FUTUREX

WHITEPAPER

# *Service Overview: Next-Generation Financial Cloud HSMs*

VirtuCrypt Cloud Hardware Security Modules

# TABLE OF CONTENTS

# VIRTUCRYPT CLOUD SERVICES OVERVIEW

VirtuCrypt, Futurex's cloud hardware security module (HSM) and key management platform, is an award-winning provider of enterprise-class cloud security services. VirtuCrypt provides cloud-based access to Futurex's Hardened Enterprise Security Platform, a unique and innovative set of solutions for 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

What sets VirtuCrypt apart from other cloud security services is the advanced encryption and key management applications, along with FIPS 140-2 Level 3 and PCI HSM validated hardware, that powers the VirtuCrypt Hardened Enterprise Security Cloud. This, along with the unparalleled knowledge and expertise of Futurex's Solutions Architect team, form a solution that no other cloud services provider in the industry can offer.

All VirtuCrypt services are powered by industry-leading HSMs from Futurex and rely on Futurex applications for the VirtuCrypt Intelligence Portal (VIP) management interface. VirtuCrypt instances are located in multiple high-security data centers around the world. VirtuCrypt provides businesses customizable, top-of-the-line data security with cloud-level convenience and global scalability.

## HOW ORGANIZATIONS USE AND DEPLOY NEXT-GENERATION FINANCIAL CLOUD HSMS

The primary use cases for financial cloud HSMs are transaction acquiring, card and mobile issuance, and Point-to-Point Encryption (P2PE). These are detailed at length in this whitepaper. As the payments industry continues its rapid expansion and new trends, best practices, and use cases emerge, the use of financial cloud HSMs will also evolve.

Cloud HSMs can be deployed in a variety of ways, outlined at a high level below. Like the use cases for financial cloud HSMs, these deployment models are also explained in greater detail in this whitepaper.

- *Full VirtuCrypt cloud*: payment application hosted in public cloud with VirtuCrypt cloud HSMs
- *Hybrid:* on-premises Futurex HSMs and on-premises payment application, with VirtuCrypt financial cloud HSMs for scalability and disaster recovery
- *Full public cloud integration:* payment application hosted in public cloud, with native integration through public cloud to VirtuCrypt cloud HSMs

# FINANCIAL SERVICES & CLOUD HSMS

Financial businesses can utilize cloud HSMs throughout the payment journey as well as be the primary cryptographic deployment mechanism for End-to-End Encryption. Elastic like the nature of the cloud, VirtuCrypt can be variably configured & quickly integrated into critical financial acquiring, issuing, and point-to-point encryption processes. First, we will dive into the different features and capabilities of all next-generation financial cloud HSMs, before detailing the specific features of the financial acquiring, issuing, and point-to-point encryption cloud HSMs.

## CORE-TO-CLOUD ARCHITECTURE AND AUTOMATION

One of the main advantages of the next-generation financial cloud HSM is how the process of shifting your crypto architecture to the cloud is essentially automatic. This is done through instant provisioning with the VirtuCrypt Intelligence Portal (VIP), meaning you can access your device on the VIP Dashboard when it's been provisioned by the VirtuCrypt engineers. Another aspect of this automated process is the one-click migration from on-premises HSMs to cloud HSMs. This allows users to shift their infrastructure to the cloud with simply one click, instead of having to undergo an extensive maneuvering process. VirtuCrypt also provides a cloud HSM Software Development Kit (SDK) for natively integrating cloud crypto processing and key management into your own applications and services, whether on-premises or in the cloud.

## CLOUD HSM MANAGEMENT AND SNAPSHOT TECHNOLOGY

Another new feature of the next-generation cloud HSM is the ability to take cloud HSM snapshots for backup, migration to new environments, or streamlining new deployments. These cloud HSM snapshots allow for easier management of the system because the user is able to save the instance of the cloud HSM. With cloud HSM snapshots, the user can enable and disable cloud HSMs with the click of a button for both testing and production environments. They can also store cloud HSM snapshots on the VirtuCrypt cloud HSM backup service and re-provision them on-demand. With these cloud HSM snapshots, users can also build cloud HSM templates that make establishing new environments simple and eliminates configuration errors. Through these snapshots, cloud HSM major keys can be randomly generated, cloned from existing cloud HSMs, compliantly loaded using VirtuCrypt's key agent services, or fully customer-loaded and controlled from anywhere in the world.

