



# The Simple Guide to Encryption Key Management

Understanding Common  
Key Management Methods  
and Encryption Solutions

# The Simple Guide to Encryption Key Management

**Understanding Common  
Key Management Methods  
and Encryption Solutions**

## **In this Guide**

The Four Pillars of Key  
Management

The Key to Maximum  
Privacy and Security

Three Key  
Management Solutions

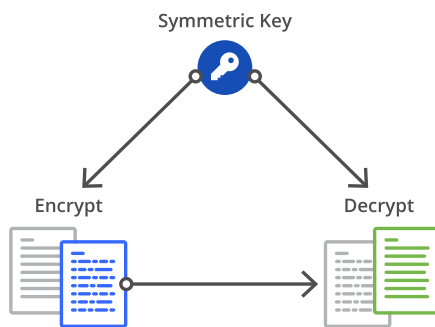
## INTRODUCTION

Without encryption, there are no keys, so it's important to know how modern encryption works before digging into the broader world of key management.

From a high level, the concept of encryption is simple: Plain text content—such as an email or document—needs to be protected so that only the intended recipient(s) is able to access and read.

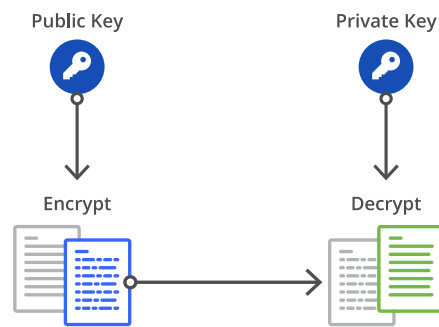
In order to do this, a key is required to jumble plain text into undetectable ciphertext. Depending on the type of encryption used, recipients will need an encryption key to convert that ciphertext back to its original plain text form.

There are two common forms of encryption used today:



**Symmetric key encryption** uses the same key to encrypt and decrypt the data. A simple example is a password-protected PDF. The creator of that PDF uses a passcode to secure the document, and authorized recipients use that same passcode to view the PDF in plain text form.

Symmetric encryption can protect data at-rest, but it is not typically seen as an effective way to send encrypted data securely across different platforms. After all, how can the sender ensure that the key gets safely transmitted to the recipient?



**Asymmetric encryption** was created to address this concern. Asymmetric encryption uses two keys: one to encrypt data, and one to decrypt it. It's often referred to as public key encryption, because people who use it make the encryption key public, but keep the decryption key private.

With asymmetric encryption, anyone can send out an email or file encrypted with the recipient's public key, but only the recipient can read it, since only he has the private decryption key. The creation of multiple keys in asymmetric encryption adds complexities to key management.

Regardless of the type of encryption, keys are required both to encrypt and decrypt whatever content you're protecting, so you must be careful to secure them just as you would the content itself.

Sounds simple enough, right? Not exactly.

In today's world, interactions are increasingly happening online which pose security risks when you need to share sensitive data, including encryption keys. What's more, the number of methods organizations use to communicate online is constantly growing.

Even though you create and store encrypted files in one application, you might also need to move those same files to another app or share them as an email attachment. Encryption keys don't always work when applied to different platforms, which means you often must manage multiple key exchanges for the same piece of data. In order for that to effectively occur, encryption keys must be easily and safely distributable at scale.

We account for these complexities like we do most other problems: we assume our technology providers will resolve them.

To ensure that your online data remains protected, it's critical to understand the different components of encryption key management, so that you know the right questions to ask when evaluating new and existing encryption technologies.

Blindly leaving key management to third parties means your information is exposed and could be accessed without your knowledge or consent.



# 1

## The Four Pillars of Key Management

In 2018, [more data was stolen](#) than ever before, with a total of 4.5 billion records compromised in the first half of the year alone. And intellectual property theft costs U.S. companies as much as [\\$600 billion](#) each year.

