

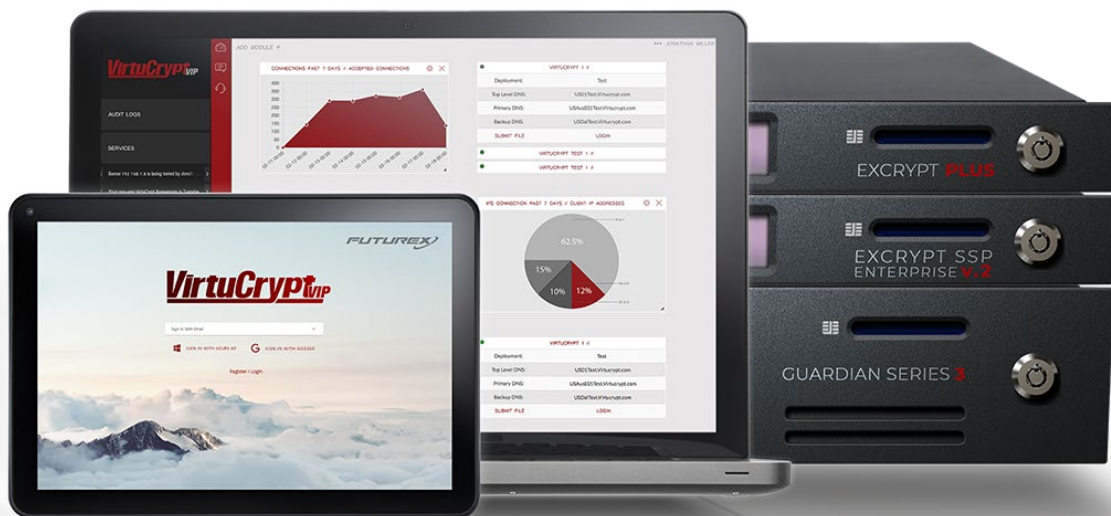
FUTUREX

WHITEPAPER



Service Overview: Next-Generation Cloud HSMs

VirtuCrypt Cloud Hardware Security Modules



The information provided in this document is considered proprietary and confidential.

TABLE OF CONTENTS

TABLE OF CONTENTS.....1

VIRTUCRYPT CLOUD SERVICES OVERVIEW 2

 ADVANCED CLOUD ENCRYPTION & KEY MANAGEMENT, POWERED BY FUTUREX HSMS 2

 HOW ORGANIZATIONS USE AND DEPLOY NEXT-GENERATION CLOUD HSMS.....2

GENERAL PURPOSE CLOUD HSMS 3

 CORE-TO-CLOUD ARCHITECTURE AND AUTOMATION.....3

 CLOUD HSM MANAGEMENT AND SNAPSHOT TECHNOLOGY.....3

 CRYPTO INFRASTRUCTURE INTELLIGENCE AND ORCHESTRATION.....3

INFRASTRUCTURE DESIGN & DEPLOYMENT 4

COMPLIANCE 6

KEY MANAGEMENT METHODS FOR CLOUD HSMS 7

 BRING YOUR OWN KEYS.....7

 KEY AGENT SERVICES 7

 HSM-GENERATED KEYS.....7

SERVICE STRUCTURE: FUNCTIONALITY, THROUGHPUT, AND HIGH AVAILABILITY 8

EXPANSION OVER TIME 9

 METHODS FOR EXPANSION 9

SUMMARY.....9

VIRTUCRYPT CLOUD SERVICES OVERVIEW

VirtuCrypt is Futurex's award-winning cloud hardware security module (HSM) and key management platform. VirtuCrypt provides cloud-based access to Futurex's cryptographic solution suite: encryption, key management, tokenization, PKI & certificate authority, data protection, remote key loading for POS/ATM/IoT, and much more.



