Magic™

TECHNICAL OVERVIEW

Delegated Key Management System

Contents

Introduction

Magic™'s Delegated Key Management System (DKMS) is a patented key management architecture designed to enhance the security, scalability, and user experience of applications, particularly in the context of blockchain wallets.

Magic's DKMS was originally developed in 2018, emerging from an extensive research endeavor. During that period, the landscape of startups focusing on the scalability of web3 wallets for enterprises was sparse. Recognizing this void, Magic's founding team discerned a unique opportunity to engineer a web3 wallet capable of accommodating billions of users while upholding enterprise-grade security standards.

A comprehensive evaluation of existing key management system (KMS) methodologies revealed their inability to fully align with our multifaceted objectives around security, scalability, and user experience. Consequently, Magic's founding team embarked on the creation of our proprietary KMS. This strategic initiative propelled Magic into its current position as the foremost Wallet-as-a-Service (WaaS) provider, serving enterprises across the global landscape.

DKMS delegates the key encryption and decryption operations to a trusted 3rd-party Hardware Security Module (HSM) provider, helping to ensure that sensitive cryptographic operations remain beyond the reach of the Magic infrastructure. This whitepaper aims to provide an overview into the various aspects of Magic's DKMS system, from key generation and storage to access control and security.

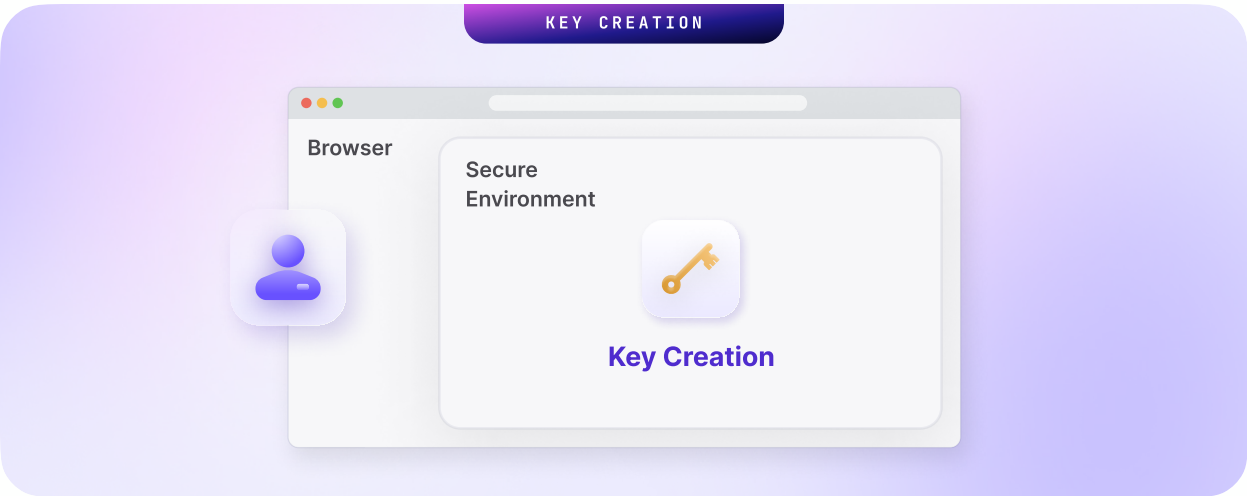
Delegated Key Management System

Magic's Delegated Key Management System (DKMS) architecture is based on the principle of delegating and isolating cryptographic key management to a secure client-side iframe environment that is not accessible by anyone—including Magic—only by the end-user. By doing so, it significantly enhances the security of sensitive operations, such as private key generation and blockchain transaction signing. The key components of the DKMS architecture are as follows:

Client-Side Key Generation

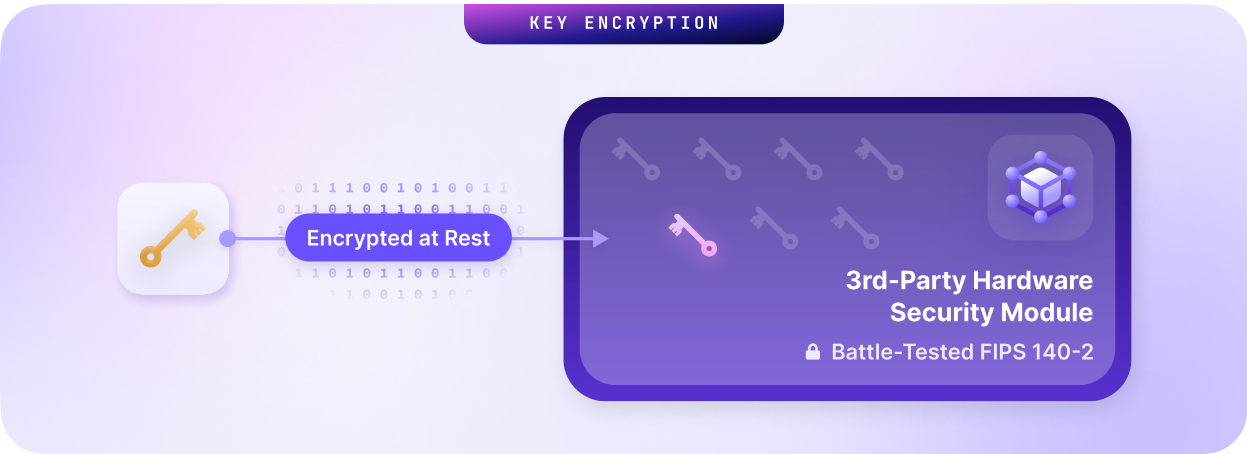
The client-side key generation and encryption process is central to the security of Magic's DKMS. By generating key pairs with a high level of entropy and immediately encrypting the private key within a trusted HSM, Magic can prevent the private key material from being exposed to potential attackers.

When a new user interacts with an application using Magic, a public-and-private key pair is generated inside a client-side secure environment (iFrame). These keys are created with cryptographically secure pseudo-random 256-bits of entropy, leveraging open-source libraries for all Magic-supported blockchains. Moreover, the encrypted private key is stored within Magic's infrastructure, allowing users to access it securely when needed for authorized operations. Note that Magic does not persist unencrypted private keys in Magic's servers nor in the client-side secure environment.



Third-Party HSM Encryption

Once generated, the private key is immediately encrypted by the trusted 3rd-party HSM provider. This encryption process allows the private key to remain secure, and Magic has no access to the unencrypted key material.



Third-Party HSM Access Controls

To access a 3rd-party HSM for cryptographic operations such as transaction signing, user authentication is a mandatory step. This authentication can be accomplished through either Magic's identity provider (IdP) or the application's own IdP (ex: Google, Auth0, Microsoft, etc.).

Upon successful authentication, the user will receive a time-bound access token generated by a 3rd-party identity provider—for this, Magic leverages AWS Cognito as the 3rd-party identity provider. This time-bound access token can be traded for scoped credentials. The scoped credentials provide the user's client side with temporary authorization to access the HSM exclusively for private key encryption and decryption operations. Magic cannot forge nor intercept the scoped credentials because they are generated by the operations between the user's client side iframe and the 3rd-party HSM provider. Both access tokens and scoped credentials are created dynamically. This mechanism allows key encryption and decryption to bypass Magic infrastructure entirely, keeping Magic from being able to access the private key at any part of this flow.

Signing in Secure Environment Context

Key operations, such as private key generation and transaction signing, only occur within the secure iFrame environment context on the client side. This approach prevents private keys from being exposed outside of this secure environment for maximum security.

