unbound security

Unbound CORE

Cryptographic Orchestration Reimagined for the Enterprise

Whitepaper

Prof. Yehuda Lindell,
CEO and Co-founder

Introduction

The Transition of Cryptography in Securing Digital Environments

There is no doubt that cryptography has played an important role in the digital revolution. For just one simple example, eCommerce could not have happened without public-key cryptography that enables payment credentials (e.g., credit card numbers) to be sent securely over the Internet. However, the role of cryptography in securing the digital world of 20 years ago is very different to its role in enterprises today. Cryptography has transitioned from an important yet marginal tool to a set of methodologies that are central to securing enterprise systems.

In the past, the belief was that attackers could be kept outside of our private networks and data centers. As a result, encryption was primarily needed when data was being sent between sites (encryption of data-in-transit). Encryption was sometimes also used to encrypt storage (encryption of data-at-rest), but mainly due to the fear that the physical media holding the data could be stolen or in order to prevent leaks when disks and tapes were disposed of. Today, it is well understood that attackers are everywhere, and we cannot rely on having a strong perimeter to keep them out. This requires organization to deploy zero trust solutions, where security is preserved even when attackers do manage to get into the network.

The challenge is further compounded when we understand that our networks themselves are far less under our control than in the past, specifically due to the continued demand to digitize data.

Bring your own device (BYOD) initiatives required organizations need to support a myriad of devices of different types, including devices belonging to employees. In addition, IT infrastructure no longer resides in a local data center but is spread across multiple data centers and clouds. All of this needs to be managed remotely, and with far greater speed than in the past. Business needs are primary, and IT and security must support business agility, not impede them. This means the ability to quickly support business initiatives, cloud migration, new standards and infrastructure, and more.

Since we can no longer rely on keeping the attackers out of our networks, today cryptographic solutions play a far more central role in security than ever before. Cryptography is used in authentication, encryption of data in many different scenarios (in databases, on storage, as virtual machines), for signing on business transactions to ensure integrity, for signing on code to prevent the propagation of malware, to protect new digital assets (like crypto assets), and much more. As we will see, the necessity to deploy cryptographic solutions across the enterprise, at the pace needed by business, brings with it many challenges.

A Fragmented Cryptographic Space

One of the challenges of the field of cybersecurity is that it includes many different techniques and solutions that need to be seamlessly used together. Many of these tools, like firewalls, anomaly detection, honeypots, anti-virus and anti-malware, sandboxing, data loss prevention, and more, have nothing at all to do with cryptography. However, there are also many different types of security solutions that do utilize cryptography in an inherent way, and these are very diverse as well.

There are multiple ways of authenticating humans to provide or prevent them access to systems, including passwords, OTPs (tokens, SMS, mobile), smartcards, federated authentication (e.g., via SAML), and more.

There are also many protocols to authenticate machines and protect the communication between them, — including SSH, TLS and IPsec, — which in turn rely on a PKI that needs to be managed. Multiple encryption solutions are needed for encrypting storage, VMs, databases and more which need to be supported in on-premise data centers and often also in multiple clouds. Throw in code signing (necessary for anyone developing any code, which is almost every enterprise today), and possibly new initiatives in the area of crypto assets, and the cryptographic diversity is messy and overwhelming.

This is all compounded by the fact that all cryptographic solutions rely on secret keys, and all of those keys need to be managed, very often with different management systems and consoles. There are different management systems for different hardware security module (HSM) vendors, different cloud key management systems (KMS) and cloud HSMs, as well as keys used in home-grown DIY solutions. In addition, the management of keys in HSMs, KMSs and so on is separate from the management of keys for authenticating users (e.g., smartcards, OTP tokens, etc.). As a result, managing all of these is a nightmare. First, administrators need to learn many different systems, increasing the required headcount and cost. Second, this impacts security, since it is very difficult to deploy consistent company-wide policies across diverse systems (that sometimes don't even offer the same capabilities). Third, this results in a lack of visibility across the organization and makes it hard to obtain a single audit of all operations, with well-known ramifications. It is not impossible to achieve a good enough result, but it is extremely hard and so it invites mistakes and very often important administration tasks are just not carried out.

In general, the current cryptographic space is highly fragmented. Multiple point and siloed solutions result in management pain, lack of visibility, agility, and flexibility with the added high cost of deployment in different environments.

