FORTKNOXSTER

WHITEPAPER

Encryption-as-a-Service.

Version 1.2 ● 21 November 2017

FORT

KNOXSTER

“If you spend more on coffee than on IT security, you will be hacked for sure.”

Quote: Richard Clarke, US Government cyber-security expert.

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. In no event shall we nor our advisors be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if we or our advisors have been advised of the possibility of such damages.

Document lifetime

We may occasionally update online documentation between releases of the related software. Consequently, if this document was not downloaded recently, it may not contain up-to-date information. Please refer to FortKnoxster.com for the most current information.

Product information — For documentation, release notes, software updates, or for information about products, licensing, and service, please refer to FortKnoxster.com.

Technical support — For technical support, please refer to FortKnoxster.com and select Support. On the Support page you will see several options, including one for making a request.

Your comments

We value your opinion. Suggestions will help us continue to improve the accuracy, organization and overall quality of the user publications, so please feel free to email hello@FortKnoxster.com with any queries.

If you have comments or questions about specific information or procedures, please include the title and, if available, the revision, the page numbers, and any other details that will help us locate the subject that you are addressing.

Trademarks

FortKnoxster is a pending reg. trademark of FortKnoxster Ltd.

Table of Contents

Executive Summary....3
Introduction....4
Challenge....5
What is FortKnoxster?....7
Our Mission Statement....11
Why Use Encryption?....12
Why Use blockchain?....13
Our Technology....14
The Token Ecosystem....19
Token Sale Offering....21
FortKnoxster Roadmap....24
Our Team....25
Final Words....29
Appendix 1: Technology Overview....30
Appendix 2: The Upcoming GDPR Law....39
Appendix 3: Terms of Service....41
Appendix 4: Privacy Policy....45

Executive Summary

Our world is changing faster than ever and it's hard to keep up with new trends, buzz-words, and emerging technologies. The use of the blockchain technology is at an all-time-high. The number of different crypto currencies are now counted in the thousands, when it comes to different tokens, coins, digital assets or whatever one chooses to call them.

Unfortunately, the rate of cyber-crimes is also at an all-time-high and being online has never been as unsafe as now. Hacks, mass-surveillance espionage, virus, malware, espionage, phishing, extortion… the list of attacks is long and it keeps growing day by day, as the attackers are getting more sophisticated, aggressive and creative.

FBI states that we have entered a cyber-crime epidemic and that cyber-crimes have surpassed "normal" old-school crimes - both in force and damage.

The team behind FortKnoxster, who are experienced cyber-security and crypto engineers, has spent over 3 years developing a "Fort Knox" of an end-to-end encrypted communication platform.

"FortKnoxster has leveraged the use of the blockchain and sophisticated end-to-end encryption techniques into a user friendly all-in-one communication platform, where users can communicate privately and safely, be it through inbox, chat, phone/video calls, file-storage etc. FortKnoxster eliminates the risk of hacks, cyber-threats and centralised government surveillance."

FortKnoxster is the world's first turnkey peer-to-peer encrypted communication platform and can in short be described as:

"Telegram on steroids"

FortKnoxster is all you need to communicate, interact and work safely in an online world dominated by growing cyber-crimes.

FortKnoxster is one of the few token sales backed by a working product.

Introduction

FortKnoxster is a cyber-security company, specialized in developing secure and encrypted communication solutions. The company has developed a unique encryption platform, which is primarily aimed at the B2C market.

The platform comes as an E-a-a-S solution (Encryption-as-a-Service).

FortKnoxster has been designed with a unique architecture and features, which enables everybody to use our platform for all their communications and data-storage needs.

FortKnoxster addresses one of the biggest challenges in our modern society;

To protect communications and data from cyber-criminals - and at the same time maintain a very high level of privacy.

New complex regulations, increasing adoption of new technologies (IoT, BYOD, cloud-services etc.) have fuelled the need for enhanced security and encryption more than ever. The new laws and regulations are very strict, and FortKnoxster offers one of the best "plug-and-play" solutions to comply with most of these new laws.

FortKnoxster can be used by anyone at any time, regardless of you being on a laptop/desktop or on-the-go with your smartphone or tablet.

The FortKnoxster platform has been penetration tested by a range of good (and bad) hackers and "cypherpunks" worldwide - and has "passed its exam", as nobody has managed to compromise our platform in any way or access any end-to-end encrypted accounts or content.

"Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting. Encryption is the most important privacy-preserving technology we have."

Quote; Bruce Schneier, American cryptographer, computer security professional, privacy specialist and writer.

Challenge

Online connection is now essential for almost everybody, creating new opportunities for innovation, interaction with friends and business partners - and global growth.

Cyber-crime, cyber-criminals and their tools are becoming more diverse and sophisticated. Cyber-crime now comes in a variety of forms, and unless consumers, businesses, and governments act now, cyber-crimes could threaten the fundament of our society in many devastating ways.

In the near future, as ubiquitous computing technology pervades more of our lives, these threats will grow. The intuitive interfaces that we increasingly value – and depend on – are often where all the problems arise.

Using the Internet and communicating online, has never been as unsafe as now - and it gets worse every day. Hackers pose a huge threat with cyber-crime forecast to cost over $3 trillion by 2019, according to Juniper Research.

"Cyber-crime is the greatest threat to every company in the world"

Quote: IBM CEO Ginni Rometty

Today's cyber-criminals are often highly motivated professionals, well-funded by competing enterprises, criminal organizations or nation-states, which are persistent in their efforts to break through and damage the opponent as much as possible.

According to a fresh PWC survey, both small and large enterprises have seen a sharp rise in online security breaches, reporting that over 80% of enterprises and SMEs suffered a security breach last year. Most executive respondents expect that there will be more security incidents ahead and there is "no good news" when talking about cyber-security (or lack of) in the future.

Also, the cost of the actual breaches continues to soar and has more than doubled in one year. An average enterprise with 500 employees, which experience an online security breach, ends up with a net bill of over 3.5 million USD in lost sales, business disruption, recovery of assets, loss of clients, fines & compensations, etc. And adding to this is the damaged image and humiliation.

In the last few years we have heard much about the power of big data, which is allowing companies to offer more tailored, targeted and personalised products and services than ever before. The benefit of this to the consumer may be obvious, but it raises many ethical questions, and not just when personal data is in the hands of unscrupulous businesses.

It's been clear for some time that data laws (or lack of) did damage consumers and their privacy and has resulted in the enforcement of the GDPR law. (General Data Protection Regulation). The law aims to give citizens more control over their data and to create a uniformity of rules to enforce across the continent. The huge challenges for most companies are now, how to comply with this new rather strict law which kicks in on the 25th May 2018.

Some of the biggest companies of our time like Google and Facebook have been created by gathering and using user data of its users to advertise to 3rd Parties. Everything you do or say inside these platforms gets recorded, stored, analysed and the main point of having you there, is to make money on your profile and whereabouts.

Add to this the general mass surveillance by most governments tracking and logging everything you do online 24/7 – and stores it forever. And even more intimidating – these government servers get hacked all the time so your data is in the hands of criminals…

Needless to say, there are many potential dangers (and ethical issues) associated with the proliferation of digital profiling, from hacking, to discrimination, to an Orwellian surveillance state. There's a big difference between what companies could and should know.

Online activity leaves footprints -- log files, access entries or data that is created in the systems they used. Once these privacy controls are rolled back, Internet Service Providers will be able to sell the information they capture about how you and your patrons use the Internet.

The loss of online privacy is making it a lot easier for IT-criminals as those giant companies on a regular basis get hacked and all (your) data are now in the hands of potential hostile organisations or people who seek to profit from your data.