## CRYPTO INFRASTRUCTURE INTELLIGENCE AND ORCHESTRATION

All next-generation financial cloud HSMs have features that simplify monitoring and allow for easier HSM orchestration. HSM orchestration allows cloud HSMs to be provisioned or modified based on user-defined scenarios. Some ways that users can they have centralized log management with audit-friendly reporting and integrated alerting and monitoring with user-definable push notifications. The ability to integrate natively with third-party applications and cloud monitoring tools also increases the flexibility for the user.

# THE ROLE OF FINANCIAL 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 the steps carried out between merchants and banks for processing credit and debit transactions, either through 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 FINANCIAL HSM ARCHITECTURES

Financial data security architecture has evolved over time and developed extensively to reach where most organizations that deploy HSM and payment application infrastructures are today. What began as a purely on-premises infrastructure is now transitioning to an almost entirely cloud-hosted one.

Initially, a payment application and HSMs to handle cryptographic processing were managed on-premises at an organization's own data centers. 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, 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 opt 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, 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.

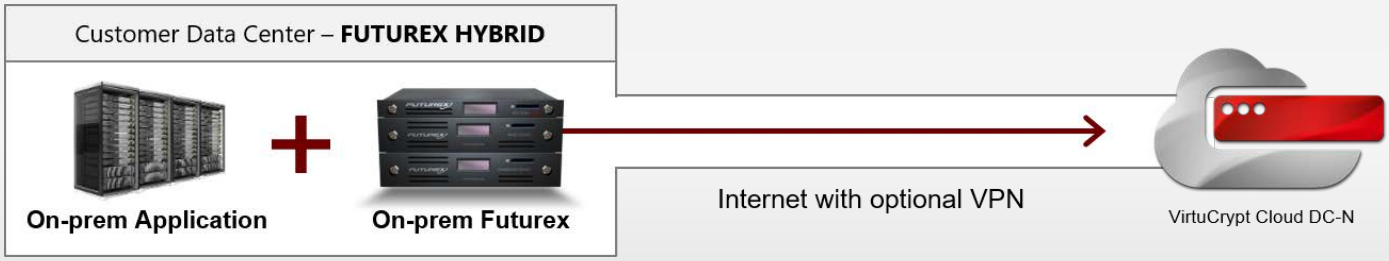
## INFRASTRUCTURE DESIGN & DEPLOYMENT

VirtuCrypt's next-generation financial cloud 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 financial processing ecosystem.

### HYBRID

The hybrid model contains both on-premises Futurex HSMs and VirtuCrypt next-generation financial cloud HSMs. This model is often used by organizations who have large on-premises HSM estates, letting them slowly transition to the cloud over time.

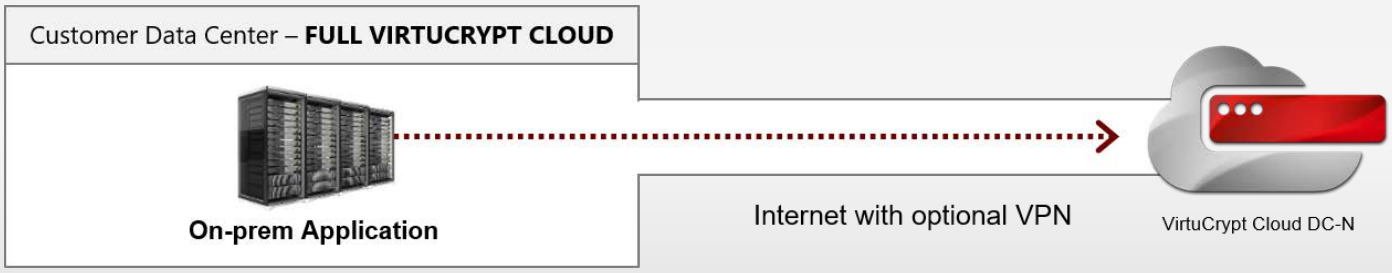
It also provides an option for failover, where the cloud HSMs only process production traffic if the on-premises HSMs are unavailable. Finally, the third typical use case for a hybrid infrastructure is scalability. If an organization sees an unexpectedly high volume, cloud HSMs can seamlessly provide additional capacity, preventing slowdowns or outages.




