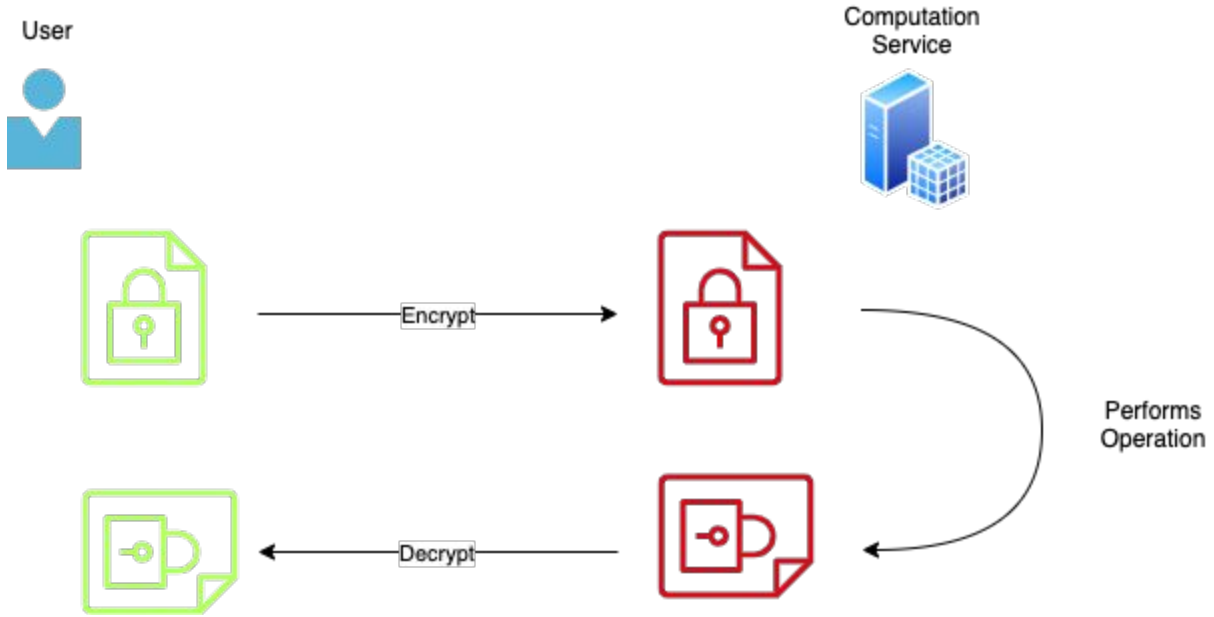
EXTROPY.IO

Associated Technology

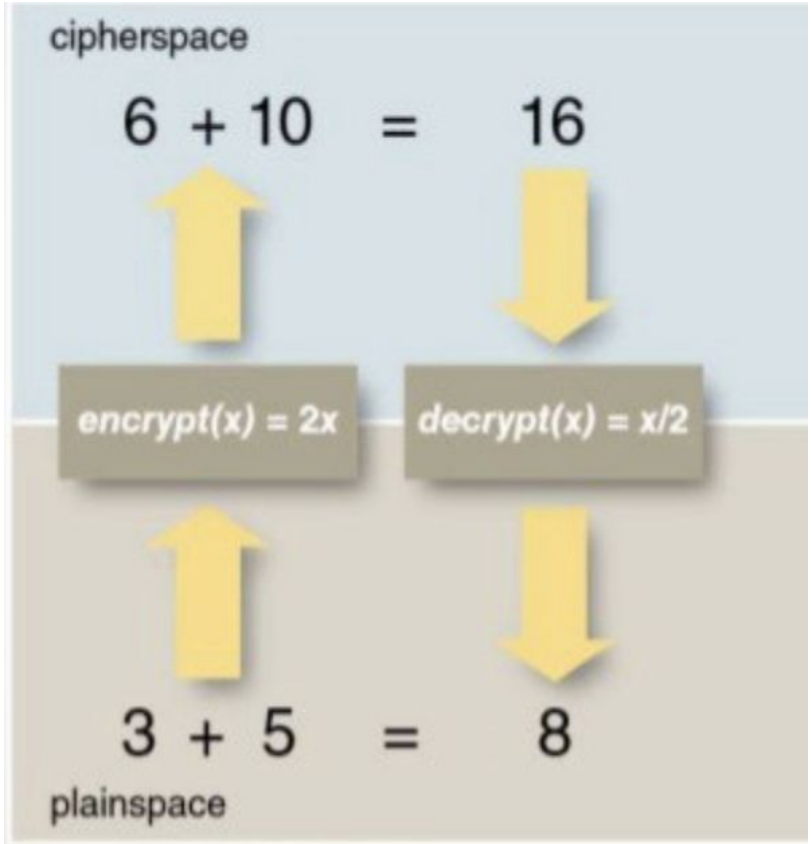
Homomorphic Encryption

Fully or Somewhat

EXTROPY.IO


User
Computation Service
Encrypt
Performs Operation
Decrypt

EXTROPY.IO



Applications

- Analysis of medical data
- Preventing satellite collisions
- Machine Learning on encrypted data