New Settings and Threats Require New Approaches

Today's digital landscape and the new threats that confront us require enterprises to adopt a new approach to deploying and managing the multitude of cryptographic security solutions that they have. The new approach requires a transition on multiple levels:

- **From hardware only to hybrid hardware and software:** Legacy key protection relied solely on hardware solutions (like HSMs, smartcards and tokens). In today's environments where everything is virtualized and much is remote, and enterprises are moving more and more to hybrid and multi-cloud deployments, pure hardware solutions constitute a significant obstacle. As a result, software solutions for key protection with strong guarantees are needed to replace and complement existing hardware solutions.

- **From siloed to unified key management:** Legacy key protection and management was comprised of multiple different solutions for different business problems and different environments. A unified approach with one platform that can support all cryptographic solutions in any environment is needed today.

- **From disparate to integrated key management and key protection:** Legacy key protection provides only basic management, and legacy dedicated key management solutions are often siloed and not integrated with key protection. Indeed, the notions of key management and protection are often used synonymously, although they are very different. Key protection refers to preventing the key from being stolen, and there are multiple hardware and software solutions for this; we call these solutions key stores. Key management refers to the administration of these key stores and the keys within, including security aspects like access control, and key size and key rotation policies. However, when they are separate solutions, policies are enforced at the key manager level only and not at the key store, making it possible to bypass them. A unified platform that provides integrated key protection and management is needed.

- **From key theft to key misuse prevention:** Legacy key protection solutions address the problem of key theft only. There is no doubt that the security risk due to cryptographic key theft is the greatest.

However, the problem of key misuse – where an attacker breaches a machine that is authorized to carry out operations – is not adequately addressed in existing solutions. Today, key misuse must be addressed as an integral part of key protection.

- **From rigid to agile infrastructure:** Legacy key protection and management solutions are rigid and slow moving. In today's agile environments, cryptographic infrastructure needs to adapt quickly. Cryptography standards are continually changing: updates need to be rolled out quickly, new threats need to be considered (like the possibility of quantum computers appearing over the coming 1-2 decades), and new problems need to be solved (like PII tokenization and format-preserving encryption to protect data while in use in existing applications). Today's cryptographic infrastructure needs to support agility.

- **From slow to fast deployment:** Legacy cryptographic solutions that relied on solely on hardware were slow to deploy. In today's business environment, enterprise security teams need to offer on-demand cryptographic services internally in order to quickly support business initiatives and needs.

In modern environments, cryptography is needed everywhere. However, this cannot work if the cryptographic infrastructure we are using is the same as in the 1990s. The fragmented legacy cryptographic infrastructure does not support modern business needs and is in desperate need of modernization.

Unbound CORE Technology

The aforementioned challenges with legacy key protection and management solutions need to be addressed on three levels. First, modern solutions are needed that are based on openness and transparency and support a collaborative world where different vendors seamlessly coexist. Second, new modern software that works in modern environments using modern computing paradigms needs to be built. Third, a new technological approach is needed to be able to deliver a software key store with proven security guarantees to complement legacy hardware, and to support new security requirements like cryptographically enforced key misuse prevention.

In this section, we will describe this new technological approach. The philosophy behind legacy solutions is to build a fortress around the machine or device that holds key material and prevent any attacker from breaching that machine. In today's zero-trust environments, this is very problematic, especially when considering software-only solutions.

> A completely different paradigm is to protect cryptographic keys and secrets by never having them reside in any single place at any single time (even in memory), and to force an attacker to simultaneously breach multiple machines in order to learn anything.

If this could be achieved, then there would be no single point of security failure, and strong separations between the different machines would make it extremely hard to breach.

This goal may appear to be impossible – how can one carry out cryptographic operations such as decryption or signing, without holding the key? Fortunately, a methodology called *Multiparty Computation (MPC)*, also known as threshold cryptography in the context of protecting keys, is able to do exactly this. Using MPC, the secret key is generated so that it is split into two or more parts called shares, such that all shares are needed in order to get any information about the key. These different shares reside on different servers and devices, so that an attacker would have to breach them all in order to steal the key. MPC protocols enable the different machines holding key shares to interact (running an MPC protocol) so that they receive the result of the operation without revealing to each other anything whatsoever about the key. This means that the key remains fully protected, even while in use.