### FULL VIRTUCRYPT CLOUD

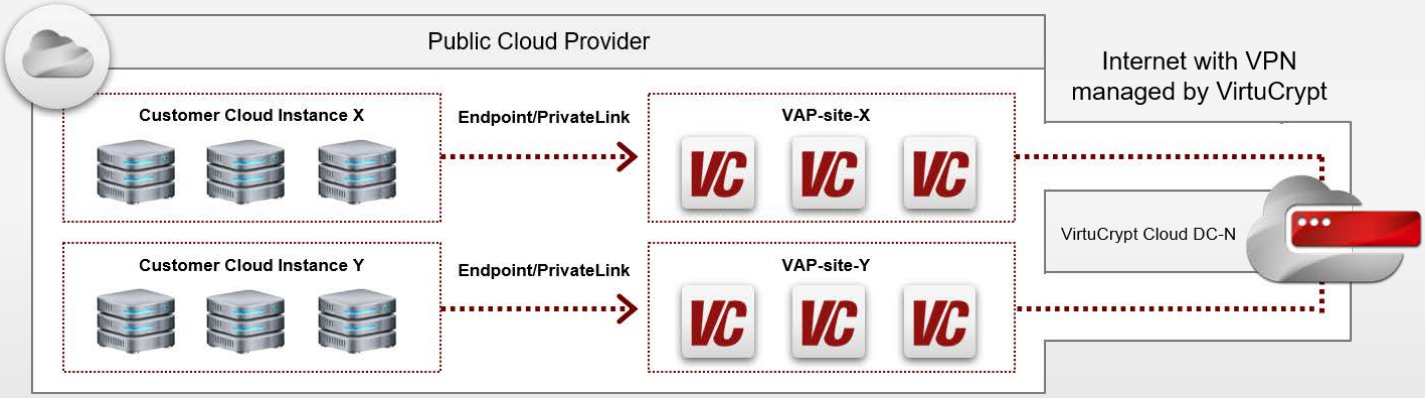
Many organizations opt to have their payment application hosted on-premises and their HSM ecosystem hosted with VirtuCrypt. With VirtuCrypt, organizations have a cloud HSM with the full encryption and key management functionalities of a physical HSM. These organizations reap the benefits of hosting their 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.




To integrate applications in the public cloud with VirtuCrypt, the user must register for a VirtuCrypt cloud HSM 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, which is a turnkey connection security between on-premises apps, cloud-hosted applications, and cloud HSMs.

Once the CryptoTunnel has been 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. 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 VAP 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 financial cloud HSM in VirtuCrypt and the payment application hosted in the customer's VPC at the public cloud provider can begin.

### 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. To ensure critical data is not lost, it is best practice to integrate a fail over system that efficiently mirrors production data.

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 next-generation financial cloud HSM to another, in the event of an outage.

### STREAMLINED DEPLOYMENT AND SELF-SERVICE CAPABILITIES

One of the benefits of the next-generation financial cloud HSM is that the deployment is simplified and streamlined to ease the burden on the customer and decrease the time to market. With on-demand provisioning of cloud HSMs for financial acquiring and issuing as well as instant provisioning for common payment host applications, with recommended settings built-in, users can access their cloud HSMs much quicker than previously. Users can configure cloud HSMs in the Cryptoverse, which allows enterprise key schema for comprehensive, cross-platform security with TLS-secured mutual authentication and strong encryption across all endpoints. In the Cryptoverse, connection whitelisting ensures only trusted applications can access cloud HSM services. VirtuCrypt also offers deployment in different PCI zones (acquiring/point-to-point encry ption, issuing, or test) to meet compliance requirements.

## CLOUD HSM FUNCTIONALITY OVERVIEW: FINANCIAL ACQUIRING

### PIN TRANSLATION & VERIFICATION

Cloud HSMs can perform the critical cryptographic functions necessary to translate and validate PIN blocks. Organizations can configure VirtuCrypt next-generation financial cloud HSMs to execute multiple translation commands needed to prepare PIN blocks for each transaction zone. These commands include:

- TPIN: Translate PIN blocks from one key to another
- TPIN IBM: Translate the incoming PIN block encrypted via the IBM 4736 ATM algorithm
- TPIN DUKPT: Allows the incoming DUKPT encrypted PIN block to be translated under an outgoing key

Like PIN translation, VirtuCrypt next-generation financial cloud HSMs support a variety of PIN verification methods including Visa, NCR, Diebold, ICM 3624, and IBM 4736 and can be configured to operate with offline & online PIN solutions.

## EMV VALIDATION

As EMV (originally Europay, Mastercard, and Visa) has become the standard when issuing payment cards, financial organizations must continue to expand their capabilities to effectively manage EMV validation & response. Organizations can offload EMV authorization request (ARQC) validation & response generation (ARPC) to next-generation financial cloud HSMs and quickly receive validation of EMV card transactions prior to approving funds for a purchase.

