A web-application architecture for Secure Cloud Computing
In the beginning...

- Your data-center
- Your mainframe or mini-computer
- Your network
- Your single-tiered monolithic applications
- Your Operations staff
The PC-LAN

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

Provable regulatory compliance!
The WWW

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

Provable regulatory compliance!
The Cloud

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

Provable regulatory compliance!
What's needed

An architecture that secures your data in Public Clouds while proving compliance to regulations!

Provable regulatory compliance!
The Paradigm Shift

• **Regulatory Compliant Cloud Computing**
  
  – **Regulated Zone**
    • Enterprise Key Management Infrastructure (EKMI)
    • Encrypts/Tokenizes sensitive data
    • Typically, 10-20% of business application
  
  – **Cloud Zone**
    • Stores all public data and tokens
    • Typically, 80-90% of business application
    • NO CRYPTOGRAPHY

Provable regulatory compliance!
Basic web application

Provable regulatory compliance!
A variation

Provable regulatory compliance!
SECURE CLOUD COMPUTING FOR E-COMMERCE
Provable regulatory compliance!
Provable regulatory compliance!
Provable regulatory compliance!
Provable regulatory compliance!
Provable regulatory compliance!
Provable regulatory compliance!
Provable regulatory compliance!
Public Cloud

Provable regulatory compliance!

Regulated Zone

Cloud Zone

Customer ID
Billing Address
Order Detail
Tokens

Token

Web Application

Customer ID
Name
Credit Card Number
Card Expiry Date
Card Verification Value
Amount
Phone
E-mail address
Private Cloud

Provable regulatory compliance!
Caveats 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 a LAN HSM 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 outside the Cloud
- Assume the worst (that your applications and data are operating on the open internet) and design for it
EKM in the Cloud?

Provable regulatory compliance!
Resources

- Regulatory Compliant Cloud Computing (RC3)
  - http://www.infoq.com/articles/regulatory-compliant-cloud-computing
- StrongAuth KeyAppliance
  - http://www.strongauth.com
- Cryptographic engine (designed for the Cloud)
  - http://www.cryptoengine.org
Provable regulatory compliance!
RC3 Implementation

- Document-management e-commerce company in the 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!
Provable regulatory compliance!