FUTUREX

Whitepaper

Next-Generation Cloud Payment HSMs

VirtuCrypt Cloud Hardware Security Modules

TABLE OF CONTENTS

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 payment 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 PAYMENT HSMS

The primary use cases for cloud payment HSMs are transaction acquiring and card and mobile issuance, including functions such as point-to-point encryption (P2PE) and database encryption. 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:

Cloud payment HSMs can be deployed in a variety of ways, outlined at a high level below. Like the use cases for cloud payment 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 cloud payment 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

CLOUD PAYMENT HSMS

Cloud payment HSMs handle all common encryption tasks and form the basis of an organization's enterprise data security ecosystem. With 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 payment HSMs.

CORE-TO-CLOUD ARCHITECTURE AND AUTOMATION

A big advantage of the Futurex cloud payment 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 PAYMENT HSM MANAGEMENT AND SNAPSHOT TECHNOLOGY

The Futurex cloud payment 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 payment HSM snapshots on the VirtuCrypt cloud HSM backup service and re-provision them on-demand. With these snapshots, users can build 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 simplify monitoring 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.

THE ROLE OF PAYMENT HSMS

Payment HSM utilization is typically split into two main categories: payment acquiring, and card and mobile issuing. Point-to-point encryption is an important part of payment acquiring. This whitepaper addresses many of the use cases that make up these categories.

PAYMENT ACQUIRING

Payment acquiring is how merchants and banks process transactions, either through traditional card-based transactions or mobile payments.

- 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

CARD AND MOBILE ISSUING

Card and mobile issuing refers to how banks issue payment cards and provisioning mobile payment tokens.

- 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

Due to PCI regulatory requirements, acquiring and issuing processes are typically carried out in separate HSMs. This restriction does not apply to organizations beyond the scope of PCI, however.

POINT-TO-POINT ENCRYPTION (P2PE)

P2PE is a compliance standard developed by the PCI Security Standards Council. The P2PE standard is the framework by which organizations encrypt card data as soon as it is captured by a payment terminal. It is a function of payment acquiring. Doing so avoids sending card data "in the clear" through merchant networks, increasing data security in general.

- 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

The data security architecture of the financial sector is in the process of transitioning away from on-premises infrastructure to cloud-hosted infrastructure. Initially, payment applications and payment HSMs were managed on-premises at an organization's own data centers. Over time, many organizations migrated to the cloud in order to increase scalability and reduce internal IT operating costs.

As organizations moved to partial cloud environments, payment applications were moved to the cloud while HSMs were maintained on-premises. This hybrid approach allowed for flexibility and redundancy for the payment application. But there was still the burden of managing HSMs on-premises. This included staff training, compliance audits, and higher up-front capital expenditure.

After fully realizing the benefits of the cloud, many payment services providers found that moving HSMs to the cloud provided more opportunities to lower their total cost of ownership (TCO) while raising efficiency. Today, many organizations host their payment applications with a public cloud provider and their HSMs with a cloud HSM service, such as Futurex's VirtuCrypt cloud payment HSM service. These organizations reap the benefits of hosting in the cloud – flexibility, customizability, reduced cost – and maintain the high standard of hardware-backed security. Organizations self-manage the connection between their payment applications and their cloud HSMs.

When using cloud HSMs that are natively integrated with public cloud providers, operational burdens are significantly reduced. Networking infrastructure is simplified, onboarding is faster, and high availability (multi-cloud and multi-region) is easier to attain. As an added bonus, 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.

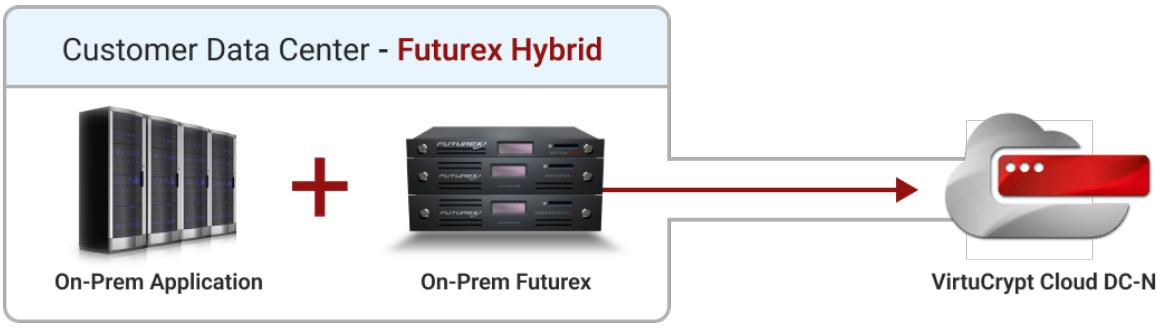
INFRASTRUCTURE DESIGN & DEPLOYMENT

VirtuCrypt's 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.