MPC has been studied in academia for over three decades and has a strong and well-founded theory. MPC protocols have mathematical proofs of security, guaranteeing that an attacker who is unable to breach all machines is unable to learn anything whatsoever about the key, even if the attacker knows the protocols being used and can run arbitrary malicious code in its attempt. More information about MPC can be found in the Unbound white papers: a Basic Introduction to MPC and a Technical Primer to MPC. A more in-depth introduction to MPC for a general computer science audience appears here, and resources for in-depth study of MPC can be found at Unbound MPC Labs.

Unbound CORE – Unified Cryptography Reimagined for the Enterprise

Unbound CORE is a fundamentally new platform-based approach to securing enterprise cryptographic infrastructures. Unbound CORE virtualizes cryptographic key stores (like HSMs and cloud key management systems) and provides a powerful layer of abstraction that provides cryptographic services to applications, wherever they are. The Unbound CORE engine is a distributed environment that builds a mesh of cryptographic key stores of all types, delivering on-demand cryptographic services at the edge. This paradigm has powerful implications, including the ability to manage all key stores in a unified manner, to deploy company-wide policies, to automate tasks like synchronization of keys, and to build a cryptographic firewall for preventing key misuse in Unbound's key store based on MPC, in physical HSMs (on-premise and in any cloud) and in cloud key management services (like AWS KMS and Azure Vault).

Virtualized cryptography. The first step towards defragmentation of the cryptographic space is to make it work like all other software works. Today, almost all environments are virtualized, providing flexibility, agility, better performance, increased efficiency, faster provisioning, improved disaster recovery, lower cost and more. Unbound CORE comes with a new software-enabled key store based on the MPC technology described in Section 2. The Unbound CORE MPC key store can be run in virtual machines or containers, providing all of the advantages of these environments. In particular, it is possible to provide micro-services and make cryptographic key services an integral part of applications, versus remote and out-of-context services using legacy technology. An Unbound key store can be spun-up with only the cryptographic functionality needed now by the application in a **container sidecar**, providing the effect of an HSM inside the application. This means that data doesn't need to be sent remotely, improving both performance and security. The improved security is due to reducing the threat landscape by not sending data remotely and by having the container hold only the necessary cryptographic functionality for that application. This provides the benefits of **edge computing** by bringing the service as close as possible to the application using it. More information about Unbound's MPC key store can be found in The Unbound MPC Key Store white paper.

An illustrative example of the advantages of this approach is Google's integration of Unbound CORE into their External Key Manager (EKM) offering. Google's EKM enables organizations to maintain ownership and control over their cryptographic keys, while using them for encryption in native Google Cloud Platform (GCP) services like Compute Engine, BigQuery and Cloud SQL. When using EKM with a physical HSM that resides in an enterprise's data center, the distance and need to enter and exit the enterprise's network incurs significant overhead. In contrast, Unbound CORE's on-demand key store can be used with one MPC party in GCP and the other in a different cloud provider in the same region. This provides the strong separation and control desired, while providing fast query response. Such an effect can only be achieved by placing the cryptographic services at the edge, where they are most accessed.

Unbound CORE virtualizes cryptographic functionality for any key store, providing the same interfaces and rich APIs for physical key stores, cloud key stores and Unbound's MPC key store. In the same way that a virtual machine separates the software functionality from the bare metal machine it runs on, so too Unbound's virtual HSM provides a unified interface and functionality independent of the physical or software key store being used.

Beyond providing universal APIs, CORE's virtualization means that all clients can authenticate in the same way (e.g., using OpenID Connect), even if the native key stores support different legacy methods.

On-demand cryptographic services. In a virtualized world, spinning up new services on-demand is straightforward and standard practice. This should be contrasted with the legacy world of physical HSMs where procurement and deployment literally take months. Unbound CORE supports on-demand deployment of virtual HSM instances that can support the business agility required to meet the needs of today's modern enterprise.

Mesh technology. In a mesh network, the different nodes (devices of whatever type) are directly connected to each other and communicate freely. This enables them to easily synchronize information, to deal with nodes that fail and are restarted, and more. Existing cryptographic infrastructure (HSMs, cloud HSMs, cloud key management systems and vaults, etc.) do not communicate in such a manner. This means that many operations need to be done manually. Unbound CORE creates a mesh of an enterprise's cryptographic devices and services.

