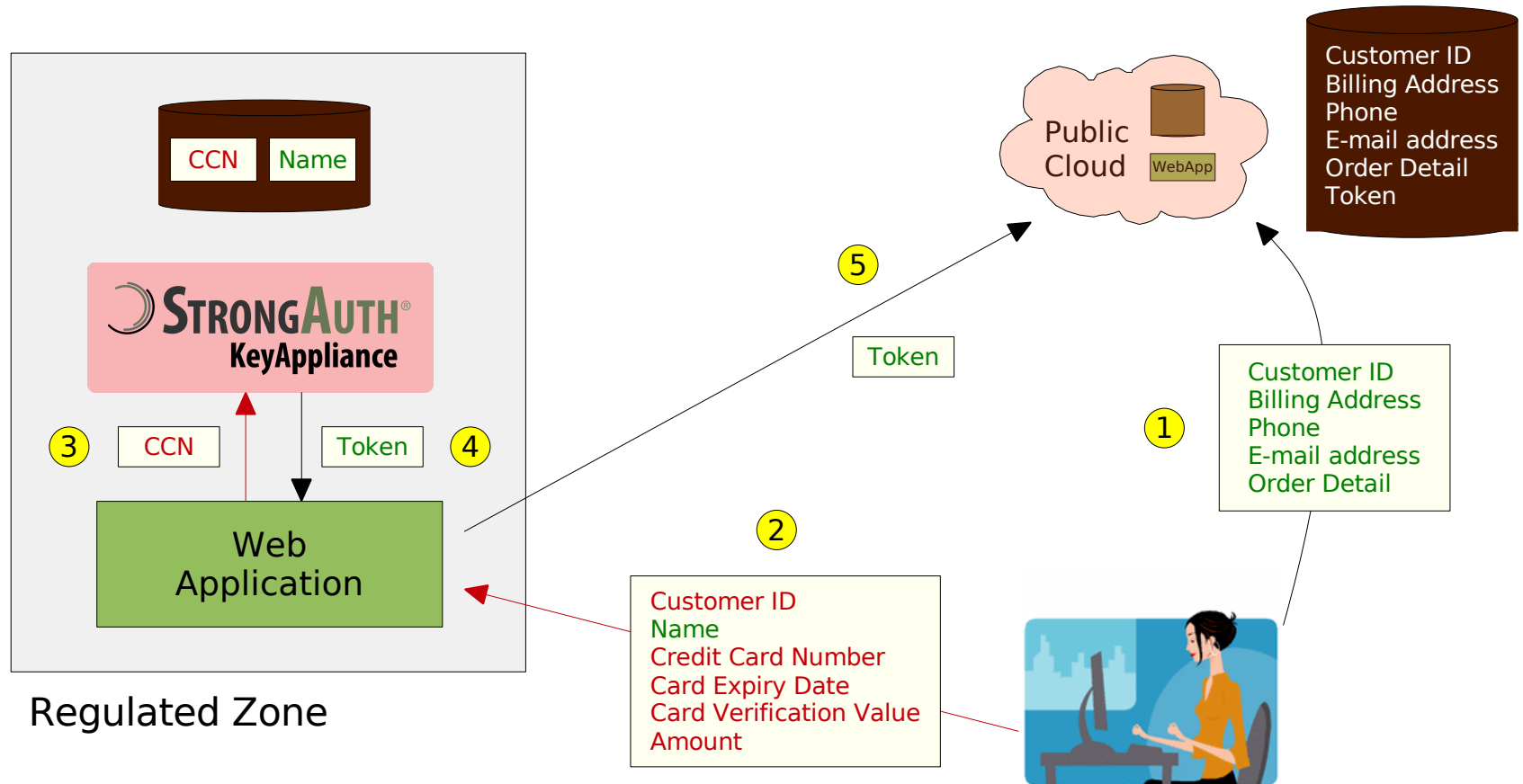
Enterprise





# STRONGAUTH® E-COMMERCE – PUBLIC CLOUD

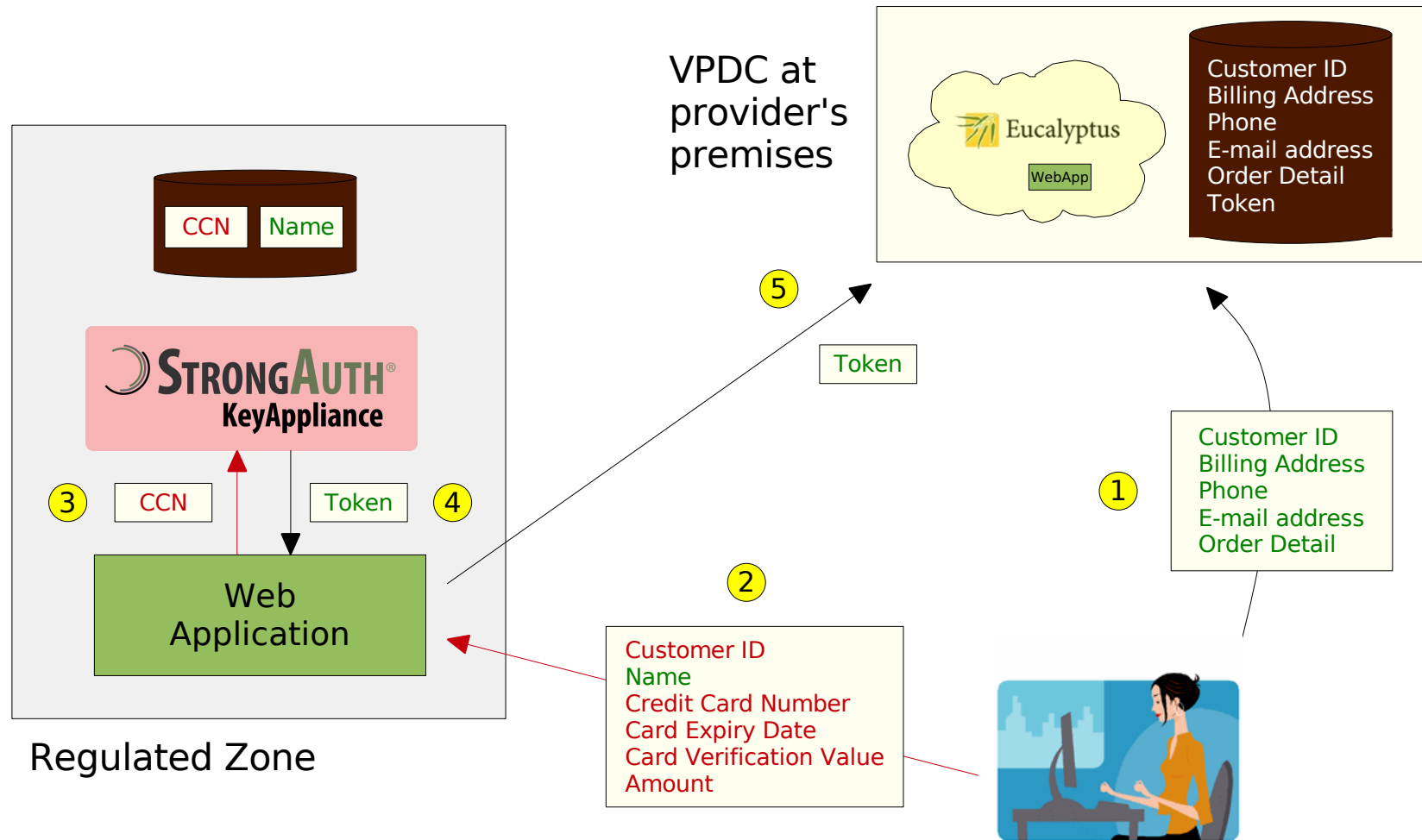
Securing the Core



Provable regulatory compliance!

