FORTKNOXSTER

白皮书

加密即服务.

版本 1.2 ● 2017年11月21日

FORT

KNOXSTER

“假如你花在喝咖啡上的钱比在IT安全还多的话，
那么你终究会被黑。”

引用：理查德 克拉克，美国政府网络安全专家

声明

本文档中提供的信息“按原样”提供，没有任何形式的担保。 即使我们或我们的顾问已被告知有可能发生此类损失，我们和我们的顾问在任何情况下都不对任何损害（包括直接，间接，附带，间接，商业利润损失或特殊损害）承担责任。

文档生命期

我们在发布相关版本软件之前可能会更新在线文档。 因此，如果最近没有下载这个文档，它可能不包含最新的信息。 请参阅FortKnoxster.com获取最新信息。

产品信息 — 有关文档，发行说明，软件更新或有关产品，许可和服务的信息，请参阅FortKnoxster.com。

技术支持 — 有关技术支持，请参阅FortKnoxster.com 并选择支持。 在支持页面上，您将看到几个选项，其中一个用于提出请求。

你的评论s

我们重视您的意见。 建议将帮助我们继续提高用户出版物的准确性，组织性和整体质量，因此请随时发送电子邮件咨询 hello@FortKnoxster.com。

如果您对特定信息或程序有任何意见或问题，请附上标题和(如果有的话)，修订版本号，页码和任何其他详细信息，以帮助我们找到您所询问的地方。

商标

FortKnoxster 是FortKnoxster Ltd 的一个待注册商标。

目录

执行摘要

我们的世界变化速度比以往任何时候都要快，很难跟上新的趋势，流行语和新兴技术。 区块链技术的使用率处于历史最高水平。 当涉及到不同的代币，硬币，数字资产或任何人选择的不同名称的数字货币的数量现在有数千种。

不幸的是，网络犯罪率也处于历史最高水平，网络从未像现在这样不安全。黑客，大规模监视间谍活动，病毒，恶意软件，间谍活动，网络钓鱼，勒索.....攻击清单很长，并且随着攻击者越来越复聪明，攻击性和富有创造性而日益增多。

联邦调查局说，我们已经进入了网络犯罪的流行期，网络犯罪已经超越了“正常”的旧式犯罪 – 无论是程度还是伤害性。

FortKnoxster 背后的团队是经验丰富的网络安全和数字货币工程师，他们花费了3 年时间开发了一个端到端的加密通信平台“Fort Knox”。

"FortKnoxster 将区块链和复杂的端到端加密技术运用到用户友好的一体化通信平台中，用户可以通过收件箱，聊天，电话/视频通话，文件等私密安全的方式进行通信 存储等 FortKnoxster 消除了黑客攻击，网络威胁和政府集中监视的风险。"

FortKnoxster 是世界上第一个成型的点对点加密通信平台，简称为：

“吃了兴奋剂的电报”

FortKnoxster 就是您需要在网络犯罪日益严重的网络世界中进行交流，互动和安全工作的一切。

FortKnoxster 是工作产品支持的少数代币销售之一。

介绍

FortKnoxster 是一家网络安全公司，专业开发安全和加密通信解决方案。 公司开发了一个独特的加密平台，主要针对B2C 市场。

平台提供E-a-a-S 解决方案(加密即服务)

FortKnoxster 的设计具有独特的架构和功能，这使得每个人都可以使用我们的平台进行所有的通信和数据存储。

FortKnoxster 解决了现代社会最大的挑战之一。

为了保护通信和数据免受网络犯罪的威胁，同时保持非常高的隐私水平。

新的复杂法规，越来越多的新技术（物联网，BYOD，云服务等）的采用促使了对安全性和加密的需求。 新的法律和法规非常严格，FortKnoxster 提供了最好的“即插即用”解决方案，以符合大多数这些新法律。

任何人都可以随时使用FortKnoxster，无论您是在笔记本电脑/台式机上还是随身携带智能手机或平板电脑。

FortKnoxster 平台已经通过了世界范围内一系列好的（和坏的）黑客和“cypherpunks”的渗透测试，并且已经通过了考试，因为没有人能够以任何方式破坏我们的平台或者访问任何端到端的 加密帐户或内容。

“加密应该默认启用，而不是只有当你正在做一些你认为值得保护的事情时才打开的功能。 加密是我们拥有的最重要的隐私保护技术。”

引用：Bruce Schneier，美国密码学货币学家，计算机安全专家，隐私专家和作家

挑战

现在在线交互几乎是每个人都必不可少的活动，为朋友和商业伙伴的互动以及全球发展，创造了新机会。

网络犯罪，网络罪犯及其工具正在变得更加多样化和复杂。网络犯罪现在以各种形式出现，除非消费者，企业和政府现在采取行动，否则网络犯罪可能以许多破坏性的方式威胁到我们社会的根本。

在不久的将来，随着无处不在的计算技术渗透到我们更多的生活中，这些威胁将会增长。我们越来越重视和依赖的直观界面经常出现所有问题。

使用互联网和在线通信，从来没有像现在这样不安全，而且每天都变得更糟。根据 Juniper Research 的数据，黑客对网络犯罪的预测构成了巨大的威胁，到 2019 年，网络犯罪的成本将超过 3 万亿美元。

“网络犯罪是每个公司在现实世界所面临的最大威胁”