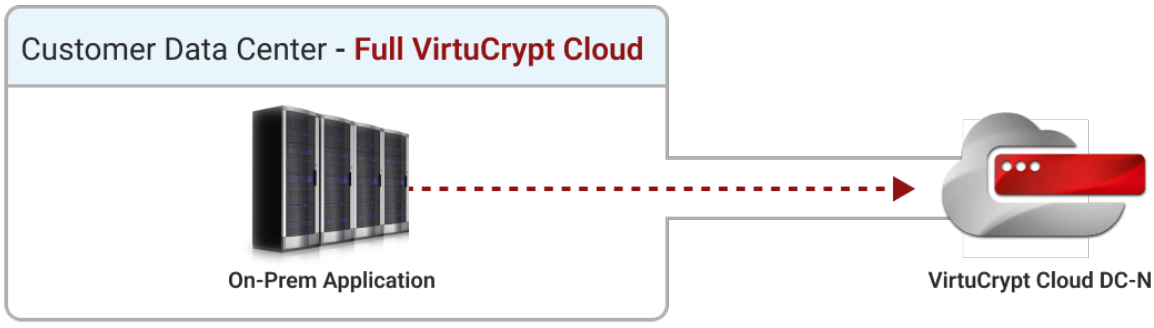
Hybrid models also provide failover, in which cloud HSMs only process traffic when on-premises HSMs are unavailable. Another advantage of hybrid infrastructures is scalability. If an organization is faced with unexpectedly high volume, cloud HSMs can supply extra capacity to prevent slowdowns or outages.



FULL VIRTUCRYPT CLOUD

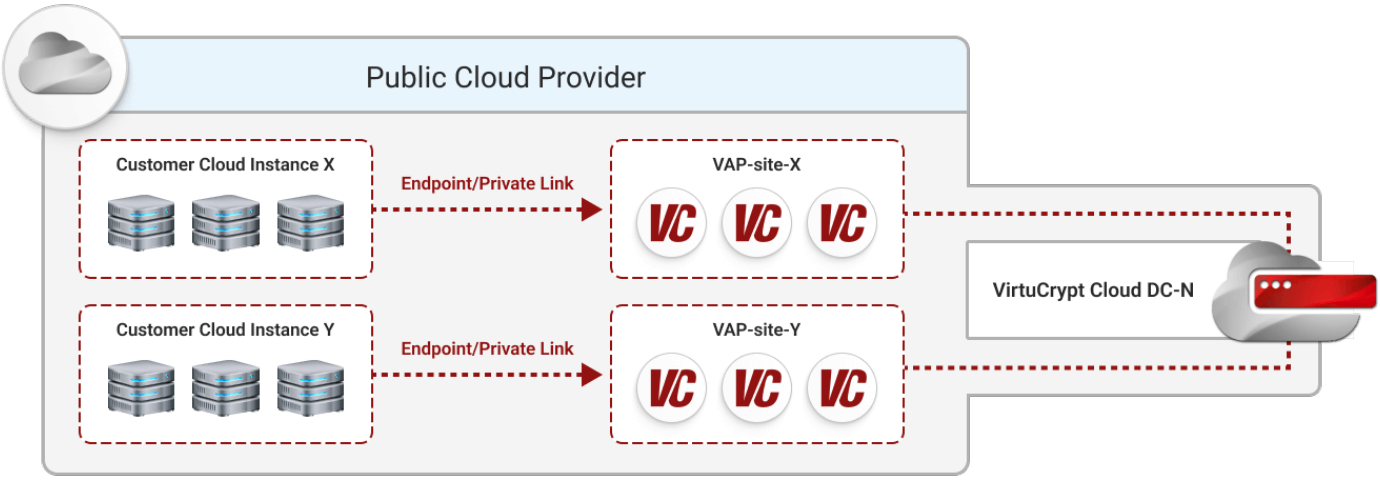
In a full cloud model, an organization hosts their entire HSM ecosystem within VirtuCrypt. With VirtuCrypt, organizations can spin up cloud HSMs on-demand with the full encryption and key management capabilities of a physical HSM. These organizations reap the benefits of hosting their HSMs in the cloud – 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.

