Whitepaper Cryptelo Platform

Secure key Management
for the
Blockchain Generation

The Solution to a Major Flaw in Today’s Digital World.

Table of contents

Disclaimer

This document is for informational purposes only and does not constitute an offer to sell or solicitation of an offer to buy shares or securities in Cryptelo, Inc. or any related or associated affiliates or any Cryptelo Tokens. Any such offer or solicitation to acquire rights to acquire Tokens will be made only by means of the Simple Agreement for Future Tokens (SAFT) and Confidential Private Placement Offering Memorandum (PPM) and in accordance with the terms of all applicable securities and other laws. The ownership of Cryptelo Tokens carries no rights, expressed or implied, other than the right to use Tokens as a means for access and usage of Cryptelo Platform service.

Introduction

One of the biggest challenge for the future of digital economy and digital world resides in preserving secrecy and ensuring privacy. But, citizens and economical actors don't just want only secrecy, they also want quantifiable secrecy. The point is not only to ensure confidentiality of data, but also to be able to be sure that confidentiality of data is ensured. On of the way to provide the expected solution to protect quantifiable privacy is to rely on cryptographic based solution.
In the cryptography as we know it, there is this common notion that almost all encryption and decryption algorithms that make critical infrastructures we use daily possible, consider as an input to the lock - the key.
Because, algorithms are computer software where source code exist on some computer and then can be leaked easily, and on the other hand, a secret key is a small element that can be more efficiently managed and kept secret (it is easier to replace a compromised key then to redevelop a complete algorithm from scratch).
And when protecting sensitive information using encryption, then, the most sensitive element is the key(s) that close or open the lock, and how key(s) are managed and not the lock itself and risk of leaking sensitive information relies on key(s) management weaknesses.
Once keys are issued, key management typically consists of three steps:

- Exchange,
- Storage,
- Use.

In each of these steps, there are significant challenges:

1. Complexity: Managing a large number of encryption keys.
2. Security: Vulnerability of keys from outside hackers and malicious insiders.
3. Data availability: Ensuring data accessibility for authorized users.

4. Scalability: Supporting multiple databases, applications and standards.
5. Governance: Defining policy driven access control and protection for data. Governance includes compliance with data protection requirements.

A key management system (KMS), also known as a cryptographic key management system (CKMS), is an integrated approach for generating, distributing and managing cryptographic keys for devices and applications. With the Internet of Things, KMS becomes a crucial part for the security of connected devices. Secure key exchange and management capable to overcome all previous challenges exist, but these capabilities are reserved only for those with advanced cryptology skills and experience - something that only some corporations and crypto geeks can manage. On another hand, as of today, the most common way to manage the asymmetric cryptography is to use the pair public/private key. A central problem with the use of public key cryptography is confidence/proof that a particular public key is authentic, in that it is correct and belongs to the person or entity claimed, and has not been tampered with or replaced by a malicious third party. The usual approach to this problem is to use a public key infrastructure (PKI), in which one or more third parties – known as certificate authorities – certify ownership of key pairs.

And finally, one of the last disruptive technology supporting the future digital era is the blockchain one. Blockchain delivers a complete different approach to storing information, making transactions, performing functions, and establishing trust, which makes it particularly suitable for environments with high security requirements for actors that might have low trust among themselves. Blockchain actual innovation is the removal of need for a trusted third party to verify the integrity of data and addresses the fundamental flaws of security by removing the human factor from the equation, which is usually the weakest link.
By leveraging a distributed ledger and taking away the risk of a single point of failure, blockchain technology has enabled end-to-end privacy and encryption while still ensuring convenience for users.
The intersection of these technologies is where Cryptelo wants to exist and lead digital evolution. We think of public/private key encrypted communication and blockchain ledgers as “secure” and providing the Crypto key management platform will deliver solution for our digital society that requires simplified and democratized access to such level of security. An innovative approach that will allow developers and companies to build security into their applications or infrastructure without the need to be a crypto expert or to allocate an exorbitant budget.

What is Cryptelo

Since 2014, the firm Cryptelo develops cutting-edge software solutions for corporate communication with the highest available level of security. Cryptelo’s unique

cryptographic design was created by the world's leading cryptologist, Dr. Klima and security expert Gen. Andor Šándor having over thirty years of experience in that domain.
Cryptelo has security-first architecture and services for encrypted data storage, key management, and communication which is vital to achieve this high standard for peace of mind, and the proper functioning of free expression and exchange of information in the digital world.

Cryptelo develops leading software platform & solutions designed for the global market and Cryptelo is constantly evolving based on increasing demands for better protect confidentiality, secrecy and privacy.

The company aspires to achieve its long-term vision of a full and fair communication environment, where the value of unique, quality ideas and the right to privacy stands high above ruthless competition practices.

Cryptelo is already offering the Cryptelo Drive, premium product designed specifically for B2B sales and provides an encrypted virtual drive for companies where users with user account can access their data via web and desktop application and can easily upload, share and edit any type of files.

But Cryptelo is also building the new generation of digital key secured management platform and services implementing *the trustless key server* concept and providing solution about fixing the *web-of-trust, C.A and other standards*.
Cryptelo company is an effective path to solve a worldwide security problem – providing totally secure shared data solution with no compromise between security and user-friendliness in removing risks of relying on third-parties in the chain of trust.

Our vision is one in which digital information is as secure as the information in a person's own mind. Human security risks can never be eliminated, but we believe that all systemic security risks have a solution.

Market Opportunity

In order to reach the objectives fulfilling our vision, Cryptelo will deliver or is already delivering innovative security solutions in different promising domains, where the following will provide our best opportunities.

Public Key Infrastructure

Back to 2011 when for the first time a major actor in the information security business get hacked, RSA. Since that day, security community knows that security, secrecy and privacy relying on 3rd parties cannot be ensured anymore.

The RSA attack itself involved a targeted phishing campaign that used a Flash object embedded in an Excel file. The assault, probably selected after reconnaissance work on social networking sites, was ultimately aimed at planting back-door malware on machines on RSA's network, according to a blog post by Uri Rivner, head of new technologies, identity protection and verification at RSA.

Consequences were disastrous, APTs, sensitive data leakage, secure ID seeds lifted, RSA's database of serial numbers compromised. In the months following the attack, RSA bought eight robots to increase manufacturing seven-fold to meet customer demand for replacement tokens and tried to limit damage to its reputation within the industry as much as possible.

