Software-Based Cryptography: Addressing the Security Challenges of Hybrid IT Environments

Securing mixed IT environments requires a scalable approach.

The acceleration of digital transformation initiatives and the shift to multicloud environments triggered by the global pandemic are driving the need for new approaches to cryptographic key management for today's modern enterprise.

Enterprise organizations have long used on-premise hardware security modules (HSMs) and other enterprise encryption key management options—including cloud-hosted services—to protect data in data centers and systems. These technologies have played a critical role in protecting businesses against compromise, primarily key theft, as well as in helping an enterprise meet compliance requirements such as those mandated by the PCI Data Security Council.

Increasingly, though, organizations are moving to hybrid cloud environments where data is fragmented and applications are scattered across a mix of on-premise data centers, private clouds, and public clouds. However, in these dynamic environments, hardware-based approaches to cryptographic key management alone don't offer the flexibility, scalability, or cost-effectiveness to encrypt everything, everywhere, all the time.

A secure software-based, cloud-agnostic key protection solution—in addition to more traditional protection schemes—addresses these issues. It can be centrally managed and yet have no single point of failure that an adversary can attack or disrupt.

The Need for an All-Encompassing Approach to Security

Data encryption has become a critical component of enterprise security strategies.

Organizations concerned about data breach risks are increasingly looking to encrypt everything, everywhere, all the time. Many consider encryption of data in transit and at rest a best practice for protecting the confidentiality and integrity of data on-premise and in public cloud environments. Requirements for encryption have increased in recent years, with the growing adoption of cloud services and the trend among many companies to steadily digitize more of their data and operations.

Further, regulations such as GDPR, PCI DSS, and HIPAA require covered entities to encrypt sensitive data. Companies that fail to comply and then suffer a breach can face substantial financial penalties and—in some cases—years of crippling regulatory oversight.

Many organizations currently rely on legacy key management systems and HSMs to meet their encryption and strong authentication objectives. The systems are often based on purpose-built hardware platforms designed to protect the confidentiality of the keys used for data encryption. These technologies offer enterprises a way to securely generate, distribute, use, store, delete, and regenerate the cryptographic keys that are used to encrypt data across the environment.

Depending on the robustness of the technology, a hardware-based key management system can be used to protect certificate authority (CA) keys; code-signing keys; and the keys used to encrypt applications, databases, storage systems, and virtual machines. Many of these systems offer strong protections against physical and virtual tampering.

Key management systems and HSMs have played, and continue to play, a critical role in enabling data encryption at many organizations. However, these point hardware-based technologies are no longer sufficient to meet the key management requirements of modern enterprises where data needs to be protected not just in on-premise systems but also in multicloud environments.

The Challenges of Traditional Encryption Systems

One of the biggest drawbacks of legacy key management systems and HSMs is that they are a physical anchor in an increasingly virtualized world. Many of these systems require physical access to install, manage, and administer. Often enterprise organizations—especially larger ones—require different key management systems for different applications and environments. However, key management systems can have different levels of complexity and behaviors that may need to be managed differently. These layered key management solutions not only represent a resource issue but they can also limit visibility and complicate the task of deploying and implementing company-wide key management policies.

Complexity coupled with limited resources can make it cost-prohibitive to manage multiple solutions. Legacy key management platforms and HSMs are often proprietary and arduous to manage, especially in fragmented, multivendor environments. Not only can these systems be costly to purchase but they can also take months to acquire and are often difficult to deploy. Additionally, many organizations require staff with specialized skills to manage their hardware-based cryptographic key management environment.

These issues can become greatly magnified when organizations have to synchronize and manage cryptographic keys across different data centers and across multicloud environments. In short, legacy key stores can seriously slow down organizations at a time when agility, flexibility, and time to market have become critical to enabling new business initiatives.

Increasingly, organizations require a key management capability that moves with them across hybrid, multicloud virtual environments. An agile solution should provide unified key management capabilities across on-premise and multicloud hybrid environments to seamlessly integrate existing policies without the need to refactor existing applications. This enables organizations to rapidly scale key management requirements up or down as needed to meet required capacity for peak times while paying only for what is actually used.

For this scalability, the platform should be cloud- and platform-agnostic so it can be deployed across any environment without concern about compatibility and integration issues. Also, to help ensure compliance with regulatory requirements and industry best practices, the encryption approach needs to support broadly

> *The ability to implement encryption anywhere and at any time enables companies to introduce new apps quickly and with full cryptographic support.*

accepted cryptographic libraries, technologies, and techniques, including those prescribed by standards such as FIPS 140-2. It should also support deep audit and reporting capabilities where every operation is logged in a secure, tamper-proof manner. The auditing support should be available across multiple key stores in a unified format and in one place.