ADVANCED CLOUD ENCRYPTION & KEY MANAGEMENT, POWERED BY FUTUREX HSMS

VirtuCrypt's advanced encryption and key management applications set it apart from other cloud security platforms. VirtuCrypt is powered by FIPS 140-2 Level 3 and PCI HSM validated hardware. Futurex cloud HSMS also support a wide range of cryptographic interfaces, such as PKCS #11, Java JCA/JCE, and Microsoft CNG. This, along with the expertise of Futurex's Solutions Architect team, form a comprehensive platform unmatched by any other cloud services provider.

You can manage VirtuCrypt services and applications in the VirtuCrypt Intelligence Portal (VIP) management interface. VirtuCrypt instances are located in high-security data centers across six continents. VirtuCrypt provides flexible and powerful data security options on a global scale, all with the convenience of the cloud.

HOW ORGANIZATIONS USE AND DEPLOY NEXT-GENERATION CLOUD HSMS

Futurex cloud HSMS handle encryption, key management, public key infrastructure (PKI), certificate authority (CA). However, their use cases and deployment models continually evolve to keep pace with modern security needs. Below are examples of how VirtuCrypt cloud HSMS may be deployed:

- *Full VirtuCrypt cloud:* application hosted in public cloud with VirtuCrypt cloud HSMS
- *Hybrid:* on-premises Futurex HSMS and on-premises applications, with VirtuCrypt cloud HSMS for scalability and disaster recovery
- *Full public cloud integration:* application workloads running in public clouds such as AWS, Microsoft Azure, or Google Cloud, with native integration to VirtuCrypt cloud HSMS

GENERAL PURPOSE CLOUD HSMS

Cloud HSMs can handle all common encryption tasks and can form the basis of an organization's enterprise data security ecosystem. Through VirtuCrypt, they can be quickly configured and integrated into existing infrastructure. This makes them great all-in-one solutions for enterprises of any size.

The next sections will explain the features and capabilities of next-generation cloud HSMs.

CORE-TO-CLOUD ARCHITECTURE AND AUTOMATION

A big advantage of the Futurex cloud HSM is the level of automation it affords. Instant provisioning within the VirtuCrypt Intelligence Portal (VIP) simplifies migration to the cloud. You can then access your device on the VIP dashboard once it's been provisioned by VirtuCrypt engineers. Another aspect of this automated process is rapid migration from on-premises HSMs to cloud HSMs. This feature allows certain users to shift their infrastructure to the cloud quickly and easily, instead of having to undergo an exhaustive migration process. VirtuCrypt also provides a cloud HSM Software Development Kit (SDK) that lets you integrate cloud cryptographic processing and key management into your organization's applications and services, whether they are on-premises or in the cloud.

CLOUD HSM MANAGEMENT AND SNAPSHOT TECHNOLOGY

The Futurex cloud HSM can take cloud HSM snapshots. These can be used for backups, migration to new systems, and streamlining new deployments. Cloud HSM snapshots allow for easy management because users can save instances of a cloud HSM. They can also enable and disable cloud HSMs with the click of a button for both testing and production environments. Users can store cloud HSM snapshots on the VirtuCrypt cloud HSM backup service and re-provision them on-demand. With these snapshots, users can build cloud HSM templates that make establishing new environments simple while preventing errors. Cloud HSM major keys can be randomly generated, cloned from existing cloud HSMs, compliantly loaded using VirtuCrypt's key agent services, and fully customer-loaded and controlled from anywhere in the world.

CRYPTO INFRASTRUCTURE INTELLIGENCE AND ORCHESTRATION

Futurex's cloud HSMs have features that simplify monitoring and create the conditions for true HSM orchestration. HSM orchestration allows cloud HSMs to be provisioned or modified based on user-defined scenarios. The VIP allows for centralized log management, audit-friendly reporting, and integrated monitoring and alerting. The ability to natively integrate with third-party applications and cloud monitoring tools gives users more flexibility.