Meanwhile, customers struggled to replace tokens and rethink their security processes. The RSA breach gave its competitors a window of opportunity as some organizations looked to alternative technologies. At that time, the blockchain technology and its associated incredible leveraging possibilities was not yet develop enough to provide pertinent answer to this security issue. Luckily, time has passed and the new era of blockchain is raising.

Cryptelo is now ready to provide a new blockchain based technology to provide greater security and cost benefits to key management that will bring new time for PKI and Certification Authority.

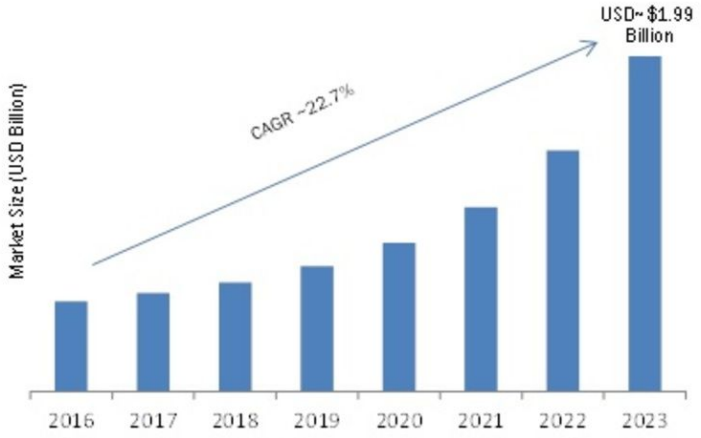
The last Market Research Future“Public Key Infrastructure Market Research Report-Forecast 2023” indicates that “*the usage of Public Key Infrastructure Market has enhanced the operational efficiency of the business at the optimum cost. These solutions support the organization to reduce the cost for storing signatures on paper, and is leading to a decreased operational cost*”

...

“*The prominent players in the Public Key Infrastructure system Market are –Docusign Inc.(U.S), Comodo Group Inc.(U.S), Kofax Ltd. (U.S), GoDaddy Inc.(U.S), GMO GlobalSign Inc. (U.S), Verisign Inc.(U.S), Gemalto N.V.(Netherlands), Signix Inc.(U.S), Ascertia Company (U.S), Secured Signing Limited (Australia)Entrust Data Cartd Corporation (U.S) and Identrust Inc.(U.S) among others.*”

...

“*The global Public Key Infrastructure market is expected to grow at USD$ ~1.99 Billion by 2023, at ~22.7% of CAGR between 2017 and 2023.*”



"*The Public Key Infrastructure market in Europe region is expected to witness rapid growth. Whereas, Asia-Pacific countries like China, Japan and South Korea is an emerging market for Public Key Infrastructure market. This market has huge potential for growth of Public Key Infrastructure specifically the country like China due to the growth rapid industrialization, and increasing focus on security threats in this region.*"

That tends to demonstrate that market for key management solutions will increase and leave space for newcomer to settle and develop innovative solutions. Especially in Europe and in Asia where it does not exist yet a real competitive market for that sector.

Furthermore, the PKI Global Trends Study OCTOBER 2016 from Ponemon Institute LLC, indicates that : "*the most significant challenge organizations will continue to face, with respect to enabling applications to use PKI, is the inability of existing PKI to support new applications for 58 percent of respondents*" which means that legacy PKI environment will not be able to support new technology/application which requires to be scalable enough. That will drive many companies in the world to challenge their current environment and include newcomers into their list of future security provider and provide Cryptelo with the opportunity to lead these newcomers.

Encryption as a service

Encryption as a Service (EaaS) technology provides a cloud-centric approach to security, where the capabilities of a single service provider can be used to encrypt data on many cloud platforms and devices, at any time, from any location and securely.

It occurs many times that security controls are bypassed by employees or individuals whenever these controls are perceived and conflicting with their need to do their job or accessing information/applications. They use the most effective tools and solutions to do their work or use applications, including cloud applications, platforms and infrastructures, from any device and any location. In order to balance efficiency, security and productivity, they need to be listened and supported. With Cryptelo Platform they won't have to sacrifice one for another.

Today EaaS is well positioned to support organization and companies to achieve that balance and especially protect data in the cloud.

Cryptelo platform is ready to provide full EaaS services. But what benefits are expected from EaaS technology and platforms ?

On first hand, EaaS avoids the disadvantages to have to manage disparate encryption technologies. Many times, it occurs that companies as well as individuals have to deal with different encryption technology to save, store, copy or transfer their data. It impacts their cost and time for management and risks associated with mixing different technologies all together.

Furthermore, encryption key management must be taken into consideration. Different technologies will require dedicated key management technologies, each of which comes with a maintenance cost and security risk, combining the cost issues of all mixed architecture.

As the single encryption source, central key storage/management can provide cost reduction and risk mitigation. A mature EaaS solution will provide options such that keys can either be owned by the provider or the consumer even if decision about who owns the keys and where they should be stored/saved is always a polemical discussion.
Cryptelo platform will provide a reliable platform that enables its core functionality accessible securely. This is how the future and pragmatic use of encryption will be best used.

On a second hand, it’s still visible that not all cloud application and not all cloud provider have not yet tackle the end-to-end encryption issues from within without being able to provide protected data in motion or data at rest in their infrastructure.

By using them alongside the Cryptelo API, there will be little or no loss of platform functionality, while enabling a better user experience and no additional costs. But many cloud platforms or cloud storage providers support extensibility and

integrations through APIs and could add encryption function to their product by using this API.

And finally, EaaS platform is able to provide secured collaborative environment allowing companies to tackle the issue of providing access to third parties securely into their cloud resources.

Cryptelo platform is integrating EaaS features with such a secure, granular encryption system support, while providing the users to benefit from the full capabilities of the cloud platform's apps, all without obstacles.

"*Encryption Software Market by Component (Solution and Services), Application (Disk Encryption, File/Folder Encryption, Communication Encryption, and Cloud Encryption), Deployment Type, Organization Size, Vertical, and Region - Global Forecast to 2022", The encryption software market size is expected to grow from USD 3.87 Billion in 2017 to USD 12.96 Billion by 2022, at a Compound Annual Growth Rate (CAGR) of 27.4%.*[1]

"*The demand for encryption software is majorly driven by stringent government regulations and the need to protect critical organizational. With the increasing demand for cloud and virtualization across different verticals, the adoption rate of encryption software among enterprises is expected to gain a major traction during the forecast period*."

