What happens in FortKnoxster – stays in FortKnoxster.

Version 3.0 - 15th of May, 2021

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

© 2021. All rights reserved.

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 www.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 https://FortKnoxster.com or https://t.me/fortknoxster or https://medium.com/fortknoxster.

Technical support — For technical support, please refer to FortKnoxster.com. On the Resources page, you will find the Knowledge Base https://fortknoxster.com/knowledge-base. If your question cannot be answered here, please send an email to support@fortknoxster.com.

Your comments

We value your opinion. Suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please feel free to email support@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™ and Crypto Suite™ are registered trademarks of FortKnoxster Ltd.
Table of Contents

Table of Contents ............................................................................................................. 2
Executive Summary .......................................................................................................... 3
Introduction ..................................................................................................................... 4
Challenge ......................................................................................................................... 5
What is FortKnoxster? ....................................................................................................... 8
Crypto Suite™ Features .................................................................................................. 9
Secure Wallet .................................................................................................................. 12
Our Mission Statement ................................................................................................... 14
Why Use Encryption? ....................................................................................................... 15
Why Use Blockchain? ..................................................................................................... 16
Our Technology ................................................................................................................ 18
Knoxstercoin (FKX) Token Utility .................................................................................. 22
Token Generation Event .................................................................................................. 25
FortKnoxster Roadmap .................................................................................................... 26
Core Team ....................................................................................................................... 27
Final Words ..................................................................................................................... 32
Appendix 1: Technology Overview ................................................................................ 33
Appendix 2: The GDPR Regulation ............................................................................... 44
Appendix 3: Terms of Service ......................................................................................... 47
Appendix 4: Privacy Policy ............................................................................................. 51
Executive Summary

Our world is changing faster than ever, and it is hard to keep up with new trends, buzzwords, and emerging technologies. The usage of blockchain technology is at an all-time high. The number of different cryptocurrencies is now counted in the thousands when it comes to different tokens, coins and digital assets.

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, phishing, extortion... the list of cyberattacks 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 cybercrimes have surpassed “normal” old-school crimes - both in force and damage.

US President Biden signed an executive order in May 2021, to improve US Cyber-defenses in light of recent ransomware attacks. The order requires all government departments to adopt improvements such as multi-factor identification login, accelerate moves to ‘cloud’ and ‘zero trust’ frameworks and ensure confidential data is kept in secure storage.

The team behind FortKnoxster, who are experienced cyber-security and crypto engineers, has spent over 5 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 centralized government surveillance."

FortKnoxster is the world’s first all-in-one peer-to-peer encrypted communication platform.

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

FortKnoxster is a cyber-security company, specialized in developing secure and end-to-end encrypted communication solutions. The company has developed a unique encryption platform, which is aimed at the B2C market and B2B 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 an extremely high level of privacy.

New complex regulations, increasing adoption of new technologies (IoT, BYOD, cloud-services etc.) have fueled 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, family 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.

Soon, 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 cybercrime forecast to reach $10.5 trillion by 2026, according to Cybersecurity Ventures.

“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.

In 2020, companies saw a huge increase in new cyber threats and challenges due to the pandemic. The Covid-19 pandemic led to significant changes in ways of working and made cybersecurity harder for many companies. Many people were suddenly working from home, which meant that cyber thieves could take advantage of the lack of secure remote connections and outdated antivirus software to gain access to both private and corporate data.

Companies will have to increase cybersecurity staff training and awareness and carry out cybersecurity vulnerability audits and risk assessments, to be in the best possible position to avoid cyber-attacks.
According to Upguard, the global cost of data breaches in 2021 is expected to reach $9 trillion annually. This is triple the amount from $3 trillion in 2015.

Apart from the huge business disruption of a data breach, there is also the loss of clients, reputational damage, fines & compensations etc.

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 personalized 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 has been clear for some time that data laws (or lack of) did damage consumers and their privacy and have resulted in the enforcement of the GDPR law. (General Data Protection Regulation). The law sets out rules and guidance about how personal data and privacy should be treated. Not adhering to the rules, could cost companies dearly. Due to Brexit in December 2020, UK was required to draw up a similar but separate GDPR. EU GDPR took effect on the 25th of May 2018 and UK-GDPR took effect 31st of January 2021.

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, analyzed 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 is 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 regularly get hacked and all (your) data are now in the hands of potentially hostile organizations 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 (unsecured) 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 are to generate as much income as possible from selling (your) data to the highest 3rd party bidder.