# STRONGAUTH<sup>®</sup> E-COMMERCE – PRIVATE CLOUD

Securing the Core

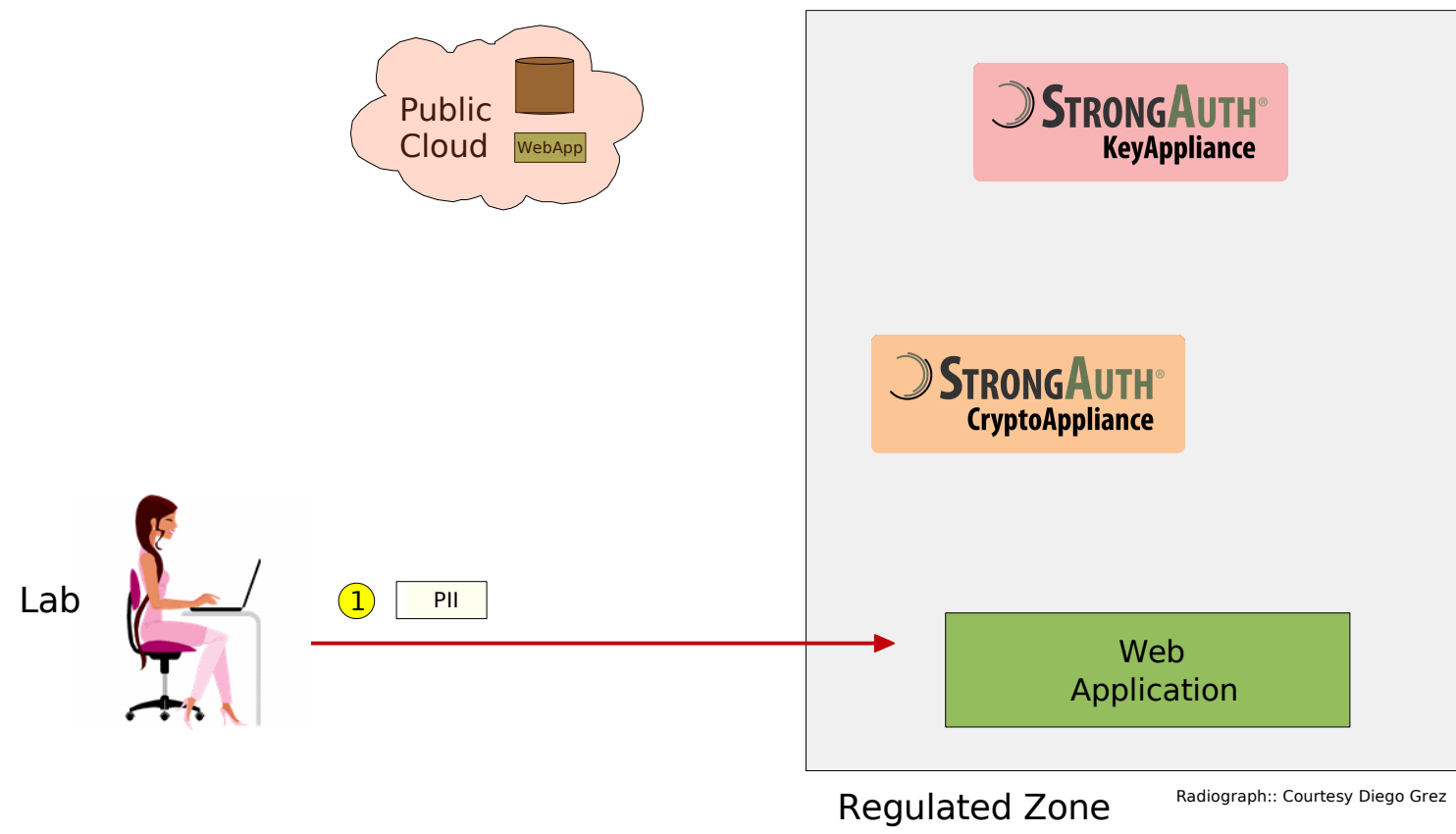


Provable regulatory compliance!



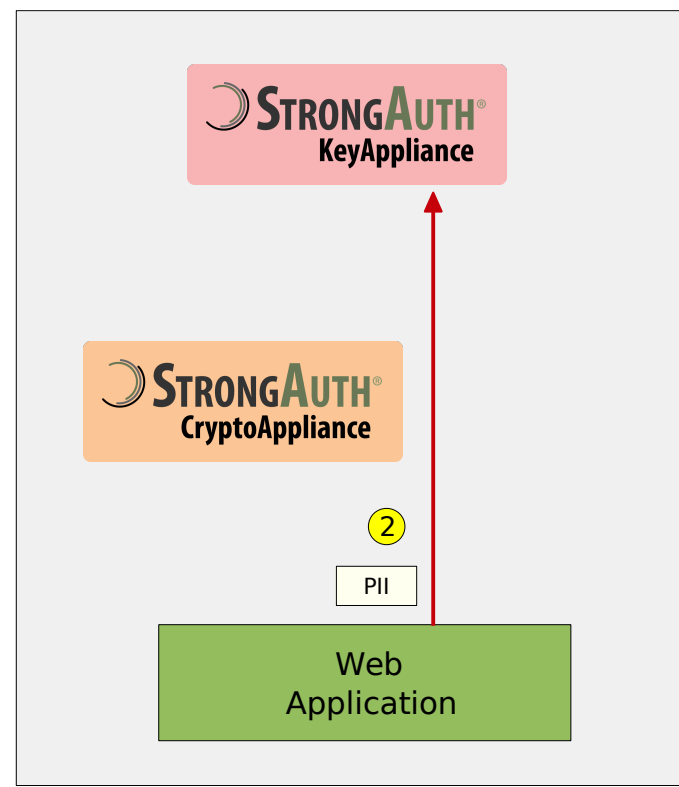
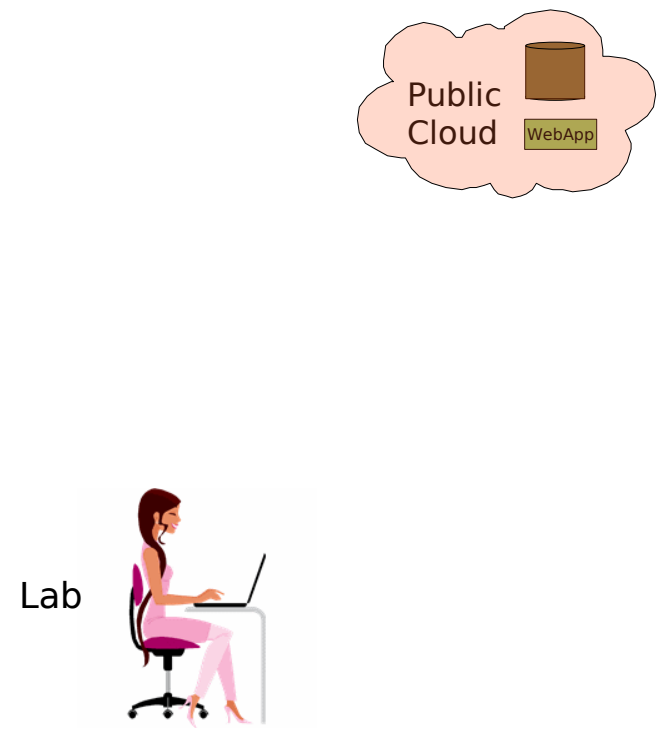
# SECURE CLOUD COMPUTING FOR HEALTHCARE

Provable regulatory compliance!