The major vendors providing encryption software solution and services are Thales e-Security (La Defense, France), Gemalto (Amsterdam, Netherlands), Symantec (California, US), Dell (Texas, US), Sophos (Abingdon, UK), McAfee (California, US), Trend Micro (Tokyo, Japan), IBM (New York, US), Microsoft (Washington, US), PKWARE (Wisconsin, US), CipherCloud (California, US), ESET (Bratislava, Slovakia).

Cloud storage encryption

Cloud encryption is a service offered by cloud storage providers whereby data, or text, is transformed using encryption algorithms and is then placed on a storage cloud. Cloud encryption is the transformation of a cloud service customer's data into ciphertext. Cloud encryption is almost identical to in-house encryption with one important difference, the cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud

[1] marketsandmarkets.com report

encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted.

Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud.

To keep costs low, some cloud providers have been offering alternatives to encryption that don't require as much processing power. These techniques include redacting or obfuscating data that needs to remain confidential or the use of proprietary encryption algorithms created by the vendor.

In the past, many businesses felt comfortable allowing the cloud provider to manage encryption keys, believing that security risks could could be managed through contracts, controls and audits. Over time it has become apparent, however, that cloud providers cannot honor such commitments when responding to government requests for information.

After two years developing its own cloud storage encryption product, Cryptelo Drive, it became available, first through sales representatives in the Czech and Slovak markets in 2016, and later, gradually to other Eastern European states, Israel and global markets through selected distributors.

Hand in hand with an increased number of paying customers and active users of the free demo products, the development of existing products is still going on in response to market demands and new security threats, as well as an expansion of the product portfolio.

With Cryptelo drive, data security is in the hands of the users themselves. They are the owners of data, they are responsible for the data and they don't have to rely on a third party (service provider).

- The data is accessible only to the person to whom you give it to yourself.
- Data cannot be obtained by hackers, IT administrators or system creators.
- Cryptelo drive protects the data itself. In cases where the server is stolen or a computer is attacked, the data cannot be recovered.
- Cryptelo drive gives users the right to privacy – it obscures their names, directory structures, file names, and the very existence of communication between users.

The marketsandmarkets.com report "*Cloud Encryption Market by Component (Solution and Service), Service Model (Infrastructure-as-a-Service, Software-as-a-Service, and Platform-as-a-Service), Organization Size, Vertical, and Region - Global Forecast to 2022", expresses that "the cloud encryption market is expected to grow from USD 529.5 Million in 2016 to USD 2,401.9 Million by 2022, at a Compound Annual Growth Rate (CAGR) of 30.1% during the forecast period*."

"Proliferation in the cloud adoption and virtualization, and stringent regulations to increase the adoption of cloud encryption solutions are some of the factors fueling the growth of the market across the globe. The base year considered for this study is 2016, and the forecast period is 2017–2022."

The major vendors providing cloud storage encryption are Sookasa, Viivo, BoxCryptor, Cryptomator, AxCrypt AB, Ncrypted, Secure Cloud Systems Inc, NewSoftwares.net, Sync, Spideroak and Tresorit.

Token Details

Our token is an ERC20 token as defined by the standards in the ethereum community.
Name: Cryptelo token
Symbol: CTL
Total supply: 850,000,000 tokens
Contract Address: Will be posted on the official website

On top of these tokens sits a crowdfunding smart contract that does the token distribution based on the rules described below.

Token allocation

Closed Investors	100,000,000.00
Public Sale	250,000,000.00
Company	250,000,000.00
Bounty	250,000,000.00

Closed investors are the ones we have picked to allow initial investment before the ICO and two weeks after the ICO for strategic purposes. In the beginning these investors have received a 50% discount on the token price for taking the extra risk to be first.
At the end of the ICO after the end of February where the strategic investors phase is completed, any tokens not sold from this phase will be burned.
Public Sale is for tokens during the ICO. At the closing of the ICO date, any remaining tokens will be burned.
Token allocation for the company expenses is split as follows:

Bounty Program is our way of funding application development in our platform. We believe that all token holders reserve a right of opinion and decision making on what is going to increase their token value. Therefore this bounty is reserved for later projects that want to be built on top of Cryptelo Platform. Token holders will vote on projects that they like and based on the amount of tokens that they hold, they will have more or less voting power to influence decisions on where does this fund go towards. Our vision is to have software build on top of Cryptelo that increases token usage, therefore value.

Token economy

Cryptelo Platform provides server API. Companies build 3rd party applications using our crypto library, that communicate by server API. Cryptelo Platform is provided as SaaS (Software as a service). API requests are paid and only way how to pay is Cryptelo Tokens. The bigger use of Cryptelo Platform will be, the higher demand of Cryptelo Tokens will be. High demand of tokens will increase its value, because total amount is limited.

Cryptelo Use Cases

Home IoT network : All IoT devices will be more securely identified when interacting within a local/home network. That can achieved through association of PKI and blockchain where all identities are trusted and cryptographically provable, they are all members of home PKI and their shared relationships are stored on log ledger based on blockchain (Root of Trust).

EaaS used to secure Email Communications : The need for companies to be able to communicate and exchange data more securely with both clients and suppliers is increasing every day. As of today, email has always been the favorite channel and then can now be addressed with blockchain based EaaS. No more need to manage certificates into an old email application, as the new email client generates a new secret key specifically for protecting that content, but the recipient must have the secret key to decrypt the content as well. After mutual successful authentication, the recipient is able to read the unencrypted after receiving automatically the secret key and the access policy defined by sender.

Cloud storage encryption :
Cryptelo Drive is an encrypted virtual drive for companies. Users with user account can access their data via web and desktop application. They can easily upload, share and edit any type of file. Exchange, store or share personal data with your client securely and ensure your technical compliance with GDPR or protect and share patient records securely. It increases protection level of your confidential information on collaborative environment among your top teams for your strategical projects.

Solution

Cryptelo uses technology similar to blockchain to deliver platform where security is not guaranteed by server software or the company and people operating it, but by protocols used. Such technology is needed when you want to empower software libraries, client applications and their users with ability to prove, that no one had tampered with their data.

Blockchain & Cryptelo

Every piece of information saved in the system is called a record. Every record has its unique ID which is computed as a hash of its contents. Records can be connected together by embedding last record ID inside new records, forming chains. These chains then have some useful properties; mainly clients can verify that:

- the chain had not been forked (two child records with same parent ID exist)
- the chain is continuous - meaning every record from the chain had been sent to the client by the server and there are no gaps. By replying the information recorded in particular record chain, the client will arrive at final state of some particular topic. Record chain is the idea upon which Cryptelo Drive (sharable, private, file storage) is built.
- every record is consistent and the data, the client received from the server hasn't been changed. Client can easily verify that the hash of the record's data resolves to the ID it already knows.