引用: IBM CEO Ginni Rometty

今天的网络犯罪分子往往是高度积极的专业人士，由竞争的企业，犯罪组织或国家资助，他们一直坚持尽可能突破和破坏对手。

根据一份新的 PWC 调查，大小企业在线安全漏洞大幅上升，报告指出，去年有 80%以上的企业和中小企业遭遇安全漏洞。大多数受访者预计未来将出现更多的安全事件，未来谈到网络安全（或缺乏）时“没有任何好消息”。

此外，实际违规的成本继续飙升，一年内翻了一番还多。一个拥有 500 名员工的普通企业在网上遭遇安全漏洞攻击，最终导致销售损失，业务中断，资产回收，客户流失，罚款和赔偿等超过 350 万美元的净账单。此外，是受损的形象和羞辱。

在过去几年里，我们已经听到了大量关于大数据的力量，这使得公司能够提供比以往更多的定制化，有针对性和个性化的产品和服务。这对消费者的好处可能是显而易见的，但是它产生了许多道德上的问题，而不仅仅是个人数据掌握在不道德的企业手中。

一段时间以来，数据法律（或缺乏）已经明显地损害了消费者的隐私，导致了 GDPR 法的执行。 （“通用数据保护条例”）。该法律旨在让公民对其数据有更多的控制权，并制定统一的规则在全世界执行。现在大多数公司面临的巨大挑战是如何遵守 2018 年 5 月 25 日这个新的严格的法律。

我们这个时代的一些最大的公司，如 Google 和 Facebook，是通过收集和使用用户的用户数据向第三方做告而创建的。你在这些平台上做的或者说的一切都被记录下来，存储和分析，让你在那里的主要目的是从你的个人资料和行踪中赚钱。

除此之外，大多数国家的政府都会进行一般性的大规模监视，全天候跟踪和记录您在线做的所有事情，并永久保存。而更令人恐惧的是 – 这些政府服务器总是被黑客攻击，所以你的数据掌握在罪犯手中

毋庸置疑，与数字化分析相关的许多潜在危险（和道德问题），从黑客攻击到歧视，再到奥威尔式监视状态。公司可以做和应该知道有很大的区别。

在线活动会留下足迹 – 日志文件，访问条目或在其使用的系统中创建的数据。一旦这些隐私控制被撤销，互联网服务提供商将能够出售他们所捕获的关于您和您的用户如何使用互联网的信息。

在线隐私的丧失使 IT 犯罪分子更容易对大公司进行黑客攻击，所有的（你的）数据现在掌握在潜在的敌对组织或试图从你的数据中获利的人手中。

尽管我们都能找到保护自己的方法，但避免跟踪和“窃取”我们数据的唯一方法就是停止使用这些免费服务，并使用像 FortKnoxster 这样的端对端加密来保护我们的通信。

什么是 FortKnoxster?

FortKnoxster 是一个一站式的沟通，协作和文件存储平台。

把它想象成所有你最喜欢的（不安全）的日常应用，如Skype，Slack，Telegram，Dropbox，Facetime，Gmail 等等的组合 - 所有这些都聚集在一个顶级的安全平台上，你可以获得最高的隐私。

上述传统的应用程序是伟大的，但他们往往带来很多安全隐患。首先，由于这些服务是免费的，“你就是产品”的含义，所有的数据和通信都被读取，存储，销售，并经常被黑客入侵。绝对
没有隐私，因为这些公司的大多数商业模式都是通过将（您的）数据出售给出价最高的三方投标人而获得尽可能多的收入。

FortKnoxster 是您的安全选择，因为我们不能（任何人不能）读取您的数据或通信，因为它是端对端加密的。即使我们可以，我们的商业模式与其他大多数商业模式是完全相反的，但是我们的业务是保护您的数据，而不是将其出售给出价最高的投标人。

FortKnoxster 非常容易使用，因为它不需要额外的插件安装。用户几乎可以在几分钟内开始运行，并可以开始享受极高的安全水平和直观的界面。

很容易邀请朋友，家人或商业伙伴进驻平台。

FortKnoxster 被设计为供大众使用，因此使用该平不需要技术知识。

如果你想试试 FortKnoxster 的免费演示，请点击这里。

FortKnoxster 主要特性:

- 收件箱

消息是端对端加密的，并且尽可能安全。给同事，客户和商业伙伴发送信息，放心。

- 分布式文件存储

存储您宝贵的加密数据 – 并确保它不会损害。轻松分享和管理文件和文件夹。

- 聊天

实时安全聊天，实现快速即时通讯。随着语音消息，群聊等等。

- 呼叫

从竞争对手或外部监控无从窥探的安全通话。您可以在网络和移动设备上获得最私密的通话。

- 群聊/会议

通过聊天，呼叫，共享文件等安全协作，通过群组会议功能 – 更智能，更安全地工作。

- 屏幕共享

我们开发了加密的屏幕共享功能，作为与合作伙伴和其他第三方进行安全协作的额外宝贵工具。

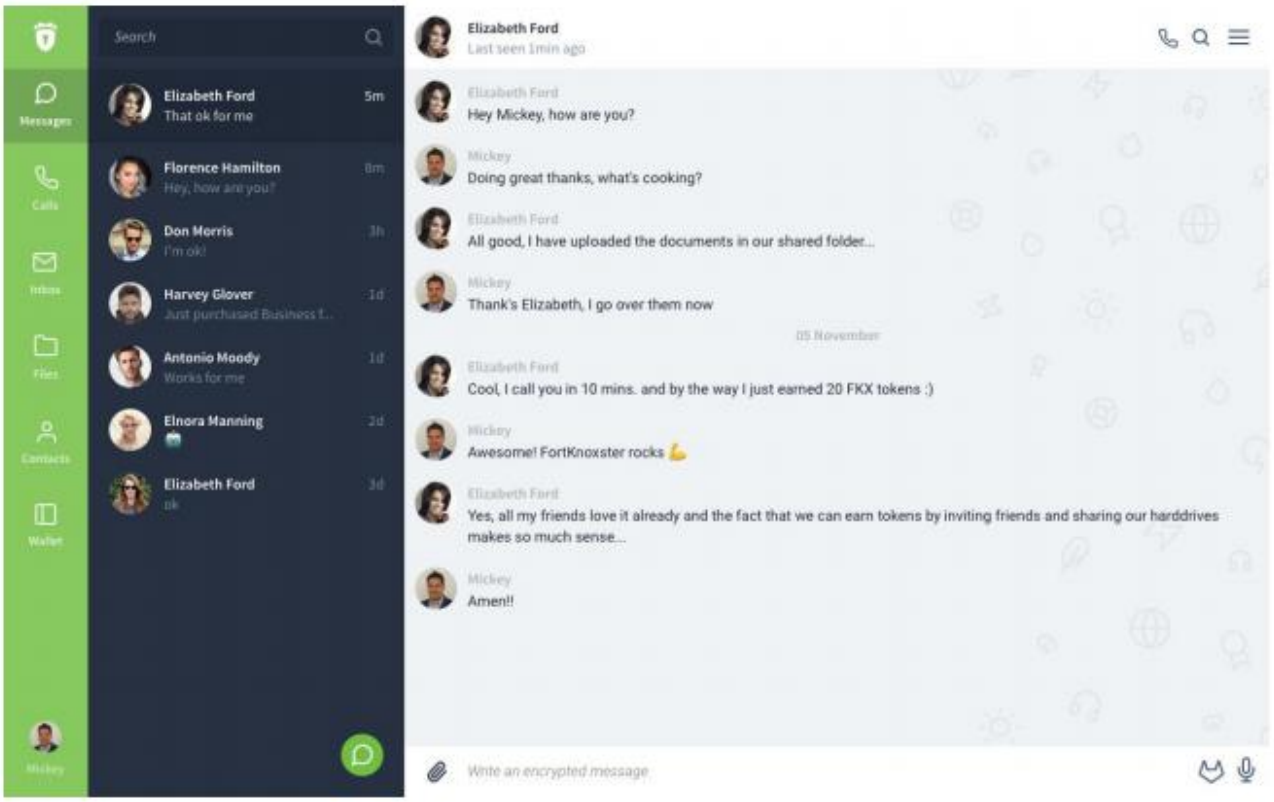
- 语音消息

发送快速的语音信息，而能节省时间，该功能在网络和应用平台上均可用。

- 直观的面板

仪表板为用户提供了所有通信和数据的总览。请参阅下一页的仪表盘和应用程序图像。

FortKnoxster 主仪表盘



FortKnoxster 手机App

我们的 iOS 和Android apps 将在2018 年1 月发布

我们的使命宣言

“FortKnoxster 将成为有史以来最安全的通信和数据存储平台...

– 并最终成为黑客，间谍或其他IT 犯罪分子的噩梦 “

为什么使用加密?

加密这个词来自希腊词“kryptos”，意思是“隐藏”或“秘密”。加密用于尽可能提高安全级别。加密的使用几乎和通讯本身一样古老。早在公元前 1900 年，一位埃及文士使用非标准的象形文字来隐藏铭文的含义。

加密是最大化电子邮件，聊天，消息，电话或文件通过“加扰”的内容安全性的一种方式

加密基本上是一种对消息或信息进行编码的过程/方法，只有授权方才可以阅读。加密是企业和军方私下安全通信的安全方式，没有其他人（即竞争对手）能够跟踪或监视通信。

加密也是保护任何人从大公司和政府到小企业和律师到普通公民的通信的主要工具。加密保护整个国家的基础设施 - 通信，电力，运输和医疗保健系统以及企业。

随着我们急切地进入智能互联设备时代，加密（如果使用的话）保护我们的电话，短信，电子邮件和云存储。随着物联网的出现，安全专家呼吁在物联网产品中实施强有力的加密，这些产品如果无人看管，可能会给个别家庭和更大的基础设施带来混乱。

当你听到加密这个词的时候，可能会想到的第一件事就是只有技术人员或极客才能理解或者使用。实际上，加密的概念并不复杂，我们的平台使加密非常容易。

加密是保护您的隐私的最佳方法。

密码学家和安全和隐私专家 Bruce Schneier 指出:

“默认情况下应该启用加密功能，而不是只有在你认为值得保护的事情时才开启。”

为什么使用区块链?

