FUTUREX

WHITEPAPER

Integrating Public Clouds with Cloud Payment HSMs

VirtuCrypt Cloud Solutions for Financial Acquiring, Issuing, and P2PE

TABLE OF CONTENTS

OVERVIEW

This whitepaper provides an overview of the architecture of cloud payment HSMs and an increasingly popular deployment approach organizations are migrating to – cloud HSMs integrated natively with public clouds.

Addressed in this document are the features and benefits of cloud integration, what components comprise the infrastructure, and how this service is deployed, focusing specifically on usage examples with Amazon Web Services, although these same principles apply to all major public cloud providers. It also discusses compliance certifications and key management methods, VirtuCrypt service models, and what capabilities exist for expansion.

CURRENT TRENDS IN PUBLIC CLOUD USAGE

In recent years, public cloud usage has been on the rise. As more businesses grow globally connected, the demand for cloud computing has increased. According to Gartner, the market for public cloud services is expected to reach $266.4 billion in 2020, growing 17 percent from the previous year. The threats against data security are growing as well, and users need protection without sacrificing cost and efficiency. The benefits of using the public cloud have been part of why we've seen more of a shift towards it in the last few years. These benefits include cost-efficiency, flexibility, speed of deployment, and in many cases, higher security as well.

An increasingly popular choice for public cloud usage is direct integration with other services and applications housed outside the public cloud itself. Integrating on-premises hardware with cloud-based applications or connecting Software-as-a-Service (SaaS) solutions to separate cloud applications unifies data and improves sharing and visibility.

SaaS, the largest market segment of the public cloud services, is expected to grow to $116 billion in 2020, according to Gartner. This growth is attributed to increasing demand in workload and applications that cannot be accommodated solely by on-premises data centers. As the demand for cloud services increases and many financial acquiring, issuing, and Point-to-Point Encryption (P2PE) application providers take a cloud-native approach, organizations are looking to their payment hardware security module (HSM) vendors for cloud solutions.

PUBLIC CLOUD PROVIDERS SUPPORTING NATIVE HSM INTEGRATION

THE ROLE OF PAYMENT HSMS

Financial HSM utilization is typically split into three different categories: acquiring, issuing, and Point-to-Point Encryption (P2PE). This whitepaper addresses many, though not all, of the use cases that make up these categories.

FINANCIAL ACQUIRING

Financial acquiring focuses on how merchants and banks process credit and debit transactions. This happens through either traditional card-based transactions or mobile payments. For this reason, the functions of financial acquiring HSMs tend to focus more on verification for the banks and merchants.

- PIN (translation and verification)
  - 3DES and AES PIN blocks
  - All PIN validation methods (ISO 8583, Visa, and many others)
- CVV generation and validation
  - All card brands (Visa, MasterCard, Amex, Discover, and others)
  - All variations (CVV, CVV2, CVC, CVC2, Dynamic CVV, etc.)
- EMV validation
  - ARQC validation and ARPC generation
  - All current and past key derivation methods
- Message Authentication Code (MAC) generation and verification
  - ISO 9797 Part 3 (financial MAC)
  - CMAC
- Key management
  - Network key exchange
  - Key derivation methods (DUKPT, ISO 800-108)
- Mobile payment acceptance
  - Google Pay, Apple Pay, and Samsung Pay token acceptance

FINANCIAL ISSUING

Financial issuing focuses on issuing payment cards and provisioning mobile payment tokens. Due to regulatory requirements, financial acquiring and financial issuing processes are typically carried out inside separate HSMs.

- PIN (PIN & offset generation)
  - IBM 3624, Visa, Diebold
- Online & mobile PIN management
  - Supports translating PIN from RSA to symmetric PIN block
  - Asymmetric cryptography for mobile app integration
- EMV key generation & derivation
  - Supports card personalization and data preparation
  - All current and past key derivation methods
- Mobile payment token issuance
  - Google Pay, Apple Pay, and Samsung Pay token issuance

FINANCIAL POINT-TO-POINT ENCRYPTION

P2PE is a secure method for transmitting cardholder data from the point of sale to the merchant host. This technology renders information unreadable during transit, with the data usable only after it is safely decrypted at its destination.