Although we can all find ways to protect ourselves, the only real way to avoid the tracking and "stealing" of our data is to stop using these free services altogether and protect our communications with end-to-end encryption like FortKnoxster.

What is FortKnoxster?

FortKnoxster is a one-stop communication, collaboration and file storage platform.

Think of it as a mix of all your favorite (unsecure) everyday apps like Skype, Slack, Telegram, Dropbox, Facetime, Gmail etc. - all gathered in one top secure platform with the highest privacy you can achieve.

The above-mentioned conventional apps are great, but they often come with many security challenges. First of all, as these services are free, "you are the product" meaning, all your data and communication are being read, stored, sold – and often hacked where they are stored. There is absolutely no privacy as most of these companies' business models is to generate as much income as possible from selling (your) data to the highest 3. party bidder.

FortKnoxster is your safe alternative, as we can't (nor can't anybody else) read your data or communications at all, because it is end-to-end encrypted. Even if we could, our business model is exactly the opposite as most others, we are in the business of protecting your data, not selling it to the highest bidder.

FortKnoxster is extremely easy to use as it requires no extra plug-in instalments what so ever. Users are literally up running within minutes and can start to enjoy the extreme safety level and intuitive interface.

It is also easy to invite friends, family or business-partners into the platform.

FortKnoxster was designed to be used by everyone and hence there is no need for technical knowledge in order to use the platform.

If you want to try a free demo of FortKnoxster, please click here.

FortKnoxster Main Features:

- **Inbox**

Messages are end-to-end encrypted and as secure as it gets. Send messages to colleagues, clients and business partners with peace of mind.

- **Distributed File Storage**

Store your valuable data encrypted – and make sure it stays yours. Easy to share and manage files and folders seamlessly.

- **Chat**

Real-time secure chat for fast and instant communications. Comes with voice messages, group chat and much more.

- **Calling**

Secure calling without snooping from competitors or external surveillance. The most private calling you can get on both web and mobile.

- **Group Calling/Conferencing**

Collaborate securely by chatting, calling, sharing files etc., via the group conferencing feature – work smarter and more secure.

- **Screen Sharing**

We have developed encrypted screen-sharing as an extra valuable tool to collaborate securely with partners and other 3rd parties.

- **Voice Messages**

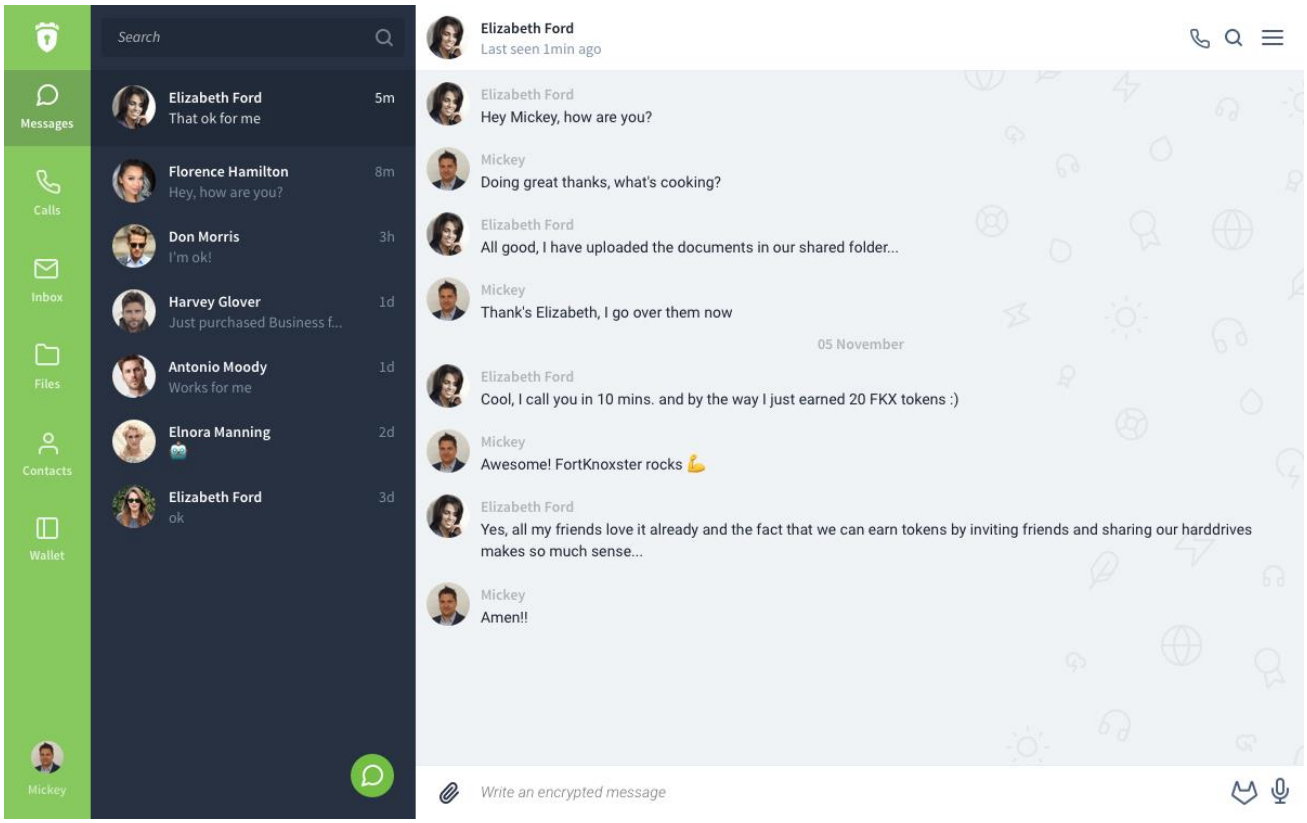
Send quick voice messages without calling. Saves time and the feature is available both on web and app platforms.

- **Intuitive Dashboard**

The dashboard gives users a total overview of all communications and data.

Please see next page for dashboard and app images.

FortKnoxster Main Dashboard



FortKnoxster Mobile App

Our iOS and Android apps will be launched January 2018.

Our Mission Statement

"FortKnoxster will be the safest communication and data storage platform ever built...

- and eventually be the nightmare of any hacker, spy or other IT-criminal "

Why Use Encryption?

The word encryption comes from the Greek word "kryptos", meaning "hidden" or "secret". Encryption is used to enhance security levels to the highest possible. The use of encryption is nearly as old as the art of communication itself. As early as 1900 BC, an Egyptian scribe used non-standard hieroglyphs to hide the meaning of an inscription.

Encryption is a way to maximize the security of i.e. an email message, chat message, call or file by "scrambling" the contents.

Encryption is basically a process/method of encoding messages or information in such a way that only authorized parties can read it. Encryption is a safe way for enterprises and military to communicate privately and securely, without others (i.e. competitors) being able to follow or spy on the communications.

Encryption is also the primary tool that protects the communications of anyone from big companies and governments to small businesses and lawyers to regular citizens. Encryption protects infrastructures of entire countries – communications, power, transportation and healthcare systems, and businesses.

As we eagerly moved into the era of smart, connected devices, encryption (if used) protects our phone calls, text messages, emails, and cloud storage. With the advent of the Internet of Things, security experts call for the implementation of strong encryption in the IoT products, which, when left unattended, could cause chaos to individual households and larger infrastructures.

When you hear the word encryption, the first thing that might come to mind is that it's something only techies or geeks would understand, or use. In reality, the idea of encryption isn't that complicated at all and our platform has made it very easy to use encryption.