## MAC GENERATION & VERIFICATION

Centralizing authorization processes into a single security platform like VirtuCrypt greatly reduces key management complexity and unnecessary risk. Ensure strong data integrity and authenticity by generating and verifying message authentication code (MAC) in cloud HSMs specifically configured for financial services industry.

Our cloud HSMs can be configured to:

- Generate standard, DUKPT, or hashed messaging code
- Generate ISO Variant 3, or HMAC and PBKDF2 obfuscated value
- Verify standard MAC and MAC using DUKPT
- Generate & verify cipher-based MAC (CMAC)

## FINANCIAL KEY MANAGEMENT & DERIVATION

Proper encryption key management for network keys is vital to any financial processing environment. VirtuCrypt's next-generation financial cloud HSMs support a range of features used for these purposes:

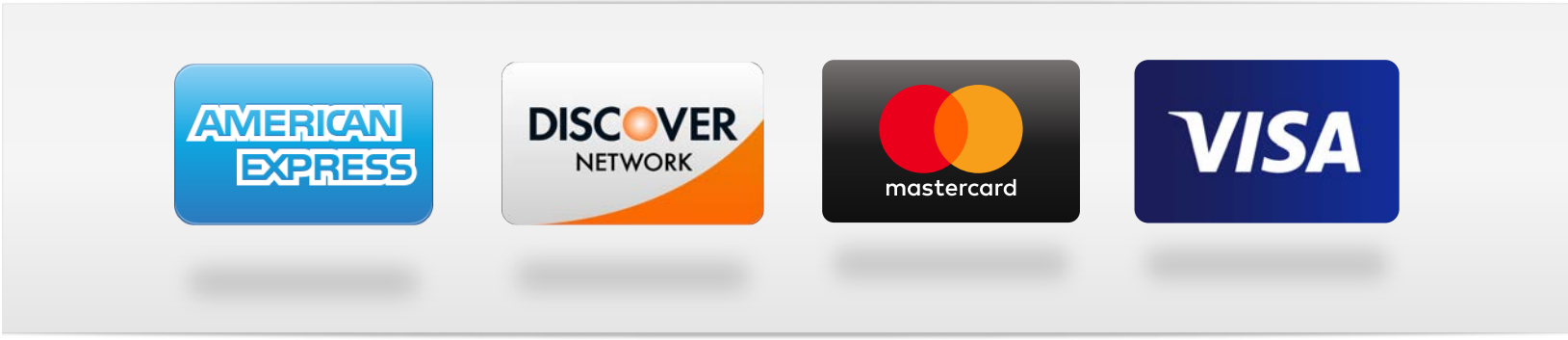
- Network key exchange under a common Key Exchange Key (KEK)
- Key translation between a range of formats
- Key derivation for a variety of methods including DUKPT & ISO 800-108 recommended methods (Counter, Feedback, and Double-Pipeline Iteration)
- Mastercard On Behalf Key Management (OBKM)

## CVV GENERATION & VALIDATION

Organizations can securely d validate card security codes (CVC, CVV, CVC2, CSC) from major payment providers including Visa, MasterCard, Discover and American Express with next-gen financial cloud HSMs. Administrators can appropriately configure cloud HSMs to generate and verify specific types of verification codes through API commands.

- Card Identification Number (CID)
- Card Security Code (CSC)
- Card Validation Code (CVC & CVC2)
- Card Verification Data (CVD)
- Card Verification Value (CVV)

VirtuCrypt financial cloud HSMs can also be configured to validate CVVs with set validation conditions. Configurable conditions include output length, card verification key referencing, compatibility modes, and other functions.




## MOBILE PAYMENTS ACCEPTANCE

VirtuCrypt next-generation financial cloud HSMs are compliant and compatible with Google Pay, Apple Pay, and Samsung Pay. The services related to mobile payments include:

- Decrypting Apple Pay, Google Pay, Samsung Pay tokens
- Generating Host Card Emulation (HCE) mobile cryptograms, magstripe verification values, and mobile keys
- Verifying HCE mobile cryptograms and magstripe verification values