CLOUD PAYMENT HSM FUNCTIONALITY OVERVIEW: PAYMENT ACQUIRING

PIN TRANSLATION & VERIFICATION

Organizations can configure VirtuCrypt cloud payment HSMs to translate and validate PIN blocks. The cloud payment HSMs execute the 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 cloud payment 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

EMV (originally Europay, Mastercard, and Visa) has become the standard when issuing payment cards. As such, 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 cloud payment HSMs to quickly receive validation of EMV card transactions prior to approving funds for a purchase.

MAC GENERATION & VERIFICATION

You can eliminate the complexity and risk of key management by centralizing authorization processes into VirtuCrypt. Ensure strong data integrity and authenticity by generating and verifying message authentication code (MAC) in cloud HSMs specifically configured for the payments industry.

Our cloud payment 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)

KEY MANAGEMENT & DERIVATION

Proper encryption key management for network keys is vital to any payment processing environment. VirtuCrypt's next-generation cloud payment 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 validate card security codes (CVC, CVV, CVC2, CSC) from major payment providers including Visa, MasterCard, Discover and American Express with next-gen cloud payment 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 cloud payment 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 cloud payment HSMs support 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

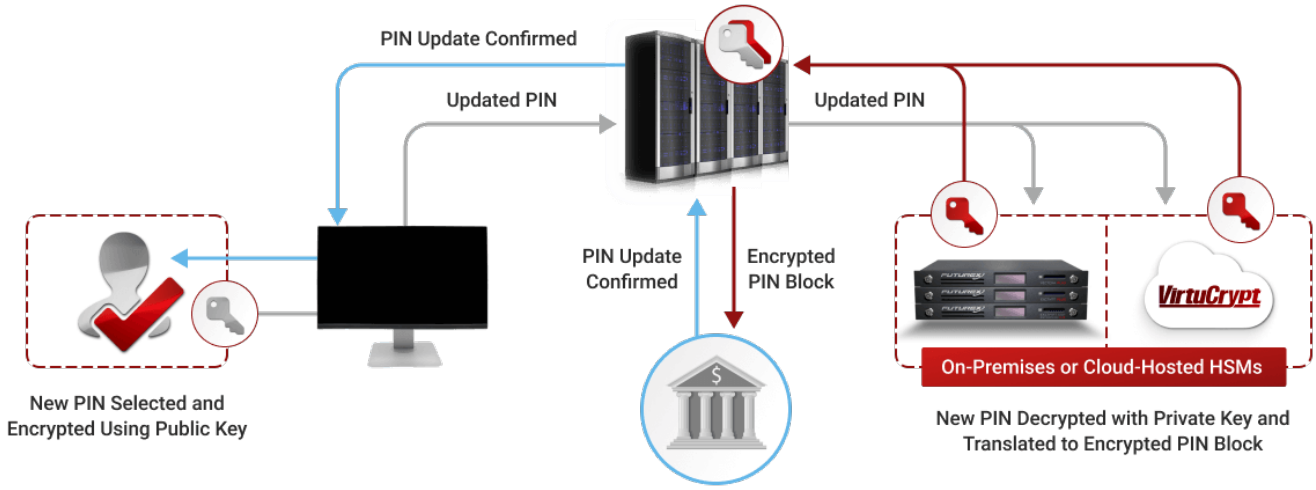
CLOUD HSM FUNCTIONALITY OVERVIEW: CARD AND MOBILE ISSUING

PIN (PIN AND OFFSET GENERATION)

VirtuCrypt next-generation cloud payment HSMs can generate PIN and PIN offset values during payment card issuance. All major PIN generation algorithms are supported. Offsets can be generated from clear PINs or encrypted PIN blocks. 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 new methods of accountholder authentication and PIN management has increased. This increase in demand coincides with a growing number of devices and access points to payment systems and ecommerce. Just as solutions have been introduced into the market for software-based PIN entry, 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 is encrypted using the web browser or app's RSA public key. It is then sent to the VirtuCrypt service instance. Within its 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 stored in the issuer's PIN database for future use.

EMV KEY GENERATION AND DERIVATION

Cloud payment 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 (PKI).