- Cardholder data decryption
  - Supports 3DES and AES P2PE
  - Supports multiple key derivation method, including DUKPT
  - Supports Format Preserving Encryption, including VAES and BPS
- Cardholder data translation
  - Supports translating to processor-specific data formats
  - Supports multiple cipher translations
- Point-to-Point Encryption key management
  - Full point-to-point key management lifecycle supported, including distribution to relevant entities

A HISTORY OF PAYMENT HSM ARCHITECTURES

Financial data security architecture has evolved over time. Now, most financial organizations deploy some form of HSM and payment application infrastructures. What began as on-premises infrastructure is transitioning to an almost entirely cloud-hosted infrastructure.

Initially, payment applications and HSMs were managed on-premises at an organization's own data centers, as shown in item #1 above. While this structure can be beneficial for organizations operating their own data centers, many others began to move towards the cloud in order to increase scalability, redundancy, and reduce internal IT operations so they can increase focus on their own core competencies.

As organizations began moving towards a partial cloud environment, shown in item #2 above, payment applications were placed in the cloud while HSMs were maintained on-premises. This hybrid approach allows for greater flexibility and redundancy for the payment application, but the burden of managing HSMs on-premises, including staff training, compliance audits, and higher up-front capital expenditure, were still there.

After fully realizing the benefits of the cloud for their payment applications, many financial services providers found that moving the HSM component to the cloud provided even more opportunities for maintaining a secure, robust, and scalable cryptographic infrastructure. Today, many organizations take the approach shown in item #3 above, opting to have their payment application hosted with the public cloud provider and their HSMs with a cloud HSM service such as Futurex's VirtuCrypt offering. These organizations reap the benefits of hosting in the cloud – complete flexibility, customizability, reduced cost – as well as maintain the high standard of hardware security and encryption capabilities. Organizations self-manage the connection between their payment applications and their cloud HSMs.

Now, even more organizations are wanting to take full advantage of the services provided by a public cloud provider. When using cloud HSMs that are natively integrated with public cloud providers, as shown in item #4 above, operational burdens are significantly reduced. Networking infrastructure is made much simpler, onboarding is fast, establishing multi-cloud and multi-region high availability is a near-turnkey process, and operational tasks like invoicing and payments are built on top of the organization's existing public cloud account management structure.

These advantages of the full cloud integration model are detailed at length in the next section of this whitepaper.

WHY INTEGRATE CLOUD PAYMENT HSMS NATIVELY WITH PUBLIC CLOUDS?

Many organizations are pursuing integrated solutions that migrate the HSM and payment application to the cloud with full integration. It is not as common to host the HSM and host application independently or on-premises. There are several features of this new model that draw organizations in:

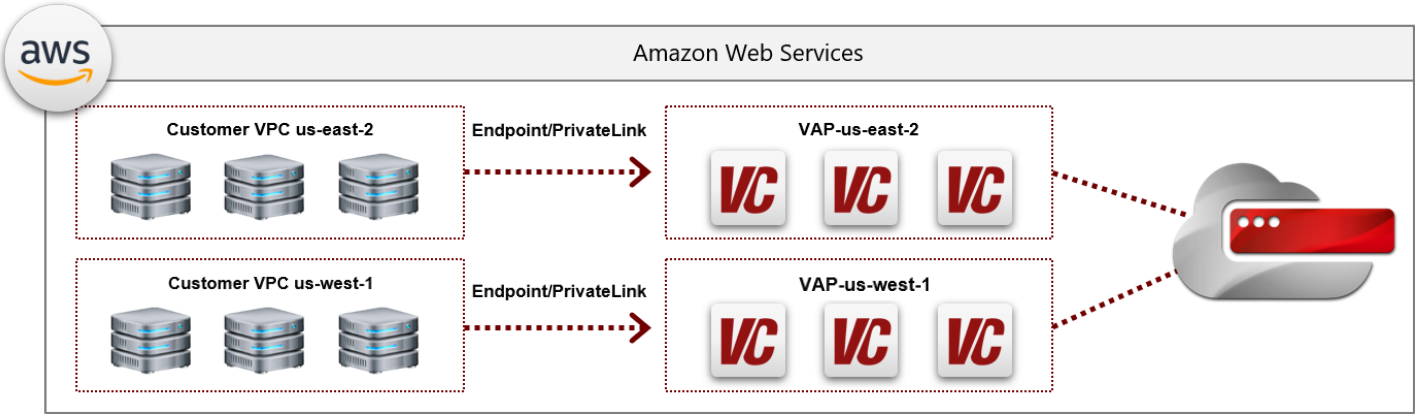
- Easy onboarding and renewals, performed through an organization's existing public cloud account
- Secure communication from the public cloud to VirtuCrypt cloud HSMs, with no direct Internet routing
- VirtuCrypt cloud HSM routing based on region, for multiple regions and multiple clouds
- VirtuCrypt data center failover and monitoring by region