# CLOUD HSM FUNCTIONALITY OVERVIEW: FINANCIAL ISSUING

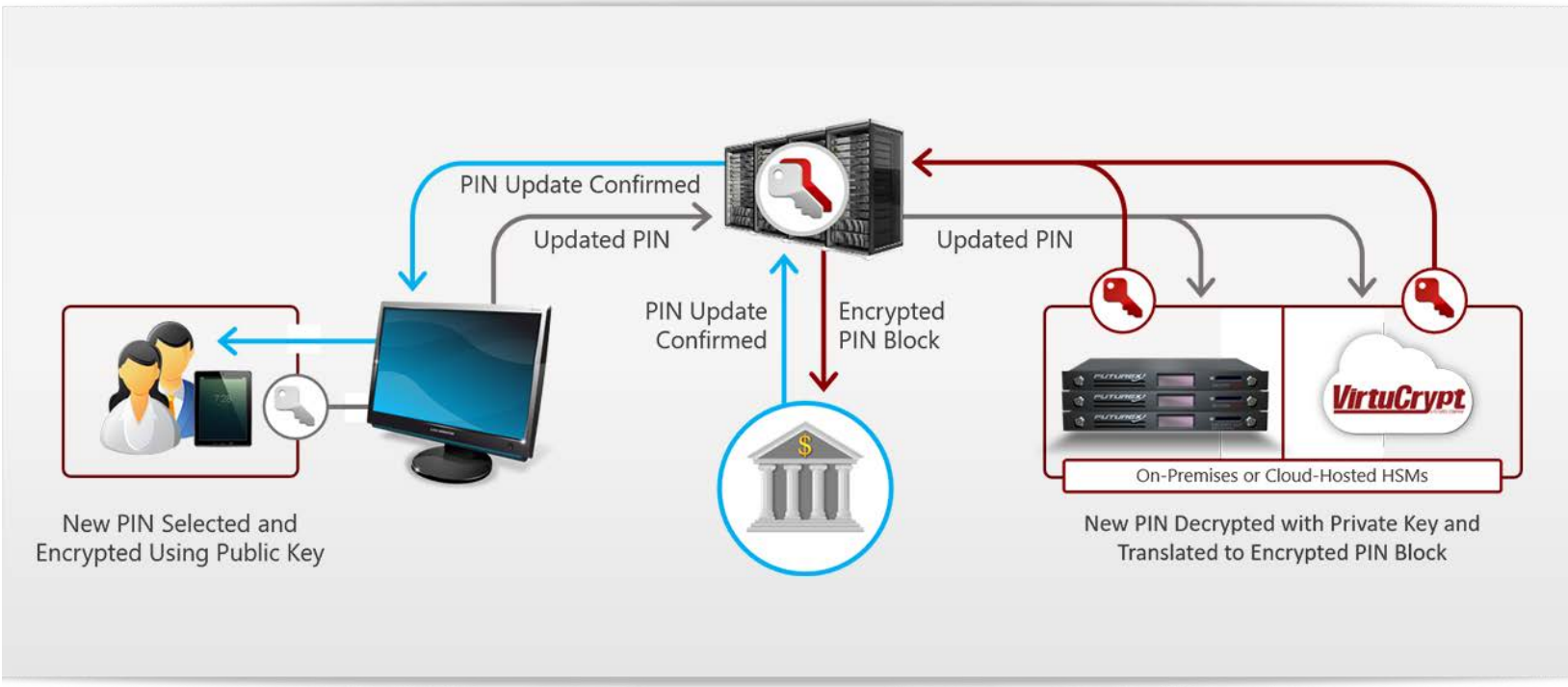
## PIN (PIN AND OFFSET GENERATION)

VirtuCrypt next-generation financial cloud HSMs can be utilized to generate PIN and PIN offset values during payment card issuance. All major PIN generation algorithms are supported by our next-generation financial cloud HSMs and can be configured to output the desired PIN type as needed. Offsets can be generated from clear PINs or encrypted PIN blocks.

In addition, cloud HSMs can be configured to generate new offsets without changing the customer PIN, encrypting clear PINs, and generating offsets of a clear PIN.

## MOBILE AND WEB PIN MANAGEMENT

The demand for additional methods of accountholder authentication and PIN management has increased with the growth in number of devices and access points to financial systems and ecommerce. Just as solutions have been introduced into the market for software-based PIN entry for purchases, so have techniques for cloud-based PIN issuance and management.




When performing a PIN change through an issuer's website or mobile app, the new PIN, encrypted using the web browser or app's RSA public key, is sent to the VirtuCrypt service instance. Within its secure, FIPS 140-2 Level 3 and PCI HSM compliant boundary, the HSM translates that PIN into an encrypted symmetric PIN block and provides it in a response which can then be stored in the issuer's PIN database for future use.