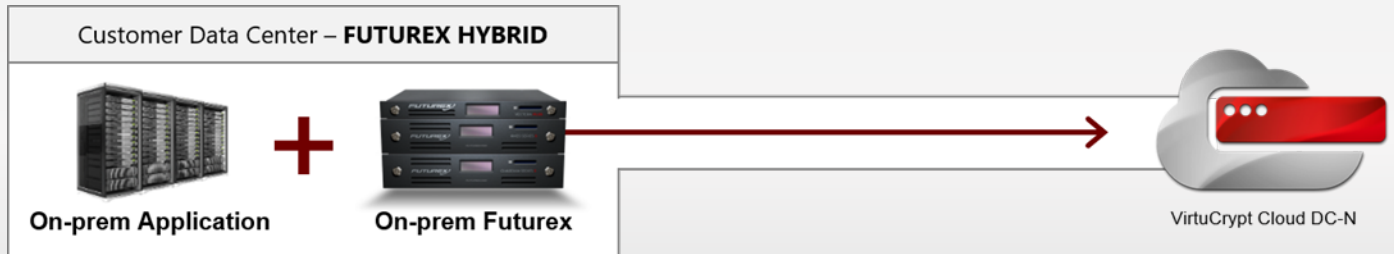
INFRASTRUCTURE DESIGN & DEPLOYMENT

VirtuCrypt's cloud HSM infrastructure can be deployed in either a hybrid environment or a full cloud environment. No model is objectively better than the other, but organizations should carefully consider their short-term and long-term goals when deciding how to integrate cloud HSMs into their cryptographic ecosystem.

HYBRID

The hybrid model contains both on-premises Futurex HSMs and VirtuCrypt cloud HSMs. Organizations with large on-premises HSM estates may prefer a hybrid model. It lets them slowly transition to the cloud over time.

Hybrid models also provide failover, in which cloud HSMs only process traffic when on-premises HSMs are unavailable. Another advantage of hybrid infrastructures is scalability. If an organization is faced with unexpectedly high volume, cloud HSMs can supply extra capacity to prevent slowdowns or outages.



FULL VIRTUCRYPT CLOUD

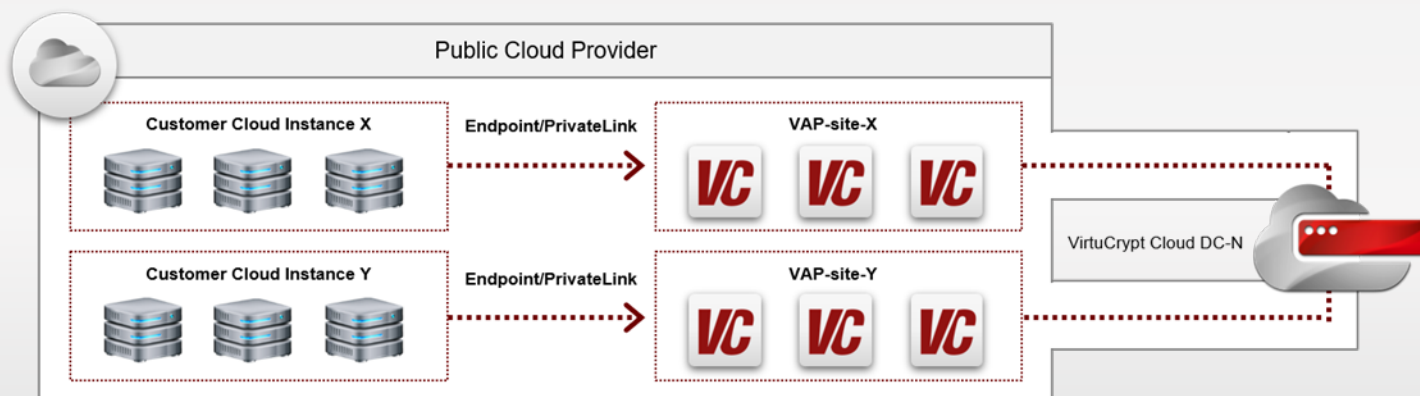
In a full cloud model, an organization would host their entire HSM ecosystem within VirtuCrypt. With VirtuCrypt, organizations can spin up cloud HSMs on-demand with the full encryption and key management capabilities of a physical HSM. These organizations reap the benefits of hosting their HSMs in the cloud – complete flexibility, customizability, and reduced cost – as well as maintain the high standard of hardware security.