Records

Record is the smallest piece of information client can store on the server. Parts of the record can be stored in plaintext and parts can be encrypted. Each record can have a parent making it a part of the chain. Each record has to conform to a predefined structure and can consist of any of following sections:

Record Policy

This section stores (in plaintext) public parts of keys which are needed to operate on this record. Currently the most important key is the **write** key, which allows clients to append more records to the chain. If a write key is specified, then any client trying to append to that record has to sign its new record with appropriate secret key. Server (and other clients) can then verify that the appended record comes from someone who proved to know the right secret key and they can do so without knowing the private key themselves.

Public part

Holds any information which can/must be seen in plaintext by other clients, or actors in the system.

Private part

Stores information in ciphertext and is opaque to any other actor in the system, who does not hold the key required to decrypt it.

Signature

If the record is guarded by a write key, then each appended child record must also be signed by that key. This allows the server and other clients to verify, that the new record has been created by someone who has gained access to the write key.

Record Hash

Record hash (record id) is computed from all the parts mentioned earlier, effectively protecting whole record from unwanted modifications. Hashing a record is precisely specified, to be sure, that different clients (on possibly different platforms) come up with same value for same input. Our hashing scheme is built upon Merkle trees.

Root record

Root record is special kind of record, since it is the first node in the record chain and does not have any parent. Right now only root records have policy embedded in them, and the whole record chain then shares this policy.

Appending to the chain

If someone wants to append to arbitrary chain which has a write key defined in its policy, he must cryptographically sign his record with the appropriate write private key. This signature then allows anyone to verify if such modification comes from someone who has the knowledge of the right key.

Cryptelo library can then handle the task of distributing correct keys among selected actors to selected record chains in the system.
Right now we are able to distribute the key needed to decrypt the private part of the record separately from the write key. This means that user sharing access to a chain can pick if he wants the other party to have either read access only, or both read&write access.

User identity

For all purposes the system only relies on identity verification based on asymmetric cryptography.
Users, on the other hand, want to communicate with people they know by name not by their public keys, which are used to implement the system.
This is usually achieved by employing two different ways of thinking about user identity:

PKI and CA

Public key infrastructure is a way of binding public key to an identity. The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Systems and users trusting the CA can then trust the mapping of Public keys and the identities issued by the CA. But Certificate Authorities present Single point of failures. When compromised, all users trusting the CA are in danger of their communication being spoofed, since they can no longer be sure they are communicating with the correct person or entity.
PKI is the building block of Transport Layer Security (TLS), client-server communication encryption scheme. TLS usage is growing as users need to transmit and share increasingly more sensitive data with online services and other users, all that in the environment of ever present threat of eavesdropping and state-level surveillance. TLS relies on certificates being granted by trusted CAs. However, the CA ecosystem is fragile and prone to compromises and operational errors. Failures resulting in CA granting certificates to 3rd parties, which did not control target domains have happened all over the world, including US (Comodo), China (CNNIC), France (ANSSI). Recently, Symantec (more than 20% of certificate share) issued certificates without properly validating ownership of target domains and is now in process of being deprecated and removed from trusted CAs of Chrome (most widely used web browser).
Multi

Web of trust

Web of trust is decentralized alternative to the centralized trust model of a public key infrastructure (PKI). Identity certificates containing owner information and public key can be digitally signed by other users who, by that act, endorse the association of that public key with the entity listed in the certificate.
It also allows each person to have his own group of people, which the person trusts, or by employing some vetting scheme, sharing these endorsements and trusting them among groups of people.
Each new certificate has to be endorsed by some or all members of the group to become trustworthy for the clients, depending on vetting scheme employed. It might be difficult or time consuming to reach enough users to get the endorsements needed to pass the required threshold.

Cryptelo & Present User Identity

Currently, all user identities need to be verified by a single gatekeeper. Verified identities and corresponding public keys are then signed by him and stored on the server. Thanks to this process we are able to mitigate the risk of MITM and attackers impersonating regular users. This process proved to be cumbersome for bigger groups of people. Based on feedback from existing customers (SMBs and corporations), user verification process has to be easier and more flexible to integrate, but still has to provide same level of protection, on which the rest of the system relies.

Currently we are researching and considering the implementation of Hierarchical Deterministic Key Pairs to ensure user anonymity in the blockchain. This feature is currently entering PoC phase and might still be removed, if we find it unsuitable or better solution will be found.

Identity in the Blockchain

As part of the effort of building a platform we want to embrace blockchain technology and use it to store user identities. This will provide us with transparency, auditability, immutability and verifiability of critical part of our platform.

Every customer can create their own group. Each group's name is reflected as a domain name on the internet. Prior to the group being deployed, the *Administrator* has to prove control of associated domain. After successfully verifying namespace domain, Smart Contract, which will be responsible for user identity verification, will be appended to the blockchain. This contract can then be used to revoke membership later and provides public record and insight into a critical part of the system.

Namespace verification

Namespace is equal to standard domain name on internet, which the *Administrator* has to prove is under his control. The verification process will require either placing information at correct endpoint, or creating specific DNS records. Namespace will be deactivate when the verification fails. Verification is an ongoing process and if the *Administrator* wants the namespace to be active, ownership checks have to pass regularly.

Hierarchical Deterministic Key Pair

To preserve user anonymity in the blockchain we are considering implementation of HD Key Pairs. The way it works is that each identity in our system has its own generated seed key, from which use, time and record specific keys are created at almost every interaction that requires access rights (creation or modification). Therefore the user has a different key for every record or smart contract. Generating the keys in this manner, allows us to increase the security of the whole system. In case one of the keys is somehow compromised, only the information related to that specific key gets compromised. All the other records remain safe. As we have seen in major hacks of different cryptosystems including exchanges, they are usually compromised as a whole. Fragmenting our system means that in case of a break in

we are still safe for the most part of the system and we can intervene and undo the damage faster.
Since the user has their seed keys, it means that all of the data encrypted by derived keys can be decrypted and any damage undone from the seed key. In this manner if we have to perform an intervention in a part of the system we can do it by notifying the user and having them use their seed keys.

