NUCYPHER

NuCypher KMS Primer

Draft August 6, 2017

ABSTRACT

NuCypher KMS is a decentralized Key Management System (KMS) that enables public blockchains to securely store and manipulate private, encrypted data. It leverages state-of-the-art proxy re-encryption technology to embed access controls directly into encryption and a decentralized network of nodes to provide key management operations. It provides encryption and cryptographic access controls, without reliance on a central service provider. By enabling private, encrypted data sharing, it provides the security infrastructure for sensitive applications from healthcare to identity management to decentralized content marketplaces. NuCypher KMS will be an essential part of secure decentralized applications, just as SSL/TLS is an essential part of every secure web application.

BACKGROUND

Key Management Systems

A key management system (KMS) is an integrated approach for generating, distributing, and managing private encryption keys for devices and applications. As the root of trust, it's critical that a KMS is appropriately configured, managed, and protected. Historically, this has meant deploying a KMS on-premises in hardware security modules (physical devices used to safeguard digital keys) or using tools like HashiCorp's Vault. However, this requires a high degree of technical sophistication as well as upfront capital investment.

To ease the technical burden and to provide more competitive pricing, vendors like Amazon CloudHSM, Google Cloud KMS, and Azure Key Vault have begun offering KMS as a service.

However, these offerings necessitate placing an undue level of trust in the service provider, which may be inappropriate for security-critical applications. It also exposes users to censorship, service rejection, and even cybercrime or economic espionage.

Blockchain

Consensus networks, such as Bitcoin and Ethereum, are promising solutions to this centralization problem. However, due to their public nature, they are severely limited in their ability to store, share, and manipulate private, encrypted data. Moreover, they employ a volunteer network of nodes, which is subject to constant churn and not as reliable as central infrastructure when it comes to availability and enforcing access management rules.

Public-Key Encryption

Public-key encryption (PKE) is a type of encryption where two parties (a sender and a receiver) exchange information without any required common secret. Instead, each party has their own public-private key pair. The lack of a shared secret makes PKE particularly effective for communicating across insecure networks and channels. And it is one of the most critical cryptographic primitives in consensus networks. However, as a cryptographic access control it is limited in several ways:

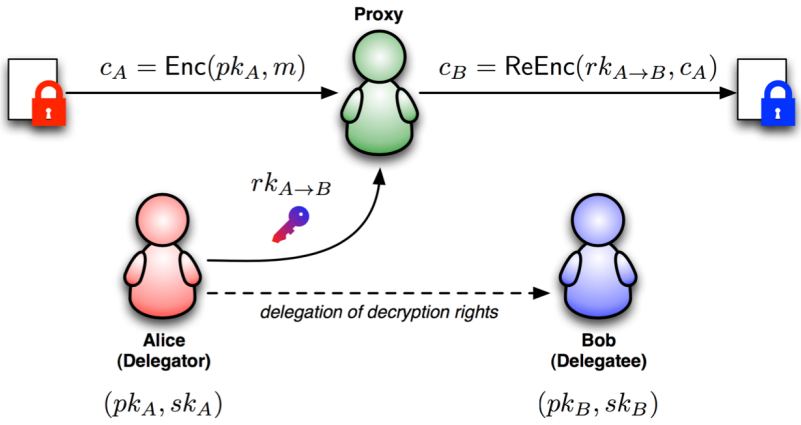
- It requires advance knowledge of the intended recipient;
- It does not scale well when there are multiple intended recipients, such as a group chat;
- Once an encrypted message has been shared with the holder of the associated private key, access cannot be revoked.

Proxy Re-Encryption for Distributed Systems

Proxy re-encryption (PRE) is a type of public-key encryption (PKE) that allows a proxy entity to transform ciphertexts from one public key to another, without learning anything about the underlying message.

Compared to existing PKE protocols which are ideal for 1-to-1 communication, PRE is more scalable for N-to-N communication with arbitrary numbers of data producers and consumers. It doesn't require knowing the recipient of a message in advance, as re-encryption tokens can be created and applied at any point.

These properties, and its ability to securely delegate access to private, encrypted information, make it an ideal candidate for constructing cryptographic access controls for distributed systems such as blockchain, internet of things (IoT), and big data.



PRODUCT DESCRIPTION

NuCypher KMS

NuCypher KMS is a decentralized key management system (KMS), encryption, and access control service. It enables secret storage and private, encrypted data sharing in public consensus networks, like Ethereum.