This option is often used by organizations in a transitional state. They may want to move their applications to the cloud, but they can't immediately begin the process due to technical or business reasons.



PUBLIC CLOUD WITH VIRTUCRYPT

VirtuCrypt natively integrates with public cloud providers such as AWS, Microsoft Azure, and Google Cloud. This allows for easy onboarding, flexible integration, and secure communication. With Futurex's global data center presence, organizations get wider availability through different regions, lower latency, as well as better data center failover and monitoring by region.



To integrate VirtuCrypt with applications running in public clouds, the user must register for a VirtuCrypt cloud HSM on the respective cloud provider marketplace, or if not available, sign up for an account directly with VirtuCrypt. After signing up for a service, users are directed to a VIP registration page. Customers either create a new VIP account or sign into an existing account if they are already a VirtuCrypt customer. VirtuCrypt associates the service with the account, placing the service status into a pending state while the data is connected through the backend. After the service is successfully connected to the VirtuCrypt account, the user must create a CryptoTunnel, which is a secure, TLS-authenticated connection between on-premises apps, cloud-hosted applications, and cloud HSMs.

Once the CryptoTunnel is established, the VirtuCrypt Intelligence Portal will reach out to the specified region's VirtuCrypt Access Point (VAP). A VAP uses a single set of cloud HSMs across multiple regions within a single public cloud provider. After the VirtuCrypt Intelligence Portal has contacted the VAP, a load balancer will be set up, also creating an endpoint or PrivateLink with a VAP ID that points to VirtuCrypt.

REDUNDANT BACKUP

Data loss, by natural disaster or malicious attack, represents a dire cost to organizations. Establishing a redundant backup of data acts as insurance against such an occurrence, keeping company data safe and secure. To make sure critical data is not lost, it is best practice to integrate a failover system that efficiently mirrors production data.

VirtuCrypt's facilities are fully redundant across multiple secure data centers. In the event of an outage, applications can be configured to automatically failover to a backup site, either from on-premises HSMs to VirtuCrypt, or from one VirtuCrypt cloud HSM to another.

COMPLIANCE

HSM environments must meet a range of compliance requirements. Adherence to these requirements is typically the responsibility of the company or transaction processor, but when deploying cloud HSMs, the cloud services provider bears the responsibility.

VIRTUCRYPT ENVIRONMENT CERTIFICATIONS

VirtuCrypt services undergo annual audits to ensure that all environmental compliance and certification requirements are maintained. These standards include the Payment Card Industry Data Security Standard (PCI DSS) and PCI PIN Transaction Security requirements (PTS).

- PCI DSS is a set of standards and requirements used to protect cardholder data at rest, in transit, and in use. It addresses both technical requirements and operational policies and procedures.
- PCI PTS is a set of standards and requirements that must be followed in environments accepting PIN-based payment transactions. PCI HSM requirements are managed within the overall standard of PCI PTS.

Compliance with PCI standards is enforced by the five major payment card brands who established the Payment Card Industry Security Standards Council (PCI SSC), including American Express, Discover, JCB, Mastercard, and Visa.