FortKnoxster is your safe alternative, as we can’t (nor can 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 installments whatsoever. Users are 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 download the FortKnoxster app, please click here.
Crypto Suite™ Features

Blockchain Integration
FortKnoxster uses blockchain technology to secure communications by storing a cryptographic hash of user’s public identity and keys in a decentralized smart contract.

Encrypted Messaging
Real-time secure end-to-end encrypted chat for fast and instant communications. Comes with voice messages, group chat and much more.

Secure Wallet
Store, receive and send your crypto safely with FortKnoxster’s non-custodial wallet. Transfer and receive any cryptocurrency in chat, it’s as easy as sending a message.

Encrypted File Storage
Store your valuable data, photos, and documents in your own encrypted cloud storage. Easy to share and manage files and folders seamlessly.

Encrypted Video Calls
Super secure video calling without “snoopers” on the line – nobody can access, record or hack your calls. The most private calling you can get on both web and mobile.

Encrypted Inbox
All communications and data are end-to-end encrypted and as secure as it gets. Send messages to friends, colleagues, and business partners with peace of mind.

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

Intuitive Web App
FortKnoxster is also available as a desktop web app for Windows, Mac OS and Linux – extremely easy to use on all devices.

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

FK Transfer
Transfer your Private and Identifiable Information (PII) or other confidential files using an end-to-end encrypted secure link.

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

FK Channels
Make channels and host 10.000s (or more), build your own community or entourage. Watch out Telegram and Discord!
FortKnoxster Web App
FortKnoxster App for iOS & Android
Secure Wallet

Our Crypto Suite™, combined with FortKnoxster’s secure wallet is basically the world’s most secure one-stop platform for safeguarding your digital assets and private communication. You are in complete control of your funds. By leveraging FortKnoxster’s existing encryption algorithms (for securing and verifying the identity of the sender and receiver when exchanging messages and public keys with your contacts), it makes it possible to also exchange your wallet addresses securely on the same encrypted channel. This level of trust ensures that your cryptocurrency transactions to and from your contacts, can happen safely – most importantly it gives you peace of mind. FortKnoxster also offers an encrypted backup solution of their user’s wallet secret keys, to help users avoid worst-case scenarios, such as losing access to their funds.

<Wallet>

- Multi-cryptocurrency wallet app
- Supports Bitcoin, Ethereum, Binance & more
- Send crypto as easy as sending a message
- Request crypto safely from your contacts
- QR scan for simple crypto payments

Non-custodial Wallet

Store, receive and send your crypto safely with FortKnoxster’s non-custodial wallet. Your private keys are never exposed to third parties – not even FortKnoxster.

Endless asset types

Store all your coins and tokens in a single, secure mobile wallet. We support 40 blockchains and 100K+ assets. BTC, ETH, FXX, NFT collectibles and other assets totally on your terms.

Transfer Crypto In-chat

Send and request cryptocurrency payments from your contacts directly in the end-to-end encrypted chat. Also possible to QR scan to make crypto payments.
Real-time Balance
Easy overview of your cryptocurrency portfolio with real-time balance updates. Choose your preferred Fiat currency like USD, EUR and more.

Multiple Wallets
Generate and import as many wallets as you want. FortKnoxster supports all major blockchains and cryptocurrency assets, such as Bitcoin, Ethereum and Binance.

Lock Wallet
Your wallet secret keys are secured with a PIN-code and biometric Touch ID and protected by the phone’s Trusted Execution Environment (TEE).
Our Mission Statement

“FortKnoxster is the most secure and privacy-oriented all-in-one peer-to-peer encrypted communication platform and blockchain platform.

FortKnoxster protects your online privacy and financial transactions by encrypting all your communication and data.”
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 nonstandard 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 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 the 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 state:

“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 takes 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 element 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 has built a complete ecosystem using the FHX token and smart contracts 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 describes 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 emails, 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 have the highest priority. Therefore, 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 to have achieved.

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 through a computed Merkle-tree, 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 curves (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 FortKnoxster’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 personal password is used to compute derived keys in the client, the account password, and root keys.

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

The account password is a cryptographic hash of the personal password using the PBKDF2 algorithm with SHA-256 as the hashing algorithm, which performs 50,000 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 20,000 rounds of hashing operations, and therefore computes a completely different derived key. 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 AESGCM 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:
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.

FortKnoxster enforces a decentralized trust of identities using Ethereum blockchain smart contracts and IPFS as a decentralized P2P network storage of the identity objects.