## EMV KEY GENERATION AND DERIVATION

Cloud HSMs act as the primary security devices when issuing EMV ICC chip payment cards. By integrating with data preparation and personalization systems, cloud HSMs play a critical role during issuance of the physical EMV credit, debit & prepaid cards by generating the required keys and other potential EMV requirements including:

- EMV ICC certificate and issuer CSR
- Generating dCVC3, CVC IV, and Data Authentication Code (DAC)
- Key derivation from Vendor Master Key
- Generating & verifying MAC
- Establish authority between issuer and payment scheme
- Derive Application Cryptogram (AC) card key from the AC master key & account number
- Validating EMV cryptograms

## PAYMENT CARD ISSUANCE & REPLACEMENT

Issuing prepaid EMV and debit cards presents unique operational challenges. Unlike typical prepaid debit or stored-value cards, EMV cards contain an Integrated Circuit Card (ICC) chip and are secured using a Public Key Infrastructure.

During payment card issuance, the ICC chip is loaded with encrypted data in addition to the magnetic stripe for backward compatibility. The sensitive payment card data is first prepared by the data preparation system which extracts clear sensitive data from issuing institution customer databases. The data preparation system then encrypts sensitive data using three types of keys: Data Transport Key (DTK) for customer data, Key Transport Key (KTK) for encryption keys, and PIN Transport keys (PTK) to encrypt PINs. Each key is derived from the dedicated master key generated by a cloud HSM. Cloud HSMs also provides the necessary encryption keys to the personalization machine that receives, decrypts and imprints the data from the data preparation system during the card printing process.

## MOBILE PAYMENT TOKEN ISSUANCE

For issuers allowing customers to make payments via digital wallets (such as Apple Pay, Google Pay, and Samsung Pay), an efficient payment tokenization solution is needed to avoid unnecessary transmission of payment card and PAN data. Digital wallet payment processing utilizes a specific kind of token, payment token, which differs from the acquisition and issuer tokens in that original PAN data is not exposed. Payment tokens are issued via a Token Service Provider (TSP) to registered token requestors (merchants holding payment card credentials) to be utilized as “proxy” or “surrogate” PAN data.

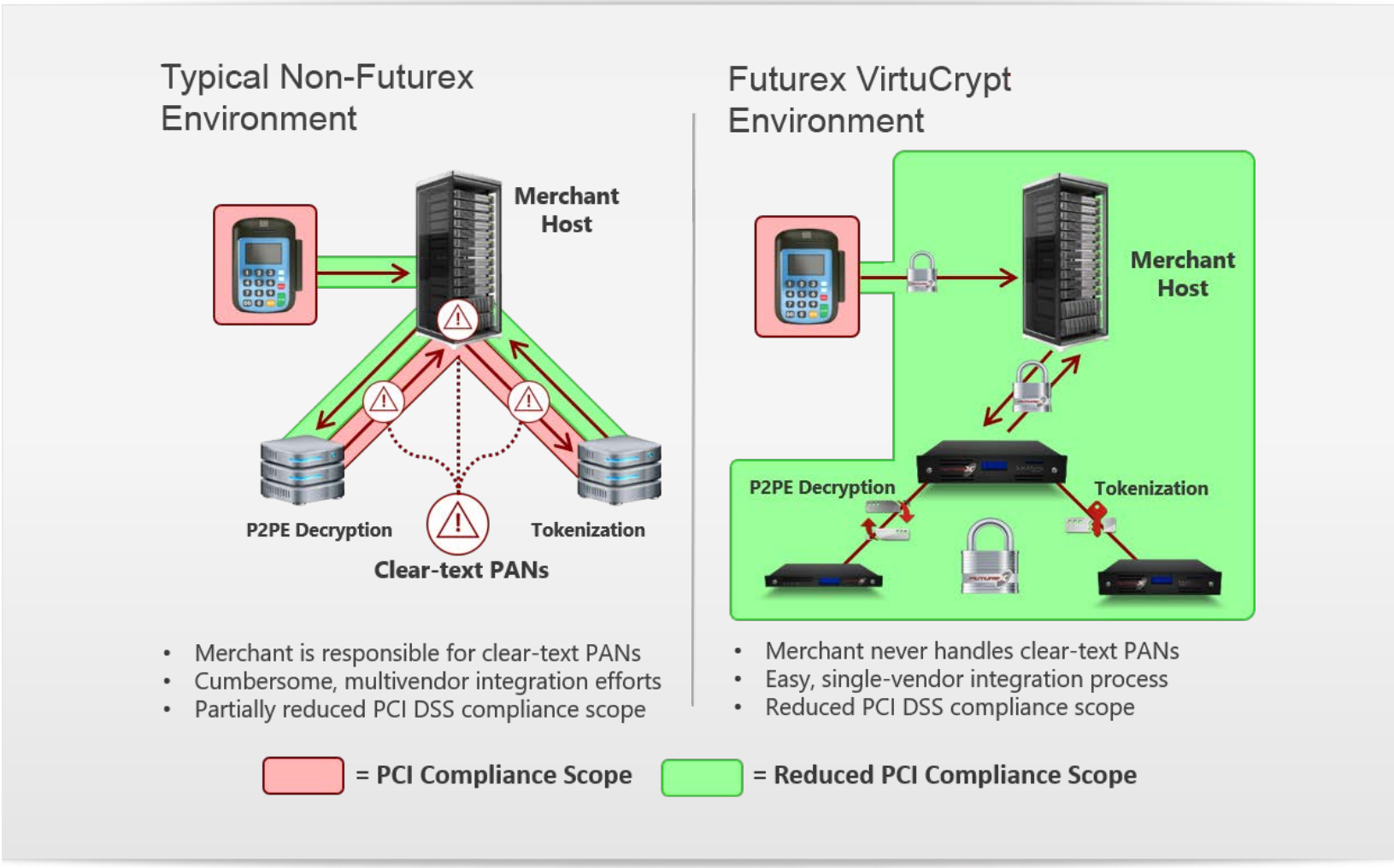
VirtuCrypt next-generation financial cloud HSMs can be integrated as independent Token Service Provider (TSP) or can be configured to allow payment networks or payment processors to become a TSP. In addition to mobile payment token issuance, VirtuCrypt tokenization and P2PE can be used in conjunction with other encryption technologies allowing organizations to potentially eliminate all clear-text PAN data from their networks.