区块链是一个去中心化的开放的分布式账本，记录了双方之间在点对点网络上的金融交易（或者几乎任何有价值的东西）。这种不断增长的记录清单通过强大的加密技术进行链接和保护，使得这些交易永久可验证，因此是不可破坏的。

“区块链解决了垄断问题”

引用：Vitalik Buterin，以太坊的投资者

由于区块链是可公开验证的，因此它提供了这样的安全性和透明度，使其成为许多类型的安全应用程序的理想选择。

FortKnoxster 利用区块链技术提供的这些功能，通过使用其智能合约，将其数字身份的中心化的信任转变成去中心化的信任，特别是以太坊区块链。

信任至关重要，是任何加密基础设施中最重要的因素。目前 FortKnoxster 的数字身份信任模型是中心化的。这种中心化的信任模式是当今常见的问题，因为它单一失败会破坏整个系统。

“集中身份会造成一个单一的故障点，并建立一个能够吸引黑客的高价值数据库，并且需要适当的控制以保持完整性。”

引用：IBM 区块链 IDC 报告，"只是时间问题”

利用区块链的分布式信任模型是一种管理数字身份的新方法，区块链技术允许用户控制自己的数字身份，并在他们同意的情况下在受信任的人之间共享和通信。因此，没有一个实体可以危害用户的数字身份，也不存在单点故障。

除了实施 FortKnoxster 的加密数字身份（公钥）的安全和去中心化的信任模型；FortKnoxster 还将使用以太坊区块链上的 FKX 代币和智能合约建立完整的生态系统，以促进订阅服务的安全交易和激励参与者。

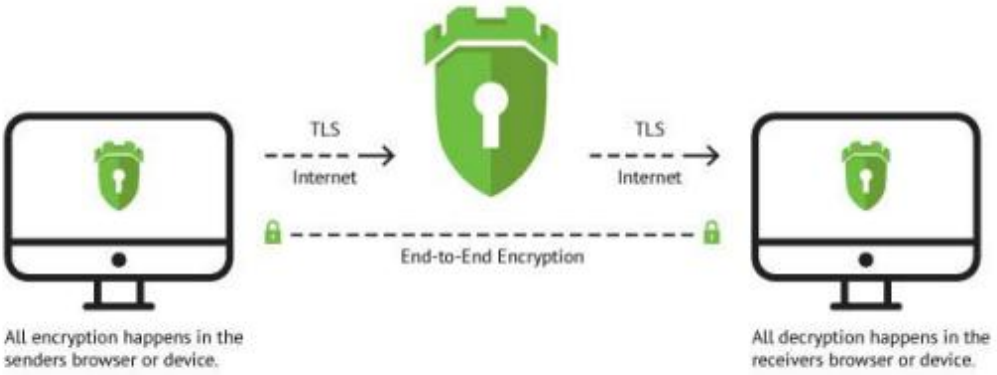
我们的技术

以下是 FortKnoxster 端到端加密的技术解释，详细介绍了使用以太坊区块链的智能合约和数字身份信任的密码设计和安全性。更详细的描述可以在附录部分找到。

FortKnoxster 是一个安全的网络和原生应用程序通信和协作平台，使用户能够安全地交换消息和文件（包括邮件，附件，聊天，群聊，通话，文档，图像，视频，语音消息，视频消息和文件），基于有效的端到端的加密。

在 FortKnoxster，安全和隐私是最重要的。这就是为什么我们通过设计构建 FortKnoxster 加密，隐私和安全架构的原因。与大多数其他在线业务不同，我们的主要目标是保护用户的隐私，这是我们引以为豪的。

下图说明了两个用户之间如何通过浏览器客户端和服务器之间的 TLS 加密连接上的 FortKnoxster 服务器进行端到端加密。



附录 1 详细描述了收件箱和聊天消息交换，文件存储和呼叫如何发生以及涉及哪些加密操作。

FortKnoxster 拥有自己的公钥基础设施（PKI），扩展到以太坊区块链。在区块链中，用户的数字身份被存储在注册表中，使用智能合约，不会被单个实体，甚至 FortKnoxster 团队所破坏。

当用户在 FortKnoxster.com 上注册时 – 在客户端浏览器中生成四组 RSA 密钥对，两组椭圆曲线（EC）密钥对和六个密钥保护器（每个私钥一个）。

这些加密和身份密钥对用于不同的服务和协议。与其他已知的加密协议不同，FortKnoxter 的每个服务或协议都需要两组密钥对，一组用于加密和解密，另一组用于签名和验证。

密钥保护器用于加密/包装只有用户自己知道的私钥。

用户的简单密码用于在客户端中形成两个密码，帐户密码和根密钥。

请注意：只有用户知道自己的普通密码，用户的普通密码和根密钥永远不会被发送到服务器是非常重要的。

账户密码是使用 SHA-256 作为散列算法的 PBKDF2 算法的密码，10000 轮散列操作(关键拉伸），并采取
用户名@域名作为盐。结果是一个强密码，它被发送到服务器，并使用 BCRYPT 密钥派生函数作为另一个加密哈希存储。此密码仅用于对用户进行身份验证，不能解密任何用户的数据。

根密钥的计算方式与帐户密码完全相同，但随机产生的盐，因此是一个完全不同的密码。根密钥形成一个 32 字节的 AES 密钥，用于 AES-KW 加密/包装密钥保护器。

此时，每个 RSA 和 EC 私钥都使用 AES-GCM 进行加密/包装，并使用 32 字节的密钥保护器进行加密，该密钥保护器由 32 字节的根密钥，每个组成一个关键容器。所有公钥和受保护的密钥容器在注册期间都会发送到服务器，以及用户详细信息，帐户密码和数字身份。