Encryption is the best method to safeguard your privacy.

Cryptographer and security and privacy specialist Bruce Schneier states:

"Encryption should be enabled for everything by default, not a feature you only turn on when you're doing something you consider worth protecting."

Why Use blockchain?

A blockchain is a decentralized and open distributed ledger, recording financial transactions (or virtually anything of value) between two parties, on a peer-to-peer network. This continuously growing list of records is linked and secured with strong cryptography, making these transactions permanently verifiable and therefore incorruptible.

"blockchain solves the problem of manipulation"

Quote: Vitalik Buterin, inventor of Ethereum

Since the blockchain is public verifiable, it provides such security and transparency that makes it ideal for many types of security applications.

FortKnoxster take advantage of these features which the blockchain technology provides, by moving its centralized trust of digital identities to a decentralized one, specifically the Ethereum blockchain, using its smart contracts.

Trust is of vital importance and is the most important elements in any crypto infrastructure. The current model of trust for digital identities in FortKnoxster is centralized. This centralized trust model is a common challenge today, as it becomes a single point of failure.

"Centralizing identity creates a single point of failure and builds a repository of high value data that can attract hackers, and proper controls need to be in place to maintain integrity."

Quote: IBM blockchain IDC report, "It Was Only a Matter of Time".

The distributed trust model, utilizing blockchain, is a new way of managing digital identities where the blockchain technology empowers users to control their own digital identity and share and communicate between trusted individuals with their consent. Therefore, no single entity can compromise a user's digital identity and there is no single point of failure present.

Besides implementing a secure and decentralized trust model of FortKnoxster's encrypted digital identities (the public keys); FortKnoxster will also build a complete ecosystem using the FKX token and smart contracts on the Ethereum blockchain to facilitate secure transactions of subscription services and incentives to participants.

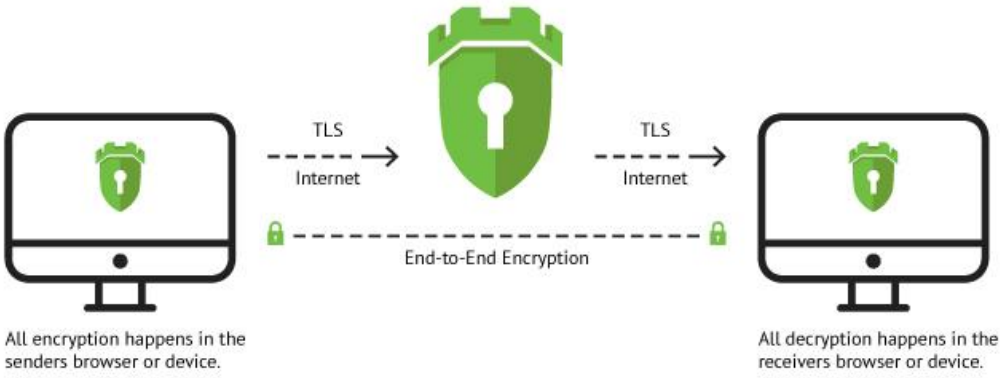
Our Technology

The following is a technical explanation of FortKnoxster's end-to-end encryption and describe in detail the crypto designs and security using the Ethereum blockchain with smart contracts and a decentralized trust of digital identities. A more detailed description is to be found in the Appendix section.

FortKnoxster is a secure web and native app communication and collaboration platform, which enables users to exchange messages and files (including mails, attachments, chats, group chats, calls, documents, images, videos, voice messages, video messages, and files) securely using strong end-to-end encryption.

At FortKnoxster, security and privacy has the highest priority. This is why we have built the FortKnoxster encryption, privacy and secure architectures **by design**. Unlike most other online businesses, it is our main goal to protect our users' privacy, which we are very proud of.

The figure below illustrates how the end-to-end encryption happens between two users, through the FortKnoxster servers on the TLS encrypted connection between the browser clients and the server.



Appendix 1 describes in detail how the inbox and chat message exchange, file storage and calling occur and what crypto operations are involved.

FortKnoxster has its own public key infrastructure (PKI), which extends to the Ethereum blockchain. In the blockchain the user's digital identity gets stored in a registry, using smart contracts and cannot get compromised by a single entity, not even by the FortKnoxster team.

When a user registers on FortKnoxster.com - four sets of RSA key-pairs are generated, two sets of elliptic curve (EC) key-pairs and 6 Key Protector(s) (one per private key) in the client's browser.

These encryption and identity key-pairs are used for different services and protocols. Unlike other known encryption protocols, each of FortKnoxter's services or protocols needs two sets of key-pairs, one for encryption and decryption and one for signing and verification.

The key protector is used to encrypt/wrap each private key which is only known to the user.

The user's plain password is used to form two passwords in the client, the account password, and the root key.

Please note: The user's plain password is only known to the user and it is very important to understand that the user's plain password and the root key are never ever sent to the servers.

The account password is a cryptographic hash of the plain password using the PBKDF2 algorithm with SHA-256 as the hashing algorithm, which performs 10000 rounds of hashing operations (key stretching) and takes the username@domain as a salt. The outcome is a strong password, which is sent to the server and stored as another cryptographic hash using the BCRYPT key derivation function. This password is only used to authenticate the user and cannot decrypt any of the users' data.

The root key is computed the exact same way as the account password, but takes a randomly generated salt, and therefore is a completely different password. The root key forms a 32-byte AES key which is used to encrypt/wrap a Key Protector with AES-KW.

At this point each RSA and EC private key are encrypted/wrapped with AES-GCM with the 32-byte Key Protector, which is locked by the 32-byte root key, each forming a key container. All the public keys and protected key containers are sent to the server during the registration, along with the user details, account password and digital identity.

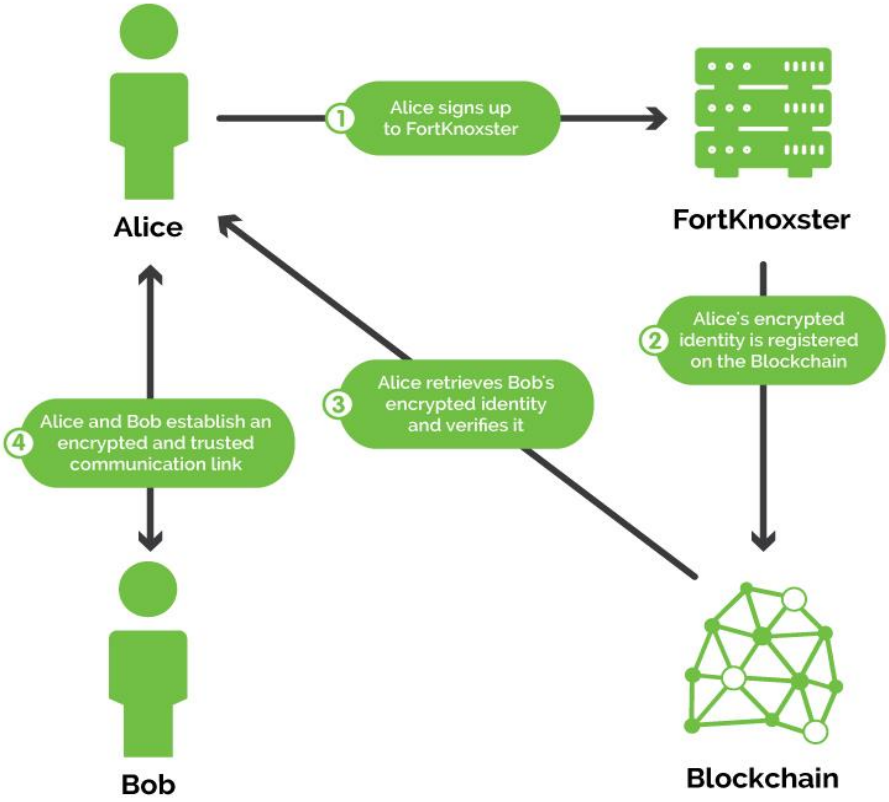
The digital identity is constructed like this (in the client browser):

digital identity = User ID + Signature

Where the Signature is computed like this:

Signature = SIGN(User ID + Public Key Fingerprint, Private Identity Key)

A separate session is established to the FortKnoxster server, where a blockchain client node runs. The node receives the digital identity from the user and creates a new transaction on the blockchain containing the digital identity to store it in the smart contract registry.