INTEGRATION SPOTLIGHT: AMAZON WEB SERVICES

An example of a public cloud provider that can be integrated with cloud payment HSMs is Amazon Web Services (AWS). Using AWS as a public cloud provider, this section provides an example of how the integration process works.

One of the main benefits of integrating cloud HSMs with AWS is the full integration with the Amazon Marketplace. As one of the largest and most widely used cloud platforms, AWS has a multitude of services that can be utilized for hosting applications & infrastructure with global availability. Using the Amazon Marketplace helps with the onboarding as well. If a client is already using AWS, the onboarding and renewal will be much simpler in terms of using the existing customer information available through AWS.

Through AWS, you can create a Virtual Private Cloud (VPC) that can connect to VirtuCrypt. A VPC allows for a logically separated section of the cloud where your organization can define its own virtual network and handle workloads. These VPCs are deployed per AWS region. With this integration, customers will be able to use VirtuCrypt Access Points (VAP) that manage access to the VirtuCrypt cloud. By using VAPs, the process of connecting to VirtuCrypt eliminates any need for direct Internet routing.



In addition to enabling access to the same VirtuCrypt cloud services from multiple AWS regions, organizations benefit from the variety of access methods, such as on-premises applications through Internet or VPN and hybrid environments. Access to all the different regions allows for lower latency, increased availability, and more robust levels of disaster recovery and redundancy.

COMPONENTS OF THE INFRASTRUCTURE

When integrating a VirtuCrypt cloud payment HSM with a public cloud, several components are incorporated to ensure the process moves smoothly. First, we will define the necessary components of the infrastructure, then we will show how the process works. In some scenarios, not all these components are required. When architecting a cloud payment HSM infrastructure, it is important to outline your organization's goals and discuss how best to achieve them both with Futurex's Solutions Architects and with your payment application provider.

The following components are used to integrate public clouds with VirtuCrypt cloud payment HSMs:

VIRTUCRYPT

- VirtuCrypt Intelligence Portal (VIP) Account
- Cryptoverse
- CryptoTunnel
- VirtuCrypt Access Point (VAP)

PUBLIC CLOUD PROVIDER

- Virtual Private Cloud (VPC)
- Endpoints/PrivateLink

VIRTUCRYPT INTELLIGENCE PORTAL (VIP) ACCOUNT

The VirtuCrypt Intelligence Portal is the primary method through which users manage their cloud payment HSM service. An account is needed on the VIP to integrate the public cloud with the cloud payment HSM. The VIP is a secure website for configuring and reviewing everything related to your organization's VirtuCrypt services. Through its dashboard, the VIP allows for secure management and monitoring of your entire cloud payment HSM environment, audit logs, and tracking account activity from a single location. Existing VirtuCrypt customers will already have accounts on the VIP, but new customers will need to create a new account on the VIP Dashboard.

CRYPTOVERSE

Utilizing a PKI managed by VirtuCrypt, a Cryptoverse isolates which services the public cloud applications have access to. A Cryptoverse is used to ensure mutual authentication and strong encryption with all endpoints, whether those are cloud HSM services, incoming connections to VirtuCrypt, access points like load balancers and edge systems, or client applications. Services are segregated by their Cryptoverse and users must download client keys and certificates for remote applications to authenticate to different services.

CRYPTOTUNNEL

A CryptoTunnel defines the connection parameters to VirtuCrypt. It consists of a name, the Cryptoverse used to authenticate incoming clients, the service that the tunnel will be routed to (the cloud HSM), the incoming channel (Internet, public cloud, etc.), the public cloud provider, the region of the public cloud that will be operated in, and any information that must be whitelisted.