These identities consist of a self-signed object containing the user ID and the user’s public identity key, which are inserted into a Merkle-
tree, whose root hash is finally stored in a smart contract on the Ethereum blockchain.

When FortKnoxster’s users connect with each other, they cryptographically sign each other as contacts, so they establish a trusted communication link between them, which can finally be verified through the blockchain guaranteeing, that any user’s public keys in fact come from the claimed user and therefore prevent MITM attacks.

This is a common cryptographic problem, to trust that the public keys belonging to a specific person. Most available solutions consist of a centralized approach, such as Certificate Authorities, but FortKnoxster uses a decentralized approach, using the Ethereum blockchain, IPFS and self-signed contacts to solve this problem.
Knoxstercoin (FKX) Token Utility

The FortKnoxster utility token ($FKX) is used for purchasing various services and for incentivizing users for different rewards achieved.

The FXX token has a clear and important usage in our application, as a means of both incentivizing further development and securing our ability to run and market FortKnoxster worldwide. The FXX token serves the purpose of being required to use FortKnoxster’s PRO features and obtain extra encrypted cloud storage.

A fixed supply of 150 Mill. FXX was generated during the token distribution. A ledger on the blockchain was created maintaining the FXX token, following the ERC-20 standard and allowing a secure mechanism for transferring FXX to other participants.

Signing up to FortKnoxster is free and 1 GB of free encrypted storage is allocated.

Users on FortKnoxster who owns FXX tokens can upgrade their account to purchase a PRO subscription to obtain:

- Extra Encrypted Storage
- Screen Sharing
- Group Conference
- Manage Unlimited Group Chats
- Manage Unlimited Folder Shares

FortKnoxster plans to introduce other PRO subscription features in the future.

The following screenshot illustrates PRO upgrade checkout step in the FortKnoxster Web App, where the PRO plan can be customized to fit the storage needs. Further, it illustrates a clear overview of the FREE features versus the PRO features.
FortKnoxster currently supports payment with the following wallets:

- Leger Hardware Wallet
- MetaMask Software Wallet
- Mobile Wallets with ERC-20 token support
- Other External Wallets with ERC-20 token support

Check out our full guide on How to upgrade your FortKnoxster account to PRO.

The below screenshot illustrates the PRO checkout step with the 1-year PRO subscription for 1,000 FXX including 10 GB FREE storage. Additional storage has a cost of 100 FXX per GB in the yearly subscription.

All prices are subject to change at any time without further notice. The current prices are available when accessing your FortKnoxster account from a desktop browser here https://web.fortknoxster.com/. Prices illustrated in this white paper may only be valid at the moment of writing.
To further contribute to the FKX ecosystem, incentive earning plans will be launched - such as:

- **Referral**
  Users get rewarded with FKX tokens, by referring friends, family and business contacts to the FortKnoxster platform through invitation.

- **Bug Bounty**
  Users can also get rewarded with FKX tokens by submitting valid security reports of the bug with PoC (Proof of Concept).
Token Generation Event

TOKEN SALE TERMS

150 Million
FKX TOKENS ISSUED

$15 Million
MAX CROWDSALE CAP

89.25 Million available for token sale.

FKX tokens will be sold for ETH and BTC.

- 59.5% SOLD IN TOKEN SALE
- 12% PARTNERS AND ADVISORS
- 11% COMMUNITY INCENTIVES
- 10% FORTKNOXSTER
- 7.5% FOUNDERS

FKX is an Ethereum ERC20 token. Token sale ends 18 Mar 2018 12:00 CET or when sold out.

The Token Generation Event ended 18 Mar 2018 12:00 CET.
FortKnoxster Roadmap

FortKnoxster Roadmap 2021

Q1
- Open Source
- Launch - FK Transfer
- FXX/USDT Pair Addition

Q2
- Binance Smart Chain Integration
- Binance Bridge
- Self-destructing Messages

Q3
- FK Crypto Suite
- Wallet Integration

Q4
- FXX Staking
- FK Channels
Core Team

Niels Klitsgaard
CEO & Co-Founder
Niels is Danish and has been an entrepreneur most of his life. His original background is from banking and he holds an MBA in International Marketing. He is a strong, but informal leader, with great communication skills. Niels has an innovative mindset and a “Nothing is impossible” attitude. He is extremely dedicated to enhancing innovation, always looking at ways to do things smarter and better. Niels has vast experience in scaling and growing companies. He is also a true privacy advocate. Niels is one of the founding partners in FortKnoxster.