While encryption is a critical part of data security, it's only as effective as the methods that protect and distribute the keys being used. Historically, people have had to sacrifice convenience for privacy in order to satisfy this principle.

Within the realm of key management, you should consider these **four main areas** as part of any comprehensive data security plan:



## Key Storage

Common email and file-sharing providers—such as Microsoft, Dropbox or Google—usually store encryption keys and the content the keys protect on their servers, which means they can access and read your unencrypted data whenever they want.

As a general principle, the person or company who stores your encrypted content should not also store the keys encrypting that content. Keeping encryption keys separate from the content they protect fulfills the best security practice of split knowledge architecture, helping prevent unwanted third-party access to unencrypted data.



## Policy Management

While encryption keys are primarily used to protect data, they can also be tied to policies that enable control capabilities for a given piece of content. Policy management allows you to add and adjust these capabilities.

By setting policies on encryption keys, the content owner can specify the recipients authorized to access the content, then revoke, expire access or prevent sharing of the keys, and thus, of the unencrypted data too. These policies can also audit when encryption keys were accessed, giving content owners insight into when their encrypted content was read, and by whom.



## Authentication

Since keys enable users to unlock your encrypted data, it's important to verify recipients' identities before giving them access. Authentication is the process of verifying that the person trying to access the content is tied to the encryption key's policy before allowing access to the encryption key and ultimately, the protected content.

Some tools—like the secure portal you may use to receive information from your doctor—require you to create a unique username and password in order to verify your identity. Only once you've successfully logged in can you view the decrypted content.

Other authentication methods rely on your existing web credentials—such as those from a Google, Microsoft or Facebook account—to authenticate. This method of authentication creates less friction since it does not require the user to remember additional login credentials.



## Authorization

This feature verifies the actions that people can take on encrypted data once they've been authenticated. Authorization enforces encryption key policies and ensures that you always maintain control of the data that's being shared.

For example, you might share an encrypted file with two people, only one of whom you want to be able to print or download it, so you create key management policies to restrict the other's access. Authorization enforces these rules, ensuring they are passed onto your recipients when they try to access the encrypted file.







# 2

## The Key to Maximum Privacy and Security

The right key management framework enables both secure and user-friendly key sharing. Once you understand each of the four pillars, you are ready to begin evaluating the right key setup for your organization.

Compared with other encryption approaches, Virtru's client-side encryption provides the best of both security and ease of use.