VIRTUCRYPT ACCESS POINT (VAP)

A VirtuCrypt Access Point (VAP) is a VirtuCrypt-owned Virtual Private Cloud. Virtual Private Clouds allow for a logically separated section of the public cloud where an organization, in this case VirtuCrypt, defines its own virtual network. The VAP enables access to VirtuCrypt from a public cloud in a secure manner without directly transiting the Internet, and it also offers connectivity for a range of other access methods. These access methods include connections from and between different public cloud provider regions (US/Canada, Europe, Latin America, for example), access from on-premises applications using a VPN, or hybrid environments.

ENDPOINTS/PRIVATELINK

The endpoint allows your organization to access VirtuCrypt in the public cloud. An endpoint must be designated on the VirtuCrypt Access Point to create the communication channel between the public cloud and the VirtuCrypt cloud payment HSM.

Onboarding

VirtuCrypt follows a standardized onboarding process which has been validated by independent third-party auditors for adherence to compliance. Our test and production environments follow similar workflows for onboarding and setup, with the exception being that production environments have stricter requirements.

By working with VirtuCrypt to establish your data security infrastructure, security is established from the source, thus removing the chance that any process-related risks or errors have occurred. The onboarding process is designed with compliance, security, and ease of use in mind.

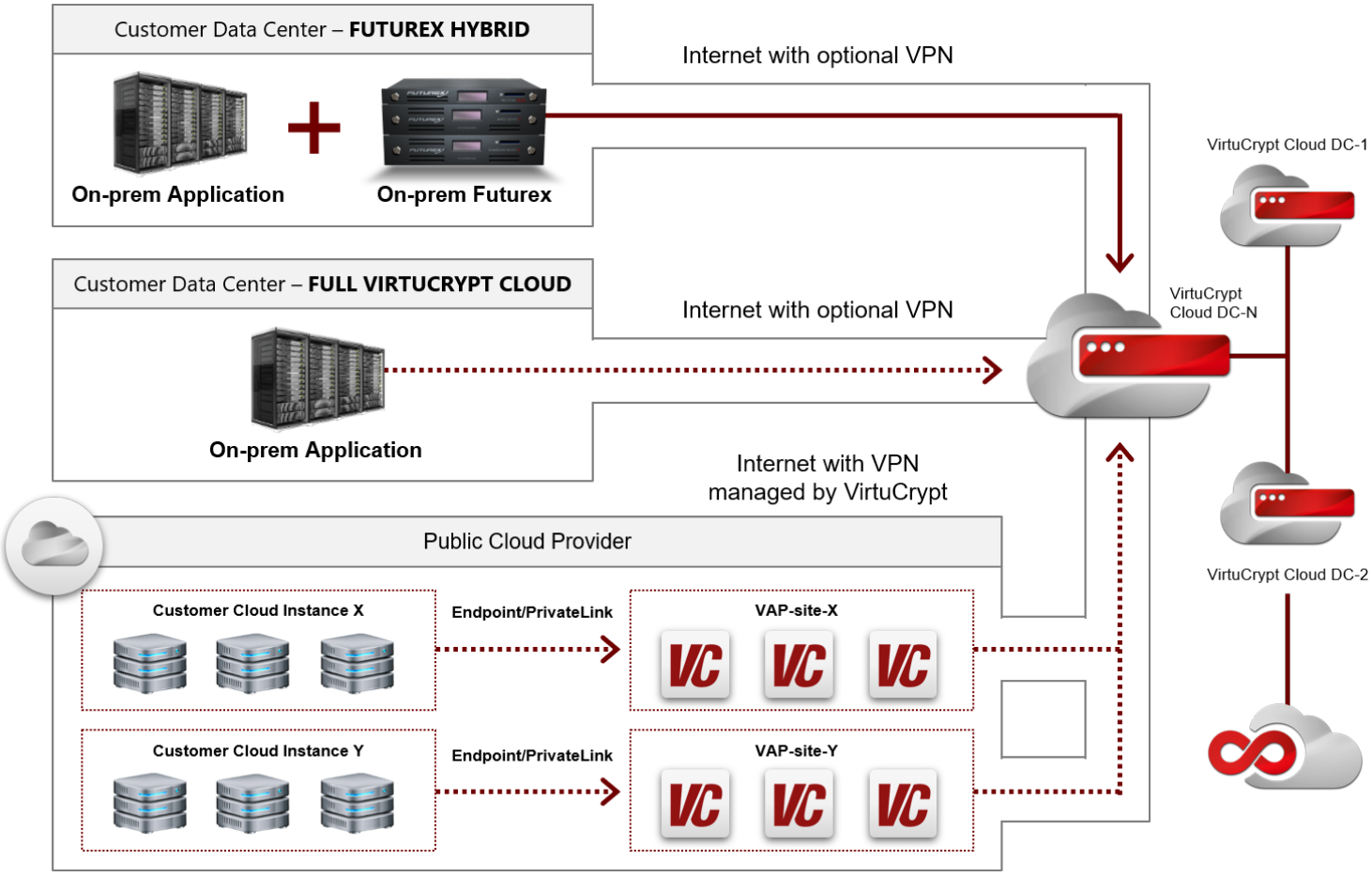
The following steps are required to complete onboarding with VirtuCrypt:

- Completion of forms and due diligence to validate personnel
- Creation of a VIP account
- Download client certificate
- Network setup and validation
- Load major keys and network keys

To deploy the VirtuCrypt cloud payment HSM service, several options are available:

- Native deployment through the public cloud (AWS Marketplace, for example)
- Futurex hybrid: on-premises payment application and on-premises Futurex HSMs
- Full VirtuCrypt cloud option #1: on-premises payment application and VirtuCrypt cloud payment HSMs
- Full VirtuCrypt cloud option #2: public cloud payment application and VirtuCrypt cloud payment HSMs

PROCESS FLOW FOR PUBLIC CLOUD INTEGRATION



The process begins by signing up for a VirtuCrypt service on the public cloud provider. The VirtuCrypt products currently offered are cloud payment HSMs for acquiring, issuing, and P2PE. Because the HSM is licensed through an online subscription, the cloud HSMs fall under the Software-as-a-Service category.

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. Once the service has been successfully connected to the VirtuCrypt account, the user must create a CryptoTunnel.

Once the CryptoTunnel has been established, the VirtuCrypt Intelligence Portal will reach out to the specified region's VirtuCrypt Access Point. Once the VirtuCrypt Intelligence Portal has contacted the VAP, a load balancer will be set up, also creating an endpoint with a VAP ID that points to VirtuCrypt.

Finally, in order to connect the VirtuCrypt Access Point to the CryptoTunnel, the VAP site-to-site VPN must be established. Once the site-to-site VPN is securely established, the communication between the cloud payment HSM in VirtuCrypt and the payment application hosted in the customer's VPC at the public cloud provider can begin.

MULTI-REGION CRYPTO PROCESSING AND HIGH AVAILABILITY

One important feature of an integrated public cloud and cloud payment HSM infrastructure is the ability to use a single cloud HSM with connections from multiple public cloud regions. This entails having a cloud service from a public cloud provider running in multiple availability regions that connect to one or more instance of VirtuCrypt.

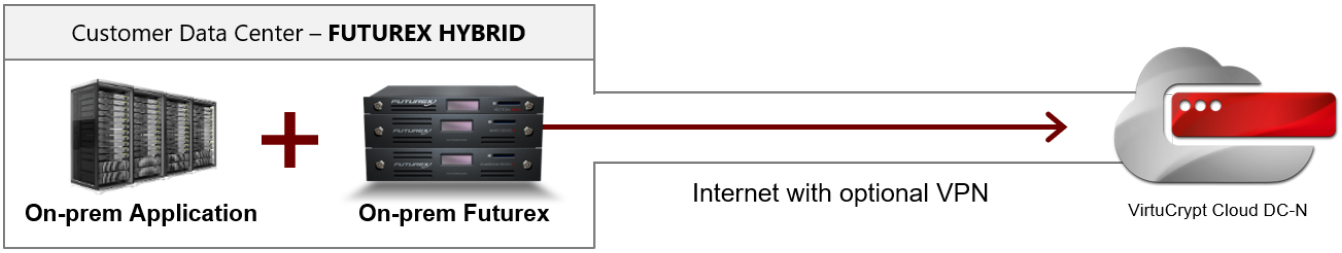
In previous infrastructure models, applications could only connect to their VirtuCrypt cloud HSMs directly over the Internet or through a customized site-to-site VPN. With this new architecture, multiple payment applications can simultaneously connect to VirtuCrypt cloud payment HSMs through the public cloud from regions spanning the globe. In turn, this increases high availability capabilities, not only creating an environment where system updates and maintenance can be accomplished without taking core systems offline, but also one where organizations that are becoming increasingly globally connected can thrive from a secure, low latency, highly scalable, and failure-resistant infrastructure.