The Benefits of Software-Defined Key Management

A software-defined approach to key management can address many of the limitations of legacy key stores and HSMs. Such an approach can give organizations the ability to encrypt areas of their on-premise infrastructure and cloud environment that they could not previously encrypt with point products.

A software-defined cryptographic management system is basically a virtual key management store that, like its physical counterpart, can be used to store, use, protect, and manage cryptographic keys and secrets. The technology enables organizations to implement a single pane of glass for centrally managing all cryptographic keys and components across modern hybrid IT environments.

Typically, the systems have a secure cryptographic module capable of running on heterogeneous physical infrastructure that performs the key generation, storage, and processing functions. One important trait of these modules is their ability to scale up rapidly to support sudden surges in demand for authentication or encryption services.

By adopting a software-defined approach to cryptography, organizations can add flexibility to their key management environment. A virtual key protection and management system can help organizations implement encryption without requiring a dedicated hardware purchase. Companies can use it to immediately boost security in areas of the infrastructure where hardware-based key management is not currently in use.

The ability to implement encryption anywhere and at any time enables companies to introduce new apps quickly and with full cryptographic support. In addition, a software-based approach can help organizations centralize key management and apply policies more consistently across data centers and varied infrastructure.

Critical Requirements of Software-Defined Key Management

One of the most critical requirements of software-defined cryptography is that it can have no single point of failure—meaning that cryptographic keys cannot reside in memory on a single machine at any time. A technology called Multiparty Computation (MPC) addresses this issue, splitting each secret key into a random number of parts, or shares, and distributing them across multiple systems. Specific protocols associated with MPC ensure that the different machines holding the shares are able to carry out computational operations without ever uniting the shares or revealing any details about them to each other. The MPC approach guarantees that the only way attackers can compromise keys in a software-defined cryptography model is if they can breach all machines simultaneously.

The ability to distribute key shares across on-premise and cloud systems enables organizations to virtualize their cryptographic infrastructure and explore new possibilities for digital services based on trust. When used as part of a multilayered security model, MPC enables a software-defined cryptographic platform that supports all standard cryptographic operations and algorithms, including RSA decryption and signing, AES, ECC-ECDH, and EdDSA. Because MPC does not change the algorithm itself but only the manner in which computation is carried out, Unbound CORE for virtual HSMs (vHSMs) based on the technology can receive FIPS 140-2 Level 1 and Level 2 certification.

Pure software-based key protection is easier to deploy than traditional hardware-bound key management systems and specialized HSMs. Organizations can use the approach to address multiple use cases, such as database encryption, virtual machine encryption, and storage-level encryption. The software-based approach complements existing infrastructure, whether hardware or virtual, and may deliver a centralized method for cryptographic key management across any type of infrastructure.

Independently or in coexistence with traditional HSMs, Unbound CORE for virtual HSMs enable better business agility, because they can be deployed like any other new virtual machine. They mean that organizations don't have to be limited to their hardware-based HSM or key management system whenever a new application is being deployed that requires encryption, authentication, and other cryptographic services—whether on premise, in the cloud, or in multiple clouds. Refactoring applications to work with hybrid infrastructure scenarios can often take months to accomplish and can seriously slow down the deployment of new applications.

Software-defined key management systems are platform-agnostic and can run in any location or infrastructure, so organizations can centrally manage and administer cryptographic keys across on-premise data centers and hybrid cloud environments. That's very different from hardware-based systems, where key generation, deletion, rotation, and other functions need to be implemented separately for different environments.

With a software-defined system, an organization that wants to replicate a fully virtualized data center in another geolocation can secure the cryptographic infrastructure in the new location the same way it would deploy any other application.

Ultimately, the ability to coexist with existing infrastructure—or stand up a completely virtual HSM instance—offers more flexibility and centralized management capability. It also reduces the cost of building systems and going to market. By implementing these capabilities on demand or via self-service, organizations can utilize only the resources they actually consume, with the added benefit of rapidly scaling up or down if required.

Conclusion

Virtualization and the shift to hybrid and multicloud environments have exposed limitations in hardware-only approaches to cryptographic key management and protection. A hardware/software or software-defined key management approach—when used as part of a multilayered security model—can offer all the benefits of a traditional HSM in a more scalable, flexible, and cost-effective manner.

Learn more about secure cryptographic infrastructure. Visit Unbound Security.

LEARN MORE