Virtru Customer Key Server

Host your own keys and let Virtru manage policies and key exchanges to ensure privacy wherever your data is created or shared.

Customer-Hosted Keys for Full Control of Your Data

You don't trust the bank with the key to your safety deposit box, so why trust third party security providers to host your encryption keys? The Virtru Customer Key Server (CKS) removes third party trust concerns by letting you host your own encryption keys and integrate with hardware security modules (HSMs) for absolute data control.

Encryption Key Management that Unlocks the Power of Privacy

Privacy

Host your own keys so that unauthorized parties can never access your data, ensuring it stays private.

Compliance

Meet data protection and residency requirements for CJIS, GDPR, HIPAA, PCI, CCPA, ITAR, and more.

Surveillance Prevention

Avoid blind subpoenas that force security and cloud vendors to give governments your data without authorization. Only you can respond to government data requests.

More than 20,000 organizations trust Virtru for data security and privacy protection.

NETFLIX EmblemHealth Maryland

"...the most important aspect of encryption is good key management, including customer control of the keys."

Gartner

Research Note: *Staying Secured in the Cloud is a Shared Responsibility,* Steve Riley, Sept 2018

Zero Trust

Split knowledge architecture separates keys from content. You're never forced to trust Virtru or cloud service providers with access to your data.

Audit

Maintain visibility over all encryption key exchanges and policies and integrate with your SIEM for insights that strengthen threat response and compliance workflows.

Easy Enablement

Virtru CKS deploys rapidly with Docker containers to align with your existing IT and key management infrastructure for enterprise scale implementations with low overhead.

Flexible, Layered Encryption Key Hosting Options

Choose from several hosting options to align with your key management processes and security requirements.

Fully-Hosted Keys

Virtru generates a unique AES 256-bit symmetric key on the client to protect each email and file, then sends it to the Virtru ACM via a secure TLS-protected channel hosted in AWS and secured with HSM arrays.

Customer-Hosted Keys

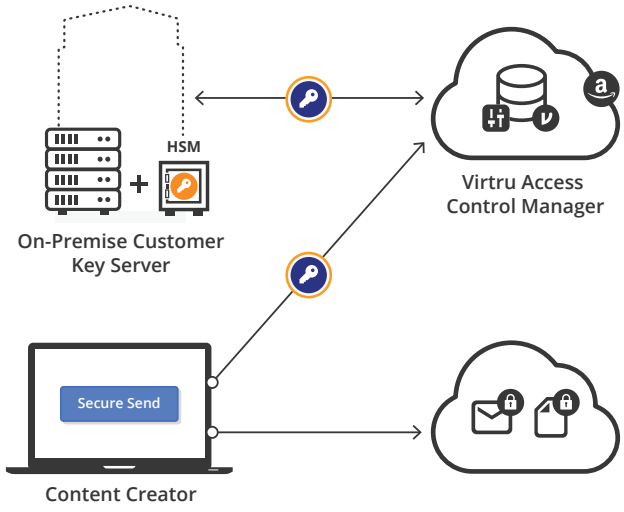
You host asymmetric encryption keys on-premises that protect every Virtru client key, for a crucial layer of protection that ensures client keys are never stored or transmitted in the clear.

HSM Integration

Virtru CKS brokers encryption and decryption requests on the Virtru platform by securely accessing your HSM-managed private keys leveraging the PKCS #11 and KMIP protocols.

Key and Policy Management - Virtru Access Control Manager

Virtru Access Control Manager (ACM) manages encryption key policies and authenticates key exchanges. Hosted in AWS to ensure maximum performance and availability.



virtru

Learn how to unlock the power of privacy with Virtru CKS by contacting us today at **virtru.com/contact-us**.