The above figure illustrates, a newly signed up user Alice, setting up its digital identity. The figure also illustrates, the retrieval of Bob's digital identity for verification, before any encrypted communication link can be established. Bob will also have done this verification of Alice's digital identity beforehand.

The FortKnoxster services consume a lot of storage, such as files, message attachments and file-transfers.

FortKnoxster's entire storage infrastructure will be built in a decentralized distributed storage on a P2P network using the well-known IPFS. Users can rent their hard disk(s) and earn FKX tokens on storage usage and bandwidth usage.

This is the equivalent of crypto-currency mining, but instead of using the CPU/GPU to mine blocks, available hard disk storage is used to allocate storage.

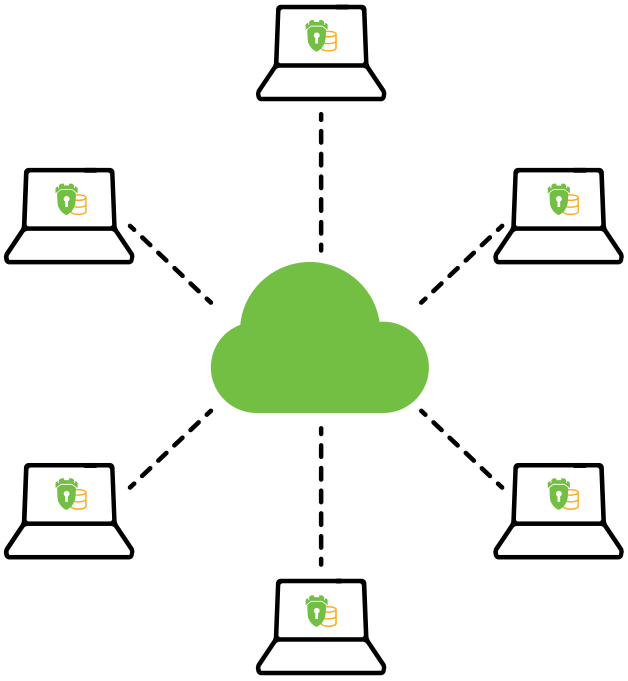
To become a storage miner, 3 easy steps are required:

1) Install the storage miner desktop or console software, which will be available for Mac/Linux/Windows.

2) Provide an ERC20 token pay-out wallet address to receive payments in FKX.

3) Select disk location and how much storage you can spare.

Removing centralized storage servers reduces storage cost and improves access speed and reliability. All encrypted files are spread across multiple nodes and replicated multiple times. No single host holds any significant piece of a file or any complete file.



FortKnoxster provides a decentralized distributed storage P2P network, where all files are end-to-end encrypted using keys that only the uploader holds.

The FortKnoxster users will upload files and attachments from the web interface and from the apps, and these encrypted files will be spread out on the decentralized storage, consisting of all the FKX storage miners, with a fair balanced distribution.

The Token Ecosystem

The FortKnoxster token (FKX) will be used for purchasing various services and for incentivizing users for different rewards achieved.

The FKX token will have a clear and important usage in our application, as a means of both incentivizing further development and securing our ability run and market FortKnoxster worldwide. The FKX token serves the purpose of being required in order to use FortKnoxster.

A fixed supply for FKX will be created during the token sale (135 Mill.) A ledger on the blockchain will be created maintaining the FKX token, following the ERC20 standard and allowing a secure mechanism for transferring FKX to other participants.

Users on FortKnoxster who own FKX tokens, will be able to purchase service subscriptions such as:

- **Encrypted Storage**

  Signing up to FortKnoxster is free and the limited free encrypted storage will be allocated. To increase the encrypted storage the user will purchase credits for fixed amounts with the FKX token.

FortKnoxster will in the future also introduce other services and subscription to be exchanged for FKX tokens.

To further contribute to the FKX ecosystem, incentive earning-plans will be launched - such as:

- **Rent Hard Drive**

  Users get rewarded in FKX token for renting out their hard disk space as part of FortKnoxster's decentralized storage.

- **Referral**

  Users get rewarded with a fixed FKX token amount, by inviting other users to the platform.

- **Loyalty**

  Users get rewarded with FKX tokens, when using the various services based on a usage formula reaching different user levels.

- **Token Sale Bounty**

  During the token sale period, FKX tokens will be rewarded to our community users who are actively participating in our bounty program. More information can be found on BitcoinTalk.

- **Bug Bounty**

  Users can also get rewarded with FKX tokens by submitting valid security reports of the bug with PoC (Proof of Concept). This bounty reward system also works for existing white-hat hackers participating in our bounty program, by referencing the submitted report and user profile.

Token Sale Offering

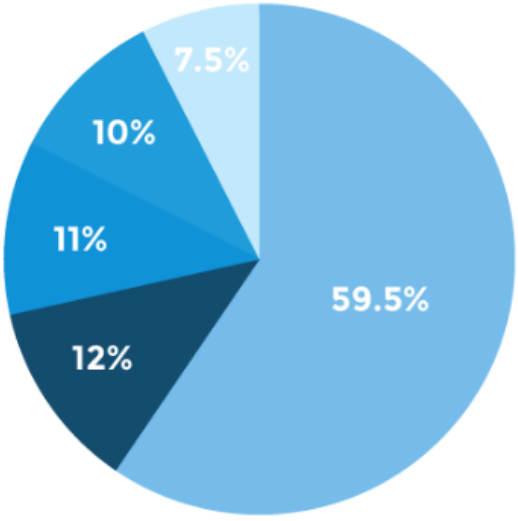
TOKEN SALE TERMS

135 Million
FKX TOKENS ISSUED

$15 Million
MAX CROWDSALE CAP

80.325 Million available for token sale.

FKX tokens will be sold for ETH.



FKX is an Ethereum ERC20 token.
Token sale ends 18 Mar 2017 12:00 CET or when sold out.

Early birds can pre-register here:

https://fortknoxster.typeform.com/to/IRTwjP

The pre-token sale will begin on Monday 5 February 2018 and will have a 20% token bonus.

The public token sale will begin on Monday 19 February 2018 at 12:00 CET. To take part, visit this link:

https://fortknoxster.com/token-sale.

1 USD = 5.25 FKX. The ETH/FKX rate will be published on our website. It will be locked 4-6 hours before the crowd sale starts.

Name, address and email will be required from all participants contributing to the FKX sale. Participants will be asked to confirm they are eligible under the terms of service.

IMPORTANT INFO: FortKnoxster will NEVER solicit payments via Telegram nor any other media and/or sites.

The address for the token sale will be published only on the FortKnoxster official website – https://fortknoxster.com.

No other site will officially publish the token sale address. NEVER send any ETH to addresses taken from anywhere else other that the FortKnoxster official website.