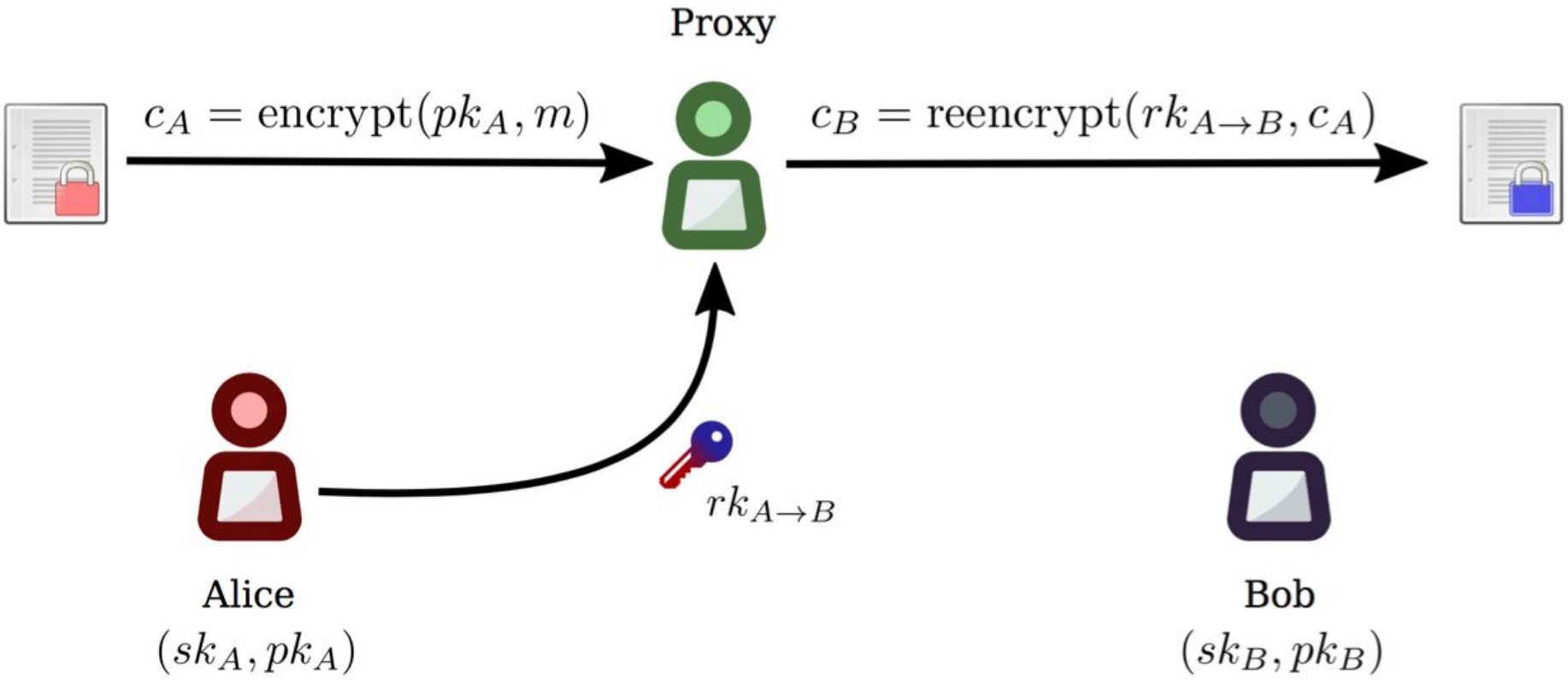
Proxy Re-encryption

Key Management problems

NuCypher KMS

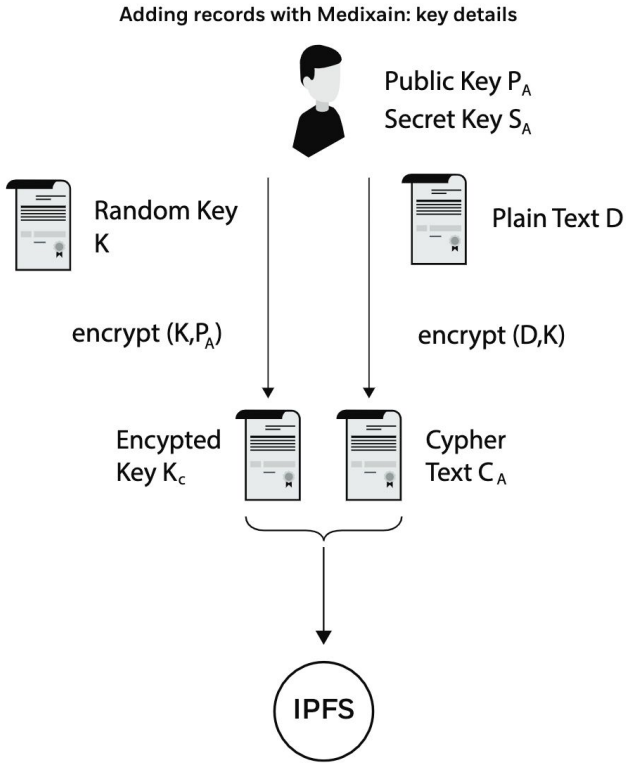
NuCypher KMS is a decentralized Key Management System (KMS) that addresses the limitations of using consensus networks to securely store and manipulate private, encrypted data [1]. It provides encryption and cryptographic access control, performed by a decentralized network, leveraging proxy re-encryption [2]. Unlike centralized KMS as a service solutions, it doesn't require trusting a service provider. NuCypher KMS enables sharing of sensitive data for both decentralized and centralized applications, providing security infrastructure for applications from healthcare to identity management to decentralized content marketplaces. NuCypher KMS will be an essential part of decentralized applications, just as SSL/TLS is an essential part of every secure web application.

Blog


Proxy
$c_A = \text{encrypt}(pk_A, m)$
$c_B = \text{reencrypt}(rk_{A \to B}, c_A)$
$rk_{A \to B}$
Alice
(sk_A, pk_A)
Bob
(sk_B, pk_B)

Medixain

White Paper



Some recent projects using NuCypher

This feed is always for sale - Harberger Tax on digital assets

NuBox - Browser plugin for IPFS

Snowden - Encrypting social media messages