Susanne Firouzbakhsh
COO
A compliance professional with 30 years of experience in Investment banking. Working in various operational roles in Copenhagen and New York, but mainly in London where she has spent most of her life. She has strong commercial and analytical awareness. Works effectively across geographies, building relationships with a range of stakeholders to ensure compliance & continuously looking to improve processes, services and partnerships.
Mickey Joe Nathan Johnnysson  
**CEO & Co-Founder**

Mickey is Danish and has spent most of his adult life playing with computers and developing software. Mickey has a master in computer science and is a great leader and team player.

His major passions are computer engineering, crypto and Blockchain, and he enjoys any technical challenge, especially if it’s the cutting-edge technology and innovative kind. To be able to create something great, innovative and useful for others and that can change their lives in some way to the better, is what usually drives and motivates Mickey.

---

Rasmus Birger Christiansen  
**CPO & Co-Founder**

A digital and telecommunications executive with 20+ years of international experience holding multiple senior management roles.

Passionate about digitization and the transformation of the digital landscape across industries with particular attention to secure communications and privacy.

Solid background and wealth of knowledge in management of mobile networks both from a functional and security perspective.

A true believer of privacy and the ability to freely communicate.
Jon Sterling  
**CSO**  
Jon has spent his career in sales and sales management roles in US and UK. He works at the intersection of sales, marketing and technology and has been involved in the cryptocurrency space since 2016. Jon’s specialty is building organizations from the ground up.

He has built and led high-performance teams in some of the most competitive markets in the world. His background in finance has served him well as an occasional angel investor and startup advisor, and he devotes his spare time to a few select charity organizations.

Carlos Fernandez  
**CDO**  
Passionate with technology and blockchain enthusiast, full of entrepreneurial spirit with 10 years’ experience in business management specialized in hospitality, operations, product, technology, and marketing.

He has experience from various stages of companies from large franchises to small start-ups, and from various industries including food and beverage, co-working spaces, and online businesses.
Advisors

Baz van Zelm
Advisor
Accomplished and goals-oriented real estate, equities and private equity/venture capital professional with solid capital markets experience.

Strong track record for over two decades in investment banking and asset management. Currently CIO of large Amsterdam-based Single Family Office.

Eddy de Heij
Advisor
Entrepreneur with over 25 years of experience in Media, Marketing and Data (Privacy). Gut Investor in several cool, thrilling and sometimes profitable startups.
Andreas Jakobsson
Advisor
Andreas has extensive international experience in business operations as a strategy consultant, and as a leader in industry roles.

He is a supporter of data privacy and has invested in multiple blockchain technology projects.

David Orban
Advisor
David is one of the early adopters of blockchain technologies and an active crypto investor since 2010. David is a true visionary and he was one of the first to own Ethereum during the Ethereum launch in 2014. David is an investor, 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.
Final Words

FortKnoxster is founded by Danish entrepreneurs and cyber-security experts, with extensive experience in the field of online security and cyber defense. 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 technical 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.

**Private Keys Protection**

When a user registers on FortKnoxster.com – 4 sets of RSA key-pairs are generated, 3 sets of elliptic curve (EC) key-pairs and 7 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, such as inbox, chat, calling, file storage & account...
settings. Unlike other known encryption protocols, each of FortKnoxster’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 personal password is used to compute derived keys in the client, the account password, and the root keys.

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

The account password is a cryptographic hash of the personal password using the PBKDF2 algorithm with SHA-256 as the hashing algorithm, which performs 20,000 rounds of hashing operations (key stretching) and takes the username@fortknoxster.com 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 32-byte randomly generated salt and 50,000 rounds of hashing, 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 AESGCM 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 and account password.

When a user changes a password, the account password is changed the same way as above and all the key protectors are re-encrypted with the new root key computed the same crypto operations above and replaced in the key containers.

When a user enables the account recovery feature, a new key protector is added to each key container, using the recovery key as the root key in the above crypto operations.
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 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 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 contact’s 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 to 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 a 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 HMACSHA256 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 signaling 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 signaling is done to exchange certain information and set up the call.

This signaling 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.

“The Web Cryptography API defines a low-level interface to interacting with cryptographic key material that is managed or exposed by user agents. The API itself is agnostic of the underlying implementation of key storage but provides a common set of interfaces that allow rich web applications to perform operations such as signature generation and verification, hashing and verification, encryption and decryption, without requiring access to the raw keying material.”