Unbound CORE's MPC key stores form a native mesh network, communicating directly with each other to synchronize policies, administrator operations, cryptographic keys, and so on. Unbound CORE expands the mesh functionality also to historically siloed solutions like HSMs, cloud HSMs and cloud KMSs, by orchestrating the coordination between them. The result is an effective mesh of the entire enterprise's cryptographic infrastructure, greatly simplifying operations and administration.

Unbound CORE transcends borders, and connects key stores of all types (HSM, cloud HSM, cloud KMS and the Unbound MPC key store), with the result being a multi-site, multi-platform, multi-geography and multi-cloud mesh.

High availability. An immediate benefit of Unbound's virtualized cryptographic infrastructure and mesh is the triviality and low cost of achieving high availability and disaster recovery. Multiple virtual key stores can be easily deployed across different geolocations, and Unbound CORE automatically routes requests to other instances in cases of outages.

Key misuse prevention. Existing HSMs do not effectively protect against key misuse, as they only offer basic authentication and authorization mechanisms. Clients of an HSM are machines that are authorized to use certain keys. One only needs to breach or have access to such a machine in order to command the HSM and use its keys. An attacker breaching any machine that is authorized to access an HSM and request cryptographic operations can carry out those operations, exactly like a legitimate application. In some important cases, it suffices to misuse a key once in order to carry out a devastating attack. For example, a single misuse of a root CA key can provide an attacker with a valid certificate that can be used to impersonate legitimate entities in the system, a single misuse of a code signing key can enable an attacker to distribute malware that is accepted by all as valid code, and a single misuse of a signing key for crypto assets is all that is needed to steal all of the funds protected by that key. In addition to the above, a lot of damage can be made by an attacker fraudulently using decryption and other keys. This critical security issue is simply not dealt with by HSMs and other key stores today, beyond verifying that the client connecting is generally authorized. This is a critical flaw in existing cryptographic infrastructure.

Unbound CORE achieves integrated key misuse prevention via two main innovations:

- **Quorum authorization:** Existing key stores like HSMs and KMSs carry out cryptographic operations for any client that is authenticated. This means that an attacker breaching such a client is free to carry out any operation they like. With quorum authorization, it is possible to define a quorum of entities that need to approve an operation. A quorum may be comprised of machines and/or of humans (where humans approve via their mobile or personal computer), and can be flexibly defined (e.g., 3-out-of-5 of one set and 1-out-of-2 of another set have to approve). Human approvers are used for extremely critical operations that happen occasionally (like code signing on a final release or a large transfer of crypto assets), and machine-only quorums can be used even for high frequency operations. Importantly, quorum authorization is cryptographically enforced, and so there is no machine in the network that can be accessed to bypass it.

Quorum authorization can also be used to define maker/checker workflows for business transactions that are cryptographically enforced.

- **Key misuse policy engine:** Unbound CORE enables organizations to define dynamic policies on key usage that are enforced by multiple entities. A policy is a set of rules that governs if an operation is allowed to take place. Importantly, these rules are dynamic and so can leverage external information gatherers and decision makers. Rules can range from basic elements like time of day, location of client and rate limiting to advanced checks like KYC and AML for financial transactions, fraud detection, anomaly detection tools (queried before and not after the operation), and any other security technology or tool. Utilizing quorum authorization, the policy can be cryptographically enforced at multiple points, ensuring that no single element can be bypassed. The result is a policy that can be defined centrally and enforced distributed.

Cryptography firewall. A firewall is a tool used to monitor access to a network and ensure that only authorized traffic is allowed. The key misuse prevention provided by Unbound CORE serves as a cryptography firewall, monitoring usage of cryptographic keys of all types, and ensuring that only legitimate operations are allowed. We stress that the key misuse mechanism cannot be bypassed by directly breaching a machine that issues a request, since the quorum verification is carried out by multiple participants, removing any single point of failure. This is a new paradigm for key protection, and one that fills a gaping hole in legacy solutions.