It uses a decentralized network to remove the reliance on central service providers, proxy re-encryption for cryptographic access controls, and a token incentive mechanism to ensure the reliability, availability, and correctness of cryptographic operations.

Use Cases & Application Ecosystem

NuCypher KMS provides the infrastructure for a variety of applications that require sharing of private, encrypted data as a basic functionality. The ability to condition decryption operations on public actions that occur on a blockchain, such as the publication of certain messages, payments made between specific addresses, and other events, is a powerful addition to the decentralized infrastructure stack.

- **Sharing encrypted files (“Decentralized Dropbox”)**
  Files can be encrypted client-side and stored in decentralized filesystems like IPFS, Sia, Storj, or Swarm, or centralized ones like S3. The files can be easily shared with approved third-parties by providing a re-encryption token based on the third-party’s public key. The third-party's access permission can be easily revoked by removing the re-encryption token from the network.

- **End-to-end encrypted group chat ("Encrypted Slack")**
  PRE is an ideal primitive for end-to-end encrypted group messaging, in which multiple participants require read and write access to a channel. Members can easily be added or removed to the chat by issuing or revoking a re-encryption token. This avoids the overhead of encrypting and sending messages multiple times, individually for each participant.

- **Patient-controlled electronic health records (EHR)**
  A patient-controlled EHR can be created in which the patient owns their data and encryption keys, as opposed to centralized systems like Epic. The data can be stored in a centralized or decentralized backend. When the patient wants to share their encrypted data with a hospital or insurance company, they issue a re-encryption token, which grants temporary access to the third-party.

- **Decentralized digital rights management (DDRM)**
  Cryptographic access controls can act as a decentralized DRM. Access controls can be embedded into the encryption itself so that they follow the data wherever it goes. Conditional re-encryption tokens can be controlled by a smart contract and released only upon payment. Services like a decentralized Netflix or an encrypted marketplace selling software, apps, photos, and other digital content can now be built.

- **Blind identity management**
  A blind identity management service can be constructed using NuCypher KMS. Identities can be encrypted client-side and stored with the identity management provider. Users can create re-encryption keys for approved applications. The service re-encrypts

identity credentials for said third-party applications, without the identity provider ever having access.

- **Secret credentials management for scripts and backend apps**
  NuCypher KMS is ideal for the storage of any secrets, such as sensitive environment variables, database credentials, and API keys. For scripts, a re-encryption token can be generated for the duration of a script, then revoked. For example, developers can safely store encrypted database credentials on GitHub, giving temporary access to these credentials once an instance is deployed. Even if the GitHub repository is public, the credentials cannot be used by an unauthorized person.

- **Shared credentials and enterprise password management**
  NuCypher KMS can be used for shared credentials that employees use to access web services. An audit log can be built to monitor who accesses what secrets. When an employee leaves, it is easy to revoke access or even roll keys.

- **Mandatory access logging**
  In some corporate and enterprise settings, clients must publish access logs for sensitive files. This requires that each file access be recorded and conditional re-encryption can be used to mandate these logging rules.

- **Mobile device management (MDM) and revocation**
  In an enterprise MDM setting, re-encryption tokens can be created for valid devices. When a device is lost or retired, the re-encryption token can be deleted to revoke the device's access. This avoids the problem of re-organizing hierarchical key trees.

TOKEN ECONOMICS

Protocol economies consist of a network of miners that contributes work to provide a scarce resource and that is rewarded when said resource is consumed. In NuCypher KMS, miners are re-encryption nodes. Anyone can become a miner and their rewards are differentiated based on the amount of re-encryption operations provided.

Access to the scarce re-encryption services must be controlled and allocated to the highest value uses. The mechanism by which we achieve this is *KMS Token*. It is both the reward miners get for contributing work and the price consumers (or owners of the data) pay for access to re-encryption services.

Functionality and Necessity

Vitally, the token incentivizes correctness of computation and security of the system. Since miners must stake KMS Tokens in order to perform re-encryption services, the tokens can used as collateral which miners risk if they commit any wrongdoing. If miners cheat—by providing fake data instead of re-encrypted data, leaking re-encryption keys, or being offline for too long while claiming to be available—other network participants can challenge them and claim a fraction of the miner's security deposit.

