



## CryptoHub Solution Brief

### THE **ALL-IN-ONE**, HARDWARE-BACKED CRYPTOGRAPHIC PLATFORM

#### A New Dynamic to Solve Cryptographic Sprawl



Simplifying cryptographic complexity in your infrastructure is a significant cybersecurity hurdle. Many organizations face deployment and management challenges when using multiple vendor solutions. This complexity, originating from industry acquisitions, brings visible and unseen obstacles despite aiming for a unified solution.

CryptoHub is the industry's only all-in-one cryptographic platform built on a common code base. This unique advantage significantly reduces deployment time for cryptographic services, surpassing rival solutions by over 90%.

Traditional cryptography infrastructure involves various products from different vendors, requires specialized and expensive expertise, and costly integration and maintenance services. This model just does not work for the modern enterprise.

Available as an on-premises appliance, a containerized cloud instance, or through Futurex's VirtuCrypt SaaS with 13 data centers worldwide, CryptoHub facilitates instant deployment and seamless integration, empowering organizations to dynamically provision any payment or general-purpose cryptographic solution on demand.

#### The Challenge of Legacy Systems



Legacy cryptographic systems rely on fragmented solutions, necessitating separate hardware security modules (HSMs) for general data protection and payment security. They also require separate systems for standard functions like PKI and CA. This patchwork approach leads to integration complexities, security vulnerabilities, and operational inefficiencies, hindering organizations from effectively combating modern cyber threats.

CryptoHub eliminates cryptographic sprawl by consolidating functionalities into a unified platform. With CryptoHub, organizations gain unparalleled simplicity, security, and scalability. CryptoHub enhances operational efficiency and streamlines operations, and future-proofs data protection strategies by offering a single solution for diverse cryptographic needs.

Forward-thinking IT leaders are embracing CryptoHub as a strategic investment, unlocking comprehensive encryption that adapts alongside evolving cyber threats for robust data protection.