Management – a single pane of glass. Since Unbound CORE connects to key stores of all types, it provides administrators the ability to manage an entire enterprise's cryptographic infrastructure from a single management console. This provides a unified way of working across different key stores. Administrators can authenticate in a uniform way (e.g., using OpenID Connect, even if the native key store does not support it) and management tasks no longer need to be repeated for each different key store. In particular, this means that it is possible to set companywide policies and ensure that they are enforced globally. Examples of such policies include cryptographic parameters (which algorithms and which key sizes are allowed), key rotation (how often and for which types of keys), access control (who can use what key and for which purpose), and key usage limitations (rate limiting, dependence on time of day, and so on). It is important to understand that not only must administrators today set up such policies separately in multiple different systems, but they may also not even be able to define a fully consistent policy since the policy capabilities are different in different systems. In addition, all operations related to the cryptographic infrastructure (whether they be administrative or key usage related) are centrally logged in a tamper-resistant audit. Connecting this log to a SIEM system provides full visibility into all cryptographic operations taking place across an enterprise, improving threat detection and forensic capabilities.

Unbound CORE provides centralized management for a decentralized system, yielding the best combination possible.

Universal API. Applications can consume cryptographic services using a multitude of standard libraries, like PKCS11, JCA, Microsoft CNG, KMIP and OpenSSL. Unbound CORE provides a single interface between these libraries and key stores. This powerful abstraction enables applications to utilize key stores using any API, irrespective of what API that key store natively supports. For example, using Unbound CORE, applications can use keys in Azure Vault via the PKCS11 or KMIP libraries, even though Azure Vault does not support PKCS11 or KMIP at all. Furthermore, applications that use Unbound CORE API can remain agnostic to whether a key is in Unbound's MPC key store, a physical HSM, a cloud HSM, or any other Unbound supported key store. This provides great flexibility, separating the physical nature of the key store from its usage. In addition to the above, Unbound CORE provides a powerful and simple REST API that can be used from any application language. Unbound's REST API supports the best standard cryptographic methods, removing the onus of choosing which encryption or signing algorithm to use from the developer, also reducing the possibility of mistakes. Unbound's REST API also supports advanced cryptographic methods like tokenization (aka format-preserving encryption).

Crypto agility. The cryptographic world is a very dynamic one. Algorithms become outdated and sometimes even broken, key sizes need to be increased, new standards for how to carry out cryptographic operations are introduced, and flaws are sometimes found with existing standards. As a result, it is crucial that cryptographic infrastructure and code be agile, meaning that it can be quickly updated when flaws are discovered, or new standards are required. Hardware solutions are by definition slow to update, and legacy libraries (like PKCS11) are far from agile. Unbound CORE's MPC key store can be quickly updated as it is software, and its REST API (for all key stores) provides optimal code agility since nothing needs to be changed in the code when algorithms and methods are updated.

Zero-trust cryptography. According to NIST Special Publication 800-207: "zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. ... Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise- owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource." Unbound CORE is particularly suited to zero-trust settings since cryptographic keys are never revealed on any single device, and cryptographic services can be spun up on-demand according to need in any environment and on any device. In addition, the integrated key misuse prevention prevents attackers inside the network and residing on authorized clients from carrying out arbitrary cryptographic operations.

Unbound CORE Multilayered Cryptography

Unbound recognizes that enterprises never have a single cryptographic problem that needs to be solved. As such, the power of Unbound CORE is in the breadth of the platform, providing key management and protection across the enterprise and across all cryptographic infrastructure solutions. Unbound CORE is best understood by considering the three layers of cryptographic infrastructure:

Layer 1– key store foundation: At the foundation of CORE lie different key stores that actually hold the cryptographic key material and carry out operations. Unbound supports its own software-only key store based on MPC, as well as common physical HSMs, cloud HSMs, cloud key management systems, and key stores utilizing secure enclaves. In addition, Unbound CORE can act as external key manager for Google Cloud. Unbound's key misuse prevention capabilities constitute a virtual cryptography firewall around all supported key stores.

Layer 2 – virtualization and key management: This layer of the CORE architecture consists of the CORE virtual HSM, which is an abstract key store so that applications can consume cryptographic services in the same way, independent of the store being used and the environment it is run in (on-premise or any cloud). This layer also provides all of the administrative and management capabilities, including authentication and authorization, policy enforcement, tamper proof audit and more, for all key stores in the foundation layer.

