UNBOUND

( MATH OVER MATTER )

# Control, manage and protect keys from across all sites and workloads from a single pane of glass.

## Software-Defined Key Protection & Key Management

Unbound has decoupled trust from infrastructure. Based on **cryptographic breakthroughs** that draw strength from math (not matter), Unbound Key Control (UKC) is the first solution to offer a truly abstracted key management that meets the high levels of security once only attainable through hardware-based perimeter-centric models. Built upon Unbound's platform-agnostic **vHSM technology**, UKC can be deployed across your entire decentralized hybrid cloud and geo-distributed environments without disrupting existing application workflows. All key management and user management operations are fully automated using a REST API, giving you the ability to scale up or down, create partitions and users, register clients and revoke keys immediately across your entire global infrastructure.

**Stretch the boundaries of your security infrastructure to centrally manage all crypto keys, secrets and certificates across your network (including BYOD, public cloud and virtual machines) from a single pane of glass.**

## Breaking the Boundaries of Traditional Key Management & Protection

Locking keys within physical boundaries was generally accepted as the safest method of key protection. It protects against the single point of failure created by traditional key-management methodologies, where keys often appeared in the clear during their lifecycle – while being generated, in use, or at rest. Therefore, the best way to protect keys from being compromised was to lock them within dedicated hardware.

## Mathematically Proven Guarantees of Security

Unbound Key Control safeguards key material with mathematically-proven security guarantees:

- Each private key is stored in two separate random shares. These shares are never combined at any point in time.
- The key material **never exists in the clear** either in memory, disk or over the network **at any point throughout the key lifecycle**, including key creation, in-use (e.g. for signing, decryption) and at-rest.
- Obtaining key material requires compromise of **both** pair nodes **simultaneously**.

### Benefits & Features

- Mathematically proven security guarantee – the key material never exists in the clear throughout its lifecycle including creation, in-use and at-rest
- Multi-site, Multi-Cloud Hybrid IT support: Control and manage keys anywhere – on-premise, in the cloud – any cloud service provider
- Fully elastic and scalable enterprise key management
- Full deployment, provisioning and management automation
- Support all industry standard HSM and Key Management APIs as well as all standard crypto algorithms
- REST APIs for crypto and management for superb developer experience

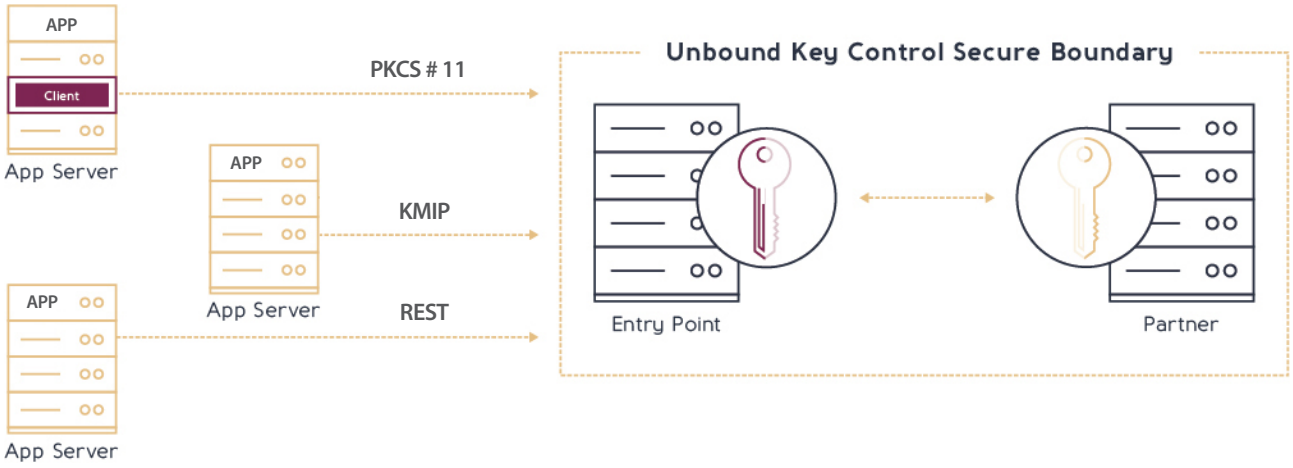
### Use Cases

Unbound Key Control supports any General Purpose HSM and KMIP use cases including:

- Database Encryption
- Application Level Encryption
- Code Signing
- Public Key Infrastructure
- Authentication
- Document Signing
- SSL/TLS

## Non-Continuous Secure Boundary – a New Dimension for Security

The UKC system is comprised from one or more pairs of standard servers that are installed and managed by the customer. Each of these pairs is comprised of an Entry Point and a Partner. Together, they form the secure boundary of the UKC. Application servers within the network connect to the entry point for consuming cryptographic services for the keys that are managed within the UKC.




## Eliminating the Single Point of Failure

Unbound Key Control eliminates this single point of failure by ensuring that your most sensitive keys never exist in the clear at any point in their lifecycle – not even when generated, while in use or while at rest. This feature stretches the secure boundary far beyond the traditional physical casing, creating endless options for separation of the Key Control nodes such as:

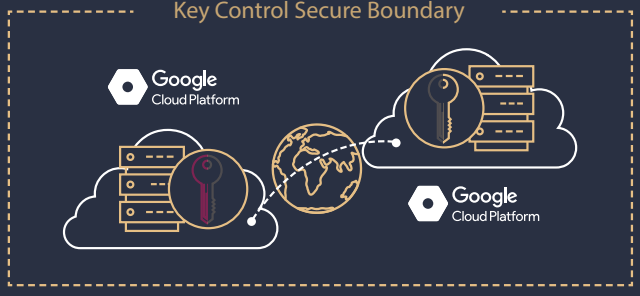
- Separate locations/entities, e.g. networks, geographical locations, cloud availability zones, cloud service providers, cloud/on-premise sites
- Separate credentials and access controls
- Separate software stacks (e.g. different operating systems)

Best practices and hardening guidelines for secure UKC deployment are provided by Unbound to ensure secure setup for any environment or use case.

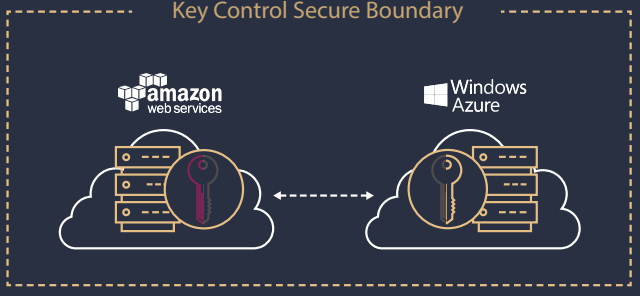
# Key Management is now Simple – for the Cloud, On-premises and Hybrid Environments including VMs and Containers

Unbound Key Control is the first solution to truly abstract key management, as vHSM technology allows secure management of cryptographic keys on any standard platform including physical/virtual machines and containers. Various deployment options are available with full flexibility on choosing location of nodes for the Key Control cluster. For example, you can install the system with one node on your on-premise data center and one on your cloud service provider of choice, allowing usage of keys by any cloud application but allowing you full auditing and control, ensuring key material is never in the clear either in the cloud or on-premises.

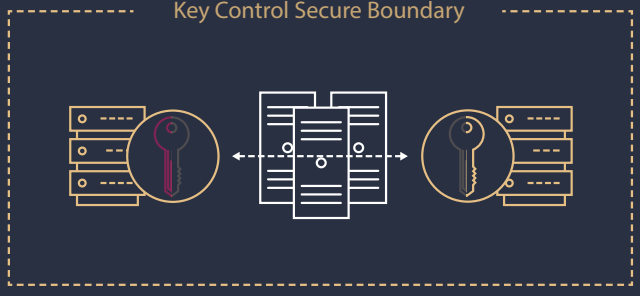
### Same Cloud Provider, Different Regions / Availability Zones