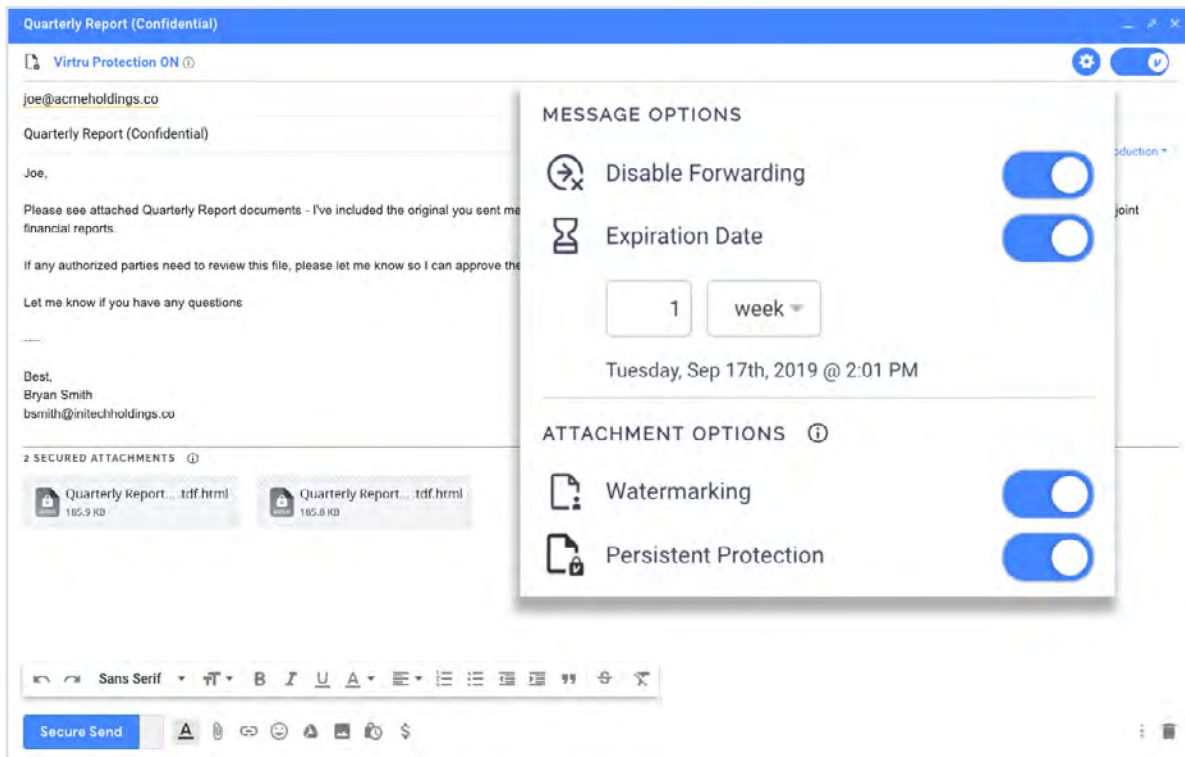
To ensure security, administrators can use Virtru to monitor data going in and out of their domain and view audit trails of when keys have been accessed, thus gaining insight into when emails have been read and by whom.

 <b>Key Storage</b>	 <b>Policy Management</b>	 <b>Authentication</b>	 <b>Authorization</b>
<p>Encryption keys are always stored separate from encrypted content. Encrypted content is stored on the email and file platform provider's cloud server infrastructure. Symmetric keys are hosted on AWS (with Virtru providing an additional layer of authentication), while asymmetric keys can be hosted exclusively on customer premises.</p>	<p>Revoke access, set expiration dates, disable forwarding and watermark documents upon encryption. Virtru can also see granular audit trails for shared content.</p>	<p>Verification made easy with either existing email credentials or a message verification link.</p>	<p>Managed exclusively by Virtru Access Control Manager (ACM).</p>



Equally as important, Virtru also ensures a frictionless experience by enabling encryption directly within existing email and file sharing platforms—such as Gmail, Google Drive and Microsoft Outlook. Virtru seamlessly hooks into these tools to encrypt data on the client-side, before it ever leaves your device.

A user-friendly interface gives administrators the ability to monitor data going in and out of their domain from a centralized dashboard and view audit trails of when keys have been accessed, thus gaining insight into when emails have been read and by whom.





# 3

## Three Key Management Solutions

Virtru offers multiple key management options to enable easy-to-use email and file encryption that protects data wherever it is shared and prevents third parties from ever accessing unencrypted content. Distributed architecture with dual layers of protection ensures total control over who can access the keys securing your most sensitive data.

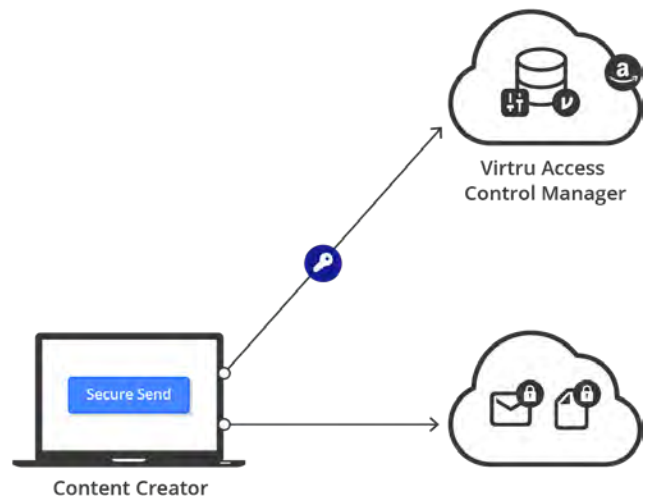
# 1 Fully Hosted Keys

Your organization can be up and running in minutes with our fully hosted key management option. The Virtru ACM is at the heart of Virtru's fully-hosted, SaaS-based key management infrastructure, managing the encryption keys and the access control policies tied to them and authenticating requests for encryption keys to control access to protected email and files. Virtru ACM is hosted in AWS to ensure maximum performance and availability.