A full list of environment certifications and standards met by VirtuCrypt is listed here:

- PCI P2PE – Decryption Management Component - Reference # 2017-01115.001
- PCI DSS – Performed by External Assessor
- PCI PIN – Performed by External Assessor
- Visa Approved Service Provider – ESO, Merchant Servicer, TPS-PIN
- Acquirer/issuer specific validations

FUTUREX HARDWARE CERTIFICATIONS

As previously mentioned, the VirtuCrypt cloud is powered by a vast array of Futurex HSMs, key management servers, and other technologies regionally distributed across highly secure data centers. All Futurex HSMs within VirtuCrypt services are FIPS 140-2 Level 3-validated secure cryptographic devices (SCDs) and are compliant with PCI, and ASC X9.24 Part 1 and 2 requirements.

- FIPS 140-2 Level 3, certificate number 3373 for the GSP3000 cryptographic module
- PCI HSM, approval number 4-10219 for the GSP3000 cryptographic module and 4-10230

KEY MANAGEMENT METHODS FOR CLOUD HSMS

When VirtuCrypt cloud HSMS are provisioned, securely loading encryption keys is a critical step. There are several methods by which administrators can securely load major keys into VirtuCrypt cloud HSMS. These include Bring Your Own Key (BYOK), key agent services, and HSM-generated keys.

BRING YOUR OWN KEYS

Organizations requiring self-management of encryption keys to protect their most sensitive data through the Bring Your Own Key (BYOK) method can confidently manage keys in VirtuCrypt cloud HSMS. The Excrypt Touch is Futurex's FIPS 140-2 Level 3 and PCI HSM validated tablet that allows organizations to securely manage their own encryption keys from anywhere in the world. With the Excrypt Touch, administrators can securely establish a remote TLS connection with mutual authentication and load clear master keys to VirtuCrypt cloud HSMS.

Transferring keys to VirtuCrypt cloud HSMS with the Excrypt Touch uses double encipherment for key components. Double encipherment adds additional security by requiring the components to be encrypted by two separate keys. Therefore, to decrypt the data to a useful and readable state, the double encipherment process must be reversed, again using the two entirely separate key pairs. The keys used for this purpose are protected further by being ephemeral. Ephemeral keys are temporary, can only be used once, and never leave the devices in the clear. As soon as the ephemeral keys have been used to encrypt or decrypt the data, they are destroyed in temporary memory.



KEY AGENT SERVICES

For organizations that need key management assistance, Futurex's key agent team can compliantly load keys into VirtuCrypt cloud HSMS. With this service, VirtuCrypt handles, loads, and stores key components, but the ownership of the keys remains with the customer throughout this process.

This method is the most common one used by organizations in need of key management assistance. When using these services, certain compliance requirements must be fulfilled that relate specifically to the secure shipment of components. As part of the onboarding and key loading process, customers are provided with detailed instructions.

HSM-GENERATED KEYS

Administrators can randomly generate major keys using the random number generator (RNG) inherent to their cloud HSMS. This RNG is a FIPS 140-2 Level 3 validated entropy source.

SERVICE STRUCTURE: FUNCTIONALITY, THROUGHPUT, AND HIGH AVAILABILITY

VirtuCrypt cloud HSMs are offered in several different models. Your organization can choose a model depending on your desired level of functionality, level of throughput, redundancy, and high availability.

FUNCTIONALITY

A VirtuCrypt cloud HSM can be customized to include whatever functionality your organization needs. Customize and deploy cloud HSMs to support encryption, increase system redundancy, or easily back up and clone cloud HSMs. Take advantage of automated deployment, user-managed high availability clusters, on-demand HSM provisioning, and rapid cloud migration.



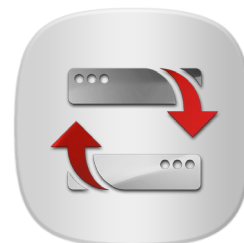
THROUGHPUT

VirtuCrypt cloud HSMs offer different levels of throughput which can be scaled according to need, starting at 50 transactions per second (TPS) and scaling to 250 TPS, 1,000 TPS, and beyond. Throughput is measured using 3DES PIN block translations. A higher throughput will allow for increased efficiency, but the desired level will depend on the size and needs of an organization. If additional throughput is desired, more HSMs can be added.