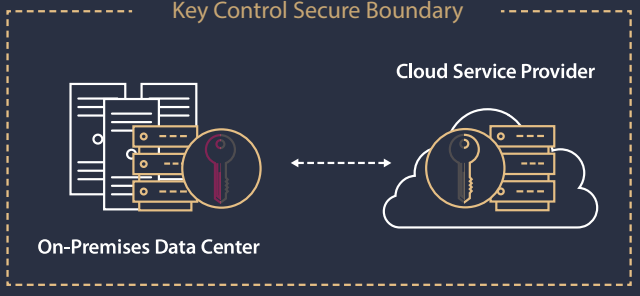

### Different Cloud Providers




### On-Premises Data Centers

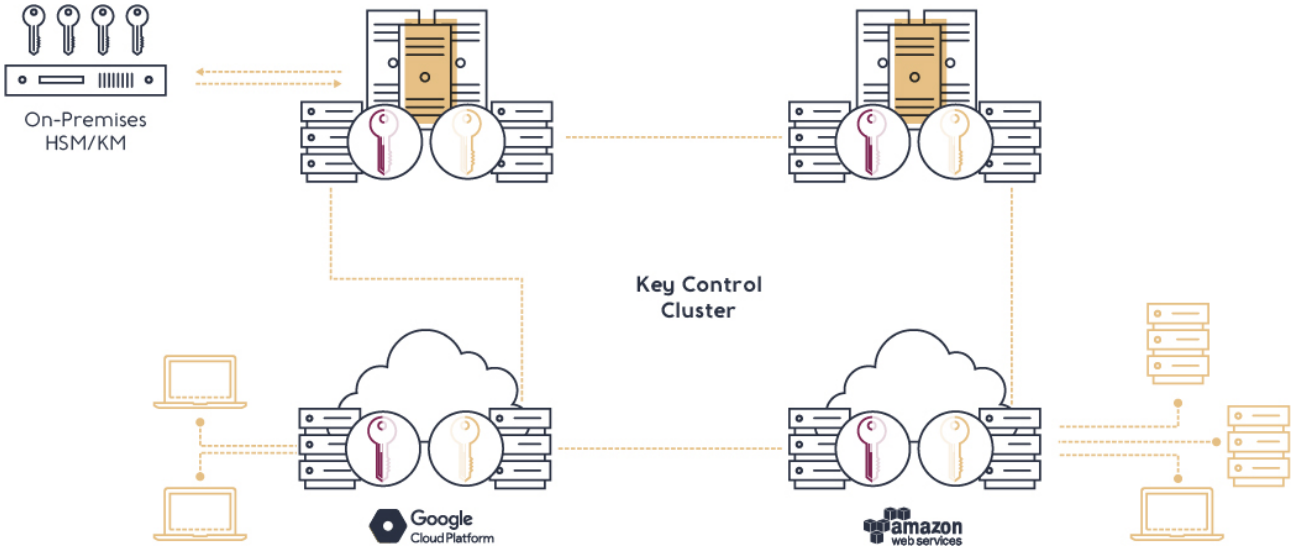



### Hybrid Deployments



## No More Silos – One Cluster to Manage Them All

Unbound's pure software key management supports HSM crypto APIs and includes a KMIP server, which allows you to protect and manage all keys from all your workloads: on-premise, in the cloud – with any cloud service provider (CSP). You can use a unified cluster of UKC to manage all your keys from one central management system. Keys are synced automatically between all different sites and workloads to ensure no more key management in silos.




## Transparent Integration & Automation of the Key Management Infrastructure

UKC can be deployed easily without disrupting the existing workflow of applications. Unbound supports full key lifecycle management including partitioning, Control Your Own Key (CYOK), key generation, wrap/unwrap, renewal, archiving, rotation and revocation of all types of standard cryptographic keys.

UKC is fully transparent to the calling application and supports all crypto APIs such as KMIP, PKCS #11, Microsoft CNG, OpenSSL engine, JAVA JCE, Unbound SDK for. NET, and Python PHP.

UKC includes a command line interface (CLI) and REST APIs for crypto operations and key management. These tools enable fully automating system installation, deployment, ongoing operation, and management, saving you and your team precious time otherwise spent on manual, labor-intensive tasks.