## CLOUD HSM FUNCTIONALITY OVERVIEW: FINANCIAL POINT-TO-POINT ENCRYPTION

Point-to-Point Encryption, also known as P2PE, is a robust technique for encrypting data from the moment which cardholder data is captured until it has entered the secure network of the transaction processor. In P2PE secured environments, sensitive cardholder data, which includes the Primary Account Number (PAN), is initially encrypted at the first point of interaction. The encrypted data is sent to the transaction processor, where it is decrypted within the confines of a hardware security module, and then is sent to the card issuer for validation. To meet your organization's specific needs, VirtuCrypt can be configured to create a secure P2PE environment through remote key loading and advanced encryption & translation techniques that support DKUPT derived keys and both 3DES and AES encryption.

### CARDHOLDER DATA DECRYPTION (USING FPE AND DUKPT)

After cardholder data is encrypted at a Point-of-Sales (POS) or ATM terminal, data is securely transmitted and decrypted utilizing related keys generated/housed by a cloud HSM (Excrypt Plus) under a secure TLS management platform (Guardian Series 3).



## DECRYPTION USING FORMAT-PRESERVING ENCRYPTION

Format-preserving encryption (FPE) allows organizations to encrypt data in the same format as the original data, hence the name "format preserving." For example, a PAN is typically between 8 and 19 numeric digits, and when using format-preserving encryption, the encrypted PAN data will have the same number of digits. Format-preserving encryption is utilized by organizations with strict database schemas that require field values to share the same length and format.

### Example

*Encrypted PAN#: 9356030022219797*
*Decrypted PAN#: 4012888888881881*

## DECRYPTION USING DUKPT

Derived Unique Key Per Transaction (DUKPT) safeguards data, such as Personal Identification Numbers (PIN) or cardholder Primary Account Numbers (PAN), by providing unique encryption keys for every transaction. Each key cannot lead back to the original key upon which it was based. Each transaction key is erased after use.

Essentially, one Base Derivation Key (BDK) is used to initiate the DUKPT process. The BDK itself is never exposed, but instead is used to create another key, called an initial key. This initial key is injected into the new Point-of-Sale (POS) device along with a Key Serial Number (KSN) containing identifying information for the host application. The initial key is used to create a pool of encryption keys, and during each transaction, one of the keys is selected from the pool to encrypt information. After the data is sent to the device, the current key is used to create additional future keys, and then it is erased, removing any information about a previous transaction.

To decrypt data that was encrypted using the Triple DES (3DES) algorithm under a key derived from a DUKPT BDK, a cloud HSM must perform the key derivation process to generate the key needed to decipher the PAN data. Transmitted along with the encrypted PAN data is the Key Serial Number (KSN) which consists of a Device ID and device transaction counter. From the KSN, the receiver then generates the Initial Key and from that generates the Future Key that was used by the device and then the actual key that was used to encrypt the data. With this key, the receiver will be able to decrypt the data.