All FKX distributed to the founders and the company will be time locked by 12 months. After the token sale has finalized, all remaining tokens that were not sold (and were eligible) in the crowd sale will be burned automatically in the Ethereum smart contract. Exactly 1 week after the crowd sale has ended, the FKX tokens will become transferable.

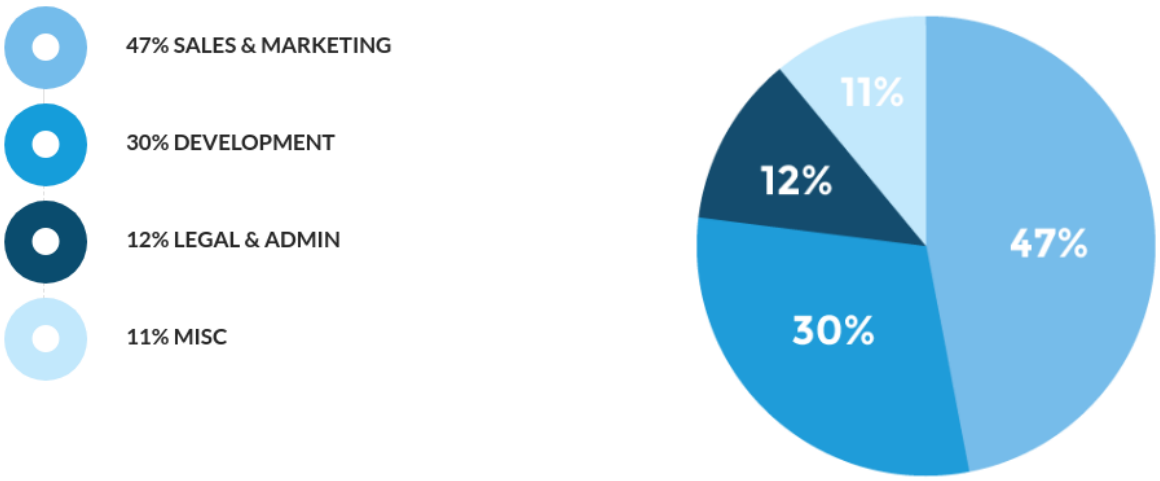
Community incentives examples: Community rewards, airdrops, bounties, competitions, dedicated contributors, Bancor liquidity pool and alike.

Residents of the United States and Singapore cannot participate in the FortKnoxster token sale and token distribution.

You can participate in the FortKnoxster token sale if you are neither a US and Singapore citizen nor permanent resident of the United States or Singapore,

nor have a primary residence or domicile in the United States and Singapore, including Puerto Rico, the US Virgin Islands and any other territories of the United States.

BUDGET OVERVIEW



FortKnoxster Roadmap

Q3 2013

EDWARD SNOWDEN REVELATIONS
Snowden, a former NSA contractor leaks highly classified secrets about illegal government spying and lack of general online privacy.

Q1 2014

RESEARCH STARTS
Inspired by the Snowden leaks, research begins with the goal to create the most secure communication platform to help solve the problem.

Q3 2014

DEVELOPMENT STARTS
Core encryption architecture and security layers are being designed and initial development begins.

Q2 2015

ALPHA TESTING
The first alpha version is tested by security professionals and hackers from all around the world.

Q3 2015

ADDITIONAL FEATURES
A range of additional security features are developed and implemented and tested successfully.

Q2 2016

PRIVATE BETA
A selected group of live testers are identified from various continents in order to test the scalability and further security tests are performed.

Q4 2016

LIVE USERS
Initial live users are using the platform and mobile apps with excellent response.

Q2 2017

CODE RE-WRITE
We decided to re-write our entire code-base and crypto structure, in order to prepare for Blockchain integration and de-centralized storage.

Q3 2017

TOKEN SALE PLANNING
Token sale process is initiated and the FortKnoxster white paper is published. The FortKnoxster demo platform is launched.

Q1 2018

TOKEN SALE FINALIZED
The FKX token sale ends and the FKX tokens are distributed. The core ecosystem development using smart contracts on the Ethereum Blockchain is in process.

Q2 2018

BLOCKCHAIN TESTING
The back-end implementation of the decentralized digital identity, decentralized storage and ecosystem (payment, loyalty, reward incentives) using smart contracts on the Ethereum Blockchain is tested.

Q3 2018

PUBLIC LAUNCH
FortKnoxster officially launches its decentralized Blockchain Digital Identity infrastructure and the encrypted group calling feature for the web and native apps. Our new invite and referral function in the FKX ecosystem with incentives is also launched.

Our Team

Rasmus Birger Christiansen

CEO & Co-Founder

Along with a degree in Engineering, Rasmus has 20+ years experience within telecommunications. He's a privacy-advocate by heart, a strong leader and a cyber-security professional.

Mickey Joe Nathan Johnnysson

CTO & Co-Founder

A strong analytical mindset has served Mickey well in his 15+ years as a full-stack software developer. His major passions are computer engineering, crypto and Blockchain.

René Krainert

CFO

René has been an accountant and financial controller for almost 20 years. He has a strong background within finance and accounting, both as a hands-on controller, strategic planner and Excel guru.

Emin Roblack

Head of Design

In need of creation? Emin is your man. With a penchant for design, graphics and animations, he has an imitable talent for converting simple ideas into complex graphics.

Aram Ispiryan

Lead iOS Developer

Backed by a master's in Computer Science, Aram provides an innovative approach to communication. His main strengths lie in iOS systems using real time audio/video and chat applications.

Armen Sisakyan

Lead Android Developer

Armen brings Android development to the highest level of quality and performance. He has a deep understanding of communication protocols serving millions of users in a high availability mode.

ADVISORS

David Orban

Blockchain Expert

David is an entrepreneur, author, blogger, keynote speaker, and thought leader of the global technology landscape. His entrepreneurial accomplishments span several companies founded and grown over more than twenty years.

Henok Tekle

Blockchain Expert

Henok (Hen) Tekle is a prominent cryptocurrency angel investor, content creator, thought leader, and advisor to token projects. Hen is a frequent attendee and speaker at Blockchain gatherings and has also founded and managed several cryptocurrency communities.

Stig Abildsø

Entrepreneur & Investor

Stig has built several Danish companies from scratch to successful exits within the IT sector. The ultimate entrepreneur.

Eddy De Heij

Entrepreneur & Investor

With a large portfolio of investments worldwide, Eddy is a serial entrepreneur, investor and writer.

Michael Vivet

Senior IT Consultant

Michael is assisting with strategical and tactical counselling, as well as backend and service development.

Carlos Benvenuti

Entrepreneur & Investor

Carlos has been in the crypto space for several years. He is a professional coach, advisor and investor.

Final Words

FortKnoxster is founded by Danish entrepreneurs and cyber-security experts, with an extensive experience in the field of online security and cyber-defence. The founders have already established proof of concept.

The FortKnoxster platform has huge, scalable worldwide potential. It is the world's first end-to-end encryption platform, offering turnkey encryption with a large suite of features including Blockchain implementation.

The combination of our team, business model, the extremely scalable market potential and the rising cyber-security demand from both individuals and enterprises, will make FortKnoxster a market-leading player within the cyber-security field.

By utilizing our advanced cryptographic solutions combined with the power of the blockchain's decentralized structure, FortKnoxster will help make the world a safer place – and we will dominate the global encryption market by being the "go-to" encryption solution anywhere – and for everybody.

Appendix 1: Technology Overview

Key Terms

Below is the list of key terms used throughout the technology explanations.