CONNECTION ARCHITECTURE: PUBLIC CLOUD INTEGRATION WITH CLOUD PAYMENT HSMS

VirtuCrypt's cloud payment HSM infrastructure can be deployed in either a hybrid environment or a fully-cloud environment. This section outlines these options and reviews some of the key differences between them. No one model is objectively better than the other, and organizations should carefully consider their near-term and long-term goals when making decisions about how to integrate cloud HSMs in their payment processing ecosystem.

HYBRID

The VirtuCrypt hybrid model contains both on-premises Futurex HSMs and cloud HSMs in VirtuCrypt. This model is often used by organizations who possess considerable on-premises HSM estates that are not fully depreciated, giving them a way to slowly transition workload to the cloud over time. It also provides an option for failover, where the VirtuCrypt cloud payment HSMs only process production traffic if the on-premises HSM infrastructure is unavailable. Finally, the third typical use case for a hybrid infrastructure is scalability. If an organization sees an unexpectedly high processing volume, the cloud HSMs can seamlessly provide additional capacity, preventing slowdowns or outages.



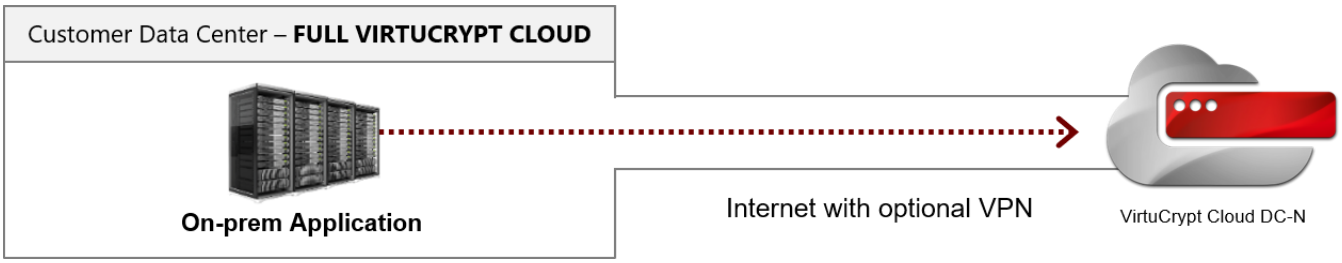
REDUNDANT BACKUP

Data loss, by natural disaster or malicious attack, can cost an organization beyond measure. Establishing a redundant backup of data acts as insurance against such an occurrence, keeping company data safe and secure. VirtuCrypt's facilities are fully redundant across multiple secure SSAE 16 (SOC 1, 2, and 3), PCI DSS, and HIPAA-compliant hosting facilities. Payment applications can be configured to automatically fail over to a backup site, either from on-premises to VirtuCrypt or from one VirtuCrypt cloud HSM to another, in the event of an outage.

FULL VIRTUCRYPT CLOUD

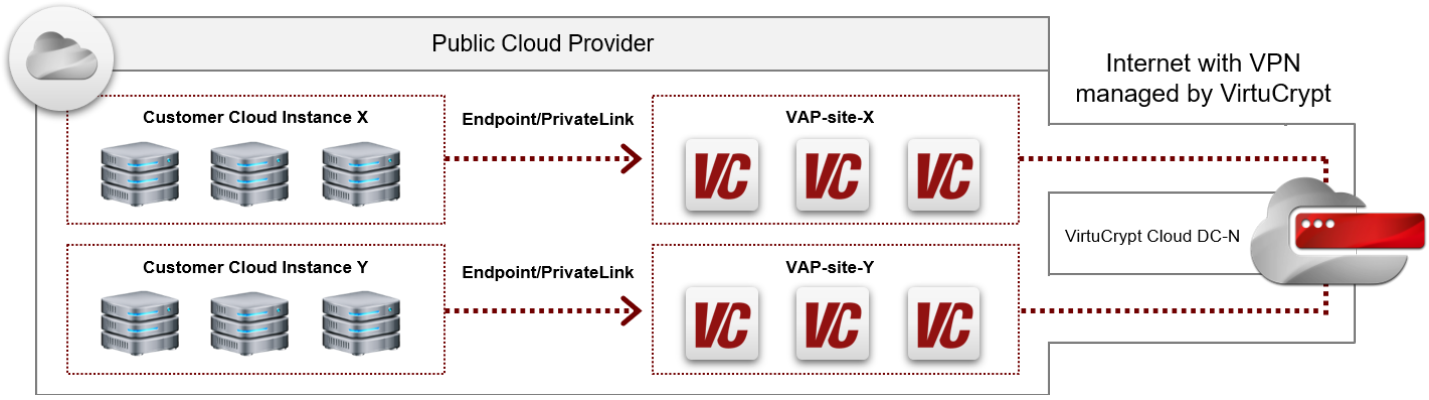
Many organizations opt to have their payment application hosted on-premises and their HSM ecosystem hosted with VirtuCrypt. With VirtuCrypt, organizations have a cloud HSM with the full encryption and key management functionalities of a physical HSM. These organizations reap the benefits of hosting their HSMs in the cloud – complete flexibility, customizability, reduced cost – as well as maintain the high standard of hardware security.