Upon successful authentication and issuance of a time-bound access token that grants access to the HSM encryption and decryption operations, user's client-side iFrame retrieves the encrypted private key from Magic's servers and decrypts the key via the HSM that allows the user to sign a blockchain transaction corresponding to the wallet. Once the signing operation is completed, the unencrypted private keys are wiped from memory. To reiterate, Magic does not persist unencrypted private keys in any of Magic's servers at any point in time, nor in the client-side secure environment.

Account Recovery

End-users can restore their wallets as long as they have access to the identity system or account provided by Magic's customer, effectively eliminating the need for a separate wallet account recovery process. This setup is made possible as a result of Magic's non-custodial DKMS architecture, which can be seamlessly integrated with a customer's identity system and Magic's Wallet SDK.

Note that Magic's customers have the flexibility to incorporate supplementary authentication methods for enhanced wallet recovery security.

Moreover, Magic's customers possess the ability to enable their end-users to export their private keys or seed phrases, adding an additional layer of control and convenience.

Company Security & Compliance

Background

Security compliance is a vital part of Magic's comprehensive security program. At Magic, we understand that trust is extremely important in any successful business relationship. As such, we recognize that compliance with security regulations and industry-standard frameworks is not merely a checkbox exercise but a measurement of our dedication to the security and privacy of our customers. Magic is the first Wallet-as-a-Service (WaaS) provider to attain SOC 2 Type 2, SOC 3 Type 2, ISO 27001 and HIPAA attestations, further underscoring our commitment to security.

We communicate trust to our clients by providing tangible evidence that our security approach aligns with industry best practices and regulatory requirements.

External Audits

SOC 2 Type 2

Magic's systems, processes and controls undergo rigorous audits conducted by an industry-leading assessment provider as part of our SOC 2 Type 2 external assessment process. These reports are produced annually and are available after executing an NDA on Magic's Trust Center.

SOC 3 Type 2

As part of Magic's external assessment process, SOC 3 Type 2 reports are produced annually. While an NDA is required to access Magic's SOC 2 Type 2 report, the SOC 3 Type 2 report is public and can be obtained without an NDA on Magic's Trust Center.

ISO 27001

Magic is ISO 27001:2013 certified, an internationally recognized standard for Information Security Management Systems (ISMS). Following an extensive audit by an industry-leading assessment provider, this certification confirms that Magic meets the highest standards for establishing, implementing, maintaining and continually improving ISMS. Magic's ISO 27001:2013 certification is available after executing an NDA on Magic's Trust Center.

HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. Magic's products and services are HIPAA compliant and undergo rigorous HIPAA-specific audits annually. Magic's HIPAA Type 2 report is available after executing an NDA on on Magic's Trust Center.

External Penetration Testing

Magic's infrastructure undergoes significant penetration testing of the codebase and deployment infrastructure at least once a year. Magic utilizes an industry-leading assessment provider for external penetration testing, and penetration test executive summaries are available on Magic's Trust Center.

Bug Bounty Program

We value the community's input regarding vulnerabilities and potential bugs in our application. Magic participates in a bug bounty program facilitated by HackerOne.

Conclusion

Magic's Delegated Key Management System (DKMS) represents a significant advancement in the field of application security, particularly for blockchain-based applications. By delegating encryption and decryption operations to a trusted 3rd-party HSM provider, Magic ensures the utmost security, scalability, and performance.

Users can be confident that their private keys will not be exposed or persisted outside of the secure environment, which is accessible only by the end-user, thus minimizing the risk of key compromise and helping ensure that neither Magic nor the 3rd-party HSM, as well as any other party other than the end-user's client side iFrame, has custody of the decrypted private keys.

Magic's innovative DKMS architecture provides a robust solution for securing cryptographic operations in applications.

Please note that the above is for informational purposes only. Magic does not provide any legal or security advising of any kind. To understand legal and security risks for your business, you should seek independent advice from qualified legal counsel and security experts.

For more details, visit Magic's developer docs

- Full DKMS whitepaper
- Security and compliance details
- Latest SDK and blockchain support

docs.magic.link →