All key materials are generated using a CSPRNG (Cryptographically Secure Pseudo-Random Number Generator) seeded with high-quality entropy as truly random values using the operating system's entropy source.

- **account password** – Password based derived key used for authentication using the PBKDF2 algorithm with SHA-256 as the hashing algorithm and seeded with salt.
- **root key** – Password based derived key using the PBKDF2 algorithm with SHA-256 as the hashing algorithm and seeded with a random salt. The derived key is used for encrypting and decrypting a Key Protector using AES 256-bit in KW mode.
- **User ID** – A self-generated unique identifier to identify a user in the FortKnoxster system and on the blockchain.
- **Public Key Fingerprint** – A unique cryptographic hash of the user's public keys used to form the digital identity on the blockchain.
- **digital identity** – A key/value record stored on the blockchain containing the User ID and a digital signature of the User ID and the Public Key Fingerprint.
- **Private Encryption Key** – Private key used for decryption using RSA-OAEP 2048-bit algorithm scheme with SHA-256 as the hashing algorithm.
- **Private Identity Key** – Private key used for digitally signing an encrypted message, using RSASSA-PKCS1-v1_5 2048-bit algorithm scheme with SHA-256 as the hashing algorithm.
- **Public Encryption Key** – Public key used for AES key encryption using RSA-OAEP 2048-bit algorithm scheme with SHA-256 as the hashing algorithm.

- **Public Identity Key** – Public key used for message signature verification using RSASSA-PKCS1-v1_5 2048-bit algorithm scheme with SHA-256 as the hashing algorithm.
- **Key Protector** – Random generated 32-byte key used for encrypting/wrapping and decryption/unwrapping a private key using AES 256-bit encryption in GCM mode.
- **key container** – A flexible crypto box container structure to hold an encrypted/wrapped private key with its Key Protector(s).
- **Message Key** – Random generated 32-byte one-time key used for message and file encryption and decryption using AES 256-bit encryption in CBC mode or GCM mode.
- **Group Key** – Random generated 32-byte session key used for encryption and decryption of group message using AES 256-bit encryption in GCM mode.

Key Pairs

The RSA key-pairs used for encryption and decryption, each consists of a Public Encryption Key and a Private Encryption Key and uses the RSA-OAEP 2048-bit algorithm scheme with SHA-256 as the hashing algorithm.

The RSA key-pairs used for signing and verification, each consist of a Public Identity Key and a Private Identity Key and uses the RSASSA-PKCS1-v1_5 2048-bit algorithm scheme with SHA-256 as the hashing algorithm.

The EC key pair used for deriving a shared secret key in a key agreement consists of a public and a private key and uses the ECDH P521-bit algorithm.

The EC key pair used for signing and verification consists of a Public Identity Key and a Private Identity Key and uses the ECDSA P521-bit algorithm.

Contacts & Key Exchange

A common problem in encryption systems, is the secure key exchange of public keys between users, making sure that the obtained key indeed belongs to the intended recipient.

FortKnoxster protects against such potential Man-In-The-Middle (MITM) attacks, by leveraging on the blockchain technology in conjunction with a self-signed contact list.

A user can invite other users into the platform or connect with any existing users on the platform.

Each user keeps a contact list where each contact record is digitally signed with the user's Private Identity Key and contains all the contact details such as name, user id and the public keys. The contact gets signed during a contact request/accept process. This process involves retrieving the contact's digital identity from the blockchain and verify it in the client by computing the same Public Key Fingerprint from the contacts public keys and then verify the Signature with the contact's Public Identity Key.

Once the contact is verified, it is then signed and added to the user's own contact list. From then on, the user can trust this contact and will verify the contact before using its public keys to exchange messages, files or calls.

Should the contact verification fail, the message exchange with that contact is not carried out and the user is alerted with a warning.

Message Exchange

When a user sends an inbox or chat message to another user, the following happens in the sending user's client:

1. If there were any attachments, they have already each been encrypted with its own generated Message Key and a Mac of the encrypted file has been taken using the HMAC algorithm with SHA-256 and the file's Message Key. And at this point, the encrypted attachments have already been uploaded the servers and a unique id has been assigned to each attachment.

2. A new Message Key for the message object is then generated.

3. The plain message with any attachments meta-data, attachments Message Key's, attachments HMAC signatures and attachments IDs are encrypted with the message's Message Key.

4. The ciphertext (encrypted message) is signed using the sending user's Private Identity Key.

    a. Before signing the ciphertext, the Private Identity Key is first decrypted with the user's Key Protector which was decrypted in the browser client with the root key and stored in the browser's session storage when the user logged in.

5. The Message Key used to encrypt the message is then encrypted using the receiving user's Public Encryption Key.
    a. If a message has multiple recipients this process in 5) is repeated with each recipient's Public Encryption Key.
6. The encrypted message, the message signature, and the encrypted recipient keys are then sent to the servers where they are stored.
7. Before storing the message, the server application verifies each message in case of message tampering. This is done using the sending user's Public Identity Key.

When a user receives a new inbox or chat message, the following happens in the receiving user's browser client:

1. The signature of the encrypted message is verified with the sending user's Public Identity Key.
2. The encrypted Message Key is then decrypted with the user's Private Encryption Key.
    a. Before decrypting the ciphertext, the Private Encryption Key is first decrypted with the user's Key Protector which was decrypted in the browser client with the root key and stored in the browser's session storage when the user logged in.
3. The retrieved Message Key is then used to decrypt the encrypted message.
4. If there were any attachments the receiving user can download each encrypted attachment which will be verified for integrity with HMAC-SHA256 using the Message Key and then decrypted using the same Message Key.

Group chat messaging is designed to handle a lot of members and a large amount of group chat messages. This is achieved with a server-side fan-out, which means a user sends a single message to the server and the server sends a copy of the message to each group member. This design transmits as little data as possible.

When a group chat is created the following happens:

1. The creating user generates a Group Key.

2. The Group Key is then encrypted with each member's Public Encryption Key.

For all subsequent messages to the group:

1. The sender retrieves the Group Key by decrypting it with the Private Encryption Key.
2. The sender encrypts the plain message with the Group Key using GCM mode, which allows for message authentication during encryption and decryption.
3. The sender signs the encrypted message with his/her Private Identity Key.
4. The sender transmits the encrypted message and the signature to the server, which does server-side fan-out to all the group members.

The group chat messaging is also the foundation for the group call signalling protocol which happens over the same XMPP group chat channel.

Cloud Storage & File Sharing

Larger files and attachments are also end-to-end encrypted.

File attachments (documents, images, videos etc.) refer to inbox attachments and chat file transfers and are encrypted the exact same way, with a Message Key per file using CBC mode. A MAC signature is then computed using the HMAC algorithm with SHA-256 and the file's own Message Key as the key to the HMAC function.

Cloud Storage files are encrypted the same way, however, to be able to handle large file uploads, the files are chunked into smaller files and encrypted with a Message Key using GCM mode.

An additional two sets of RSA key-pairs were generated specifically for Cloud Storage use and file and folder sharing.

The folder tree structure is kept in separate JSON folder structures which contain ID pointers and AES keys to its children folders and files. Those JSON structures are encrypted with a Message Key using GCM mode and are signed with the user's Private Identity Key. The random AES key along with a unique ID is kept in the parent JSON folder structure which is also encrypted and signed.

When a user shares a folder with other users, the Message Key for the JSON structure is encrypted with each user's Public Encryption Key and the encrypted JSON structure is then signed with the sharing user's Private Identity Key.

The sharing user is the owner of the shared folder and can define read and write permission for each member of the folder.