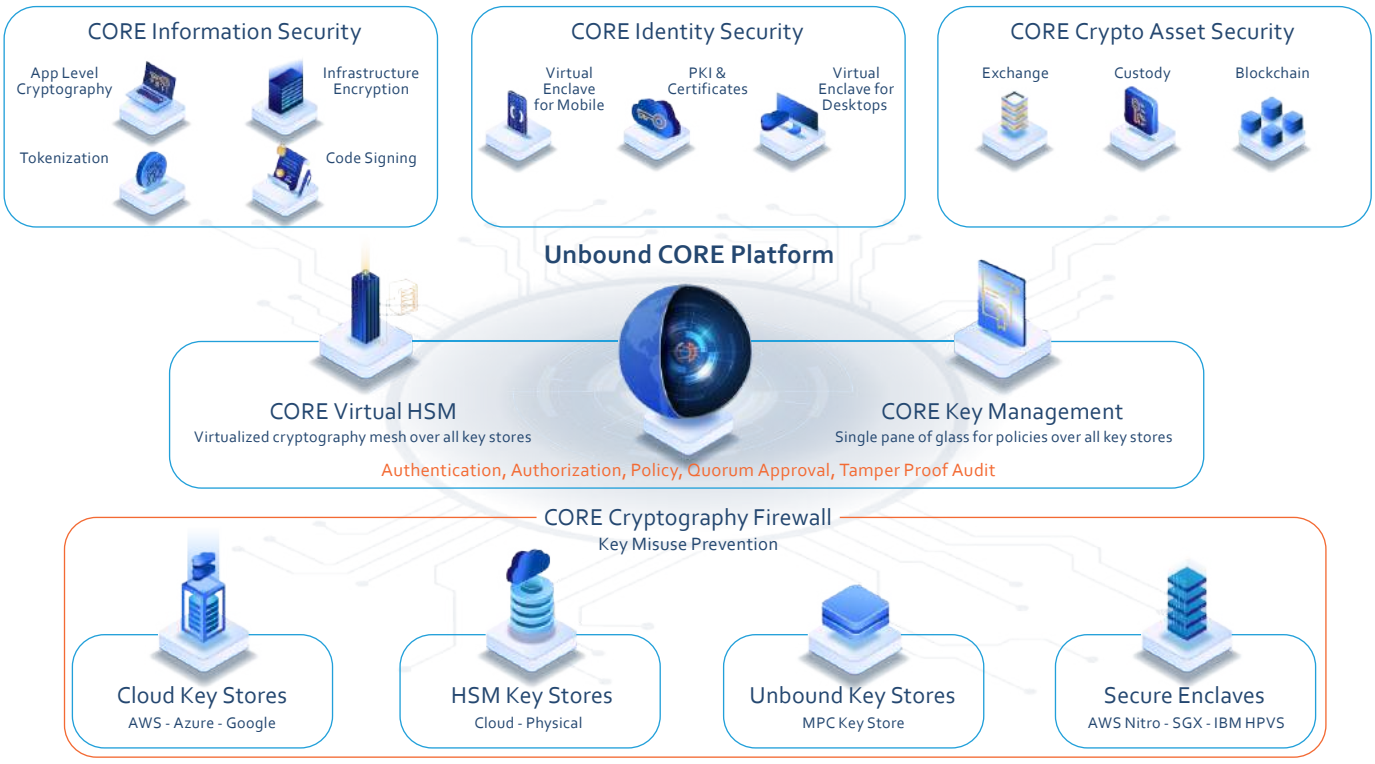
Layer 3 – solutions: The final layer of the CORE architecture is comprised of cryptographic solutions to business problems. These problems can be classified into three categories:

- **Information Security:** This refers to all of the problems of privacy and integrity of data in an enterprise and includes everything that was classically done using physical HSMs. This includes encryption of storage, virtual machines, databases, as well as protection of the keys used for code signing, transaction signing, protecting secrets vaults, and more. In addition, Unbound CORE offers built-in solutions for advanced cryptographic operations like tokenization of PII and credit card numbers. Finally, it supports any application consuming cryptographic services, via a rich set of APIs.