Network Effects

An interesting property of NuCypher KMS is that security improves as the number of network participants grows. As additional re-encryption nodes enter the network, the lower the chance of collusion. This improves both

the security and censorship-resistance of the system, providing powerful network effects and meaningful first mover advantages.

Market-based Pricing

The price of re-encryption services and KMS Tokens responds to market forces. If the demand for re-encryption services exceeds the supply provided by available nodes, the yield on a miner's staked tokens will be high, attracting new entrants. Conversely, if too many re-encryption nodes enter the market, the price for re-encryption services will go down, making the yield on staked tokens less attractive and driving out excess supply.

Additionally, as the application ecosystem using NuCypher KMS grows, the demand for re-encryption services and KMS Tokens will increase.

COMPANY & TEAM

Company Background

NuCypher is a venture-funded security and encryption platform for distributed systems, including big data, blockchain, cloud, and IoT. The company recently launched on-stage at TechCrunch Disrupt as a finalist in the Startup Battlefield and is the first Y Combinator-backed company to run a token sale. NuCypher was incubated at Accenture's FinTech Innovation Lab in London, where it refined its proxy re-encryption technology with tier 1 global banks and financial institutions.

The company is backed by leading Silicon Valley investors, including Y Combinator, NewGen Capital, Base Ventures, and Mission & Market.

Existing Products & Services

NuCypher's current product offerings cater to big data platforms like Hadoop and Kafka. It sells primarily to large financial institutions with

stringent security and compliance requirements, helping them securely move from on-premises to the public cloud, comply with data protection regulations, and share sensitive data with customers, partners, and regulators.

The company supports open-source versions of its Hadoop and Kafka products, which are available on GitHub. Inquiries related to the company's enterprise versions can be directed to founders@nucypher.com.

Team

The founders are a team of seasoned open-source software engineers who created ZeroDB, a popular open-source encrypted database that created a practical way to search, sort, and query encrypted data.

MacLane Wilkison, CEO

MacLane is a software engineer and former investment banker at Morgan Stanley, where he provided M&A and financing services to enterprises in technology, media, and telecommunications. He is a graduate of the University of North Carolina.

maclane@nucypher.com

Dr. Michael Egorov, CTO

Michael is a physicist and scientist from the Moscow Institute of Physics and Technology. A bronze medalist in the 2003 International Physics Olympiad, he studied ultra-cold atoms as a post-doc. Prior to NuCypher, he built infrastructure tools at LinkedIn.

michael@nucypher.com

Dr. David Núñez

David is a post-doc at NICS Lab. His research interests include applied cryptography, cloud security, and identity management/privacy. An expert in PRE, his PhD thesis is *New Security Definitions, Constructions and Applications of Proxy Re-encryption*.

Prof. Isaac Agudo

Isaac is an Associate Professor at the University of Malaga. His research interests include applied cryptography for IoT/cloud, digital identity, and authentication/authorization/delegation. He and David are co-inventors of NTRUReEncrypt, quantum-proof PRE.

Prof. Dave Evans

Dave is a Professor of Computer Science at the University of Virginia and Faculty Director of the Secure Computation research group. His research interests include secure multi-party computation, adversarial machine learning, and web security.

John Bantleman

John is a serial entrepreneur with three decades of experience managing high-growth software companies. Most recently, he was the CEO of RainStor, a big data compression company acquired by Teradata (NYSE: TDC). As CEO, he led LBMS and Evolve Software to public offerings on the Nasdaq.

Tony Bishop

Tony is a VP at Equinix and the author of *Next Generation Data Centers*. He is the former Chief Strategy Officer at 451 Research, Global Head of Enterprise Data Centers at Morgan Stanley, and SVP and Chief Architect at Wells Fargo. He was the founder and CEO of Adaptivity, a cloud migration company acquired by EMC.

SUMMARY

NuCypher KMS is a decentralized key management service and cryptographic access control layer for the blockchain and decentralized applications. Developers and enterprises alike can leverage it to create highly-secure applications in healthcare, financial services, and more.

By bringing private data sharing and computation to the public blockchain, NuCypher enables everything from encrypted content marketplaces to secret credentials management to patient-controlled electronic health records.

Today's applications require a more scalable public-key encryption that is better-suited for the kind of data sharing required in modern, distributed systems. To achieve this, NuCypher is pioneering proxy re-encryption, just as RSA Security ushered in a new era of public-key encryption in the 1980s.

tokensale@nucypher.com

NUCYPHER