Calling & Conferencing

Audio/video one-to-one calls, group calls and screen sharing are also end-to-end encrypted and use the WebRTC technology for real-time audio and video communication.

WebRTC uses Secure Real-time Transport Protocol (DTLS-SRTP) for establishing and encrypting media streams.

Before a peer-to-peer call is established between two or more users, some signalling is done to exchange certain information and set up the call.

This signalling is done over the existing Chat/XMPP channel and is also end-to-end encrypted using the same encryption scheme for message exchange with AES/RSA as described previously above.

Native Android & iOS Apps

The Android and iOS apps contain the same inbox, chat, group chat and calling features as the web client and integrates closely with the system and will receive push notifications on various events such as new inbox and chat messages and incoming calls.

The end-to-end encryption is designed and developed using the same strong encryption and algorithms as in the browser clients. For the iOS and Android apps, the end-to-end encryption layer has been developed as a single cross-platform library written in C++ using the latest OpenSSL distribution, and which is used in both apps.

Web Crypto API

The web browsers implement the latest browser capabilities and use the Web Cryptography API (Web Crypto API), which is a web standard defined at the World Wide Web Consortium (W3C) which allows for cryptographic operations in Javascript web client applications.

Using Web Crypto API makes the crypto design and its implementation highly stable and efficient when performing various crypto operations, as it leverages on the browser's own crypto stack implementation and which makes robust cryptographic algorithms available, compared to other pure Javascript crypto implementations.

Web Security

Cross-Site Scripting (XSS) attacks are probably the most widely spread type of attacks on web applications and happen when malicious scripts are injected into websites to target end users.

The goal of an XSS attack is to make some browser script execute in the victim's browser on infected sites and to steal sensitive information such as a session cookie from an authenticated user and then send it back to the attacker's server. The attacker can then gain access to the victim's account on that specific website by using this session cookie. Such an attack can be done without the victim's knowledge.

This kind of attack has been performed on well-known services such as WhatsApp, where the attacker was able to completely hi-jack some victim's WhatsApp account and being able to control that victim's account.

Websites and web applications are vulnerable to XSS attacks typically when user inputs are not filtered correctly.

FortKnoxster implements several security measures to make sure our users are protected against any kind of XSS attacks, by making sure user inputs such as an inbox or chat message are escaped and sanitized before displaying it, in the receiver's browser. Furthermore, our web application and server configurations have been optimized to set the **HTTPOnly** cookie flag, **X-XSS-Protection**, and **Content-Security-Policy** response headers.

Our research in **Content Security Policy (CSP)** has resulted in a very strict CSP configuration, by not allowing any kind of external sources to be loaded inside the FortKnoxster environment.

CSP is supported in all modern browsers and protects against XSS by whitelisting allowed sources of script, style, media and other resources when you visit a website.

To have this kind of protection, the CSP configurations need to be done in the web server configurations and is a special response header (Content-

Security-Policy) sent from the server back to the browser, when a page is requested.

We have taken these extra security measures to make sure our CSP configurations are as strict as possible by whitelisting only internal resources, and thereby blacklisting any kind of external loading of resources in the client's browser when visiting our website and using our services, and therefore enforce our user's privacy.

Cross Site Request Forgery (CSRF/XSRF) is a special kind of attack, where the attacker can trick the victim in to perform unwanted actions, such as authorizing a bank transfer.

FortKnoxster prevents CSRF vulnerabilities by including a unique session token on each HTTP request and a special XSRF cookie.

Furthermore, the FortKnoxster session cookie is encrypted with AES-CBC 256-bit and a mac using the HMAC function, taking a server key as input.

Phishing is a type of social engineering attack. The attacker masquerades as the trusted site, tricking the victim to perform unwanted actions, such as stealing login credentials, credit card details and other sensitive data.

FortKnoxster implements several security measures to also prevent these kinds of attacks.

Account Security

To protect users from any kind of account attacks, FortKnoxster enforces various security measures and offer the following account security features:

- Two-Factor Authentication with TOTP, SMS and FIDO U2F.
- Restrict account access by IP and country.
- Security audit log.
- Web Application Firewall (WAF) filtering web requests.
- Automated account blocking when Brute Force attacks or other abuses are detected.

Transport Layer Security

All communication between the clients (web browsers, Android app, iOS app) and the servers are layered with an extra separate strict encryption channel. Only TLS 1.2 is supported and is configured with the strongest cipher suites available, including a 4096-bit Diffie-Hellman parameter for DHE cipher suites.

The strong TLS configurations enable HTTP Strict Transport Security (HSTS), OCSP Stapling, Forward Secrecy and protect against all known attacks such as Beast, Heartbleed, Poodle and many more.

Algorithm Overview

Below is an overview of the encryption algorithms and crypto operations used in the FortKnoxster end-to-end encryption crypto design.

Algorithm	Encrypt	Decrypt	Sign	Verify	Derive	Digest	Wrap	Unwrap
RSASSA-PKCS1-v1_5			✓	✓				
RSA-OAEP	✓	✓						
ECDSA			✓	✓				
ECDH					✓			
AES-CBC	✓	✓						
AES-GCM	✓	✓					✓	✓
AES-KW							✓	✓
HMAC			✓	✓				
PBKDF2					✓			
BCRYPT					✓			
SHA-256						✓		

Appendix 2: The Upcoming GDPR Law

Below is a short description of the coming GDPR law. FortKnoxster is a good and relevant tool to comply with the strict GDPR law and easy to implement in any organisation regardless of size and industry.

The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

Businesses urgently need to bring their operations into compliance with the new data protection regime. Here are the most important takeaways from the GDPR.

When

The law takes effect May 25, 2018, after which enforcement will begin against the non-compliant entities. Until then, existing national data protection laws apply, which include national security laws, or employment laws and free speech.

Who

The new European Data Protection Regulation applies to any business irrespective of its business activity or sector of economy, if:

a business is established in the EU, or subject to EU laws.

a business is established outside the EU, but a) offers services or goods to EU residents; b) monitors the EU residents' behaviour.

For example, the "Runkeeper app" tracking its European users is liable, even though it is a North American company without an office in the EU.

The European Data Protection Regulation introduces a significant expansion of the liable businesses and now applies to non-European entities dealing with private data of the European residents.

This also means tech giants like Google, Facebook, Yahoo and Microsoft will have to comply. Otherwise, the implications include hefty fines.

Fines

Breaching of the European Data Protection Regulation results in fines. The maximum fine for a single breach is either €20 million, or 4% of annual global turnover, whichever is greater. The amount is set intentionally high as to attract the attention of the C-suite to the problem of data protection and compliance with the new regulation.

Encryption is the solution

The GDPR regulation provides specific suggestions for what kinds of security actions might be considered "appropriate to the risk," including:

Encryption of personal data.

The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data.

The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.

A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

While the European Data Protection Regulation brings good news to the end users mostly, it's not all bad news, more work and bigger spending for the businesses. There is one particularly valuable piece in the regulation that stipulates that companies should meet users' "reasonable expectations of data privacy." The regulation then suggests that encryption, anonymity, and authorization tokens meet those expectations. If your company encrypts corporate data and user data at rest and in transit, also when dealing with third-party contractors, and keeps the keys on the company premises, safe and encrypted, too, you will effectively prove that you meet the "reasonable expectations of privacy" of an individual.

Appendix 3: Terms of Service

Terms of Service

Effective: August 1, 2017

These Terms of Service ("Terms") cover your use and access to the Service named "FortKnoxster", ("Service") provided by FortKnoxster Ltd. By using our Services, you're agreeing to be bound by these Terms, and to also review our Privacy policies. If you're using our Services for an organization or other legal entity, you're agreeing to these Terms on behalf of that organization. FortKnoxster Ltd. reserves the right to change this agreement at any time.