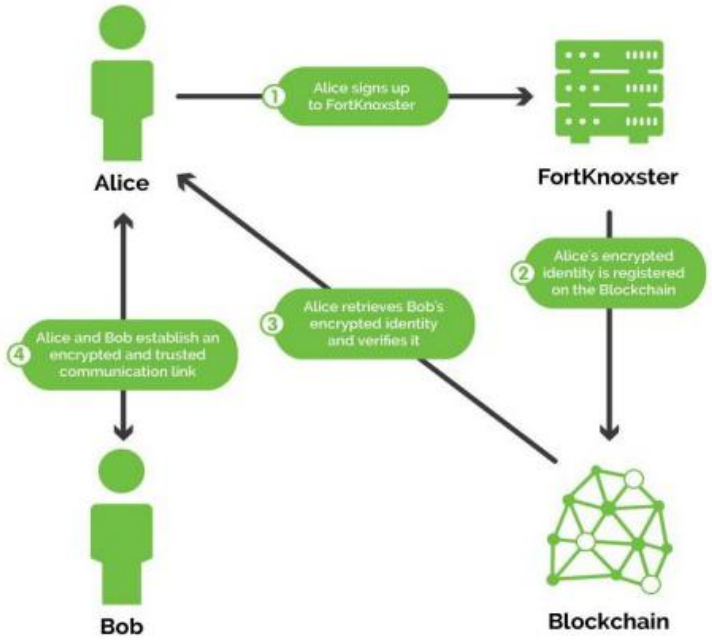
数字身份是这样构造的（在客户端浏览器中）：

数字身份 = 用户 ID + 签名

签名是这样计算出来的：

签名= 签（用户 ID + 公有私钥，私有身份密钥）

FortKnoxster 服务器上建立了一个独立的会话，区块链客户端节点运行。节点从用户接收数字身份，并在包含数字身份的区块链上创建新的交易，以将其存储在智能合同注册表中。



上图说明了一个新注册的用户 Alice，建立了其数字身份。该图还示出了在任何加密的通信链路可以建立之前检索 Bob 的数字身份以进行验证。 Bob 也会对 Alice 的数字身份进行验证预先。

FortKnoxster 服务会消耗大量的存储空间，例如文件，消息附件和文件传输。

FortKnoxster 的整个存储基础设施将使用知名的 IPFS 构建在 P2P 网络的分布式存储中。用户可以租用他们的硬盘并获得有关存储使用情况和带宽使用情况的 FKX 代币。

这相当于加密货币挖矿，但不是使用 CPU / GPU 来挖，而是使用可用的硬盘存储来分配存储空间。

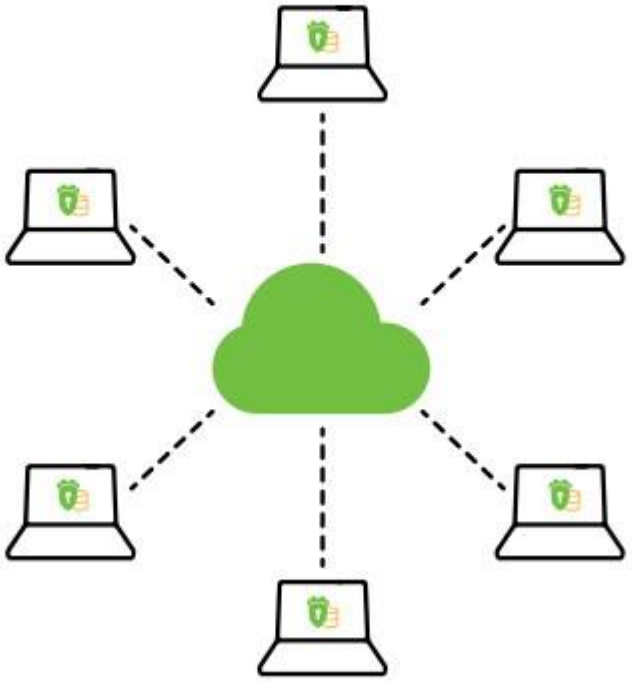
要成为一个存储矿工，需要 3 个简单的步骤:

1) 安装适用于 Mac / Linux / Windows 的存储矿工桌面或控制台软件。

2) FKX. 提供 ERC20 代币支付钱包地址以接收付款 FKX。

3) 选择磁盘位置和多少存储空间

移除中心化的存储服务器可降低存储成本，并提高访问速度和可靠性。所有加密的文件都分布在多个节点上并复制多次。没有一个主机会保存任何重要的文件或任何完整的文件。



FortKnoxster 提供了一个去中心化的分布式存储 P2P 网络，所有的文件都是使用只有上传器的密钥进行端对端加密的。

FortKnoxster 用户将从网络界面和应用程序上传文件和附件，这些加密文件将分散在由所有 FKX 存储矿工组成的分散存储中，并以公平均衡的方式分发。

代币生态系统

FortKnoxster 代币（FKX）将用于购买各种服务，并激励用户获得不同的奖励。

FKX 代币在我们的应用程序中将具有明确的重要用途，作为激励进一步发展和确保我们在全球范围内运行和销售 FortKnoxster 的能力的方式。 FKX 代币用于使用 FortKnoxster 所需的目的。

FKX 的固定的供应量将在代币销售（135 Mill。）期间创建。区块链上的分类账将根据 ERC20 标准创建并维护 FKX 代币，并允许将 FKX 转让给其他参与者的安全机制。

