UNBOUND

(MATH OVER MATTER)

Unbound Key Control For Azure Marketplace

The Secure-As-Hardware Software With a Mathematical Proof

Unbound Key Control (UKC) is the first software-only key management and key protection system that delivers hardware-level security guarantees. Unlike traditional software approaches that rely on obfuscation algorithms, whitebox cryptography, or security-by-obscurity techniques, UKC draws its strength from Unbound's vHSM (Virtual Hardware Security Module) technology. This solution is backed by a rigorous security proof made possible by mathematically-proven multiparty computation (MPC) algorithms. UKC combines the high-level security once only attainable with hardware with the agility, scalability, and efficiency of software – crucial attributes for today's digital businesses.

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.

Eliminating the Single Point of Compromise

UKC 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, in use , or at rest. With UKC key material is never whole. Rather, each key exists only as two random key shares stored in separate locations. All operations take place without ever uniting the key shares. By eliminating the single point of failure, UKC can stretch the secure boundary far beyond a traditional physical casing.

Benefits & Features

- Fully-virtual key protection and management – now available from Azure Marketplace in a pay-as-you-go model
- Mathematically-proven security based on Unbound's vHSM technology – key material never exists in the clear throughout its lifecycle including creation, in use, and at rest
- Full control of your own key in the public cloud
- Fully-elastic and scalable enterprise key management
- Extendable to support any multi-site, multi-cloud hybrid cloud
- Full deployment, provisioning, and management automation
- Support for all industry-standard HSM and key-management APIs as well as all standard crypto algorithms
- REST APIs for crypto operations and management for superb developer experience

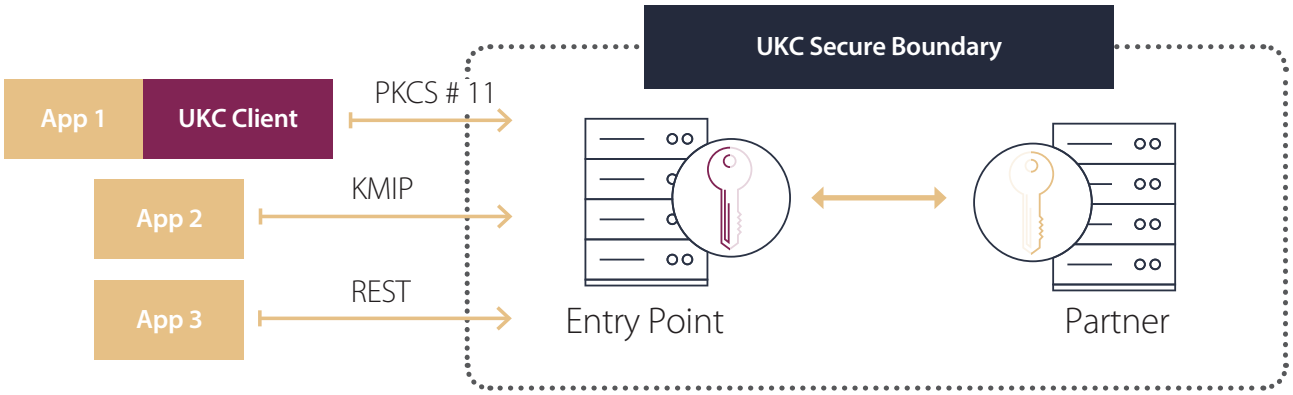
Use Cases

Unbound Key Control supports general-purpose HSM and KMIP use cases including:

- Database encryption
- Application-level encryption
- Code signing
- Blockchain key management
- Public-key infrastructure
- Authentication
- Document signing
- SSL/TLS
- Cloud application security broker (CASB)

Non-Continuous Secure Boundary – a New Dimension for Security

Each UKC system includes one or more pairs of standard servers that a customer installs and manages. Each of these pairs includes an entry point node and a partner node that each hold one share of a key. Together, these servers form the secure boundary of UKC. Application servers within the network connect to the entry point for consuming cryptographic services for the keys that are managed within UKC. All connections between UKC nodes and between entry points and application servers are protected using mutually-authenticated TLS.



