Primer on Cloud Content Encryption and Key Management
Executive Summary

Mobile workers rely on Enterprise File Sync and Sharing (EFSS) services to sync files across mobile devices, and to share files of all sizes easily with coworkers, partners, and customers. Many files in EFSS solutions contain sensitive information that must be encrypted for data security and regulatory compliance. Encryption must be used to protect data in transit from cloud to device or device to cloud, data at rest in storage in the cloud or on a device, and data in use being accessed through APIs, metadata, or search tools.

Encryption technologies use encryption keys—secret unique numerical sequences—to manage the encryption and decryption of files, limiting access to authorized users. Today, many EFSS services provide data encryption, but the services differ considerably in how and where the encryption keys are stored and managed.

Key management is oftentimes an over-looked area of EFSS security. The entity that controls the encryption keys, controls access to the encrypted content. This paper compares the key management features of the most popular types of EFSS solutions.

• On-premise cloud EFSS solutions run in an internal data center and give enterprises full control of the encryption keys for data in all three states: In transit, at rest, and in use.

• Dedicated private cloud EFSS solutions run in a hosted cloud platform, provide the agility of capital expenditure benefits of a hosted environment, while still providing better security than multi-tenant public cloud solutions with each organization provided with its own dedicated instance.

• Multi-tenant public cloud EFSS services run in a hosted cloud platform where all customer data is co-mingled in one shared environment. Many public cloud EFSS solutions fail to protect data in use, while some offer optional key management services that give customers control over encryption keys, but at an added cost.

To maintain full control over the encryption keys—and hence full control over confidential content—without added cost, enterprises should deploy an on-premise EFSS solution, such as kiteworks by Accellion, which includes on-premise key management controls built-in.
EFSS Solutions and Data Security

Today, nearly every worker is a mobile worker carrying 2 or 3 mobile devices. To be useful, mobile devices need data. That data includes the files used every day in business: files, such as contracts, product plans, customer profiles, and so on.

Few people have time to manually copy files from device-to-device throughout the day. Instead, to ensure that all devices are always up to date with the latest files, workers rely on Enterprise File Sync and Sharing (EFSS) services, which automatically sync files and folders across all the devices via the cloud—whether laptops, desktops, tablets, or smartphones—registered to a user. Workers also use EFSS for sharing files quickly and easily with other users, including external users, such as customers and partners.

EFSS is fast and convenient, but it is risky, too. Many of the files being synced and shared contain confidential information, such as Social Security numbers, credit card numbers, personnel files, or medical records. A decade ago, this content would have resided on internal file servers shielded from public access by a corporate firewall and other IT defenses. Today, thanks to EFSS, this content is being continuously replicated and distributed via the cloud across multiple users’ devices, folders, and organizational domains. As a result, this content, which previously had been secured both physically and digitally is now stored in the cloud and found wherever mobile workers happen to be carrying devices, which is to say everywhere: Remote offices, cafes and restaurants, theaters, gyms, trains, and buses—the list of locations is endless.

Storing confidential content on mobile devices puts that content at risk. An unauthorized user might pick up a device and access confidential files. Files might be intercepted over an insecure Wi-Fi transmission in a café, hotel lobby, or train. Content stored on mobile devices might become infected with mobile malware, which is then synced along with the file back onto servers and other devices. The devices might be lost or stolen. In healthcare alone, there are news stories about confidential medical records being stolen along with mobile computing devices every month. In regulated and unregulated industries alike, confidential files are routinely lost or disclosed through the mishandling or loss of mobile devices.

The Importance of Encryption

To protect confidential information, a growing number of EFSS vendors are applying encryption. Encrypting files at rest (in storage) and in transit (while being transferred or copied), prevents unauthorized users from reading or tampering with confidential files. Only users with the proper encryption key can unlock the files.

Encryption, of course, has long been a best practice for IT security. Just as there are different approaches for cloud architectures, there are different approaches for encryption and managing encryption keys. Encryption keys are secret mathematical sequences used by encryption algorithms to mathematically

---

scramble digital content for protection, and to unscramble the same content for reading.

If enterprises want to benefit from the convenience of EFSS, enterprises should carefully consider the encryption and key management services offered by the EFSS vendor chosen. IT managers should remember that even if files are entrusted to a third-party EFSS vendor, the responsibility for the security of the files ultimately lies with the enterprise, not the vendor. As the Cloud Security Alliance notes in version 3.0 of its security guidance:

“When data is transferred to a cloud, the responsibility for protecting and securing data remains with the collector or custodian of that data. When it relies on a third-party to host or process its data, the custodian of the data remains liable for any loss, damage or misuse of the data.”