Source: (W3C) Web Cryptography API http://www.w3.org/TR/WebCryptoAPI

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 Crypto API does not replace TLS & HTTPS, in fact, the Web Crypto API requires a HTTPS secure context to work.

TLS is a protocol to establish a secure and trusted client-to-server communication tunnel as a transport layer using strong encryption to serve content over HTTPS.

Web Crypto API is an interface made available for application developers to access various crypto operations enabling web application developments, with use cases such as encrypted messaging, encrypted cloud storage, document signing & sharing, data integrity protection among other use cases.
FortKnoxster uses the Web Crypto API in its advanced client end-to-end encryption design in combination with a strictly configured TLS and HTTPS.

Our code is served over HTTPS only from the https://web.fortknoxster.com origin and we DO NOT serve any external resources or cross-domain scripts.

**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 be 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 **HTTP Only** 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 webserver 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 into performing 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 256bit 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 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, such as ECDH with elliptic curve 25519 and RSA 3072bits, 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.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>Sign</th>
<th>Verify</th>
<th>Derive</th>
<th>Digest</th>
<th>Wrap</th>
<th>Unwrap</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSASSA-PKCS1-v1_5</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA-OAEP</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDH</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES-CBC</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES-GCM</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES-KW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMAC</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PBKDF2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>HKDF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BCRYPT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SHA-256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2: The GDPR Regulation

Below is a short description of the GDPR. FortKnoxster is a good and relevant tool to comply with the strict GDPR law and easy to implement in any organization 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 and privacy for all individuals in the European Union (EU) and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas and the European Economic Area.

Here are the most important takeaways from the GDPR.

When

The EU-GDPR law took effect May 25, 2018. Until then, existing national data protection laws applied, which included national security laws, or employment laws and free speech.

The UK-GDPR law took effect on 31st of January 2021, as due to Brexit, UK is no longer part of the EU.

The UK-GDPR is similar to EU-GDPR and many other countries have a similar law in place.

Who

The new European Data Protection Regulation applies to any business irrespective of its business activity or sector of the 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’ behavior.
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 the 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 General 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 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 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 organizational measures for ensuring the security of the processing.

While the European General 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

Effective: January 1, 2021

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 a username, phone number and a 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 from a parent or legal guardian to open and maintain an account. 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 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 FortKnoxster 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.

**Transferring Data**

The customer agrees that FortKnoxster and its sub-processors may transfer encrypted content and data between their servers. By signing up to FortKnoxster the customer agrees to process data on its behalf and to provide the Services in accordance with FortKnoxster features and services. Customer acknowledges that its company users use of the service is subject to FortKnoxster’s Privacy Policy and understands how FortKnoxster collects, stores, and uses data and information. Customer will make its users familiar with FortKnoxster’s Privacy Policy and Terms of Service. If customer is subject to i.e., EU data protection laws and other data protection laws, customer agrees to follow and respect the terms of this law and others.

**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, damage, loss, expense 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. Paid accounts are charged for a minimum of 1 month.

**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 advanced notice of these changes via a message to the email address associated with your account. Any changes will also be published within the FortKnoxster website.

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 Gibraltar 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.

Customer Files and Data

You understand that FortKnoxster uses strong cryptography to protect data and Customer files. As a Customer of FortKnoxster, you are fully and solely responsible and accountable for the content of Customer files. By using the Services, you guarantee that you have all required permissions for each Customer file – including copyright and other intellectual property rights – to distribute, transfer, store and/or make the content available online through the Services. You agree that your files and data used do not violate any person or applicable laws and regulations.

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, reorganization 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 the date of the 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.
Appendix 4: Privacy Policy

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, damage, loss, expense 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. Paid accounts are charged for a minimum of 1 month.

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 advanced notice of these changes via a message to the email address associated with your account. Any changes will also be published within the FortKnoxster website.

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 Gibraltar 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.

Customer Files and Data

You understand that FortKnoxster uses strong cryptography to protect data and Customer files. As a Customer of FortKnoxster, you are fully and solely responsible and accountable for the content of Customer files. By using the Services, you guarantee that you have all required permissions for each Customer file – including copyright and other intellectual property rights – to distribute, transfer, store and/or make the content available online through the Services. You agree that your files and data used do not violate any person or applicable laws and regulations.

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, reorganization 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 the date of the 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.
THANKS FOR YOUR INTEREST

For more information:
www.fortknoxster.com
or e-mail:
contact@fortknoxster.com