Azure Deployment Options

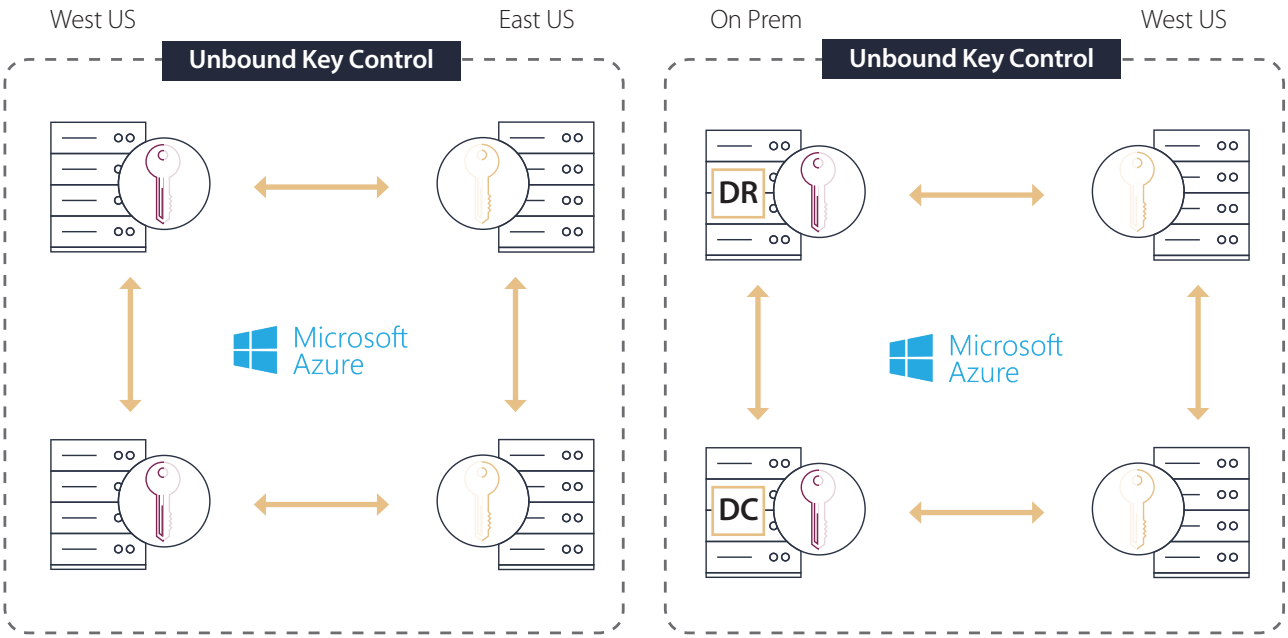
UKC is now available from Azure Marketplace in a pay-as-you-go model for deployment on a standard Azure virtual machine. You have the flexibility to choose UKC node locations in one or more Azure regions and to rapidly create an Azure deployment that meets your unique requirements.

Unbound Key Control can be deployed in two different topologies, described in detail below:

- Both nodes deployed on Azure
- One node deployed on premises, one node deployed on Azure

Control Your Own Keys (CYOK) — Azure Cloud

- **Deployment** – both UKC nodes are deployed in the Azure cloud.
- **Key Material** – is never present in the cloud in any form. All crypto operations, including key generation and key usage, occur without reconstructing the full key, even in memory.
- **High Availability (HA)** – UKC fully supports adding pairs for redundancy and supports HA in any Azure region or availability zone across the globe. Keys automatically synchronize between all nodes of the UKC cluster regardless of the cluster's location.
- **Backup and Restore** – are a simple process that can be fully automated. The customer fully controls all backup and restore processes without any involvement of the cloud service provider.
- **Auditing** – while this setup allows cloud applications to use keys, it provides you with full auditing and control. This ensures that key material is never in the clear, either in the cloud or on premises.
- **Smooth and Protected** – customers get ease in deployment and installation, as both nodes are in the Azure cloud, and a mathematically-proven guarantee that key material is never exposed in the cloud.



CYOK Hybrid

This deployment option, appropriate for the most-sensitive use cases, includes all the benefits of CYOK topology. Keys are fully resilient and cannot be compromised by any adversary in the cloud – whether the adversary is a rogue insider/admin or a subpoena. It provides unmatched levels of control for cryptographic keys in the cloud in an easy to deploy and maintain solution without any hardware dependencies.

Once deployed in one of the modes described above, the system can be used for any general purpose HSM or key management use case, such as code signing, DB encryption (TDE/always encrypted), SSL/TLS, Blockchain key management, CA/PKI, tokenization, OPE, FPE, and VM encryption.

UKC Integrations

UKC is easily deployable without disrupting existing application workflows. 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, SDK for .NET, Python PHP, and more.

