Virtru Customer Key Server

Get an additional layer of security and privacy wherever your data is created or shared by hosting your own encryption keys.

Organizations increasingly want full control of their data, including the encryption keys guarding that data. However, most cloud-managed, bring your own key (BYOK) approaches cannot deliver on Zero Trust, as they require you to trust a third-party vendor with access to your keys and plain text content.

The Virtru Customer Key Server (CKS) ensures you maintain exclusive access to secure your data:

- Create an additional key pair to protect underlying encryption keys that never leave your environment for true “hold your own key” security.
- Host on your premises, in a private cloud, or on any public cloud service.
- Have visibility over all encryption key exchanges and policies.
- Integrate with your SIEM to strengthen threat response and compliance.
- Prevent any third-party (including Virtru and other cloud, email, and security vendors) from accessing your data.

Customer-Hosted Keys to Achieve True Data Privacy

Data Protection
Host your own keys so that unauthorized parties can never access your data, ensuring it always stays in your control.

Compliance Support
Meet data sovereignty, residency, and data protection requirements including CJIS, GDPR, HIPAA, PCI, CCPA, ITAR, and more.

Surveillance Prevention
Strengthen privacy by ensuring any request to access data (including a government subpoena) has to come to your organization.
It’s Your Data, and Virtru Helps Keep It That Way

The Virtru Customer Key Server (CKS) uses asymmetric encryption on top of Virtru’s native end-to-end encryption while aligning with your existing IT and key management infrastructure for enterprise scale implementations.

Secure and Private Sending Experience
When you encrypt an email, a message key is generated, which is then encrypted with a public key. The Virtru Access Control Manager (ACM) manages and authenticates key exchanges but cannot access your data at any time. The CKS then hosts a private key that is needed to decrypt the public key and unwrap the message key. This CKS private key never leaves your environment which meets the data protection, privacy, and compliance you want.

Protected Yet Simple Recipient Experience
Your authorized recipients also have public/private key pairs. The CKS rewraps message keys with the receiving client’s public key before it is transmitted to Virtru’s servers. The receiving client contains the private key needed to unlock the rewrapped message key and finally decrypts the message. This is a seamless experience to ensure recipient ease of access.

Hardware Security Module (HSM) Integration
The Virtru Customer Key Server (CKS) brokers encryption and decryption requests on the Virtru platform and can be integrated with your HSM to manage private keys. This method leverages PKCS (Public Key Cryptographic Standard) #11 and KMIP protocols, allowing integration with a variety of HSM manufacturers.

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