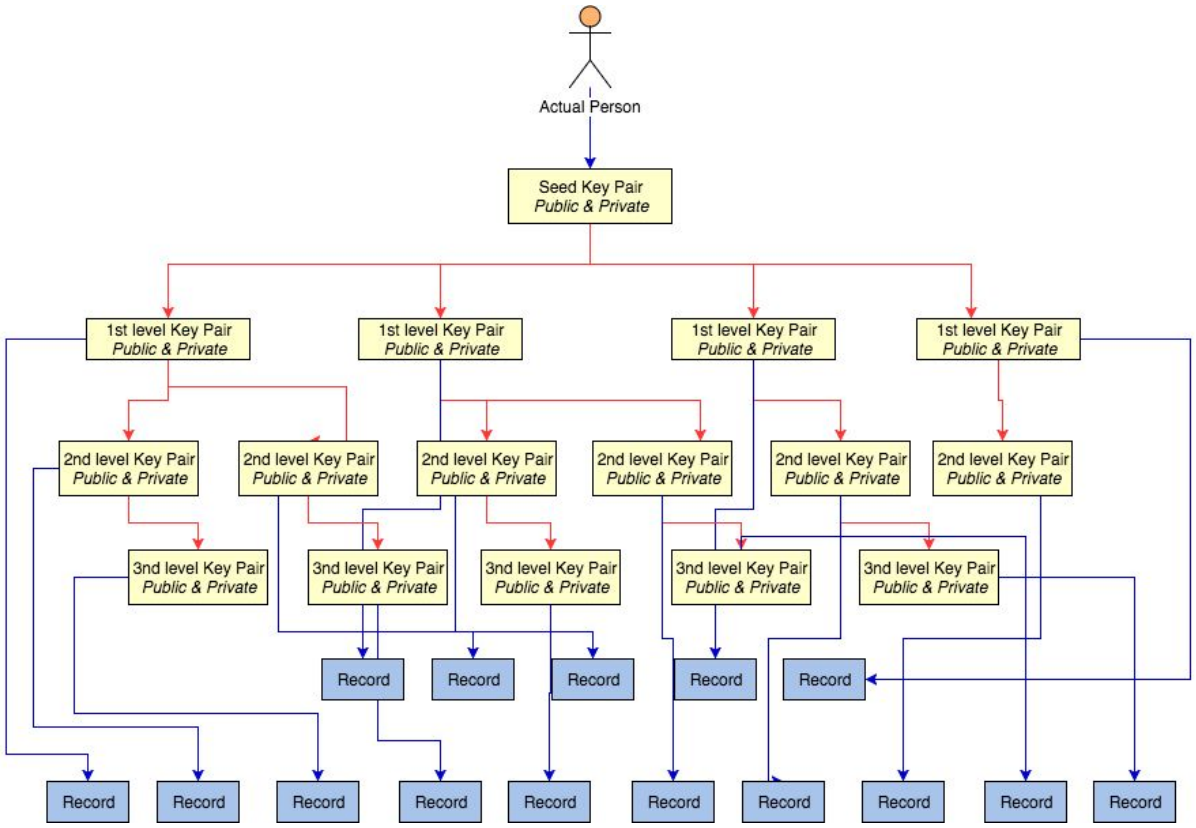


Diagram 1: Different levels of HD Keys, their relation to the person and to records

Blockchain

Common public key issue is when someone can replace the key that represents a certain identity. Blockchain is a great solution in this case because it has immutable properties that keep it completely auditable and consistent among several stakeholders. In order to achieve all these well known blockchain benefits, our architecture will store keys in the blockchain solution that consists of five main components, namely:

- Master Controller
- Business Logic
- Access Control
- Instance Specific Controller
- Instance Transactions

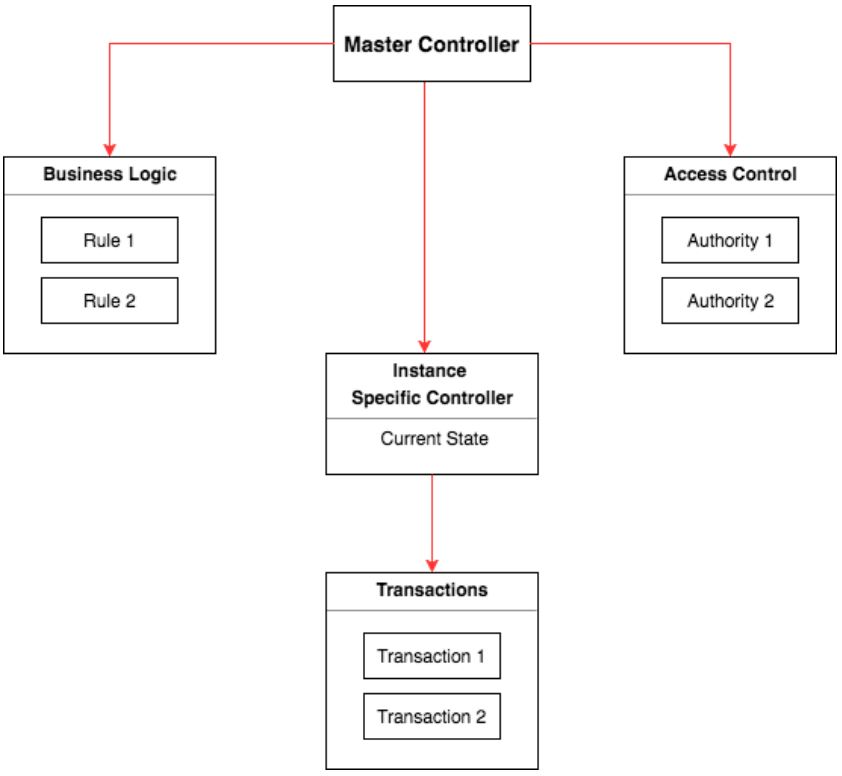


Diagram 2: Explaining components of the smart contract which we call Controller

Together these components communicate with the rest of already established Cryptelo platform while providing the main pillars of functionality that need to be reached. Using this architecture we achieve:

Consensus
All involved parties trust the technology since the access control structure is jointly defined and all state changes are confirmed in unison.

Immutability
Any change, no matter how small constitutes a forever altering of the chain and it is so immutable. Every new change pushed into the system has to confirm that it is not violating any of the previous state changes, therefore adding an extra level of immutability and security of actions to make the system tamper-proof. Timestamps are an ingrained part of the chain and they represent the exact time each event occurred.

Governance
There is no way to reverse or arbitrarily change a given public key state without having the right signatures needed for the transaction.

Independent Verifiability
At any given time whether voluntarily invoked, or in case of an event, the state of the whole chain, specific state, or small part of the chain can be verified mathematically from an independent party.