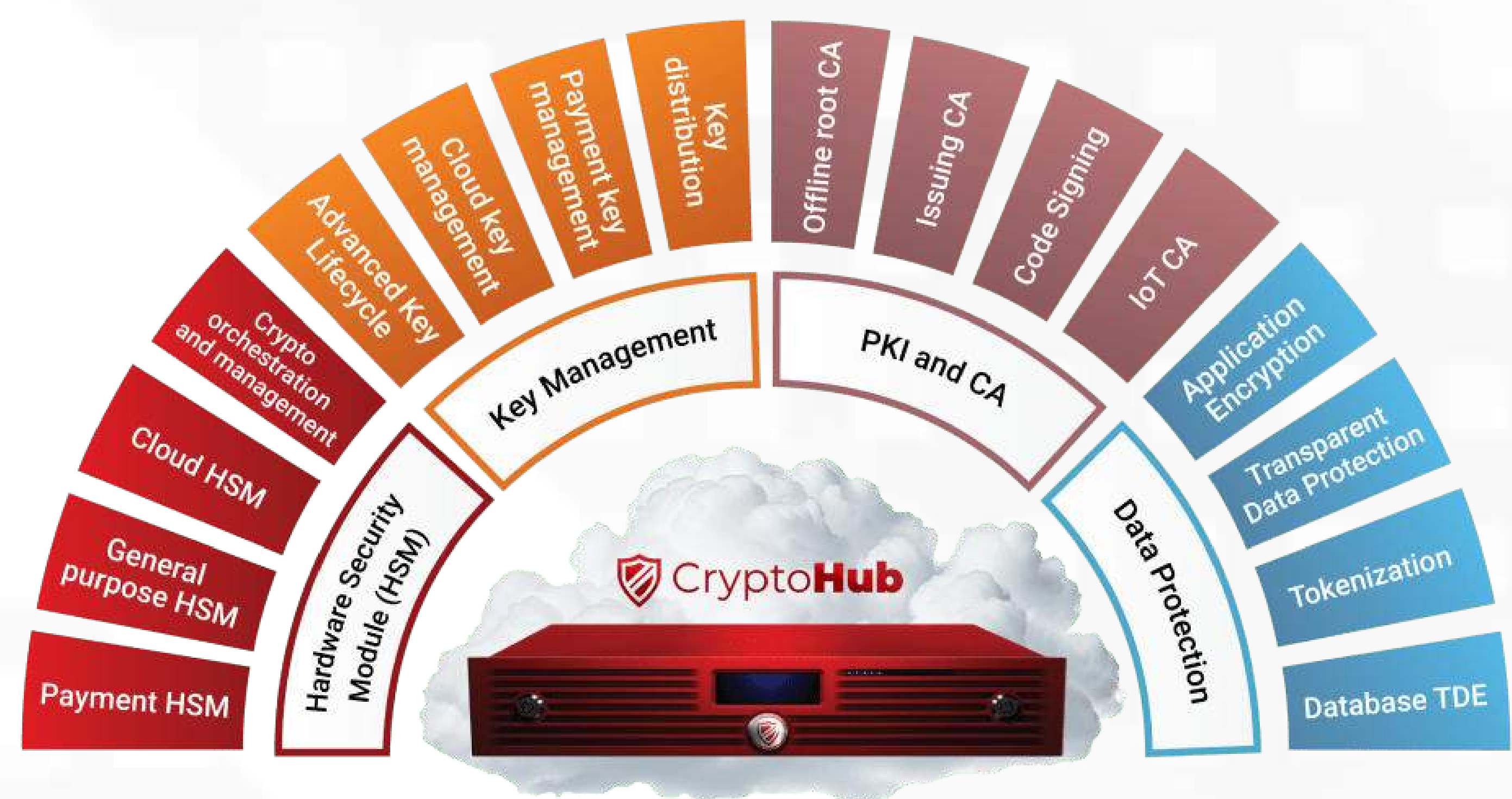




## CryptoHub Solutions



There are four core pillars of the CryptoHub platform: Hardware Security Modules (HSM), Key Management, PKI and Certificate Authority, and Data Protection. Each provides unparalleled security, efficiency, and scalability required by today's cybersecurity landscape while retaining the distinctive features of CryptoHub's unified platform, which ensures simplified management and crypto orchestration.



### **Hardware Security Modules (HSM)**

The CryptoHub HSM Series offers enterprise-class HSMs for both general-purpose and payment applications in one solution, ensuring the highest level of security for diverse use cases. With the capability to process over 100,000 transactions per second (TPS), it delivers exceptional performance without compromising security. Each HSM is rigorously tested and certified to meet regulatory standards, including FIPS 140-2 Level 3 and PCI HSM, guaranteeing compliance and peace of mind for organizations.

One of the standout features of CryptoHub HSMs is their support for all payment and general-purpose APIs and cryptographic libraries, including PKCS #11, Java, CNG, and RESTful interfaces. This broad compatibility ensures seamless integration with existing systems and applications, allowing organizations to leverage the full power of our HSMs without disruption.

CryptoHub HSMs introduce innovative segmentation capabilities through Virtual HSMs, partitioning application workloads securely. Each Virtual HSM functions independently with its own Major Keys and Security Policy, ensuring isolation and enhancing security posture.

CryptoHub HSMs minimize downtime and ensure continuous availability of cryptographic services with redundancy and failover, featuring dual, redundant power supplies and Ethernet ports for uninterrupted operation and automatic synchronization of device information to facilitate instantaneous failover.


### **Key Management**

At the heart of CryptoHub lies a sophisticated key management system that orchestrates the generation, storage, distribution, and destruction of cryptographic keys with precision and reliability. CryptoHub streamlines key management operations, eliminating the need for multiple disparate products and specialized knowledge. This unified platform enhances operational efficiency and significantly reduces integration and maintenance costs, setting a new standard in cryptographic security solutions.

CryptoHub's dynamic provisioning, powered by Futurex's HSM hypervisor, enables rapid deployment of Virtual HSM Master Keys (VMK) and cross-region clustering for maximum uptime and scalability. CryptoHub simplifies the deployment and management of key blocks, including KBPK X9.143. CryptoHub's flexible deployment options include appliance, virtual appliance, containerized appliance, or customizable service (KMaaS – Key Management as a Service), catering to diverse enterprise needs and infrastructure preferences.







CryptoHub's enterprise-grade assurance of data security is bolstered by its adherence to industry-leading standards such as FIPS 140-2 Level 3, PCI DSS, and PCI HSM. CryptoHub also leads the way with flexible key injection and supports clear key, encrypted payload key, and remote key injection capabilities that uniquely satisfy the PCI PIN control 32.9 for encrypted remote key loading.

CryptoHub is compatible with a wide range of cryptographic libraries, APIs, and protocols, which ensures seamless integration into existing cryptographic ecosystems.

In conclusion, CryptoHub's key management capabilities epitomize excellence in cryptographic security, providing organizations with the confidence and tools needed to safeguard their most valuable assets in an ever-evolving threat landscape.