A unique AES 256-bit Galois Counter Mode (GCM) symmetric data key is created on the client to protect each email and file, then delivered via a secure TLS-protected channel to Virtru ACM. The Amazon Key Management Service (KMS) protects the symmetric data keys with an additional layer of symmetric encryption that is protected by a set of AWS managed hardware security modules (HSMs).

These keys are all stored in separate locations, and the content they protect is also stored separately, for a split-knowledge architecture that is critical for organizations looking to comply with HIPAA, FERPA, CJIS or GDPR requirements that restrict third party access to sensitive data.

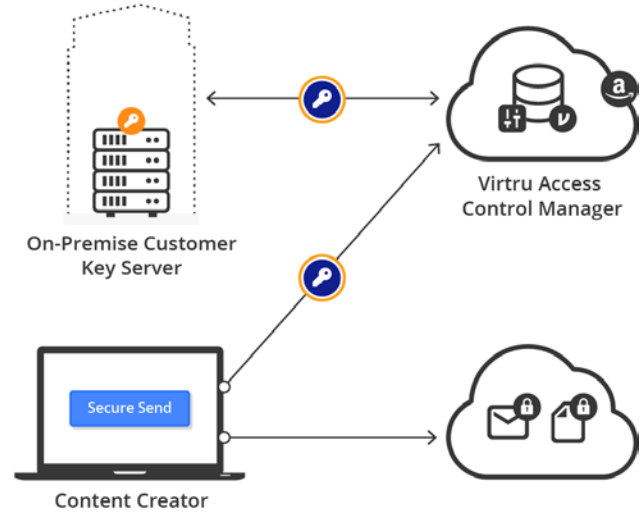
But, as we discussed, the safest way to manage encryption keys is to host them yourself, and Virtru provides that option for organizations via its Customer Key Server (CKS) capability.



## 2 Customer Hosted Keys

The Virtru CKS—hosted entirely on-premises—adds another layer of asymmetric encryption and lets organizations store and manage the asymmetric key pairs themselves for complete and exclusive access to the keys encrypting their data.

This approach utilizes RSA 2048-bit asymmetric encryption key pairs hosted in your environment. Your RSA keys are used to encrypt every data key at the client so that it is never transmitted or stored in the clear. Virtru CKS is hosted on-premises or in your private cloud, and uses Docker containers for rapid deployments. Virtru CKS works with ACM to receive and fulfill key requests for authorized users.











### You should consider the Virtru CKS if you're looking to:

- Enable easy-to-use client-side email encryption without having to trust third parties with encryption keys or unencrypted content.
- Ensure that you are the only entity that can respond to government access requests and subpoenas.
- Meet data residency requirements by specifying the locations where your encryption keys are stored.
- Destroy encryption keys to make emails permanently unreadable.

Prior to the Virtru CKS, organizations could leverage Bring Your Own Key (BYOK) approaches that allowed them to use their own keys but still required trusting their cloud provider or security vendor with hosting the keys protecting their content. This arrangement is like getting a safety deposit box but then letting the bank store its key. The cloud provider or security vendor can still access the underlying plain text content.

Virtru is the first zero-trust key distribution service in which no third party can ever access unprotected content or the data protection keys.