拥有 FKX 代币的 FortKnoxster 用户将能够购买服务订阅，例如：

- **加密存储**

  注册 FortKnoxster 是免费的，有限的免费加密存储将被分配。为了增加加密存储，用户将用 FKX 代币购买固定金额的信用额度。

FortKnoxster 将在未来也推出其他服务和订阅交换 FKX 代币。

为了进一步为 FKX 生态系统做出贡献，将推出激励性收入计划 - 例如：

- **出租硬盘**

  作为 FortKnoxster 去中心化存储的一部分，用户可以通过 FKX 代币获得奖励，将其硬盘空间租用出去。

- **推荐**

  用户通过邀请其他用户访问该平台获得固定的 FKX 代币奖励。

- **忠诚度**

  当使用基于达到不同用户级别的使用公式的各种服务时，用户得到 FKX 代币的奖励。

- 代币销售奖励

  在代币销售期间，FKX 代币将奖励给积极参与我们奖励计划的社区用户。更多信息可以在 BitcoinTalk 上找到。

- Bug 奖励

  用户还可以通过 PoC（概念验证）提交有效的安全漏洞报告，获得 FKX 代币的奖励。这个赏金奖励系统也适用于参与我们赏金计划的现有白帽黑客，参考提交的报告和用户档案。

代币出售供应

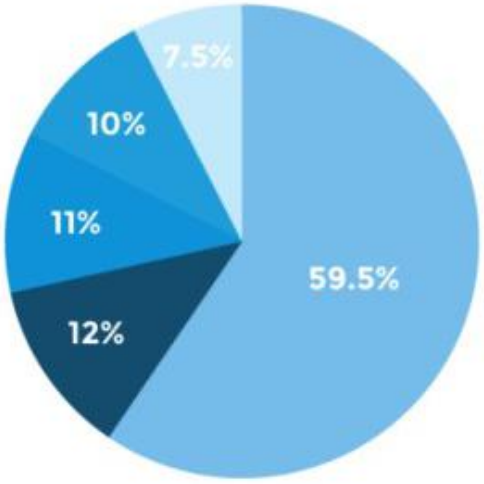
代币销售条款

135 Million
FKX代币发行量

80.325 Million 用于代币销售

$15 Million
众筹硬顶

FKX 出售募集以太坊



- 59.5%用于代币众筹
- 12%用于合作伙伴和顾问
- 11%用于社区激励
- 10% FORTKNOXSTER
- 7.5%创始人

FKX是以太坊ERC20代币
代币销售结束于2017年3月18日12：00CET或者代币销售完

到这里注册早鸟:

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

前期代牌预售将于2018 年2 月5 日星期一开始，并有20%的代币奖金。

公开代币销售将于2018 年2 月19 日星期一12:00 CET 开始。 要参与，请访问此链接:

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

1 美元= 5.25 FKX。 ETH / FKX 费率将在我们的网站上公布。

在众筹开始前4-6 小时将被锁定。所有参与FKX 销售的参与者都必须填写姓名，地址和电子邮件地址。 参与者将被要求确认他们符合服务条款。

重要信息: FortKnoxster 将永远不会通过电报或任何其他媒体和/或网站要求付款。

代币销售地址将仅在FortKnoxster 官方网站上公布 - https://fortknoxster.com.

没有其他网站会正式发布代币销售地址。 切勿将任何ETH 发送到除了FortKnoxster 官方网站上其他地方的地址。

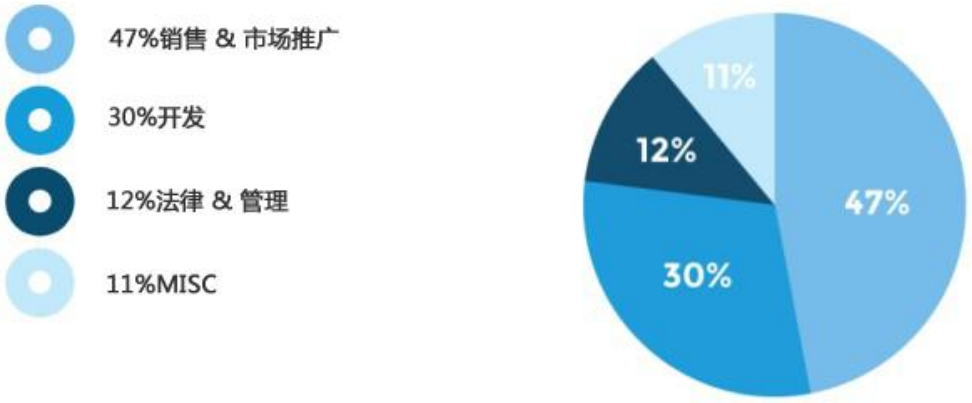
所有分发给创始人和公司的FKX 将被时间锁定12 个月。 在代币销售完成之后，剩余的所有未售出（并且符合条件）的代币将在Ethereum 智能合约中自动销毁。 在众筹结束之后的一周，FKX 代币将可以发送。

社区奖励示例：社区奖励，空投，赏金，比赛，敬业贡献者，Bancor 流动资金池等。

美国和新加坡居民不能参加FortKnoxster 代币销售和代币分发。

如果您既不是美国人也不是新加坡人，就可以参与FortKnoxster 代币销售，也不是美国或新加坡的永久居民，也不在美国和新加坡，包括波多黎各，美属维尔京群岛和美国其他任何地区拥有永久居民或住所。