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 cloud payment 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.

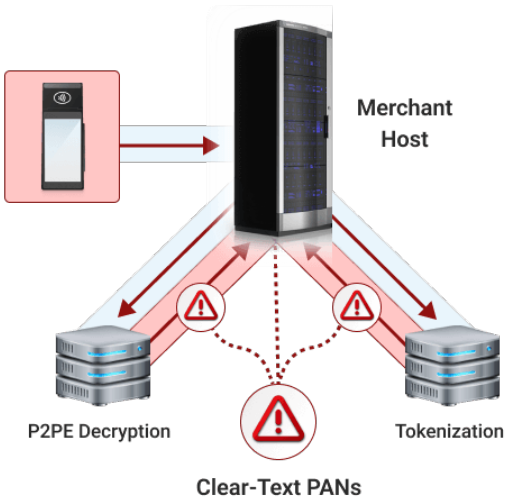
CLOUD HSM FUNCTIONALITY OVERVIEW: POINT-TO-POINT ENCRYPTION

Point-to-Point Encryption, also known as P2PE, is a security standard according to which cardholder data is encrypted at the point of interaction (POI) or point of sale (POS). The encrypted data is sent to the transaction processor, where it is decrypted within the confines of an HSM, 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)

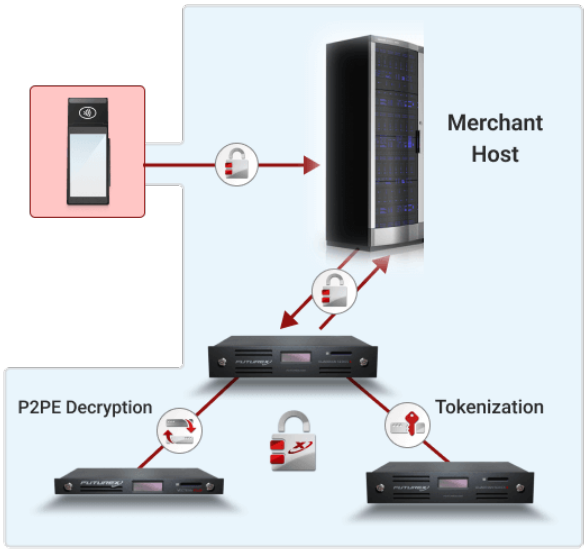
After cardholder data is encrypted at a Point-of-Sales (POS) or ATM terminal, data is securely transmitted and decrypted utilizing related keys generated/housed by a cloud HSM (Excrypt Plus) under a secure TLS management platform (Guardian Series 3).

Typical Non-Futurex Environment



- Merchant is responsible for clear-text PANs
- Cumbersome, multivendor integration efforts
- Partially reduced PCI DSS compliance scope

Futurex VirtuCrypt Environment



- Merchant never handles clear-text PANs
- Easy, single-vendor integration process
- Reduced PCI DSS compliance scope

= PCI Compliance Scope = Reduced PCI Compliance Scope

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 cloud payment 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

Payment 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 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, 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 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 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 next-generation cloud payment HSMs including Bring Your Own Key, key agent services, and HSM-generated keys.

BRING YOUR OWN KEYS (BYOK)

Organizations that need to self-manage encryption keys can confidently manage keys in VirtuCrypt next-generation cloud payment HSMs using the Bring Your Own Key (BYOK) method. 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 cloud payment 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 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 (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.

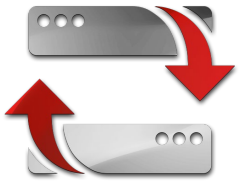
FUNCTIONALITY

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

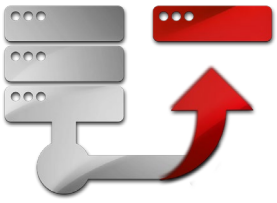
VirtuCrypt cloud HSMs offer different levels of throughput which can be scaled according to need, starting at 50 transactions per second (TPS) and scaling to 250 TPS, 1,000 TPS, and beyond. Throughput is measured using 3DES PIN block translations. A higher throughput will allow for increased efficiency, 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 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 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
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 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.

SUMMARY

Futurex's next-generation cloud payment 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.

Whether they focus on acquiring or issuing, next-generation cloud payment HSMs offer flexibility and security, with the benefits of a cloud-based environment.

VirtuCrypt cloud payment 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