Radiograph:: Courtesy Diego Grez

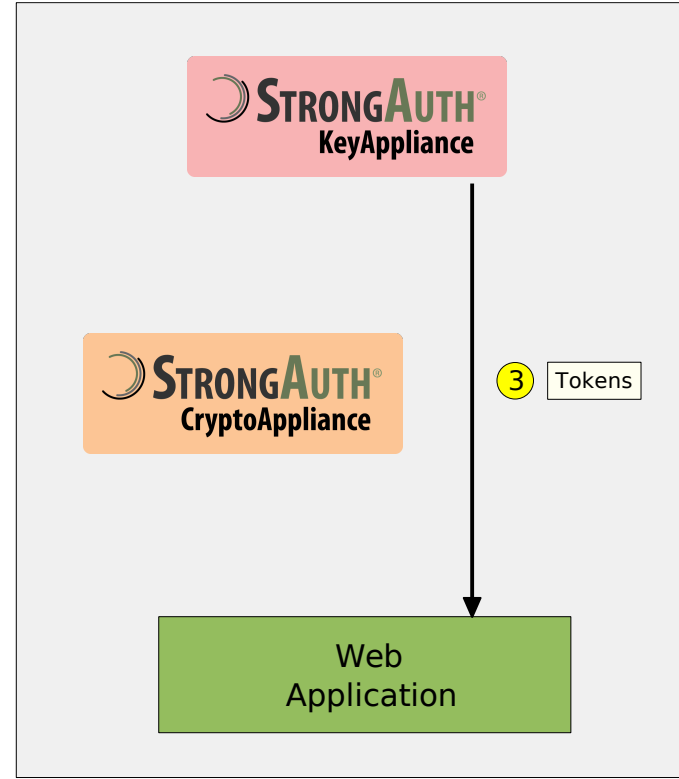
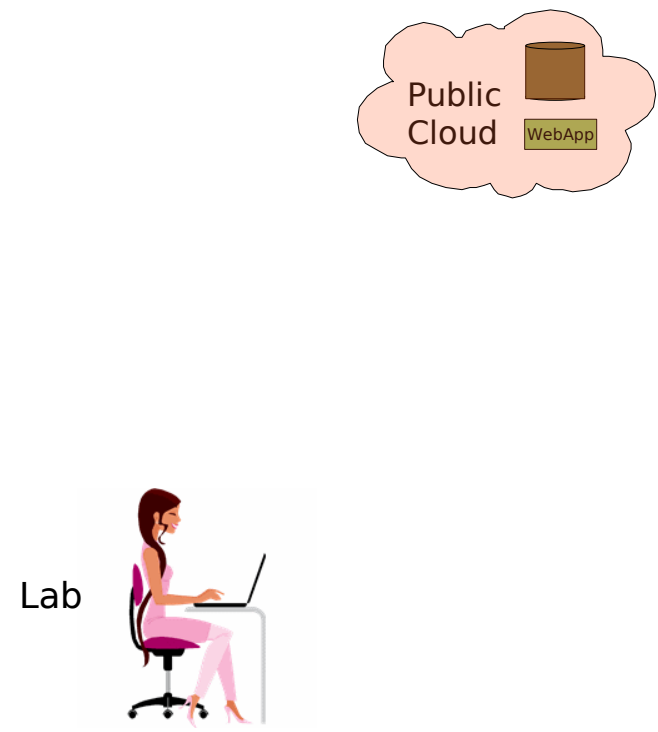
Provable regulatory compliance!



Regulated Zone

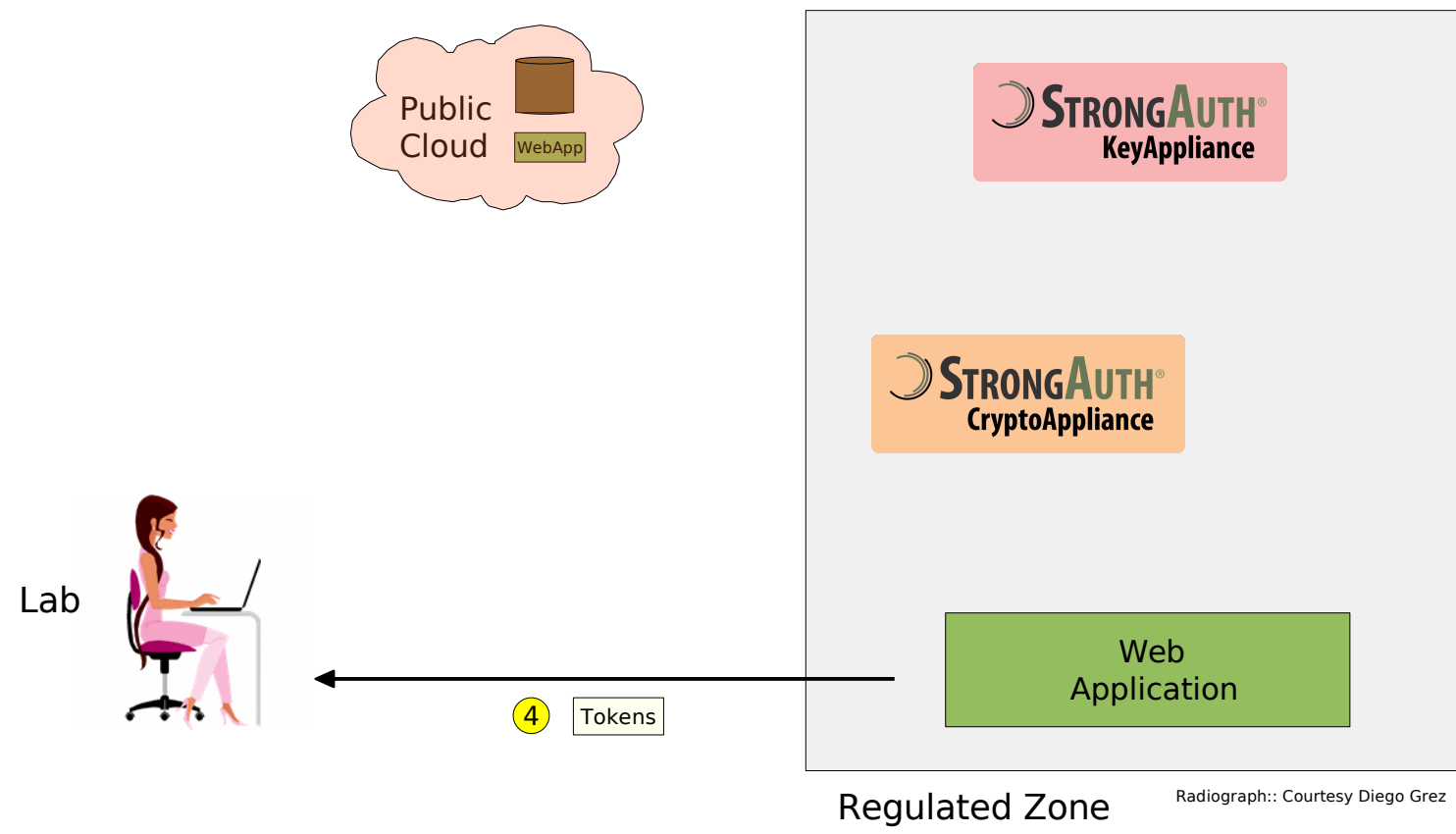
Radiograph:: Courtesy Diego Grez

Provable regulatory compliance!