This option is often used by organizations in a transitional state, where they know they want to move their payment application to the cloud but are not able to immediately begin the process, either for technical or business reasons.



PUBLIC CLOUD WITH VIRTUCRYPT

Through hosting both the HSM and host application in the cloud with full integration between the public cloud and VirtuCrypt, organizations are better able to utilize the advantages of the two services, including easy onboarding and integration, secure communication, wider availability through different regions, as well as better data center failover and monitoring by region.



COMPLIANCE

VIRTUCRYPT ENVIRONMENT CERTIFICATIONS

VirtuCrypt services undergo annual audits to ensure that all environmental compliance and certification requirements are met and 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 financial transactions. PCI HSM requirements are managed within the overall standard of PCI PTS.

Compliance with the PCI security standards is enforced by the five major payment card brands who established the Payment Card Industry Security Standards Council, including: American Express, Discover Financial Services, 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

VIRTUCRYPT FACILITIES CERTIFICATIONS

VirtuCrypt facilities are compliant with the following regulatory requirements regarding security:

- SSAE 16 (SOC 1, 2, and 3)
- PCI (see VirtuCrypt Environment Certifications below)
- TIA-942 Tier 4
- HIPAA

FUTUREX HARDWARE CERTIFICATIONS

As previously mentioned, the VirtuCrypt cloud is powered by a vast array of Futurex hardware security modules, key management servers and other technologies regionally distributed across highly secured data centers. All Futurex HSMs within its VirtuCrypt services are FIPS 140-2 Level 3-validated Secure Cryptographic Devices and are compliant with Payment Card Industry (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 payment HSMs are provisioned, securely loading encryption keys is a critical step. There are several methods in which administrators can securely load major keys into VirtuCrypt cloud HSMs including Bring Your Own Key, 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) methodology 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 payment 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 requiring key management assistance, Futurex's CTGA-accredited key agent team can compliantly load keys into VirtuCrypt cloud payment HSMs. With this service, VirtuCrypt handles the compliant handling, loading, and storing of key components, but the ownership of the keys remains with the customer throughout this process.

This method is the most common one used by financial services customers. 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 to follow.

HSM-GENERATED KEYS

Administrators can randomly generate major keys using the random number generator of their cloud HSMs, although this method of key management is very rarely used in financial environments. This is due to key exchange requirements between various stakeholders in the transaction processing workflow. Without sharing keys, these entities would not be able to communicate with each other.

SERVICE STRUCTURE: FUNCTIONALITY, THROUGHPUT, REDUNDANCY, & HIGH AVAILABILITY

VirtuCrypt cloud payment HSMs are offered in several different models. Organizations can choose a model depending on what functionalities, level of throughput and redundancy they want, and whether they desire high availability.