- **Identity Security:** Strong authentication utilizes cryptographic keys. This includes the keys used in setting up a PKI, as well as keys for authenticating machines and humans, and authorizing transactions by digitally signing them. Unbound CORE can be used to protect keys used in PKI (e.g., root CA keys, TLS keys, and so on). In addition, it includes an SDK that provides a virtual secure enclave (much like a virtual HSM) that can be used to protect keys on any mobile or enterprise workstation. The keys are protected via MPC and thus are never exposed in whole on mobiles or employee personal computers, where they are vulnerable to theft. The SDK can be used to secure access for customers via mobile to the organization's services (e.g., protecting a bank's mobile app) with far higher security and usability than existing one-time password solutions. In addition, it can be used to build virtual smartcards that are associated with employee workstations. A highly novel aspect here is that Unbound CORE is the first solution to manage both server-side keys (in HSMs and the like) and user keys (on mobiles and personal computers).

- **Crypto asset security:** Financial and other enterprises are looking closely at the crypto asset and enterprise blockchain space. This includes the new world of cryptocurrencies, but also tokenization of classic financial assets, the use of enterprise blockchain to solve cross-organization synchronization problems, and more. Unbound CORE provides key management and protection to all types of cryptographic keys used in this setting. A primary use case is that of providing custody solutions for crypto assets. Unbound CORE has built-in capabilities for quorum authorization for signing on transactions of crypto assets, a policy engine for allowed key usage, and is ready for integration with external providers to evaluate risk, deploy AML, KYC, and more. In addition, due to the irreversible nature of public blockchain transactions, quorums of human approvers can be defined (typically for large transactions). In this setting, the cryptographic key material is split between all participants, including human approver mobiles where defined. As a result, even if the entire organization's IT infrastructure is compromised, the key material is still not present without also compromising a quorum of mobiles of human approvers. As with all Unbound CORE solutions, applications deploying crypto asset security can utilize both MPC authorization as well as physical HSMs and cold storage, if desired.

See the figure below for a depiction of the Unbound CORE architecture.



An important benefit of Unbound CORE is that once the platform is deployed for one use case, it can easily be extended to more use cases. As a result, Unbound CORE supports business growth, enabling organization to quickly add cryptographic agility (support and functionality) for new business initiatives.

Preventing Single Points of Failure

A paramount benefit of Unbound CORE is the removal of single points of security failure. The basic premise of all software today is that failure and breaches happen. Furthermore, in the era of supply chain attacks, it is crucial to build a security architecture that does not completely fail when any single component fails. For example, a prudent strategy is to use two different firewalls in sequence. This ensures that if any single firewall fails (e.g., has a zero day or is infected via a supply chain attack), then the other firewall is still active.

Unbound CORE provides protection via distribution, decentralization and diversification, and so by definition moves away from single points of failure. First and foremost, Unbound's MPC key store ensures that key material does not reside in any single place. However, it goes far beyond that. Unbound CORE offers organizations the flexibility to adopt an all-encompassing platform that employs best in practice cryptography methods, while no longer forcing them to choose one security solution over another. It is possible to combine the use of physical HSMs, cloud HSMs, cloud key vaults, secure enclaves (trusted execution environments) and Unbound's MPC key store in protecting assets. Another aspect that removes the single point of failure is Unbound CORE's layer of policy verification to prevent key misuse, removing the ability to bypass controls by breaching the last node in the process. Similarly, the use of quorum authorization and quorum administration means that multiple points need to be breached in order to bypass the security guarantees, and maker/checker workflows can be cryptographically enforced. These policies and protections can be applied to all keys in any and all key stores.

There is no perfect security, but far better results than today can be achieved via solutions that provide defense in depth and promote synthesis rather than fragmentation.

Common Unbound CORE Use Cases

In this section, we will very briefly describe some common use cases for Unbound CORE.

Information Security:

- **Unbound CORE Infrastructure Encryption**
  - **Unbound CORE Transparent Database Encryption (TDE):** use Unbound CORE to encrypt common databases using TDE while securing the key in any chosen key store. TDE prevents the most common attack carried out by stealing the data from disk.
  - **Unbound CORE Virtual Machines Encryption:** Unbound CORE is a certified encryption method for VMware that allows organizations to easily encrypt their VMs. This is basic best practice that every organization must follow.
  - **Unbound CORE Storage Encryption:** Unbound CORE can also be used together with storage encryption tools like NetApp to secure the keys.
  - **Unbound CORE Secrets Vault Protection:** Unbound CORE is integrated with HashiCorp and CyberArk to protect the master keys used by these systems to protect API keys, passwords and secrets.
- **Unbound CORE App Level Cryptography:** Any application consuming cryptography of any kind can use Unbound CORE with any standard library (PKCS11, CNG, KMIP, JCA, OpenSSL, etc.) as well as with Unbound's agile REST API. The same API works for every key store and so applications need not be modified if they are moved from an on-prem setting to the cloud or between clouds, even if the key store is changed.