## ***PKI and Certificate Authority***

CryptoHub offers a comprehensive PKI and certificate authority solution, empowering organizations to establish offline root CAs, issue certificates, perform code signing, and easily manage IoT certificates.

With CryptoHub, organizations can securely manage their PKI infrastructure, ensuring the integrity and authenticity of digital certificates. Offline root CAs mitigate compromise risk by safeguarding the root of trust offline. CryptoHub's certificate issuance capabilities enable organizations to efficiently issue digital certificates for various use cases, while code signing features ensure the authenticity and integrity of software applications. Additionally, CryptoHub's IoT CA functionality simplifies the management of certificates for IoT devices, enabling secure communication and authentication. With CryptoHub, organizations can establish and maintain a robust PKI infrastructure, ensuring secure digital transactions and communications.

CryptoHub's PKI and CA capabilities form the backbone of secure communication infrastructures, facilitating mutual authentication and encryption of data exchanged between entities. By leveraging CryptoHub's offline root CA and issuing CA functionalities, organizations can establish a trusted hierarchy of digital certificates, ensuring the integrity and authenticity of digital transactions.

One of CryptoHub's key strengths lies in its versatility, catering to diverse use cases ranging from traditional enterprise environments to emerging IoT ecosystems. Whether securing payment transactions, code signing for software integrity, or provisioning certificates for IoT devices, CryptoHub's PKI and CA functionalities offer unparalleled flexibility and scalability.

Moreover, CryptoHub's support for code signing enables the organization's DevOps teams to optimize CI/CD capabilities to protect their intellectual property by digitally signing executables and firmware updates. This ensures that only authorized code is executed, mitigating the risk of tampering or unauthorized modifications.

In the evolving cybersecurity landscape, CryptoHub remains at the forefront with its commitment to standards compliance and innovation. With certifications including FIPS 140-2 Level 3 and PCI HSM, CryptoHub assures organizations that their cryptographic infrastructure meets stringent security requirements.

In conclusion, CryptoHub's PKI and CA capabilities empower organizations to establish a robust foundation for secure communication and identity management.





## Data Protection

CryptoHub's data protection capabilities encompass a range of advanced encryption techniques designed to secure data at rest, in transit, and during processing. From application encryption to transparent data protection, tokenization, and database TDE (Transparent Data Encryption), CryptoHub provides organizations with a robust framework to mitigate the risks associated with data breaches and unauthorized access.

CryptoHub's application encryption functionality enhances security by encrypting application data before storage or transmission and integrates seamlessly with existing applications. CryptoHub ensures that data remains protected even in the event of a breach, minimizing the potential impact on business operations and customer trust.

CryptoHub's transparent data protection encrypts data at the file system or disk level, ensuring that sensitive information remains secure from unauthorized access. This approach minimizes the performance overhead usually linked with encryption, enabling organizations to maintain optimal system performance while upholding security standards.

Tokenization, including vaultless tokenization, is a pivotal feature of CryptoHub, allowing organizations to swap sensitive data with non-sensitive tokens. This process significantly lowers the risk of data breaches by replacing critical information like credit card numbers or PII with tokens. Adopting vaultless tokenization ensures regulatory compliance and shields organizations from the detrimental effects of data breaches on business operations and reputation.

CryptoHub's database TDE functionality provides organizations with a robust solution for encrypting data stored in databases, ensuring that sensitive information remains protected from unauthorized access. By encrypting data transparently at the database level, CryptoHub enables organizations to maintain compliance with regulatory requirements while safeguarding sensitive information from internal and external threats.

In conclusion, CryptoHub's data protection capabilities offer organizations a comprehensive framework for safeguarding sensitive information across the enterprise.

## Executive Summary



CryptoHub revolutionizes data security with its integrated suite of cryptographic services. With powerful hardware security modules (HSMs), advanced key management, comprehensive PKI and CA, and robust data protection capabilities, CryptoHub ensures end-to-end protection for organizations worldwide.

By harnessing the power of CryptoHub, enterprises can fortify their data defenses and uphold trust with unparalleled efficiency, flexibility, and a host of industry-leading certifications. With CryptoHub, the future of data security is not just assured—it's elevated to new heights of reliability and resilience.

Learn more at [www.futurex.com/cryptohub](http://www.futurex.com/cryptohub).



[FUTUREX.COM](http://FUTUREX.COM)

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

864 Old Boerne Road,  
Bulverde, Texas 78163

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