## Embrace the Future: Elastic, Scalable & Agile Cryptography

Unbound Key Control is future-ready so your cryptography infrastructure can be too. Scalable and elastic key management lets you adapt to meet your changing needs during peaks, lows, and every point in between. Without the need for dedicated hardware, UKC software supports automated provisioning across all your applications and business lines and can be deployed as the standard cryptographic infrastructure across your entire organization.

With the emergence of quantum computing and blockchain on one hand and crypto vulnerabilities on the other, changes in crypto are happening faster than ever. Unbound Key Control is a crypto-agile system that ensures you will be up and running the latest crypto, with update cycles measured in days to weeks, not months or years[1].

[1] Asymmetric PQC decryption in hybrid mode, in accordance with NIST issued guidelines for PQC standardization (http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html)

# Technical Specifications

## Operating Systems and Platform

- Windows, Linux
- Any standard virtual/physical machine
- Cloud IaaS: All cloud service providers including AWS, Azure, Google Cloud Platform, SoftLayer
- PaaS and Containers: Docker, Kuberentes, Pivotal Cloud Foundry

## API Support

- PKCS#11, Java (JCE) Microsoft CNG, OpenSSL, REST
- KMIP server providing KMIP services to any KMIP client up to KMIP 1.2 inclusive

## Cryptography

- Full Suite B support
- Asymmetric: RSA (key sizes: 2048, 3072, 4096; modes: RAW, PKCS1, PSS, OAEP), Elliptic Curve Cryptography (ECDH with P256 | P384 | P521 curves, ECDSA with P256 | P384 | P521 | SECP256K1, EdDSA with ed25519 curve, ECPRF/ECPWD with P256), Schnorr signatures over SECP256K1)
- Symmetric: AES (key sizes: 128, 256, 512; modes: SIV, XTS, ECB, CBC, OFB, CFB, CTR, CCM, GCM, NIST_WRAP, CMAC, GMAC), Triple DES (key size: 168; modes: ECB, CBC, OFB, CFB, CTR)
- Hash: SHA (SHA-1, SHA-256, SHA-384, SHA-512), HMAC (128-256)
- Generic secret management
- Additional modules: Application level encryption, password verification, combined key and password encryption, Post-Quantum Crypto (PQC)

## Client Authentication

- Server level authentication: using client certificate, mutually authenticated TLS 1.2
- Application level authentication (optional): SAML Authentication Scheme, Active Directory

## High Availability

- Active/Active and Active/Passive modes
- Automated load balancing by Key Control Client [2]

## Management & Administration

- Admin Console via Web UI
- Command Line Interface (CLI)
- Full management REST API
- Full backup and restore functionality, no additional devices required
- Highly configurable Role Based Access Control (RBAC) model
- Multi-admin and quorum authentication – supported remotely over LAN/WAN, no physical access is necessary

## Performance Specifications

- Cryptographically isolated partitions: up to 100,000,000
- Keys: bound by disk space only
- Simultaneous connected hosts: up to 4,000
- Capacity in transactions per second (TPS) for sample configurations:

| | Basic KEY CONTROL Unit | Sample 'S' Cluster | Sample 'M' Cluster | Sample 'L' Cluster |
|---|---|---|---|---|
| | 1 pair of servers, 1 core per server | 2 pairs of servers, 1 core per server | 4 pairs of servers, 1 core per server | 16 pairs of servers, 1 core per server |
| **RSA-2048** | **100** | **200** | **400** | **1,600** |
| **ECDSA P256** | **20** | **40** | **80** | **320** |
| **AES 256 GCM** | **15** | **30** | **60** | **240** |
| **ECDH p256** | **150** | **300** | **600** | **2,400** |

Capacity is derived from the number of CPU cores in the KEY CONTROL cluster. Scaling the Basic KEY CONTROL Unit is done by scaling up or scaling out, and is fully linear, as illustrated in the sample clusters above

## Security Certifications

- FIPS 140-2 Validated
- Common Criteria (in process)

[2] Not applicable for KMIP as it is clientless.

[3]Capacity was tested with 2.1GHz CPU cores; using a faster CPU would result in higher performance figures.