Threshold Proxy Re-encryption

Umbral is a threshold proxy re-encryption scheme that powers the NuCypher network. Alice (the data owner) can delegate decryption rights to Bob for any ciphertext intended to her, through a re-encryption process performed by a set of semi-trusted proxies.

When a threshold of these proxies participate by performing re-encryption, Bob is able to combine these independent re-encryptions and decrypt the original message using his private key.

Umbral Paper

Decentralised Identifiers

EXTROPY.IO

Overview of technology

W3 standard

DIDs are URLs that associate a DID subject with a DID document allowing trustable interactions associated with that subject.
Each DID document can express cryptographic material, verification methods, or service endpoints, which provide a set of mechanisms enabling a DID controller to prove control of the DID.
Service endpoints enable trusted interactions associated with the DID subject. A DID document might contain semantics about the subject that it identifies.
A DID document might contain the DID subject itself (e.g. a data model).

EXTROPY.IO

W3 Standard for verifiable credentials

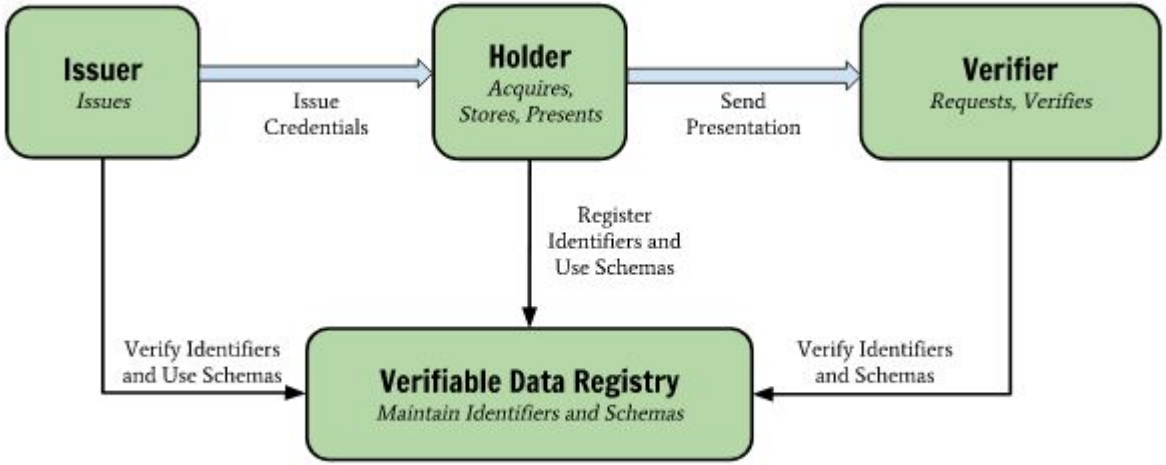


Figure 1 The roles and information flows forming the basis for this specification.