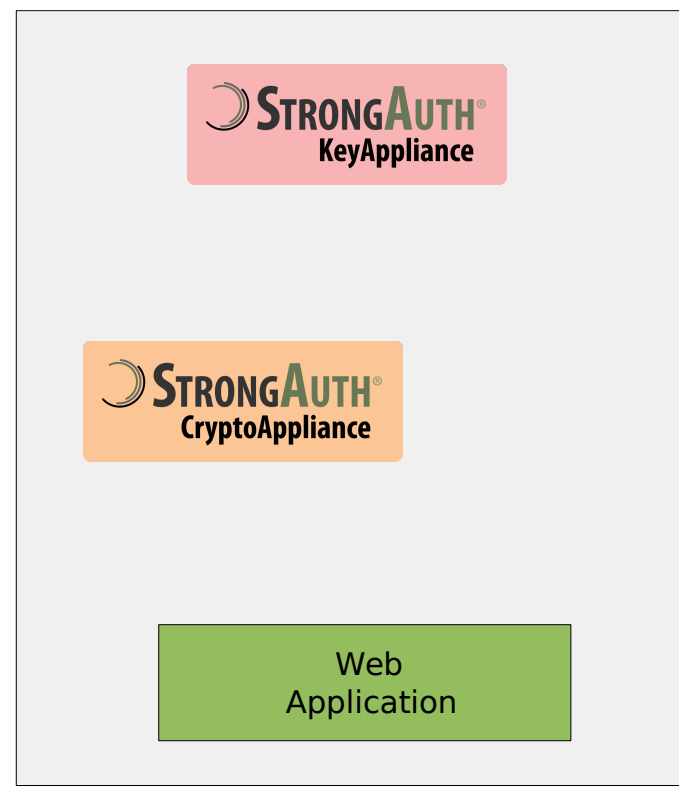
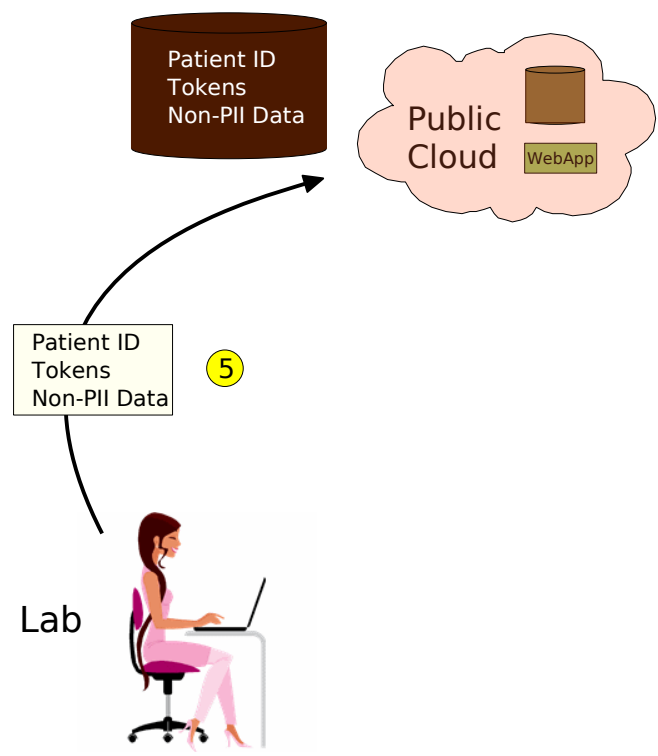


Regulated Zone

Radiograph:: Courtesy Diego Grez



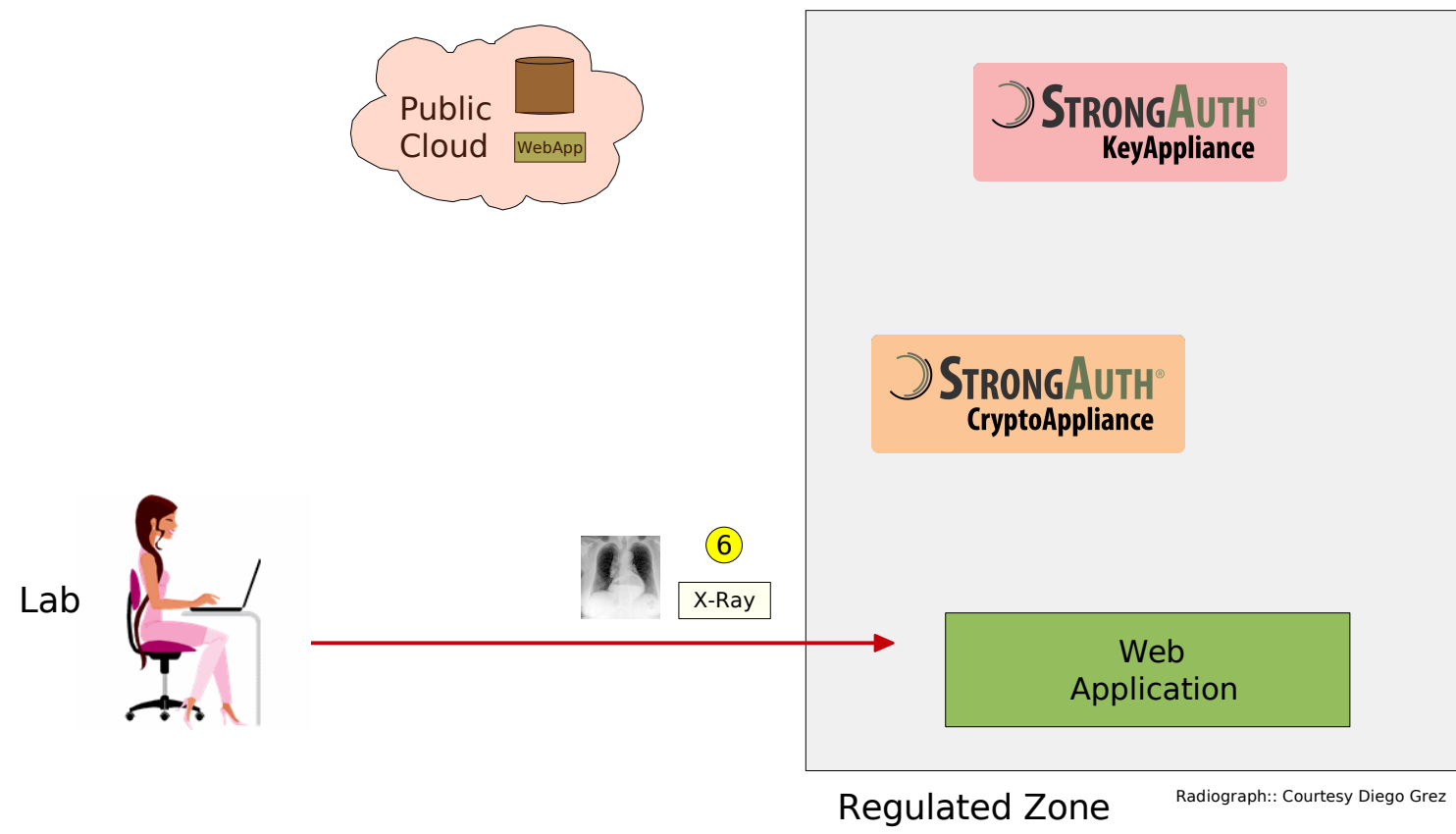
Provable regulatory compliance!