FUNCTIONALITY

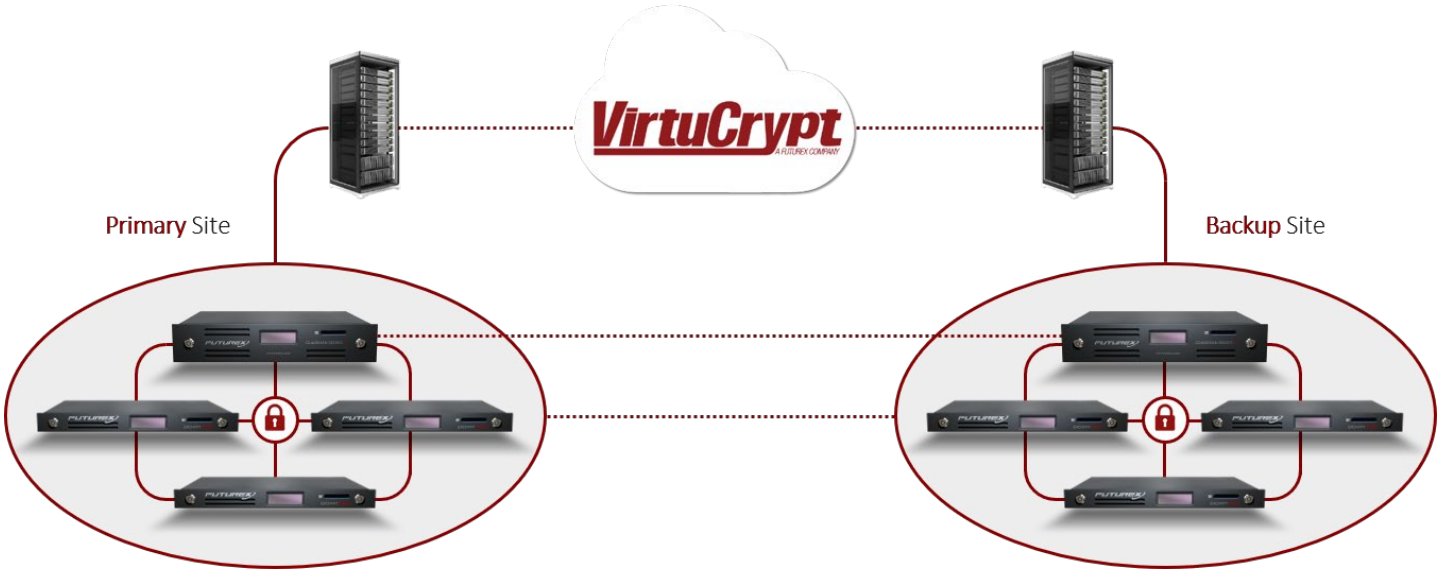
A payment HSM can be customized to include whatever functionality is desired by your organization. VirtuCrypt's cloud payment HSM service can be used with one of three different profiles: transaction acquiring, card and mobile issuance, and Point-to-Point Encryption. A profile must be selected, and organizations needing functionality from multiple profiles must set up individual cloud payment HSM instances.

THROUGHPUT

VirtuCrypt cloud payment HSMs offer three different levels of throughput. Level one provides 250 transactions per second, level two provides 600 transactions per second, and level three provides 1,000 transactions per second. 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 should 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 cloud payment HSMs offer service level agreements (SLA) directly tied to the number of cloud HSMs in use in an environment. SLA options offered are 0%, 99.9%, and 99.99%. 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 payment HSMs will stand in for unavailable on-premises HSMs. The 99.99% SLA option is 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

EXPANSION OVER TIME

There are expansion capabilities for each of the different VirtuCrypt cloud HSM service type, regardless of 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 potential data loss due to a system failure. Like increasing environment redundancy, throughput can be increased by adding more cloud HSM services.

METHODS FOR EXPANSION

There are two main methods for expansion in the VirtuCrypt cloud payment 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 payment HSM and restoring it to a new cloud HSM instance. This saves time during the configuration process and ensures all settings are the same.

When going through any expansion process, Futurex's Solutions Architects are available 24x7x365 to provide expert guidance on best practices, recommended deployment models, and to answer any technical questions.

CONCLUSION

The migration of enterprise workloads to the cloud is not slowing down, and financial services providers are no exception. With many organizations already moving their payment applications to public clouds, the question of HSM integration and whether to move these to the cloud as well is a vital one that takes careful thought and consideration.

Whether exploring VirtuCrypt cloud payment HSMs for testing and development, deploying a hybrid environment paired with existing on-premises Futurex HSMs, or fully transitioning all cryptographic processing for acquiring, issuing, and P2PE to the cloud, it is clear that cloud HSMs can provide significant advantages.

Through the models offered from VirtuCrypt, organizations have many options for customizing their HSM redundancy, throughput, and functionalities. As public cloud usage continues to rise, we will likely see more and more financial services providers taking steps like this to increase security and flexibility for their end customers.

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