The FortKnoxster Service

The FortKnoxster Service provides a system that allows a user to access our secure communication platform named FortKnoxster. In order to receive the Service, you will need to create an account consisting of an email address and password.

Access

In order to access your account, you must first log in using your FortKnoxster username and password, and then go through the verification process. After this, you have access to use the Service. The use of the Service requires you to obtain access to the Internet. You can access from a computer or a mobile device.

Account Security

By completing the registration for this Service, you agree to be bound by these Terms and Conditions and FortKnoxster's Privacy Policy, you warrant that you are at least eighteen 18 years old or that you have obtained consent to open and maintain an account from your parents. You agree to maintain the security of your password and identification and you will be fully responsible for all usage of the FortKnoxster Service. You shall immediately notify FortKnoxster Ltd of any unauthorized use of your password or account, of any loss or theft of your password or of any other breach of security.

Permitted Use

You may access and use the Service in accordance with these Terms and Conditions and subject to any operating rules/contract or posted policies that appear on the website. Any use of the Service is at your sole risk and responsibility.

No Illegal Use

You represent and warrant, as a condition of use of the Service, that you will not use the Service for any purpose that is illegal, unlawful or prohibited. You shall not subject the TEP system to any spam, denial of Service attacks, viruses or any action, activity or code that would interfere with the ordinary operation of the system.

Indemnity

You agree to defend, indemnify and hold FortKnoxster Ltd., its subsidiaries and affiliates and directors, officers, agents, contractors, shareholders, partners and employees, harmless from and against any action, claim, demand or liability, arising out of or relating to your violation of any of the Terms and Conditions of this agreement, the rights of any third party or your use or connection to this Service. The Service is provided "as is" and you agree to not hold FortKnoxster Ltd. responsible for any damages that arise as a result of the loss of use, data, information or profits connected to the performance of the Service. Furthermore, you will not hold FortKnoxster Ltd. liable, if any material is unintentionally released as the result of a security failure, vulnerability or force majeure.

Password

As we have no access to your account or data, we do not keep records of your password. If you lose your password, we cannot help you other than offering you a new account.

Paid Accounts

Billing. We will automatically charge you from the date you activate a user account and on each periodic renewal until cancellation. You're responsible for all applicable taxes, and we will charge tax and VAT when required to do so.

No Refunds. You may cancel your FortKnoxster Upgrade Account at any time, but you won't be issued a refund.

Downgrades. Your Upgrade Account will remain in effect until it is cancelled or terminated under these Terms. If you do not pay for your Upgrade Account on time, we reserve the right to suspend it or reduce your account to a free account.

Changes. We may change the fees in effect but will give you advance notice of these changes via a message to the email address associated with your account.

Intellectual Property

FortKnoxster Ltd. owns all rights, titles, and interest in and to all copyright, trademarks, trade secrets, patents or any other intellectual property of any kind or any proprietary rights in and to the Service and these rights titles and interests are protected to the fullest extent under Swiss and International laws. Without the prior written consent of FortKnoxster Ltd., you shall not use or permit any third party to use any trademarks or trade names and no content on this Service may be copied, reproduced or duplicated in any form or by any means whatsoever.

Entire Agreement

These Terms and Conditions set forth the entire agreement with respect to the subject matter hereof and supersede all prior or contemporaneous communications and proposals, whether, electronic, oral or written, between you and FortKnoxster Ltd.

Waiver

The failure of FortKnoxster Ltd. to exercise or enforce any right or provision of these Terms and Conditions shall not constitute a waiver of such right or provision.

Applicable Law

This Agreement shall be governed by and construed under the laws of Gibraltar. All actions commenced pursuant hereto shall be brought in a court of Gibraltar.

Changes

If FortKnoxster Ltd. is involved in a future merger, acquisition, re-organization or sale of our assets, your information may be transferred as part of this. We will notify you (for example, via a message to the email address associated with your account) of any such deal and outline in detail.

Effect

This agreement comes into effect on the date of your completed registration with FortKnoxster Ltd., or date of first payment and FortKnoxster Ltd. may terminate this Service at any time. Use of the Service is your consent to the Terms of this agreement.

Customer support

We will respond to support requests via email within one business day. If you have questions, ideas or concerns about our Services, please contact us at info@FortKnoxster.com.

Appendix 4: Privacy Policy

Effective: August 1, 2017

Privacy Is Our Business

FortKnoxster Ltd. values, respects and endorse the privacy and anonymity of all our users and is strongly committed to protecting the confidential security and integrity of any information in accordance with this Privacy Policy. This Privacy Policy explains FortKnoxster Ltd.'s handling of your information.

Protecting Your Information

Generally. The security of your information is imperative to us, in fact this is the core of our or business model, to protect the privacy of our users and their data. Within the technical and legal boundaries, we will keep innovating and pushing the boundaries to maintain the best private and secure communication platform.

Technically. We use physical, electronic and sophisticated security methods to prevent unauthorized access, maintain data privacy and to ensure correct protection of information. We use robust encryption technologies including AES 256, RSA 2048, Key Authentication algorithms, Secure Sockets Layer (SSL) etc. Our entire user's data is stored in encrypted form and not even the FortKnoxster Ltd. staff has any access to it whatsoever. In addition, user accounts are protected by multifactor authentication (optional).

Legally. Our servers are hosted in a Swiss highly secure data centre. Furthermore, our Secure Sockets Layers (SSL) are also of Swiss origin and hence protected by the strict Swiss privacy laws which means that FortKnoxster Ltd. cannot be compelled to any lawful interception or other attack on privacy. Again, even if data were compromised, it would be of no use as all data is highly encrypted. We also refer to the Non-Disclosure section below.

Data Collection

FortKnoxster Ltd. collects and uses anonymous user information for the following limited purposes:

1. Sent and Received Messages: We do not have access to any message content as it is highly encrypted. We do have access to the following records: Number of messages sent, storage space used, total number of messages, last login time and country code login.
2. Emails: All e-mails provided to us during the account creating procedure, are confidential information and your e-mail will never be sold, shared, given, leased or disclosed to any third parties. Due to extra security matters, your e-mail is required to send you the initial link in the account creating process.

Managing Your Data

Your data belongs to you and you can delete it at any time. Your account information can be changed anytime by logging into your account and change or delete information. If you wish to delete your account, we will erase all your remaining encrypted account data from our servers. Any free accounts that are inactive for a period of more than 12 months may be automatically deleted.

Data Storage

All data is at any given time stored in encrypted format. Temporary backups are also fully encrypted. We have no way of access your encrypted data, and hence cannot recover your password, should you lose it.

Non-Disclosure

FortKnoxster Ltd. has a zero-disclosure policy. We will not respond to any requests from authorities regarding information about users, logs, data or similar. Any authority must direct a request to the relevant authorities, which may then possibly contact us, following the protocol that the relevant legislation stipulates. We will not comply with demands from any authorities to a higher extent than the law demands.

Payments

This applies only to users who are using our "upgrade" Services. Third parties process all electronic payment transactions and FortKnoxster Ltd. does not retain any customer payment information. For administration purposes, we do need to store data on which account was paid for by a particular transaction.

Customer support

We will respond to support requests via email within one business day. If you have questions, ideas or comments about our Services, please contact us at info@FortKnoxster.com.

THANKS FOR YOUR INTEREST

For more information:

www.fortknoxster.com

or e-mail:

tokensale@fortknoxster.com

FORT

KNOXSTER