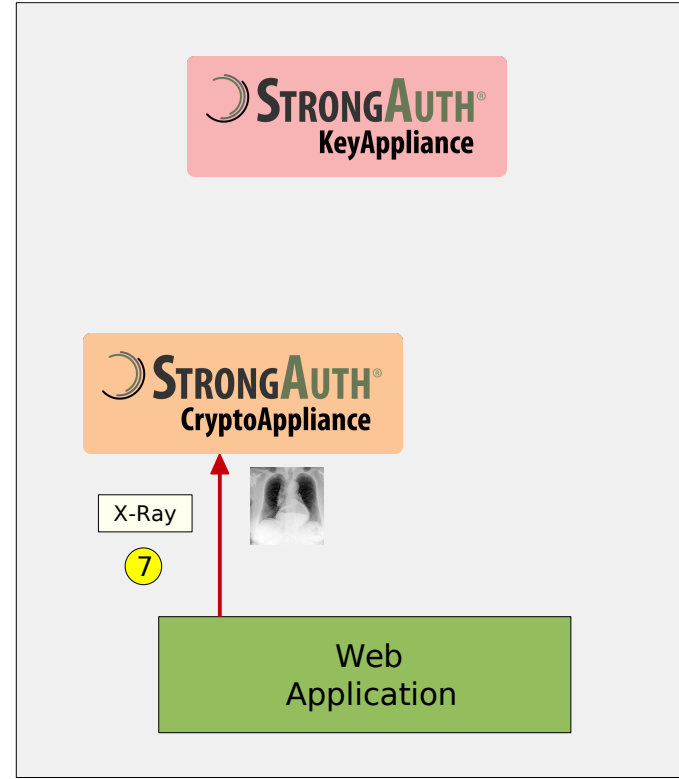
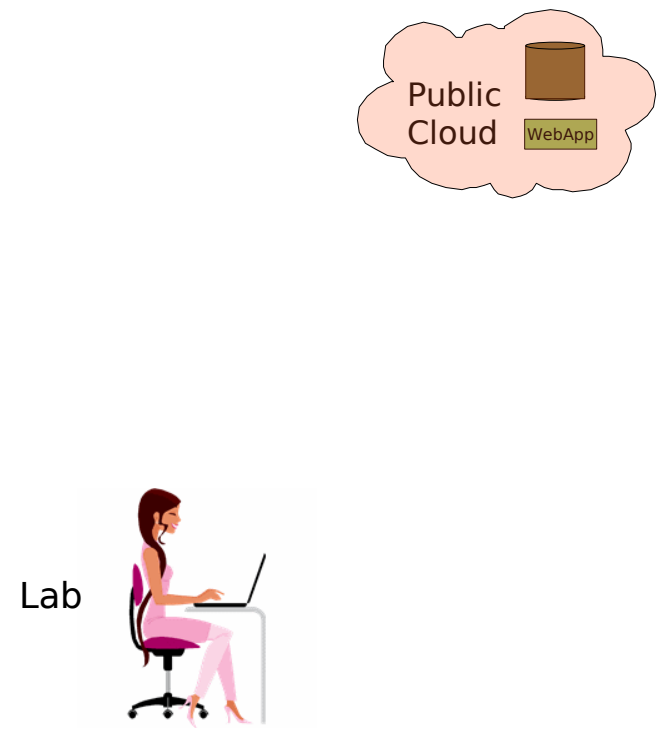
Regulated Zone

Radiograph:: Courtesy Diego Grez

Provable regulatory compliance!



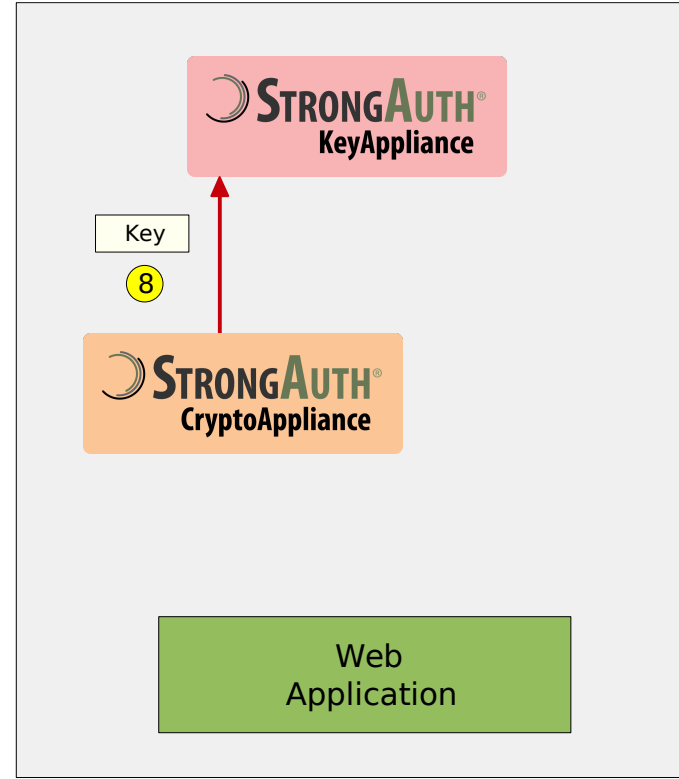
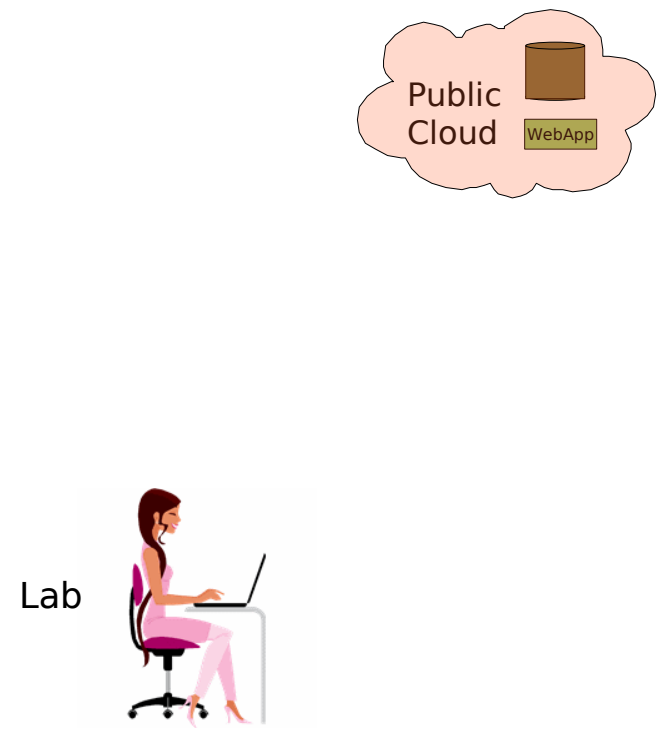
Provable regulatory compliance!