EXTROPY.IO

SSI Wallet and Verifiable Credentials

The Wallet contains verifiable credentials that can cryptographically prove to any verifier:

1. Who (or what) is the issuer;
2. To whom (or what) it was issued;
3. Whether it has been altered since it was issued;
4. Whether it has been revoked by the issuer.

EXTROPY.IO

Hyperledger Indy / Aries

EXTROPY.IO

Hyperledger Aries provides a shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials. It is infrastructure for blockchain-rooted, peer-to-peer interactions. This project consumes the cryptographic support provided by Hyperledger Ursa, to provide secure secret management and decentralized key management functionality.

- A blockchain interface layer (known as a resolver) for creating and signing blockchain transactions
- A cryptographic wallet that can be used for secure storage of cryptographic secrets and other information (the secure storage tech, not a UI) used to build blockchain clients
- An encrypted messaging system for allowing off-ledger interaction between those clients using multiple transport protocols.
- An implementation of ZKP-capable W3C verifiable credentials using the ZKP primitives found in Ursa.
- An implementation of the Decentralized Key Management System (DKMS) specification currently being incubated in Hyperledger Indy.
- A mechanism to build higher-level protocols and API-like use cases based on the secure messaging functionality described earlier.

EXTROPY.IO

Major Companies in this space

- Spherity (MPC from Unbound)
- Microsoft (https://didproject.azurewebsites.net/docs/overview.html)
- Evernym (Sovrin blockchain)
- uPort
- Civic

Spherity

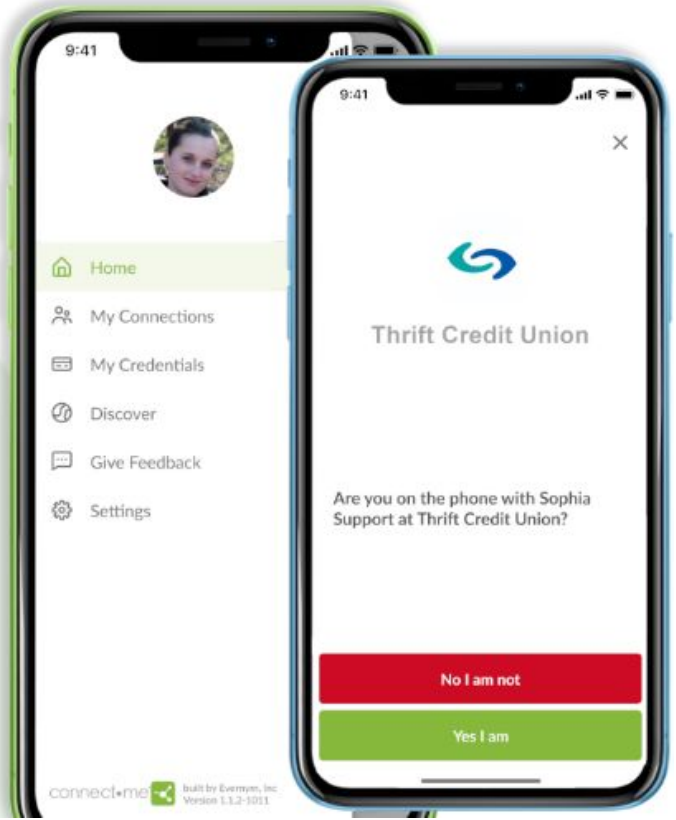
[Spherity Details]

OUR DIGITAL WALLET APP

Connect.Me

- Enable customers and end users to manage all of their digital credentials from the safety of their own phone.
- Create secure, 1:1 communication channels with peers and organizations.
- Share information with confidence, knowing that it will only be seen by you and your connection.
- Use zero-knowledge proofs to eliminate excess data collection.

The original SSI mobile wallet app, already powering live pilots across the financial services and healthcare industries.



EXTROPY.IO

KYC providers

- SecureKey (https://securekey.com/partner-directory/)
  Notable partners: Hyperledger, Intel
- Opus (www.opus.com)
  Notable partners: Experian, Financial Times
- FICO (https://www.fico.com)
  Notable partners: Honeywell, Thames Water, Santander

- Onfido
- Yoti

EXTROPY.IO

General Use Cases

- Websites and other services can verify that patrons are of a legal age, without needing name, location, age, or even birthday;
- Individuals can prove that they are employees of a certain company, or citizens eligible to vote; that they have a certain credit score; that their anonymous tip or whistleblowing is credible, etc., all without revealing their names, addresses, or other personal data;
- Pharma companies can have direct, private connections with patients who have verifiable prescriptions for their medications, without knowing who or where those patients are;
- When privately selling a car or other property, owners can prove their legal ownership without revealing any personal details;
- Internet users can participate pseudonymously in gaming, social, or other online communities.