### DUKPT Advantages

Derived keys keep information safe. The process cannot be reversed to lead back to the BDK, and if one of the keys were compromised in a POS device, it would immediately be replaced by a new key in the next transaction. Through derivation, DUKPT forms a self-recycling system that promotes security, efficiency, and ease of implementation.

## CARDHOLDER DATA TRANSLATION

When transmitting sensitive cardholder data between multiple payment institutions (zones), it is best practice to orchestrate a secure process that does not expose clear data to any institution that is not the issuing bank or financial institution. In addition to the handling of sensitive cardholder data, each zone must securely pass the PIN Encryption Key (PEK) between zones for use by the issuing bank.

To accomplish this task, the data block must be translated and encrypted between each zone through sharing of zone keys or Traffic Encryption Keys (TEK). Traffic Encryption Keys (TEKs) encrypt the data transferred between each zone and must be derived from the original master key or in the case of DUKPT the Base Derived Key (BDK). The TEKs must also be changed out frequently requiring a proper key management solution.

VirtuCrypt next-generation financial cloud HSMs can support the secure translation of sensitive cardholder data reducing PCI DSS compliance scope through the following PAN Translation Methods:

- DUKPT-to-DUKPT: data encrypted using DUKPT derived key translated to another DUKPT derived key
- DUKPT-to-Symmetric or Symmetric-to-DUKPT: data encrypted using DUKPT derived key translated to symmetric key, or vice-versa
- DUKPT-to-RSA with track data: translate and parse data from a key derived using DUKPT to an RSA public key with specific track data

## POINT-TO-POINT ENCRYPTION KEY MANAGEMENT

To meet PCI compliance standards, a cost-effective key management strategy that encompasses all phases of the encryption key lifecycle (generation, storage, distribution, destruction etc.) must be in place. Key management for Point-to-Point Encryption is no exception as financial organizations can create unnecessary complexity or manual effort due to lack of resources or technological limitations.

### REMOTE KEY MANAGEMENT

VirtuCrypt's remote key loading services leverage the power of the cloud to include all the functionality necessary for performing key management for POS terminals, ATMs, and more. With cloud HSMs and key management servers, you can exercise full key management capabilities. By rotating keys over a secured IP network, your organization can conserve the time and resources that would otherwise be spent rotating keys.

The Remote Key Management service provides:

- Key generation, distribution, injection, deletion, tracking, and certificate hierarchies
- Flawless integration with the host application that drives your organization's POS terminals or ATMs
- Remote management capabilities such as loading Master File Keys (MFK), from virtually anywhere using the Excrypt Touch tablet

# COMPLIANCE

Financial HSM environments are responsible for meeting a range of compliance requirements. Adherence to these requirements is typically the responsibility of the financial institution 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 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 PCI standards is enforced by the five major payment card brands who established the Payment Card Industry Security Standards Council, 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

## 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 financial 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 next-generation financial 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 next-generation financial 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 next-generation financial cloud HSMs.

Transferring keys to VirtuCrypt financial 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 requiring key management assistance, Futurex's CTGA-accredited key agent team can compliantly load keys into VirtuCrypt cloud financial 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, AND HIGH AVAILABILITY

VirtuCrypt financial cloud 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.

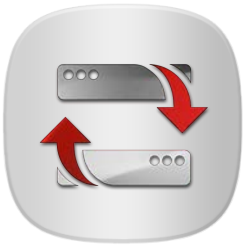
### FUNCTIONALITY

A financial HSM can be customized to include whatever functionality is desired by your organization. VirtuCrypt's financial cloud 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 financial cloud HSM instances.

### THROUGHPUT

VirtuCrypt financial cloud 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 next-generation financial cloud 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 financial cloud 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 next-generation financial cloud HSM service types, 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. Scalability can also 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 financial 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 financial 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

Next-generation financial cloud HSMs provide an effective alternative to the on-premises approach to implementing enterprise cryptography. Crypto-as-a-Service allows organizations to incorporate data security costs under operational budgetary classification (OPEX) rather than capital expenditure (CAPEX), preventing large overhead costs of acquiring and maintaining HSMs on-premises or through colocation.

Whether they focus on financial acquiring, financial issuing, or Point-to-Point encryption, next-generation financial cloud HSMs offer customers the flexibility and security they need with the benefits of a cloud-based environment.

VirtuCrypt next-generation financial cloud HSMs can be configured to support a large volume of financial services critical to payment systems and processes. 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*