Regulated Zone

Radiograph: Courtesy Diego Grez

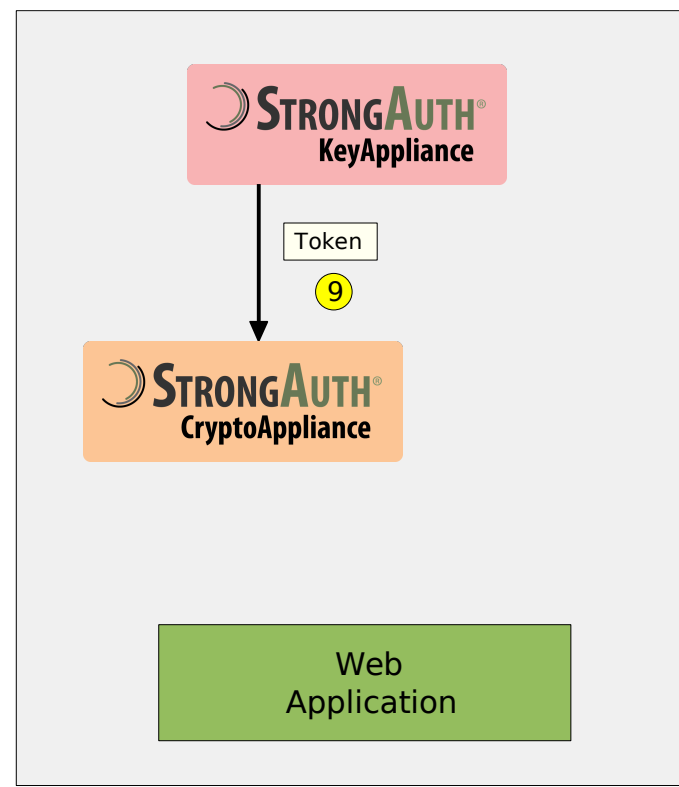
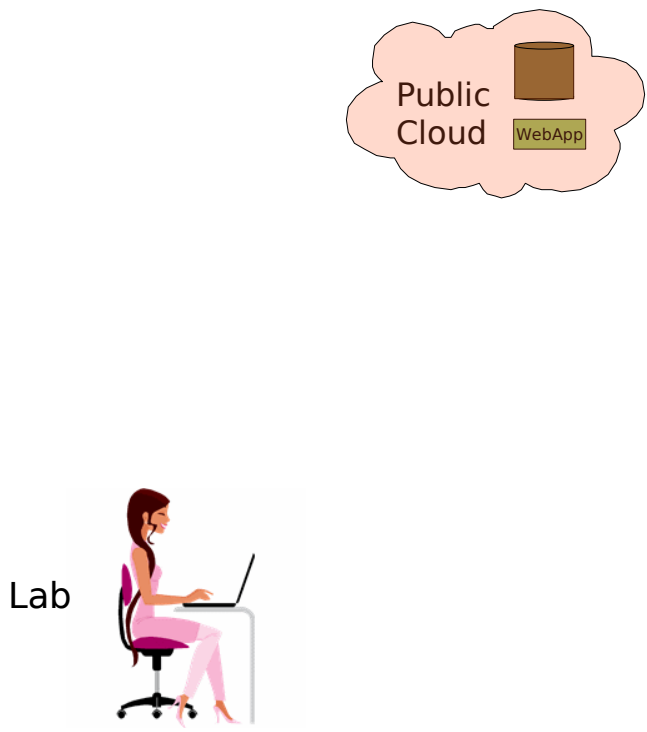
Provable regulatory compliance!



Regulated Zone

Radiograph:: Courtesy Diego Grez

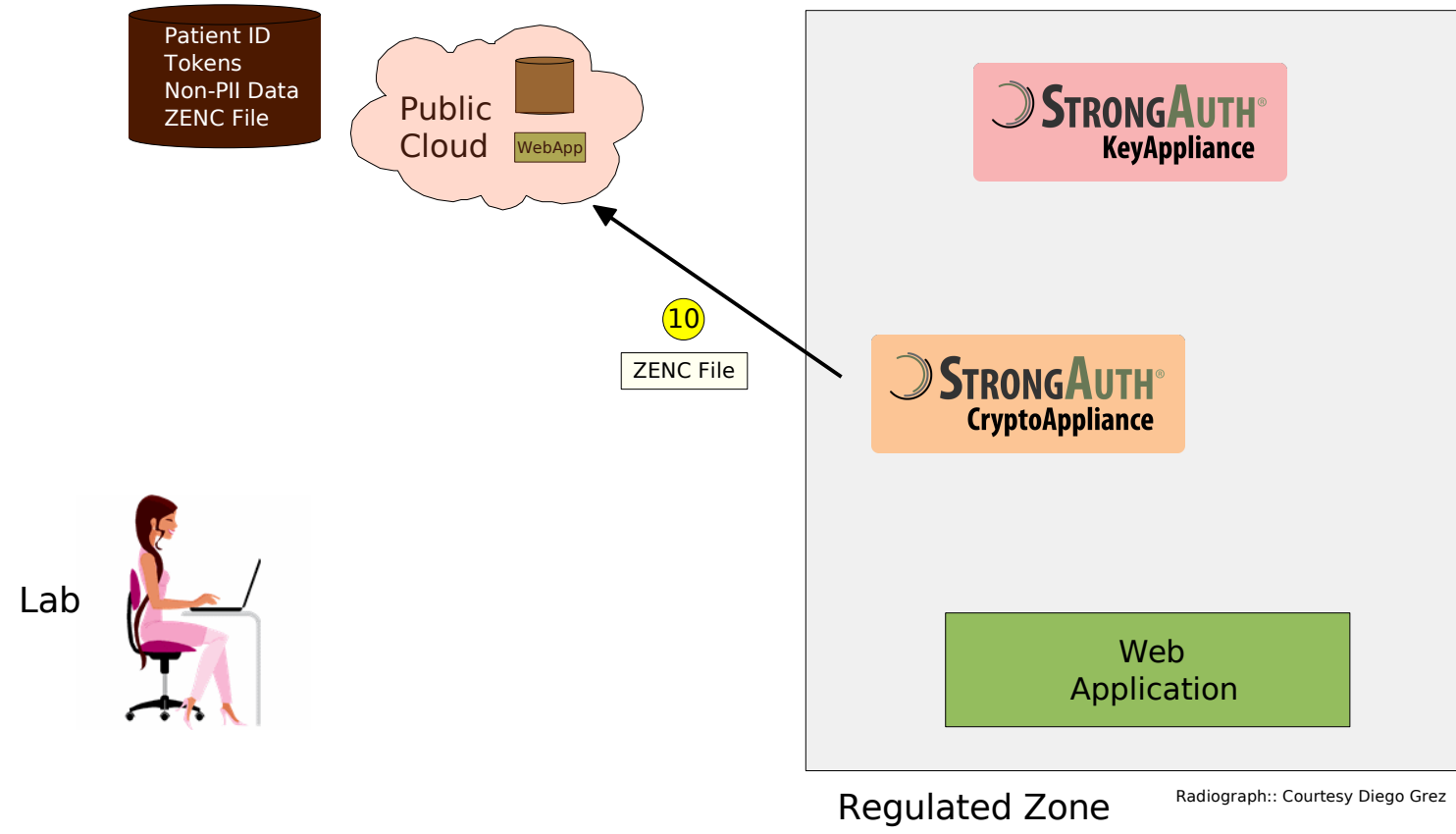
Provable regulatory compliance!