Ecosystem

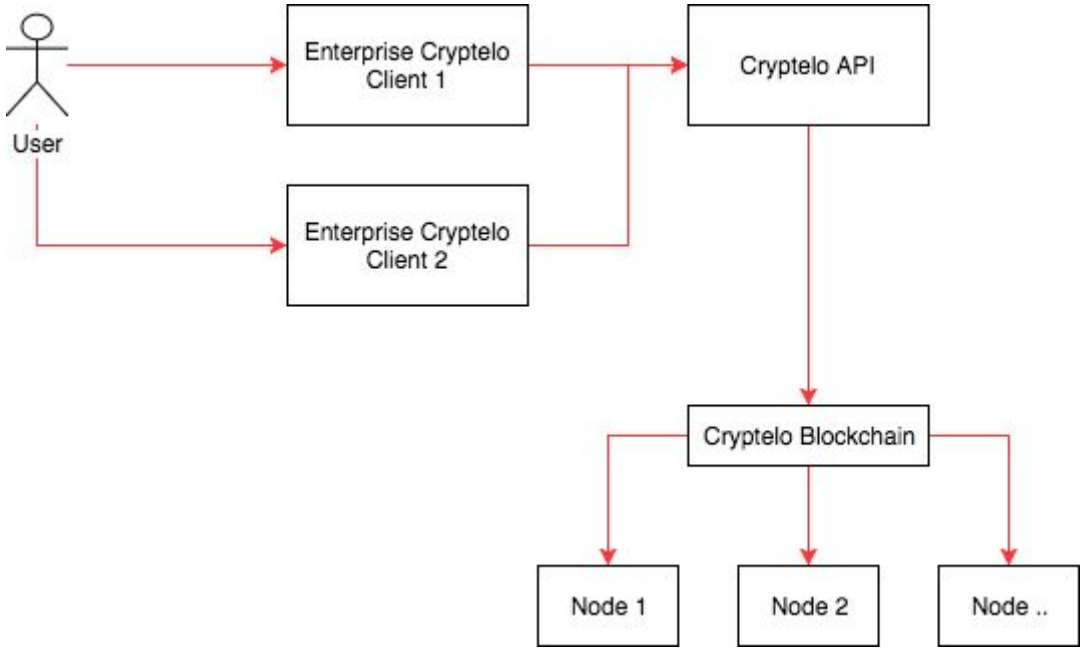


Diagram 3: High level ecosystem description: How Enterprise and users interact with Cryptelo

EaaS used to secure Email Communications : The need for companies to be able to communicate and exchange data more securely with both clients and suppliers is increasing every day. As of today, email has always been the favorite channel, which can now be addressed with blockchain based EaaS. No more need to manage certificates in an old email application. New email client can generate new secret key specifically for protecting that content, but then, the recipient must obtain the secret key to decrypt the content properly as well. This is where Cryptelo platform can help, as it delivers state of the art cryptography implementation to address these issues.

Cloud storage encryption :
Cryptelo Drive is an encrypted virtual drive for companies. Users with accounts can access their data via web, desktop and directly as part of their local file system. They can easily upload, share and edit any type of file. Exchange, store or share sensitive data with your clients and colleagues securely and ensure your technical compliance with GDPR (eg. patient records, contracts). Cryptelo Drive will increase protection of your confidential information in collaborative environment for your teams and strategical projects.

Smart Contracts and Cryptelo Platform

Current Cryptelo implementation is based exclusively on records that are described in detail above, they have their own powerful set of features focused on data security and user

privacy. But we found out that whole concept is hard to extend. To address that, we decided to integrate smart contracts and utilize their extensibility and powerful features.
New smart contract is generated at the time of creation of every record. It serves as the entity that is in complete control of associated record. It controls who, when and what sort of operations can be performed on it. We can provide smart contract templates for general use cases, with added benefit of easily implementing custom features and systems required by enterprises or regular users. Smart contracts also provide a layer of transparency and rules that are self-enforced (even Cryptelo cannot change them) and they allow anyone from anywhere to use their tokens to develop custom mini-system in form of a smart contract on top of our platform.

To achieve privacy even when we are integrating with blockchain technology, which is public in nature, we use unique key for every piece of information stored in cryptelo. Identities of users or other actors in the system, are then hidden in the private (and encrypted) part of records. Smart contracts use only the public parts of generated key pairs, which for any observer are effectively random.

