BYOK: Leveraging Cloud Encryption Without Compromising Control

Sol Cates
VP of Technical Strategy, CTO - Thales e-Security
CSO – Thales e-Security
@solcates
Let’s Begin

- So Many Clouds
- Who Does What and Where It Gets Murky
- It’s Not Just Me Telling You, And Tools You Can Use
- Encryption and Key Management Options for IaaS / PaaS
- Key Management for SaaS
- BYOK 101
- Smart Questions
- How to Apply
Data Protection Shared Responsibility Model
## Data Protection Shared Responsibility Model

<table>
<thead>
<tr>
<th>Infrastructure as a Service (IaaS)</th>
<th>Platform as a Service (PaaS)</th>
<th>Software as a Service (SaaS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Responsibility</strong></td>
<td><strong>Provider Responsibility</strong></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Application</td>
<td>Application</td>
<td>Application</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>
Cloud Security Alliance – Your Ally

- Global, nonprofit
- Building security best practices for next generation IT
- The globally authoritative source for trust in the cloud
Key CSA Resources to Make You Smarter
Cloud Controls Matrix

- Cloud supply chain risk management
  - Delineates control ownership
    - Provider, Customer
  - Ranks applicability to cloud provider type
    - SaaS vs PaaS vs IaaS
  - Anchor for security and compliance posture measurement
- Maps to global regulations and standards
  - NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings always growing
Consensus Assessment Initiative Questionnaire

• Cloud Controls Matrix companion
• Binary questions assess CCM compliance
  - Narrative explanations permitted
• Create consistent cloud provider assessment processes
• Enables cloud providers to self-assess security posture
Encryption & Key Management

Platform and data-appropriate encryption...shall be required.

- [Encryption] Keys
  - Shall not be stored in the cloud but
  - Shall be maintained by the cloud consumer or trusted key management provider.

We’re coming back to this point in a moment...
Encryption Options
# Data Protection with Encryption

## Varies by Cloud Model

<table>
<thead>
<tr>
<th>Cloud Model</th>
<th>Encryption Mechanism</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS</td>
<td>Native or Bring Your Own</td>
<td>If native, seek <strong>BYOK</strong></td>
</tr>
</tbody>
</table>
| PaaS        | - Native  
|             | - CASB  
| SaaS        | *You can’t bring your own* | If native, seek **BYOK** |
Native or Bring Your Own Encryption to IaaS?

**BYOE Advantages**
- Same architecture across multiple cloud providers
- You always control your keys

**Native Disadvantages**
- Block-level / FDE only
- No protection for data in use
Bringing Your Own Key

To IaaS Native Encryption, and PaaS and SaaS
BYOK’s origins

- BYOK was born out of necessity
  - Cloud Providers use/create/store your data
  - You want your data protected
  - Cloud Providers are starting to offer encryption, yet most hold the keys
  - Customers want/need to control their keys
    - Regulatory
    - Best practices (CSA, etc.)
Understanding *Bring Your Own Key*

- A customer supplied or managed master key, or derived key
- There are a few architecture trends to understand
  - Customer Master Key Import
    - Customer creates keys
    - Exports keys to cloud provider as master key to protect either data, or data keys
  - Derived Key Creation
    - Customer delivers Master key trusted by the provider to create derived keys for usage in the providers encryption
  - Hold Your Own Key (HYOK)
    - Provider calls customer-hosted service for encryption, key decryption or key provisioning services
Customer Master Key Import

1. Create “Import Key” in cloud
2. Import Public Key to your HSM or OpenSSL
3. Create AES Master Key in HSM/OpenSSL
4. Export Master Key wrapped with Public Import Key
5. Import Wrapped CKM to cloud
Derived Key Creation

1. Cloud Provider’s Key is encrypting
2. You create your key in HSM or OpenSSL
3. Wrap and send to your cloud provider
4. Keys combined mathematically
5. New key *you control*
Hold Your Own Key – Scenario 1

- Encryption engine and keys in your possession
  - On your premises or elsewhere
- Cloud provider sends and receives your data
  - Sends data for decryption / receives clear
  - Sends clear / received encrypted

Your Premises / Your Control

IaaS / PaaS / SaaS Providers

Please Decrypt DATA
Plain Text DATA
Please Encrypt UPDATED DATA
Encrypted DATA

Your Keys
Encryption Engine
Hardware Security Module (HSM)
Open SSL

File Systems
Databases
Hold Your Own Key – Scenario 2

- Encryption engine and encrypted key at cloud provider
- Cloud provider requests key decryption for use
Hold Your Own Key – Scenario 3

- Encryption engine in cloud
- Cloud provider requests keys for encryption and decryption
- Keys have TTL’s

Your Premises / Your Control

IaaS / PaaS / SaaS Providers

Encryption Engine

File Systems

Databases

May I have a key?

Here is a (wrapped) KEY, good til Friday
Things to consider

Derived Key and Master Key Import

- Keys are "imported" into the cloud provider
- Authorization of the keys usage is dependent on the providers model
- Doesn’t impact SLAs. Provider must guarantee key availability

Hold Your Own Key

- Master keys remain in the hands of the customer
- Authorization of the keys usage is governed by the customer
- Could impact SLAs. Customer must guarantee key availability
BYOK vs BYOE
Differences between BYOE and BYOK

BYOE
- Customer brings their own encryption and key management.
- Works great in IaaS workloads
  - It’s just another VM after all...
- CASB for SaaS and PaaS but provider can’t
  - see data
  - nor index it
  - nor analyze it
  - nor add value to it
  - and could break it...

BYOK
- CSP provides native or application encryption
- Customer brings/imports/manages their own key
- Works great in SaaS/PaaS workloads
  - Designed in encryption with customer managing the keys
- IaaS usually provides only block level encryption
  - Doesn’t reduce risk to data in use
Smart Questions
Smart Questions for IaaS

Do they offer BYOK?

- What is encrypted and how is it encrypted?
- Do I import keys, derive keys, salt key creation, or reply to a key request?
- Can I control where the key, or derived keys are used, and who can authorize usage of the key?
- How do I revoke and rotate the key(s)?
- If my keys expire... what happens?
- Does it protect from remote data breach?
- Which users and processes, have access to the key material?
When you get home
- Determine your organizations risk appetite is for cloud hosted data

Within 30 days
- Consult your CSPs to find out what BYOK approach they offer
- Ask smart questions about how BYOK works within their offering

Within 60 days
- Target a CSP to either BYOK or BYOE to get comfortable with cloud encryption
Questions?