Regulated Zone

Radiograph:: Courtesy Diego Grez

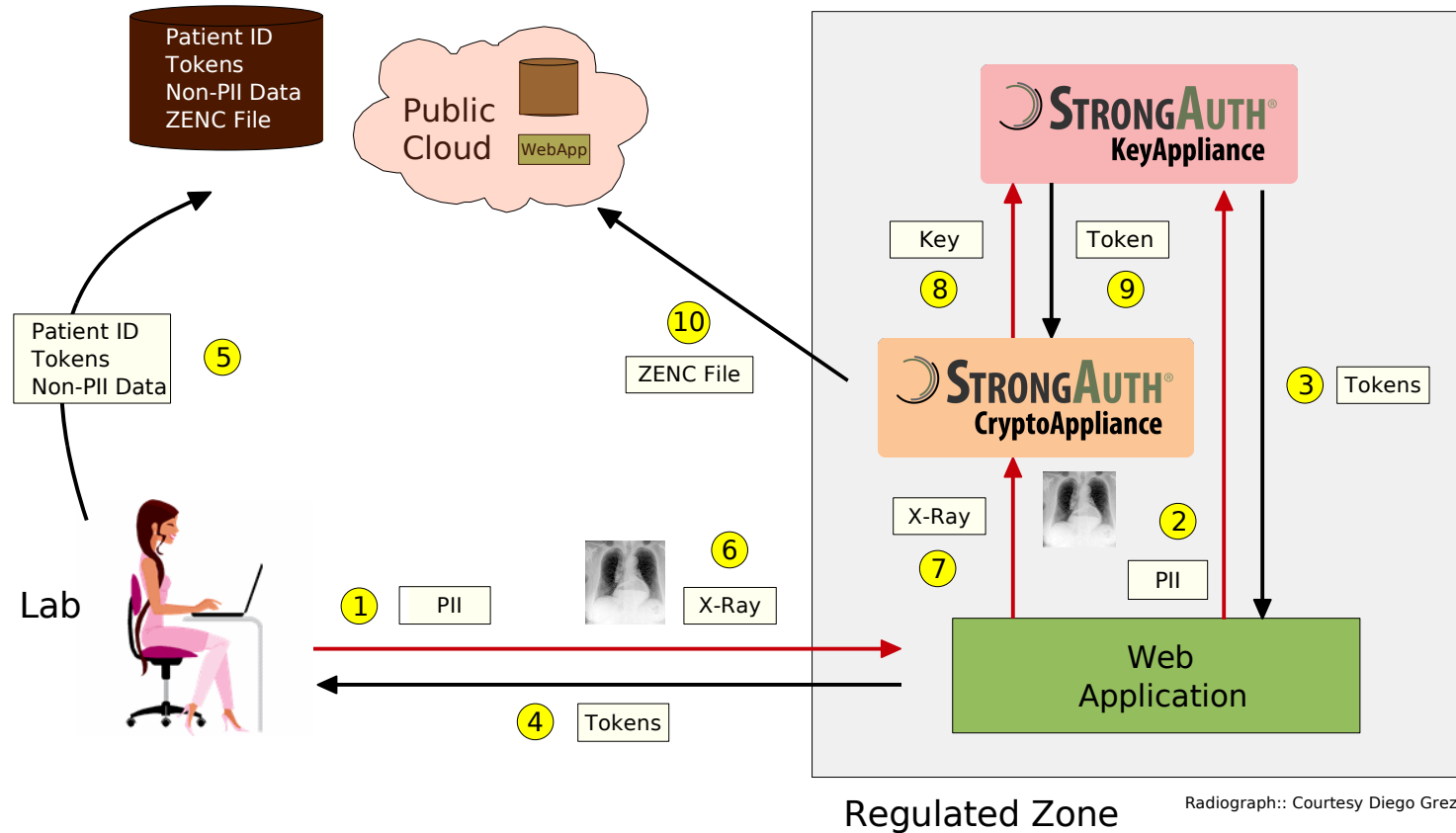
Provable regulatory compliance!



Provable regulatory compliance!

# STRONGAUTH<sup>®</sup> HEALTHCARE – PUBLIC CLOUD

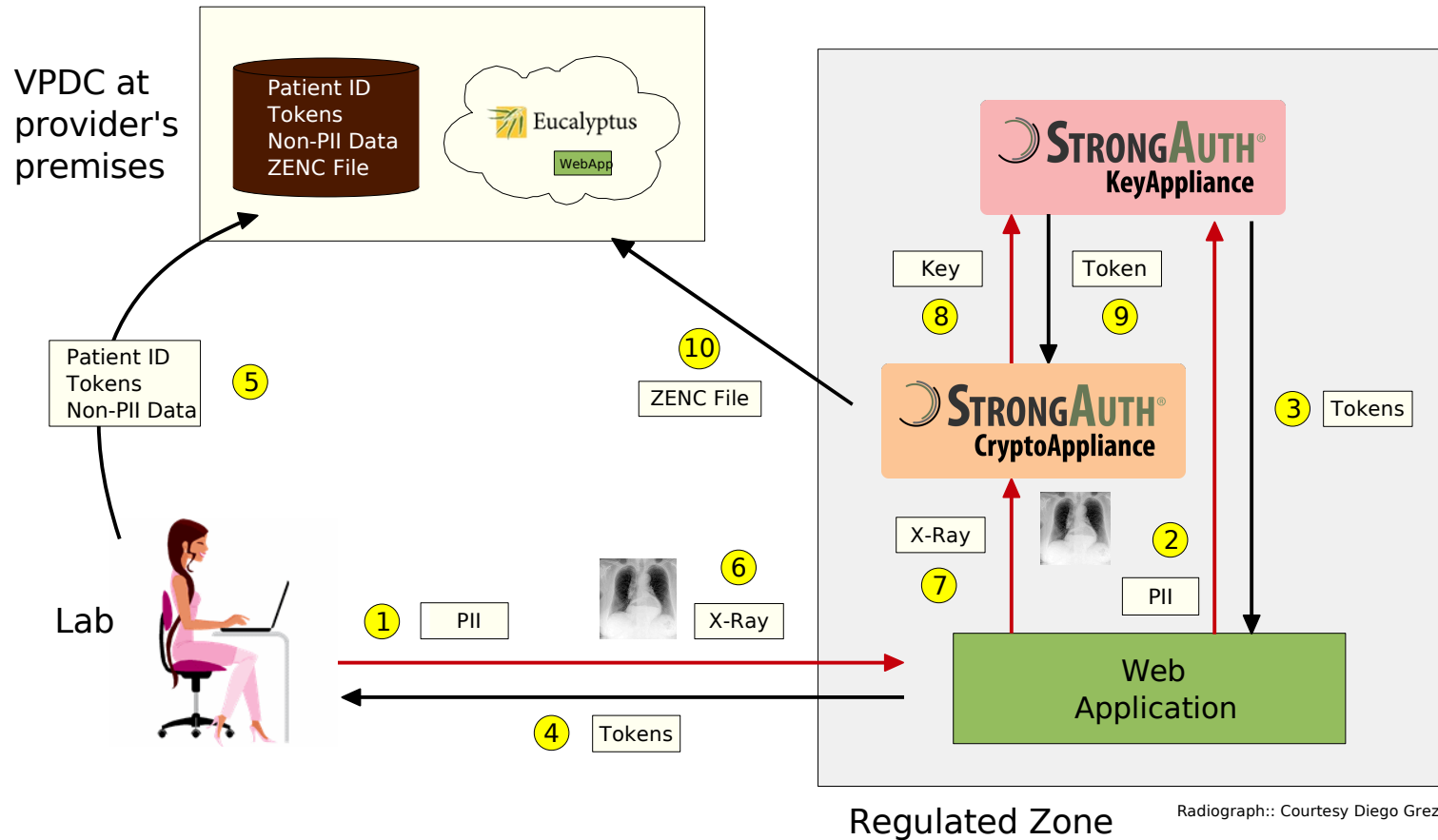
Securing the Core



Provable regulatory compliance!