预算预览



FortKnoxster 路线图

我们的团队

Rasmus Birger Christiansen

CEO & Co-Founder

除了有工程学位，拉斯穆斯有20多年的电信方面经验。 他是一个推崇隐私的人，强有力的领导者，一个网络安全专家。

Mickey Joe Nathan Johnnysson

CTO & Co-Founder

作为一个全面的软件开发人员，他拥有强大的分析能力，已经为米奇服务15年以上。 他的主要兴趣是计算机工程，密码学和区块链。

René Krainert

CFO

René做会计师和财务总监近20年。他有很强的财务和会计背景，动手能力很强，战略规划师和Excel大师。

Emin Roblack

Head of Design

需要创造吗？ 艾敏是你的人。 喜欢设计，图形和动画，他有一个模仿人才，能转换简单的想法变成复杂图形。

Aram Ispiryan

Lead iOS Developer

获得计算机科学硕士，Aram 提供了一种创新的沟通方式。 他的主要优势在于使用iOS 系统上的实时音频/视频和聊天应用程序。

Armen Sisakyan

Lead Android Developer

Armen 将Android 开发带到最高质量和性能水平。 他对在高可用性模式下为数百万用户提供服务的通信协议有着深刻的理解。

顾问

David Orban

Blockchain Expert

大卫是一位企业家，作家，博主，主题发言人和全球技术思想的领导者。 他的企业方面的成绩跨越几个公司成立和成长二十多年

Henok Tekle

Blockchain Expert

亨克（母鸡）Tekle是一个突出的加密货币天使投资者，内容创造者，思想领袖和代币项目顾问。 母鸡是一个频繁的与会者和Blockchain演讲者，也管理好几个加密货币社区。

Stig Abildsø

Entrepreneur & Investor

斯蒂格已经建立了几家丹麦公司，最终成功退出IT部门。 最后成为企业家。

Eddy De Heij

Entrepreneur & Investor

拥有包含全球范围内大量的投资组合，Eddy是一个系列企业家，投资者和作家。

Michael Vivet

高级 IT 顾问

Michael 正在协助战略和战术的制订，以及后端和服务开发。

Carlos Benvenuti

企业家 & 投资者

卡洛斯已经在密码学领域好几年了。他是一名职业教练，顾问和投资者。

最后的话

FortKnoxster 由丹麦企业家和网络安全专家创立，在网络安全和网络防御领域拥有丰富的经验。创始人已经建立了概念验证。

FortKnoxster 平台具有巨大的，可扩展的全球潜力。它是世界上第一个端到端加密平台，通过包括 Blockchain 部署在内的大量功能包括 turnkey 加密。

我们的团队，商业模式，极具扩展性的市场潜力以及来自个人和企业的网络安全需求不断上升将使 FortKnoxster 成为网络安全领域的市场领先者。

通过利用我们先进的加密解决方案和区块链去中心化的结构的强大功能，FortKnoxster 将帮助世界变得更加安全 – 我们将通过成为任何地方的“前往”加密解决方案，并为所有人主导全球加密市场。

附录1：技术预览

关键名词

以下是整个技术说明中使用的关键术语列表。所有的关键材料都是使用 CSPRNG (Cryptographically Secure 伪随机数发生器)利用操作系统的熵源，将高质量的熵作为真正的随机值进行播种。

- **账号密码** - 基于密码的衍生密钥，用于使用 SHA-256 的 PBKDF2 算法作为散列算法进行验证，并用 salt 进行播种。
- **根密码** - P 使用带有 SHA-256 的 PBKDF2 算法作为散列算法并使用随机盐播种的基于密码的派生密钥。导出的密钥用于在 KW 模式下使用 AES 256 位加密和解密密钥保护器。
- **用户 ID** - 自行生成的唯一标识符，用于标识用户 FortKnoxster 系统和区块链上。
- **公开钥匙** - 用户的唯一加密散列用于在区块链上形成数字身份的公钥。
- **数字身份** - 存储在包含用户 ID 的区块链中的键/值记录以及用户 ID 和公钥指纹的数字签名。
- **私人加密密钥** - 使用 SHA-256 作为哈希算法的 RSA-OAEP 2048 位算法方案用于解密的私钥。
- **私人身份密钥** -用于对加密消息进行数字签名的私钥，以 SHA-256 的 2048 位算法和 RSASSA-PKCS1-v1_5 算法为散列算法。
- **公开加密密钥** - 用于使用 RSA-OAEP 的 AES 密钥加密的公钥使用 SHA-256 作为哈希算法的 2048 位算法方案。

- **公开身份密钥** – 用于使用RSASSA-PKCS1-v1_5 进行消息签名，验证的公钥使用SHA-256 作为哈希算法的2048 位算法方案。
- **密钥保护器** – 随机生成的 32 字节密钥，用于在 GCM 模式下使用 AES 256 位加密对私钥进行加密/打包和解密/解包。
- **密钥存储器** – 一个灵活的密码箱容器结构，用于保存带有密钥保护器的加密/包装私钥。
- **消息密钥** – 随机生成的 32 字节一次性密钥，用于在 CBC 模式或 GCM 模式下使用 AES 256 位加密进行消息和文件加密和解密。
- **群密钥** – 随机生成的 32 字节会话密钥，用于在 GCM 模式下使用 AES 256 位加密对群组消息进行加密和解密。

密钥对

RSA 密钥对用于加密和解密，每个包含一个公共加密密钥和专用加密密钥，并使用 RSA-OAEP 以 SHA-256 作为哈希算法的 2048 位算法方案。

RSA 密钥对用于签名和验证，每个包含一个公开的身份密钥和私人身份密钥，并使用 RSASSA-PKCS1-v1_5 以 SHA-256 作为哈希算法的 2048 位算法方案。