Enterprises should ensure that the differences and security implications of various approaches to EFSS encryption are understood. That is the topic this paper will now explore. We'll begin by briefly comparing the various cloud architectures used to provide EFSS services.

**Cloud Architectures for EFSS**

There are three types of cloud architectures used for business services, such as EFSS.

**Private Cloud**

A private cloud is a cloud service that is configured and managed by the enterprise. A private cloud service typically runs in the enterprise’s own data center. Even running internally, the service is characteristically a cloud service in that it uses common cloud technologies (such as hypervisors), scales quickly and easily, and benefits from the general economy of cloud services; which, with open source software and virtual servers, have typically proven to be dramatically; even exponentially, cheaper than traditional hardware-based server farms.

**Public Cloud**

A public cloud is a cloud service that it is configured and managed by a third-party vendor, such as Amazon.com or Dropbox. The vendor stores all the data submitted to the service. Typically, the vendor distributes its customers’ data across its data centers based on its own algorithms for balancing server load and maximizing economies of scale. The vendor manages the storage, location, integrity, and encryption of the data. Enterprise customers trust that the vendor will perform this work correctly and securely.

**Hybrid Cloud**

A hybrid cloud combines one or more private clouds, and one or more public clouds. Enterprises sometimes use hybrid clouds to manage data and services internally whenever possible, while keeping the option of dynamically adding storage or compute capacity with a public cloud service should workloads suddenly increase.

---

3 https://cloudsecurityalliance.org/research/security-guidance/#_v3
Encryption and Key Management

All three types of cloud architectures support encryption. The most important difference among the three types is the matter of key management—the creation, handling, and storage of the secret keys used to encrypt data submitted to the cloud service.

Key management is as important as encryption, since the entity with access to the keys can unencrypt any protected data. The Cloud Security alliance offers this advice regarding key management for cloud services:

“Based on the Segregation of Duties security principle, key management ideally should be separated from the cloud provider hosting the data. This provides the greatest protection against both an external breach of the service provider as well as an attack originating from a privileged user/employee of the provider.

Additionally, this segregation of duties prevents the cloud provider from unauthorized disclosure of customer data, such as compliance with a subpoena, without the customer knowledge or approval. The customers should retain complete control over data and should be the only ones to comply with disclosure requests."  

The guidelines recommend that enterprises select a Remote Key Management Service in which the customer maintains the KMS or Enterprise Key Management (EKM) solution on-premise. That recommendation rules out most public cloud EFSS.

However, some EFSS vendors, such as Box, that have traditionally offered only public cloud services, are now advertising public cloud EFSS that allows customers to manage the encryption keys.

To assess the different key management solutions properly, we need to look closely at how encryption is applied to cloud data in three different scenarios: Data at rest, data in transit, and data in use.

A Closer Look at Encryption for Data in Transit, at Rest, and in Use

Data in transit refers to data being transmitted between a cloud service and one or more devices. Data at rest refers to data being stored in the cloud or on a device. Data in use refers to data being accessed through metadata, APIs, search engines, and other third-party services.

Data in Transit

Data in transit traverses wireless carriers, network infrastructure, and the public Internet. Obviously, it needs to be encrypted to be safe during this transmission. Most software solutions, including EFSS solutions, use SSL and IPSec to encrypt data in transit.

Data at Rest

Data at rest is typically encrypted using standard encryption algorithms, such as AES. Most leading content management vendors offer AES 256-bit

4 Ibid.
encryption. This is proven technology that protects data from being accessed or tampered with.

Data in Use

Data in use—which includes data accessible through open APIs and unencrypted metadata used for search—requires its own attention. Too often, this type of data is overlooked, but it can be used by snoops and attackers to make deductions about other data, and to perpetrate man-in-the-middle attacks.

Comparing Encryption Key Management Solutions

Now that the three situations in which data must be encrypted have been identified, the choices for managing the critical keys that make encryption possible can be considered. As the CSA guidelines mentions, this aspect of IT architecture is known as Encryption Key Management (EKM).

An EKM system performs two important jobs for encryption services:

• It stores the encryption keys.
• It manages the keys, authorizing access, rotation, expiration, and revocation.

When an EFSS solution needs to encrypt data, it calls the EKM to either generate or retrieve the key needed for the encryption operation.

There are three types of EKM solutions available in today’s EFFS market:

• An EKM service created by the EFSS vendor and built into its solution, giving the customer full control over both EFSS and EKM.
• An EKM service created by a public cloud service provider, such as Amazon (whose EKM is CloudHSM) or Microsoft Azure (whose EKM is Azure Key Vault) and made available to any EFSS solution running on the cloud platforms of service providers.
• Third-party, cloud-hosted EKM services, such as CipherCloud and SkyHigh Networks that can be accessed by on-premise solutions and cloud-based EFSS solutions.