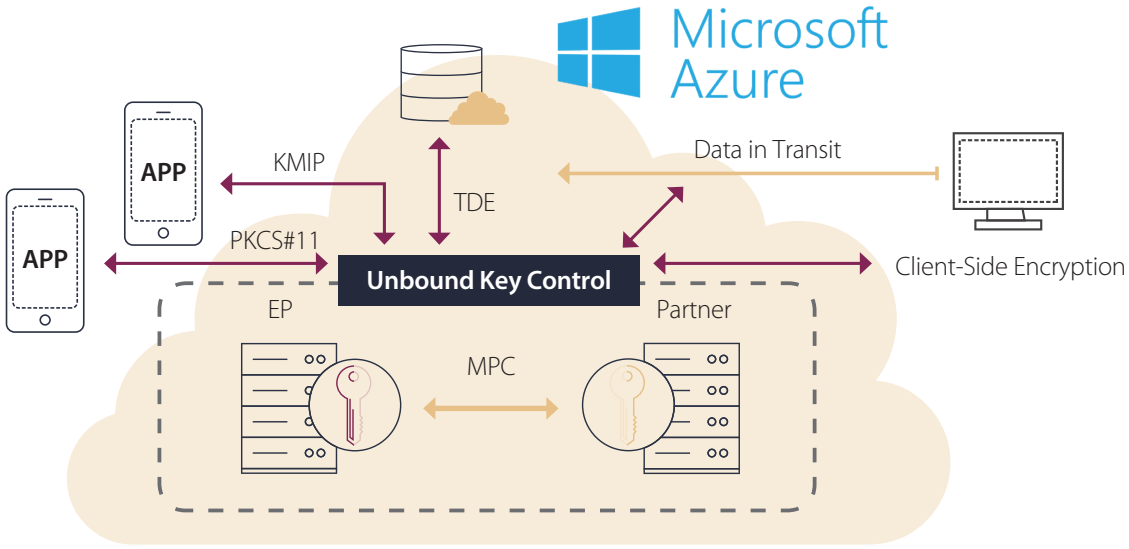
UKC includes a command line interface (CLI) and REST APIs for crypto operations and key management. These tools enable fully automating system installation, deployment, ongoing operation, and management, saving you and your team precious time otherwise spent on manual, labor-intensive tasks.

Azure Services Integrations

Unbound Key Control provides the following integrations with Azure native services:

- **Encryption in Transit** – secures your data when it transfers into or out of Azure Storage to prevent a wide range of man-in-the-middle attacks. UKC supports integration with HTTPS protocols for transit encryption.
- **Encryption at Rest** – protects data stored in databases from threats such as access by a rogue admin or malware exfiltration. UKC supports integration with Transparent Data Encryption (TDE) for SQL Server on Azure VM (IaaS).
- **Client-Side Encryption** – encrypts data before it transfers into Azure Storage in a client application and decrypts data after it transfers out of Storage. This protects data during the entire transfer, from on premise to the cloud.

Unbound is currently working on additional integrations with Azure native services.