- **Unbound CORE Tokenization and masking:** Unbound CORE provides the ability to tokenize PII and credit card numbers in a way that preserves their exact format. This means that existing applications and SaaS services can continue to be used without exposing plaintext data to them. In addition, Unbound CORE provides masking capabilities, to only return partial decryption of sensitive PII.

- **Unbound CORE Code Signing:** Unbound CORE code signing is integrated to almost all development platforms used. It provides centralized management with high security and enables organizations to move away from the ad-hoc solutions many are using today. Unbound's MPC key store is FIPS 140-2 Level 2 certified, and so can be used for the higher security EV (Extended Validation) certificates often used in code signing.

Identity Security:

- **Unbound CORE PKI:** Unbound CORE can be used to protect the root CA and other CA keys in Microsoft CA and others. In addition, it can be used for certificate protection (e.g., TLS keys), and in the future will include general certificate management.

- **Unbound CORE Virtual Enclave for Mobile:** Two-factor authentication has classically been very painful. With Unbound CORE's virtual enclave SDK, it is possible to integrate strong authentication into a mobile app, utilizing a cryptographic key that is shared between the mobile and a server and used via MPC. The cryptographic authentication key cannot be stolen from the mobile device, as it is simply not there. This provides both excellent user experience and security for services such as authentication and transaction signing with non-repudiation.

- **Unbound CORE Virtual Enclave for Desktops:** Smartcards for transaction signing and other cryptographic operations on desktops are widely understood to provide excellent security. However, the pain of delivering and maintaining smartcards for all employees is often too high. Unbound CORE's virtual enclave SDK for desktops provides the best of all worlds, delivering high security in software only.

Crypto Asset Security:

- **Unbound CORE for Crypto Assets:** Unbound CORE can be used to protect crypto assets of all kinds, from cryptocurrencies to classic financial assets that are tokenized. Unbound CORE supports the new cryptographic standards and curves used in this space and is integrated into external services to help reduce risk and achieve compliance. The solution also provides strong zero-knowledge backup of keys to ensure that a loss of funds through key is prevented. Unbound CORE is particularly suited to enterprises looking to custody crypto assets, and large exchanges who need fast transaction time with high security.

- **Unbound CORE for Enterprise Blockchain:** Public and private blockchain projects now being deployed by enterprises require cryptographic keys for protecting the nodes and signing on all blockchain transactions. Unbound CORE is integrated with Hyperledger and other popular tools and is enterprise ready.

Management:

- **Unbound CORE Cloud Key Management:** Unbound CORE can be used to manage keys in AWS KMS, AWS cloud HSMs, Azure Vault, and in physical HSMs (of course, in addition to managing keys in Unbound's MPC key store). This provides the ability to truly manage all keys from a single pane of glass.

- **Unbound CORE Google External Key Manager:** Unbound is integrated with GCP to work as an external key manager, enabling organizations to maintain control over their keys even when using GCP cloud native applications. This is important for organizations for both security and for regulatory compliance, as well as protection from the CLOUD Act.

Summary

Unbound CORE is a truly innovative solution reimagining cryptography orchestration for the enterprise. With Unbound CORE, organizations can transform their existing siloed and fragmented infrastructure into a unified solution. This provides efficiency, better security, better user experience and lower cost. For any given specific cryptographic problem, it is possible to add a point solution and increase the already fragmented space in the enterprise. Alternatively, Unbound CORE can be deployed, providing the necessary infrastructure for all cryptographic needs, of all types, in all environments and in any location.

unbound security

In a world moving toward everything encrypted, signed, and authenticated – secure and operationally efficient cryptographic infrastructure is an absolute must for enterprises. Our vision at Unbound is to be the global cryptographic orchestration platform of choice for the enterprise. By leveraging the latest advancements in multi-party computation, our platform is the industry choice to secure the world's largest banks and Fortune 500 companies. With a headquarters in New York, and an EMEA office in Tel Aviv, Unbound provides the cryptographic orchestration platform that enables enterprises worldwide to easily secure and manage all their information and digital assets.