REDUNDANCY

In addition to throughput, organizations can choose from different redundancy options. Having a single HSM at one site offers no redundancy, which is discouraged due to the potential risk of hardware failure and not having a backup. With site redundancy, two HSMs are active at one site, which increases the dependability of the system. A step up from that is full redundancy. With four HSMs at two different sites, the system is completely protected against hardware failures and data loss due to a lack of backup.



HIGH AVAILABILITY

Similar to adding redundancy to your on-premises HSM infrastructure, your organization might consider building a high availability (HA) architecture for your cloud HSM ecosystem. These architectures prevent downtime due to failures of any kind, whether from hardware or software failures or environmental damage. Having multiple cloud HSMs in different sites creates an ideal environment where system updates and maintenance can be accomplished without taking core systems offline. High availability goes beyond redundancy and can only be achieved through eliminating single points of failure, having reliable crossover or failover points, and reacting to failures in real-time.



VirtuCrypt next-generation cloud HSMs offer service level agreements (SLA) directly tied to the number of cloud HSMs in use in an environment. SLA options are offered up to 99.999%. The option without an SLA is typically used in testing, development, or non-critical environments, and the 99.9% SLA is best-suited for hybrid environments where VirtuCrypt cloud HSMs will stand in for unavailable on-premises HSMs. The 99.99% and 99.999% SLA options are intended for environments where production workloads will be handled primarily within VirtuCrypt.

SLA LEVEL	INFRASTRUCTURE
0%	One cloud HSM housed in a single VirtuCrypt data center
99.9%	Two cloud HSMs housed in a single VirtuCrypt data center
99.99%	Four cloud HSMs, with two housed in one VirtuCrypt data center and the other two housed in a second VirtuCrypt data center
99.999%	Six cloud HSMs, with three housed in one VirtuCrypt data center and the other three housed in a second VirtuCrypt data center

EXPANSION OVER TIME

Each of the different cloud HSM service types available through VirtuCrypt come with expansion capabilities. This is true whether it is a hybrid environment or fully hosted by VirtuCrypt. These can be applied over time if an organization finds that they wish to grow beyond the model they initially selected.

The simplest way of adding redundancy is by enabling additional cloud HSMs at one or more data centers. With more cloud HSMs activated at different data centers, your organization increases its reliability and backup capabilities and decreases the possibility of data loss due to a system failure. Throughput can also be increased by adding more cloud HSM services. Scalability can be adjusted through user-controlled clustering of cloud HSMs, with automated synchronization of keys and settings, flexible throughput options for environments of all sizes, and flexible high availability and SLAs for test environments up to mission-critical production applications.

METHODS FOR EXPANSION

There are two main methods for expansion in the VirtuCrypt next-generation cloud HSM infrastructure: cloning and backup/restore. Expansion through cloning entails making a 1:1 copy of an existing cloud HSM instance and is the recommended method for rapidly increasing throughput or redundancy. The backup/restore method involves taking a backup directly from a VirtuCrypt cloud HSM and restoring it to a new cloud HSM instance. This saves time during the configuration process and ensures all settings are the same.

SUMMARY

Futurex's next-generation cloud HSMs offer customers flexibility and security, along with the benefits of a cloud-based environment. VirtuCrypt provides an effective alternative to the on-premises approach to enterprise cryptography. Migrating to cloud-based cryptography – whether fully cloud or a hybrid model – eliminates the large overhead costs of acquiring and maintaining HSMs on-premises or through colocation.

VirtuCrypt cloud HSMs can be configured to support a large volume of critical services. With this enterprise-grade cloud service, organizations can create an end-to-end hardened security environment, supplement existing on-premises HSM ecosystems, and gain peace of mind that their core cryptographic infrastructure is secure, scalable, compliant, and highly available.



FUTUREX ENGINEERING CAMPUS

OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163