### What Keys and Content Can Cloud Providers Access?

Key Management Setup	Data Protection Keys	Plaintext Content	Customer-Held Keys
Existing Customer Managed Key Solutions*	 <b>YES</b>	 <b>YES</b>	 <b>NO</b>
Virtru Fully Hosted Keys	 <b>YES</b>	 <b>NO</b>	N/A
Virtru CKS	 <b>NO</b>	 <b>NO</b>	 <b>NO</b>

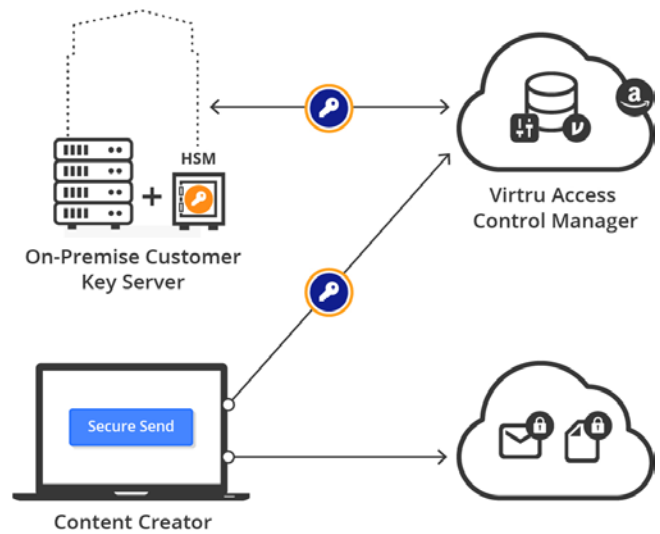
\*Such as Box KeySafe, Intralinks CMK, and SafeNet KeySecure

### 3 HSM Keys

If you need even more security, you can back up the Virtru CKS with a Hardware Security Module (HSM). The HSM is a physical device hosted on-premise by an organization to add an additional layer of encryption on top of the CKS. Virtru has validated HSM integrations with [Atos TrustWay HSM](#), and a broad range of other HSM products can be enabled via our support for PKCS (Public Key Cryptographic Standard) #11.

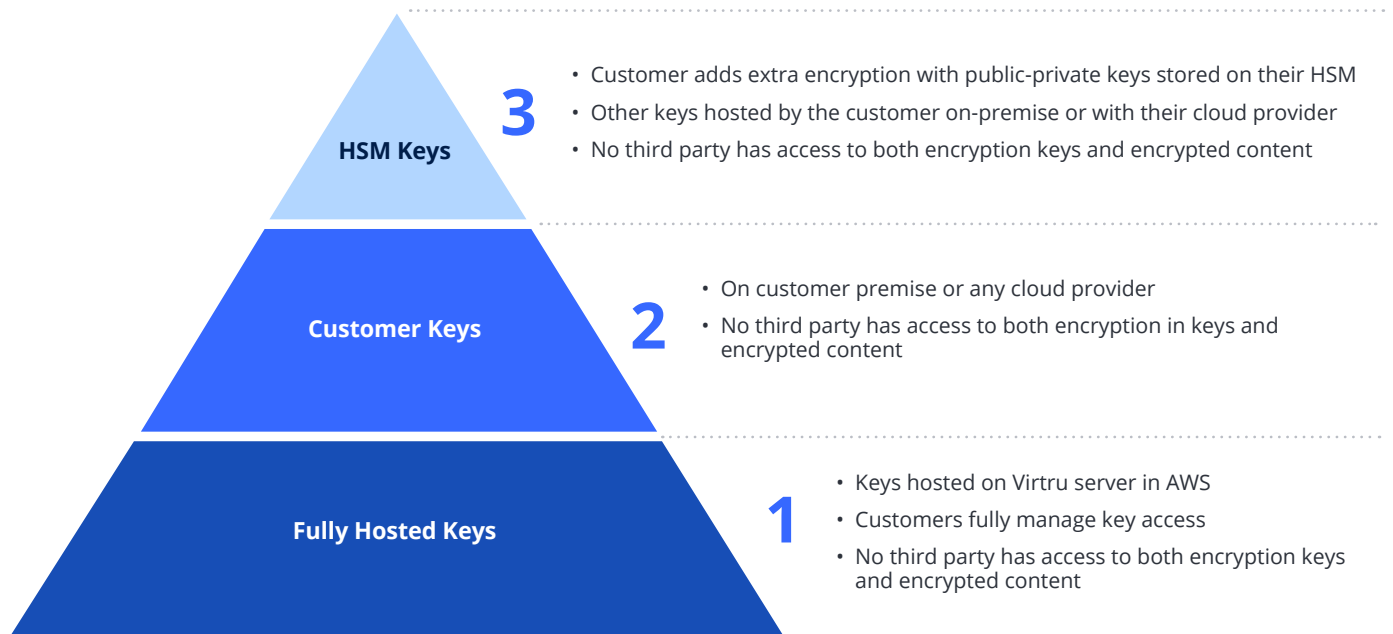
In this deployment option, your RSA encryption keys are stored in your HSM, and Virtru CKS is only used to facilitate communication between your HSM and the Virtru ACM. Leveraging the PKCS #11 protocol, CKS processes encryption and decryption requests on the Virtru platform by securely accessing HSM-managed private keys. Virtru ACM continues to support authorization workflows on the front-end.