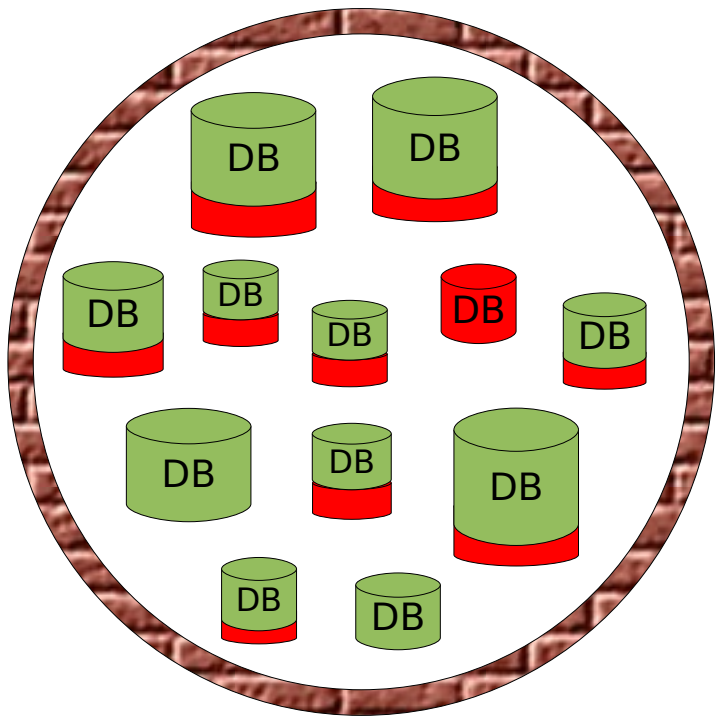
# STRONGAUTH<sup>®</sup> HEALTHCARE – PRIVATE CLOUD

Securing the Core

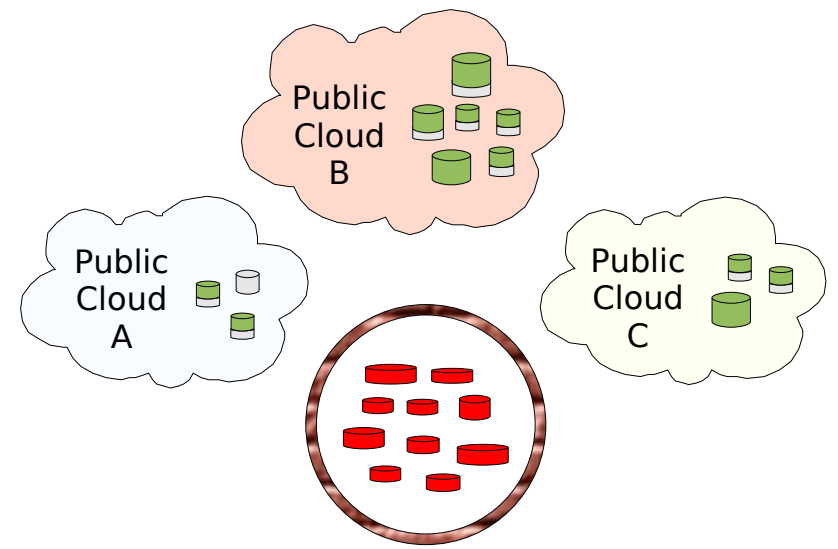


Provable regulatory compliance!

- Keys and sensitive data are **always** stored and managed in Regulated/Controlled Zone
- Public/Cloud Zone does NOT store user credentials
- Communication between zones is always in one direction: from RZ to PZ
- Servers from RZ communicate with PZ using Client-Authenticated SSL using web-services
  - Last two controls ensure that a compromise of the Cloud Zone cannot compromise the Controlled Zone

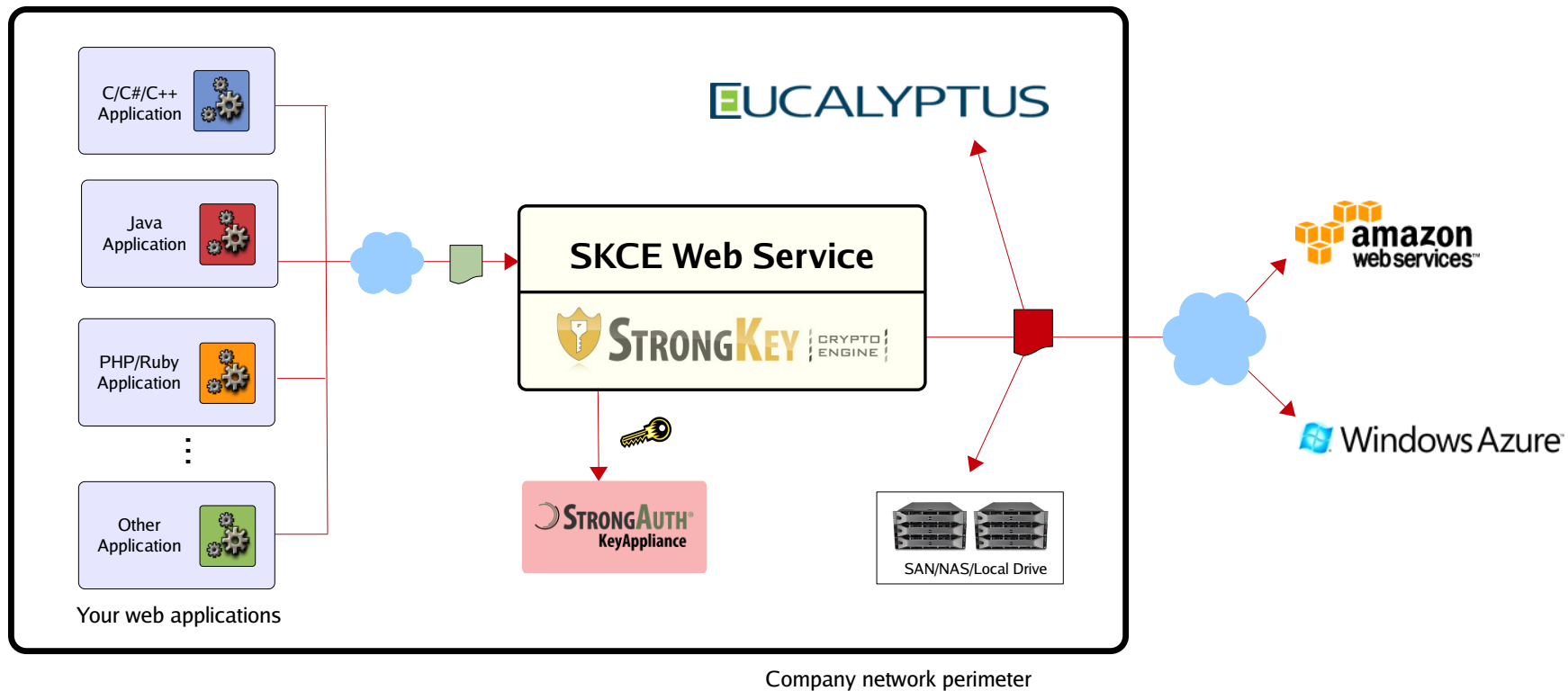





Before



After

- StrongKey CryptoEngine
  - Free and Open Source Software (FOSS)
  - Java library & SOAP-based web-services for encrypt, decrypt and move operations on files
  - Currently works with **AWS**, **Azure** and **Eucalyptus** for storage (more clouds to come)
  - Generates keys, and automatically stores/recovers them from StrongAuth's KeyAppliance
  - Integrated with AD and OpenDS for authentication & authorization (can work with other LDAP-based IDMS)
  - Download at <http://sourceforge.net/projects/skce/>



-  Plaintext file
-  Ciphertext file
-  Symmetric Key

# So, how do you start?

1. Download and install CentOS Linux
2. Download and install Eucalyptus
3. Setup a VM and Walrus
4. Download, install & run sample RC3 application\*
5. Download and configure StrongKey CryptoEngine\*
6. Run sample SKCE applications to encrypt/decrypt files in/out of Walrus buckets
7. Get public cloud account; repeat #5-6 with public cloud
8. You're doing some serious RC3 at this point!!

\* Demo KeyAppliance is available on internet for testing.  
ONLY USE TEST DATA with this appliance!

- Contact Information

Arshad Noor

[arshad.noor@strongauth.com](mailto:arshad.noor@strongauth.com)

[www.strongauth.com](http://www.strongauth.com)

[www.strongkey.org](http://www.strongkey.org)

[www.cryptoengine.org](http://www.cryptoengine.org)

<http://www.strongauth.com/pdf/RC3-WebAppArch-1.2-2.pdf>