1. Records and Smart Contracts

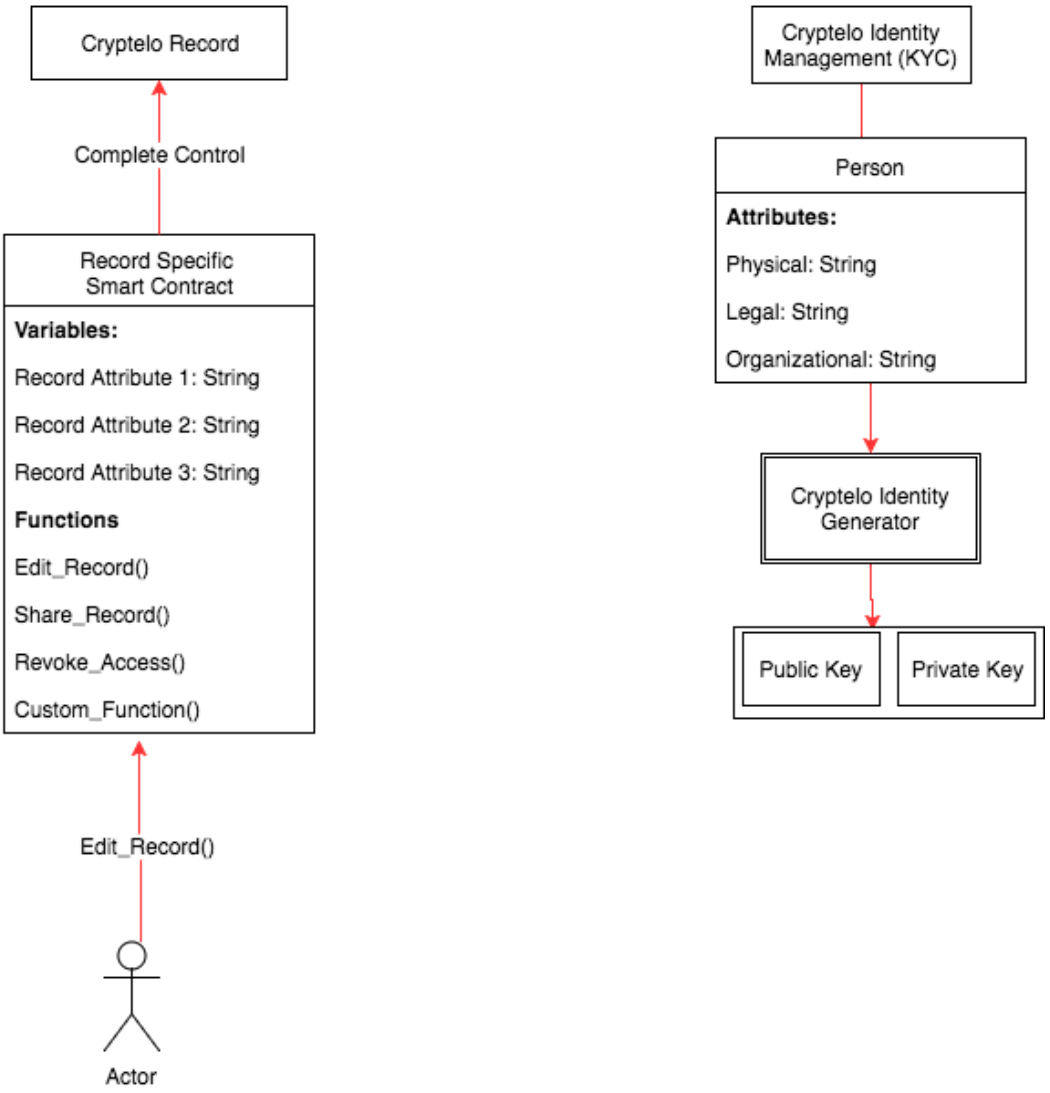


Diagram 4: How does Cryptelo connect smart contracts and the records including identity generator and management

Dev Roadmap

Milestones

- 1Y
    - blockchain and smart contract technology integration
    - server API creation
- 1,5Y
    - Library for web application
- 2Y
    - Library for android
    - Library for iOS
    - Library for IoT devices
    - Library for desktop (Windows & Mac)

Disclaimer and Risks Declaration

This document, Cryptelo website and Cryptelo Token sale is in no way a solicitation or offer to buy or sell securities. The information in this document, on the Cryptelo website and Cryptelo Token sale has not been approved or verified by the United States Securities and Exchange Commission or by any state or government securities authority. You should only purchase Cryptelo Tokens for the rights to use and access Cryptelo utilities and services. In no way does your purchase grant you equity, ownership interest, rights to revenue, or profit sharing in Cryptelo s.r.o. or any affiliated entity. Purchasing Cryptelo Tokens may not be suitable for you and involves risks that you may or may not receive value for your purchase. It is recommended that you consult an independent investment advisor and/or attorney prior to any purchase. Cryptelo s.r.o., their members, employees, managers, and shareholders shall accept no liability for any loss, financial or otherwise arising from the use of the Cryptelo services or the purchase or use of Cryptelo Tokens.
READ OUR DISCLAIMERS AND RISK FACTORS PRIOR TO ANY PURCHASE OF CRYPTELO TOKENS. YOUR PURCHASE IS AN ACCEPTANCE OF THESE DISCLAIMERS AND RISK FACTORS.

The purchase of Cryptelo Tokens is only for sophisticated purchasers who are knowledgeable and experienced in the technical and business features and risks of cryptographic tokens, token storage mechanisms and blockchain technology.

No recommendation, representation or warranty, express or implied, is given by any person as to the accuracy or completeness of the information (which includes forward-looking statements) and opinions contained in this document, and no responsibility or liability is accepted for the accuracy or sufficiency of any of the information or opinions, for any errors, omissions or misunderstandings, negligent or otherwise, or for any other communication, written or otherwise, in connection with the terms in this document. No liability is accepted for any loss, cost or damage suffered or incurred as a result of the reliance on such information, forward-looking statements, opinions or beliefs.

You should independently assess the information contained in this document, and take such additional professional, technical or other advice, or seek such other information, as you consider necessary or appropriate in respect of any decision you may make to purchase Cryptelo Tokens. You should not rely on the information contained in this document, nor on its completeness or accuracy. Any decision you make regarding the purchase of Cryptelo Tokens must be made solely on the basis of your own due diligence and at your own risk.

You agree that by purchasing Cryptelo Tokens you accept:

- You have read, understand and accept our terms, conditions, disclaimers and risk factors.
- You have read, understand and accept that the information in this document and on the Cryptelo website or ICO has not been approved or verified by the United States Securities and Exchange Commission or by any state or government securities authority.
- You have read, understand and accept that the purchase of Cryptelo Tokens does not grant you equity or ownership interest in Cryptelo s.r.o. or any affiliated entity or partnership.
- You have read, understand and accept you understand the purpose and or limitations for the use of Cryptelo Tokens.
- You have read, understand and accept how to purchase Cryptelo Tokens through the requirements listed.
- You have read, understand and accept that you have experience with, or are knowledgeable of cryptographic tokens and blockchain technology.
- You have read, understand and accept at your own risk the substantial risk factors associated with purchasing Cryptelo Tokens, cryptographic tokens, blockchain technology, cryptocurrency, and token storage.
- You have read, understand and accept the regulatory risks associated with this investment.
- You have read, understand and accept the tax and accounting treatments of your investment.
- You have read, understand and accept that by purchasing Cryptelo Tokens you hereby to the fullest extent permitted by applicable law and regulation, you will indemnify, defend and hold harmless the Cryptelo s.r.o., each affiliated company, network, and our respective past, present and future employees, officers, directors, contractors, consultants, equity holders, suppliers, vendors, service providers, agents, representatives, predecessors, successors and assigns (the "Company Parties") from and against all claims, demands, actions, damages, losses, costs and expenses (including attorneys' fees) that arise from or relate to (i) your purchase or use of the Cryptelo Tokens and or our network or affiliated networks or marketplaces, (ii) your responsibilities or obligations under this document, (iii) your violation of this document, (iv) your violation of any rights of any other person or entity, (v) your

breach of applicable laws or regulations; (vi) any fraud, negligence, misconduct or reckless carelessness committed by you in respect of any matter arising from this document or your performance of obligations under this document; (vii) any misuse by you of any technology or any intellectual property rights in respect of the Cryptelo Tokens or the marketplace; (viii) the transmission by you to any Company Party of incorrect, incomplete, inaccurate information; or (ix) the acceptance or acting upon by any Company Party of any electronic message or other communication, information or instructions purporting to come from you even if such information or instructions prove to have been incorrect or unauthorized by you.