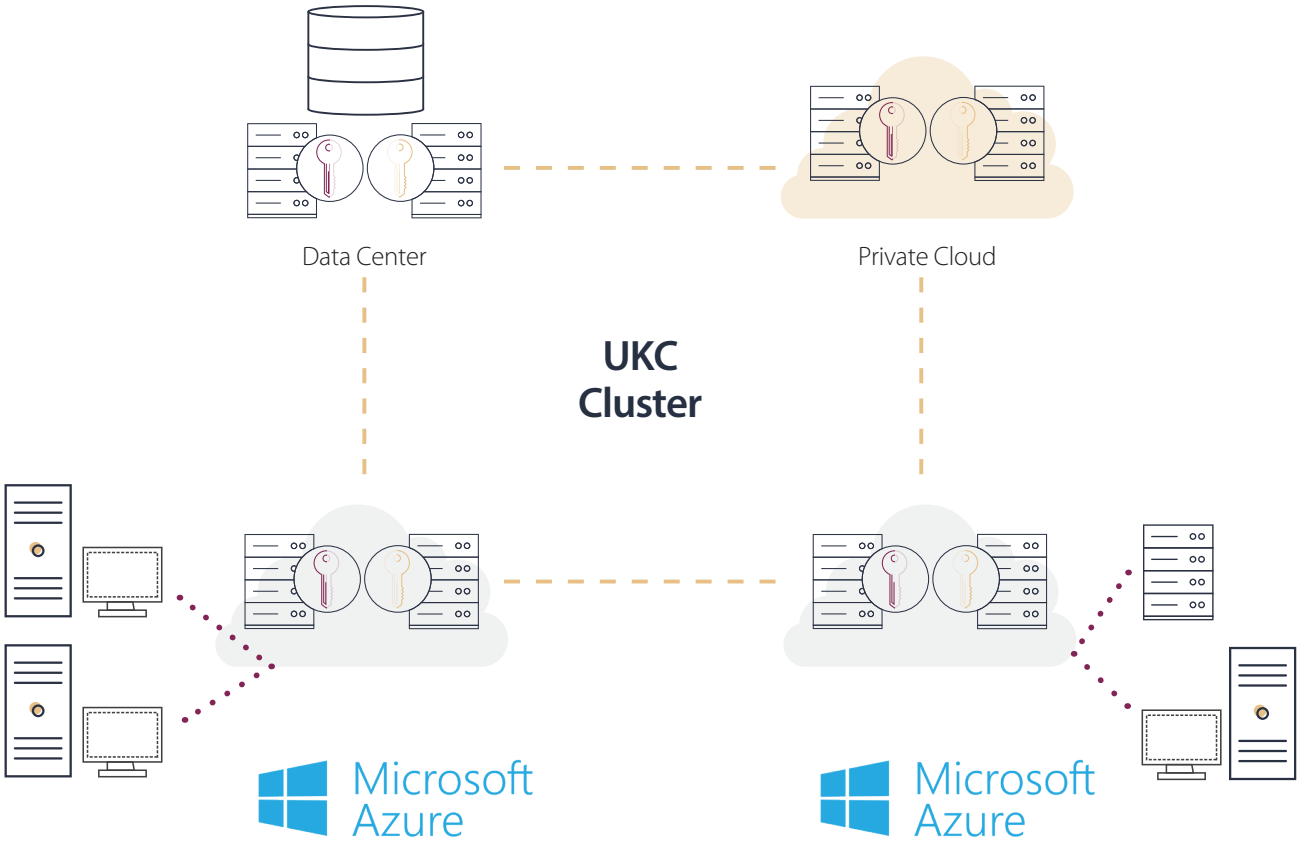
Elastic & Scalable Cryptography

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].

No More Silos – One Cluster to Manage Them All

Unbound's software-only key management supports all standard HSM crypto APIs and includes a KMIP server, letting you protect and manage all keys from all your on-premises workloads together with cloud workloads from any cloud service provider (CSP). You can now use a unified cluster of Unbound Key Control to manage all your keys from one central management system. Keys automatically sync between all your different sites and workloads to ensure no more key management in silos.



[1] Requires additional licensing.

Technical Specifications

Operating Systems and Platform

- Hardened Linux (Unbound proprietary)
- Deployment on Azure Standard_F1s VM (1 CPU, 2 GB RAM, 4 GB SSD disk)

API Support

- PKCS #11, Java JCE, Microsoft CNG, OpenSSL, REST
- KMIP server providing KMIP services to any KMIP client up to KMIP 1.3 inclusive

Cryptography

- Full Suite B support
- Asymmetric: RSA (key sizes: 2048, 3072, 4096; modes: RAW, PKCS1, PSS, OAEP), elliptic curve cryptography with P256 | P384 | P521 curves
- Symmetric: AES (key sizes: 128, 256; modes: SIV, XTS, ECB, CBC, OFB, CFB, CTR, CCM, GCM, NIST_WRAP, CMAC, GMAC), Triple DES (modes: ECB, CBC, OFB, CFB, CTR)
- Hash/HMAC: SHA-256, SHA-384
- Generic secret management
- Application-level encryption

Host Authentication

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

Management & Administration

- Browser-based admin console
- Command line interface (CLI)
- Comprehensive 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

Performance Specifications

- Cryptographically-isolated partitions: up to 5 [2]
- Keys: virtually unlimited, bound by disk space only
- Simultaneous connected clients: up to 1,000 [3]
- Capacity in transactions per second (TPS) for basic Azure Marketplace configurations:

Encryption Algorithm	Per Basic UKC Unit (1 pair of servers, 1 core per server)
RSA-2048	100
ECDSA-P256	25
AES-GCM 128 single block	200

Unbound Key Control deployed in an Azure environment enables reaching any desired performance level (in accordance with a linear scalability model) by deploying additional nodes.

Security Certifications

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

[2] Requires additional licensing.
[3] Requires additional licensing.