This is a particularly attractive model for anyone looking to use PGP or S/MIME without having to handle key exchanges manually or require their recipients to install anything.



Whether you need to meet regulatory compliance, protect intellectual property, or simply prevent third parties from accessing your content, Virtru's three key management options provide a secure, easy-to-use data protection foundation for your organization.

### Multiple Options for Enhanced Security



# Encryption Key Management Needs Assessment Checklist

The following checklist will help you to evaluate your organization's encryption key management needs and determine appropriate solutions to meet your requirements:

---

- ✓ **Does your organization use any type of email or file encryption?**
  - ✓ Does your encryption protect emails and files at rest and in-transit?
  - ✓ Does your organization use client-side encryption to share sensitive data?
  - ✓ Does your encryption provider ever have access to encrypted data?
  - ✓ Does your encryption provider ever have access to encryption keys?
- ✓ **Does your organization share data that you wouldn't want your email or file sharing provider to access?**
- ✓ **Do you trust your technology providers with your sensitive data?**
- ✓ **Do you want the ability to directly respond to government surveillance requests for your organization's data?**
- ✓ **Does your organization have any products that are competitive with any of your technology providers' products (i.e., Microsoft, Google, Amazon, etc.)?**
- ✓ **Do employees of your organization have access to sensitive data such as PII, PHI or IP?**
  - ✓ If yes, is your current encryption solution compliant with regulatory standards such as HIPAA, FERPA, CJIS, GDPR or ITAR?
- ✓ **Does your organization face any data residency requirements?**
  - ✓ If yes, does your cloud provider guarantee that your organization's email and file data will not leave your premises?
- ✓ **Do you need the ability to track where your data is shared externally?**



# Enhance Your Email and File Security Today

Protect your organization's data wherever it is shared and prevent third parties from ever accessing unencrypted content. Virtru's client-side email and file encryption is the most secure way to comply with privacy, compliance, and data residency requirements.

**Book a demo to see for yourself how it works. [virtru.com/contact-us](https://virtru.com/contact-us)**

At Virtru, we empower organizations to easily unlock the power of data while maintaining control, everywhere it's stored and shared. Creators of TDF (Trusted Data Format), the open industry standard for persistent data protection, Virtru provides flexible, easy to use, and trusted privacy technologies built on its data protection platform that govern access to data throughout its full lifecycle—from creation to transmission, storage, analysis, and sharing. More than 20,000 organizations of every size and industry trust Virtru for data security and privacy protection. For more information, visit [virtru.com](https://virtru.com) or follow us on Twitter at [@virtruprivacy](https://twitter.com/virtruprivacy).

