Table of Contents

Introduction

The proliferation of cryptographic protocols such as Transport Layer Security (TLS) transformed the concept of security on internet from a luxury affored by few into a commodity. With TLS, an average internet user is able to exchange encrypted messages online, use credit cards online, or download files; all without the fear of censorship or compromising his or her computer system.

However, TLS's usefulness is limited outside the boundaries of simple but familiar server-client architectures.

With SSL certificates, it is possible to protect users by providing identities to service providers and ways for users to authenticate them. However, as more and more devices and services are going online. authenticating only service providers is simply not enough; the days of only servers with identities are over, as every user, every device needs a certificate of its own.

We need identities for not only social network services, but digital door locks, refrigerators, and automobiles. We also need new ways for devices and services to identify and authenticate each other without human interactions.

Simply put, existing Public Key Infrastructure (PKI) for providing identities to web services is not good enough. Even Google is developing new technologies such as Certificate Transparency to supplement the shortcomings of the PKI technologies.

Most of limitations of PKI systems come from the centralized nature of PKI providers, and distributed ledger technologies such as blockchain are expected to play a huge role in supplementing and replacing the limited PKI systems.

Blocko's OpenKeyChain is intended to be a robust real life implementation of such a PKI system based on blockchain technology

OpenKeyChain enables developers and users to deploy new PKIs without huge investments by leveraging the existing public blockchain infrastructure; anyone can register and manage certificates for devices and services, and sign or encrypt messages between parties even without TLS involved.

OpenKeyChain is an open standard allowing others to review and extend its ideas. Blocko's Coinstack SDKs include reference implementations of OpenKeyChain; applications on all platforms (servers, clients, and web browers) are supported.

Domains

In order to manage identities using OpenKeyChain, a root domain needs to be created first.

A root domain is a logical equivalent of an individual PKI. Certificates issued under a domain are not compatible with certificates issued under different domains.

Usually, a single domain represents a single organization or an application.

Representation

Each domain is a logical entity; domains and certificates are represented similarily under blockchain.

Domain Organization

Under each domain, other domains and certificates reside.

A domain with a parent as another domain is called a "subdomain." A domain with a child is called a "parent domain."

A domain without any parent is called a "root domain."

Lifecycle

Registration

In order to create a domain, a domain certificate needs to be created.

An OpenKeyChain certificate is composed of a private key and a public key pair, using elliptic curve cryptography with secp256k1 curve.

The certificate created is associated with a domain through a registration record on blockchain.

A registration record is represented as a transaction using OpenKeyChain colored coin protocol. The registration record must conform to OpenKeyChain colored coin standards in order to be recognized as one.

Revocation

In order to revoke a domain created, the domain certificate used to create the domain must be used to create a revocation record on blockchain.

If the domain has a parent domain, the parent domain can revoke the domain on behalf of the domain being revoked.

Identities

With a domain or a subdomain in place, an identity for a device or a user can be created.

Lifecycle

Registration

In order to register a new identity, a certificate must be created beforehand.

An OpenKeyChain certificate for a device or a user is composed of a private key and a public key, just like a certificate for a domain or a subdomain.

The certificate created must be associated with an identity under a domain or a subdomain. A blockchain registration record represents the association.

The registratino record is stored on blockchain as a colored coin transaction, and it must be signed by the identity's parent domain or subdomain.

Revocation

In order to revoke an identity created, the domain certificate used to create the identity must be used to create a revocation record on blockchain.

The identity's parent domain or subdomain can revoke the domain on behalf as well.

Record Format

OpenKeyChain registration records are stored as colord coin transactions on blockchain. Those colored coin transactions must conform to the following rules.

- Each transaction must contain OpenKeyChain marker output in order to be considered as a valid OpenKeyChain transaction.
- A valid OpenKeyChain marker output must contain following fields.

Field	Description	Size
Marker	Magic bytes indicating that this output is an OpenKeyChain marker output. It must be 0x4B43.	2 bytes
Version	Major, Minor version information. 0x0100 for now (1.0)	2 bytes
OP code	An opcode representing an operation represented by the output.	2 bytes
Payload	Additional information or metadata.	Varies

- In order to create a subdomain or an identity under another domain or a subdomain, a new OpenKeyChain registration record transaction from the parent domain/subdomain to the subdomain/identity created must be forged and signed using the parent domain/subdomain certificate.
- The public key of the new subdomain/identity being created must be represented as an address format in the output right before the marker output. If the transaction lacks such an output before the marker output, the transaction is considered invalid.
- All following outputs after the marker output are ignored.

Channels

Conclustion