Now let’s consider the pros and cons of the following three types of EKM solutions.

Private Cloud/On-Premise EKM Solutions

Security-focused enterprises especially in verticals like financial services, healthcare, and government must comply with strict security and data governance regulations that call for practices, such as content encryption, access controls, logging, and even the periodic rotation of encryption keys.

To take advantage of cloud performance and scaling, while maintaining full control over content, organizations typically deploy private cloud/on-premise solutions for secure mobile content management.
An EKM system built into an EFSS solution works best for customers who deploy private cloud/on-premise solutions, since it provides full control over all aspects of security features, including encryption and key management. The private cloud/on-premise implementation allows organizations to benefit from many of the scalability benefits and cost savings of cloud technologies, while keeping critical security controls fully in-house and under the IT department’s watchful eye.

**Multi-Tenant Public Cloud EKM Solutions**

Typical cloud storage and content management providers have a multi-tenant cloud in which data from different customers is co-mingled and encryption keys are managed by the vendor, rather than by customers. This lack of control has been a long-standing concern to enterprises that recognize that ultimately enterprises are responsible for data security. Especially in regulated industries, such as financial services and health, concern about cloud security and key management has made IT managers reluctant to trust confidential data to the cloud.

To mitigate concerns, cloud providers like Amazon (AWS) and Microsoft Azure have introduced optional security services featuring hardware-based encryption (Amazon CloudHSM and Microsoft Azure Key Vault). For example, Amazon’s CloudHSM service provides customers with dedicated Hardware Security Modules (HSMs), which are installed in Amazon’s data centers and which customers can access at fixed addresses in EC2 clouds. By accessing HSMs, customers can control the generation, storage, use, and revocation of the encryption keys.

Even with hardware-based encryption, however, cloud-based solutions still leave data in use exposed to snooping. Through the HSM services, the EFSS vendors’ employees may be able to access data in searches and in APIs. Public cloud HSM services are an improvement over the laisser-faire security of early cloud services, but public cloud HSM services still fail to provide customers with total control over key management and encryption.

**Third-party Cloud EKM Services**

Rather than turning to cloud vendor for encryption keys, enterprise organizations also have the option of turning to other third-party services, such as CipherCloud and SkyHigh Networks. SkyHigh Networks, for examples, offers a cloud service that manages encryption for other cloud services. In effect, third-party vendors like SkyHigh are add-on services designed to provide the sorts of security features—such as encryption, Data Loss Protection (DLP) integration, and other basic enterprises IT services—that ought to have been included in the EFSS solution to begin with. Third-party cloud EKM services require enterprise customers to manage additional vendor relationships and to incur additional costs to make up for the security deficits of the EFSS services enterprise customers are also paying for.
Comparing EKM Solutions

The tables below summarize the strengths and weaknesses of various EKM models for EFSS solutions.

### Traditional EFSS

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>On-Premise</th>
<th>Dedicated Private Cloud</th>
<th>Multi-Tenant Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Manageability</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Cost</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data at Rest</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data in Transit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data in Use</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### EFSS + HSM, such as Azure Key Vault

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>On-Premise</th>
<th>Dedicated Private Cloud</th>
<th>Multi-Tenant Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manageability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cost</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data at Rest</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data in Transit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data in Use</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### EFSS + Third-party Cloud Security, such as SkyHigh Networks

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>On-Premise</th>
<th>Dedicated Private Cloud</th>
<th>Multi-Tenant Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manageability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cost</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data at Rest</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data in Transit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data in Use</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

As this table makes clear, there are really just two approaches for cloud encryption and EKM that provide adequate security for data at rest, data in transit, and data in use.

On-premise EFSS solutions that include EKM services provide protection for all three cases. The other option is a third-party cloud service provider, but this approach has the disadvantage of requiring additional costs and management.

Two vendors or one? If an enterprise wants a secure EFSS solution that doesn’t require an additional vendor to provide security, an on-premise EFSS with a built in EKM solution is the way to go.
Conclusion

EFSS services have become a necessity in this age of mobile computing. Syncing and sharing files enables mobile workers to have continuous access to important files.

Encryption is a critical part of ensuring that synced and shared data remains secure. While public clouds have become more secure over the past few years, the deployment option which provides the most comprehensive security, including the secure management of encryption keys, for the lowest cost and least complexity remains private cloud on-premise deployments of EFSS solutions.

Private cloud/On-Premise EFSS solutions ensure that mobile workers have ready access to important files, while ensuring that the files are protected through best-practice security measures that are fully under the control of the enterprise.