BY PURCHASING, OWNING AND USING CRYPTELO TOKENS, YOU EXPRESSLY ACKNOWLEDGE AND ASSUME THE FOLLOWING RISKS

1. You are purchasing Cryptelo Tokens for the rights to access and use Cryptelo utilities and services.
2. The information in this document, on the Cryptelo website and Cryptelo Tokens sale has not been approved or verified by the United States Securities and Exchange Commission or by any state or government securities authority.
3. The purchase of Cryptelo Tokens may not be suitable for you and involves a high degree of risk.
4. This document, Cryptelo website and Cryptelo Tokens sale is in no way a solicitation or offer to buy or sell securities. The purchase of Cryptelo Tokens does not grant you equity, ownership interest, rights to revenue or profit sharing in Cryptelo Company or in affiliates or partnerships.
5. We are currently in development of some of our services and features that will utilize Cryptelo Tokens and although we expect to complete development by the time lines listed, we can make no guarantees to the actual completion timeline.
6. We are dependent on raising funds in the token sale to fund certain features that we plan to integrate into our services. If we raise substantially less than our token sale goal, we will have a difficult time completing our most desired future projects.
7. We are highly dependent on the Ethereum network and blockchain technology. Disruption in either would be detrimental to Cryptelo Company and Cryptelo Tokens and may cause disruptions including loss of access to our utilities or services as well as potential loss in value for Cryptelo Tokens.
8. In the event the value of ETH fluctuates unfavorably during or after the token sale, we may be limited in our ability to fund future development projects or to maintain the network, marketplaces and affiliated relationships.

9. We can offer no assurances that a system wide failure of Ethereum, blockchain, other cryptocurrencies, trading exchanges, the internet, our own websites or any computer infrastructure would not negatively affect our tokens and owners.

10. Cryptelo Tokens is not currently listed on any cryptocurrency trading exchanges and therefore it will be difficult for you to liquidate your tokens until an exchange is established and even then, we can provide no service, support or guarantee to the pricing accuracy or your ability to liquidate your Cryptelo Tokens.

11. Cryptelo Company will not support or otherwise facilitate any secondary trading or external valuation of Cryptelo Tokens. Any such trading or valuations will be through third parties for which we can provide no guarantees, services, or support. In the event, secondary trading of Cryptelo Tokens is facilitated, these exchanges may be susceptible to fraud or manipulation. Furthermore, to the extent that third parties do ascribe an external exchange value to Cryptelo Tokens there is no guarantee as to the value which may be extremely volatile and diminish to zero.

12. Cryptelo Tokens are uninsured unless you specifically obtain private insurance to insure them. Thus, in the event of loss or loss of utility value, there is no public insurer or private insurance arranged by Cryptelo Company to offer recourse to you.

13. There are substantial risks associated with uncertain regulations and enforcement actions. It is impossible to predict or know for sure how or whether government or regulatory bodies may apply existing law and regulation with respect to such technology and its applications, including our products, services, token sale, and Cryptelo Tokens. It is likewise difficult to predict how or whether government or regulatory bodies may implement changes to law and regulation affecting distributed ledger technology and its applications, including the any and all use for the Cryptelo Tokens. Regulatory actions could severely negatively impact our products, services, marketplace, community, values, and use of Cryptelo Tokens in various ways, including but not limited through a determination that Cryptelo Tokens are a virtual commodity, a digital asset or money, securities or currency, that the purchase, sale and delivery of Cryptelo Tokens constitutes unlawful activity, or that Cryptelo Tokens are a regulated instrument that require registration or licensing of those instruments or some or all of the parties involved in the purchase, sale and delivery thereof. The Cryptelo Company may cease operations in a jurisdiction in the event that regulatory actions or changes to law or regulation, make it illegal to operate in such jurisdiction or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

14. The tax characterization of Tokens and cryptography is uncertain. You must seek your own tax advice in connection with purchasing Cryptelo Tokens, which may result in adverse tax consequences to you, including withholding taxes, income taxes and tax reporting requirements.

15. It is possible that our utilities and services will not be used by a large number of individuals, companies and other entities. A lack of use or interest could negatively impact the development of the products and services and therefore the potential utility of the Cryptelo Tokens.

16. Our Cryptelo Tokens as well as blockchain technology has limitations and is in its early stages of development. This carries multiple risks to all investors and users including many risks that we may not foresee.
17. Our price or value per Cryptelo Tokens may be effected by other cryptocurrencies such as Bitcoin and Ethereum among others. Cryptelo Company has no control over the price of other crypto currencies however we most likely will be affected by their price.
18. The cryptocurrency industry and trading exchanges have experienced several outages, thefts and are highly volatile. We will take all reasonable measures to make our network as strong and secure as possible however we cannot provide a guarantee against loss, theft or volatility now or anytime in the future.
19. We will be releasing 100% of our Cryptelo Tokens through the token sale and we will not be offering future Cryptelo Tokens through mining or alternative trading. In doing so we will limit our ability to raise future funds to grow the community and network. Although we believe releasing 100% of our Cryptelo Tokens in the token sale will help establish a reliable and trusted network and utility environment for our token holders, we cannot provide guarantees or assurances that this will happen.
20. Cryptelo Tokens holders may be subject to pay sales or income taxes that are beyond our control. It is the responsibility of each token holder to comply with all tax laws of the jurisdictions in which they reside.
21. There may be substantial other risks that are not foreseen or outlined by us at this time. All purchases of Cryptelo Tokens is subject to your own risk.

References

[1] Solving the key exchange problem
https://github.com/mutecomm/mute/blob/master/doc/keyexchangeproblem.md
[2] https://en.wikipedia.org/wiki/Certificate_authority#CA_compromise
[3] "CA-2001-04". Cert.org. Retrieved 2014-06-11.
[4]Microsoft, Inc. (2007-02-21). "Microsoft Security Bulletin MS01-017: Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard". Retrieved 2011-11-09.
[5] Bright, Peter (28 March 2011). "Independent Iranian hacker claims responsibility for Comodo hack". Ars Technica. Retrieved 2011-09-01.
[6] Bright, Peter (2011-08-30). "Another fraudulent certificate raises the same old questions about certificate authorities". Ars Technica. Retrieved 2011-09-01.
[7] Leyden, John (2011-09-06). "Inside 'Operation Black Tulip': DigiNotar hack analysed". *The Register*.
[8] "Trustwave issued a man-in-the-middle certificate". *The H Security*. 2012-02-07. Retrieved 2012-03-14.