用于在密钥协商中导出共享密钥的 EC 密钥对由公钥和私钥组成，并使用 ECDH P521 位算法。

用于签名和验证的 EC 密钥对由公共身份组成密钥和私人身份密钥，并使用 ECDSA P521 位算法。

合约 & 关键交换消息

加密系统的一个常见问题是用户之间公钥的安全密钥交换，确保获得的密钥确实属于预期的接收者。

FortKnoxster 通过利用区块链技术和自签名联系人列表来防止这种潜在的中间人（MITM）攻击。

用户可以邀请其他用户进入该平台或与该平台上的任何现有用户连接。

每个用户都会保留一个联系人列表，其中每个联系人记录都使用用户的私人密钥进行数字签名，并包含所有联系人详细信息，如姓名，用户标识和公钥。联系人在联系请求/接受过程中获得签名。此过程涉及从区块链中检索联系人的数字身份，并通过从联系人公钥中计算相同的公钥指纹，然后使用联系人的公共身份验证码来验证签名。

一旦联系人被验证，它就会被签名并添加到用户自己的联系人列表中。从此，用户可以信任该联系人并在使用其公共密钥交换消息，文件或呼叫之前验证该联系人。

如果联系人验证失败，则与该联系人进行的消息交换不会执行，用户将收到
警告。

消息发送

当用户向其他用户发送收件箱或聊天消息时，请执行以下操作
在发送用户的客户端发生：

1. 如果有任何附件，它们已经用自己生成的消息密钥加密，并且使用具有 SHA-256 的 HMAC 算法和文件的消息密钥来获取加密文件的 Mac。而在这一点上，加密的附件已经上传了服务器和一个独特的
ID 已分配给每个附件。

2. 然后生成消息对象的新消息密钥。

3. 包含任何附件元数据，附件消息密钥，附件 HMAC 签名和附件 ID 的纯文本消息都使用消息的消息密钥加密。

4. 密文（加密消息）使用发送用户的签名
私人身份密钥。

   a. 在签署密文之前，首先使用用户的密钥保护器对私人身份密钥进行解密，该密码保护器在浏览器客户机中用根密钥解密，并在用户登录时存储在浏览器的会话存储器中。

5. 然后用于加密消息的消息密钥被加密
使用接收用户的公共加密密钥。

a. 如果消息有多个收件人，则重复 5）中的过程
与每个收件人的公共加密密钥。

6. 然后将加密的消息，消息签名和加密的接收方密钥发送到存储它们的服务器。

7. 在存储消息之前，服务器应用程序在消息篡改的情况下验证每个消息。这是使用发送用户的公共身份密钥完成的。

当用户收到新的收件箱或聊天消息时，会发生以下情况
在接收用户的浏览器客户端中：

1. 加密消息的签名通过发送来验证用户的公共身份密钥。

2. 加密的消息密钥然后用用户的私有解密加密密钥。

a. 在解密密文之前，首先使用用户的密钥保护器对私钥进行解密，密钥保护器在浏览器客户机中用根密钥解密，并在用户登录时存储在浏览器的会话存储器中。

3. 检索到的消息密钥然后用于解密加密的消息。

4. 如果有任何附件，接收用户可以下载每个加密的附件，使用消息密钥对 HMAC-SHA256 进行完整性验证，然后使用相同的消息密钥进行解密。

群聊消息的目的是处理很多成员和大量的群聊消息。这是通过服务器端扇出来实现的，这意味着用户向服务器发送单条消息，服务器将消息的副本发送给每个组成员。这种设计传输尽可能少的数据。

创建群聊时，会发生以下情况：

1. 创建用户生成组密钥。

2. 然后，组密钥随每个成员的公共加密加密密钥。

对于所有随后发给该组的消息：

1. 发件人使用解密私钥来取回组密钥。

2. 发件人使用GCM 模式使用组密钥加密纯文本消息，该模式允许在加密和解密期间进行消息认证。

3. 发件人用他/她的私人身份密钥加密的消息。

4. 发送方将加密的消息和签名发送给服务器端，服务器端向所有的组成员发出。

群聊消息也是在同一个XMPP 群聊频道上发生的群呼信令协议的基础。

云存储和文件共享

较大的文件和附件也是点对点加密的。

文件附件（文档，图像，视频等）是指收件箱附件和聊天文件传输，并采用完全相同的方式进行加密，每个文件的消息密钥使用CBC 模式。 然后使用具有SHA-256 的HMAC 算法和文件自己的消息密钥作为HMAC 功能的密钥来计算MAC 签名。

云存储文件以相同的方式加密，但是，为了能够处理大文件上传，文件被分块成较小的文件，并使用GCM 模式使用消息密钥进行加密。

还特别为此生成了两套RSA 密钥对云存储使用和文件和文件夹共享。

文件夹树结构保存在单独的JSON 文件夹结构中，其中包含ID 指针和AES 密钥到其子文件夹和文件。 这些JSON 结构使用GCM 模式使用消息密钥进行加密，并使用用户的私有身份密钥进行签名。 随机的AES 密钥以及唯一的ID 保存在父JSON 文件夹结构中，该结构也被加密和签名。

当用户与其他用户共享文件夹时，JSON 结构的消息密钥将使用每个用户的 Public Encryption Key 进行加密，然后使用共享用户的Private Identity Key 对加密的JSON 结构进行签名。

共享用户是共享文件夹的所有者，可以为每个文件夹成员定义读写权限。

电话和会议

音频/视频一对一通话，群组通话和屏幕共享也是端对端加密，并使用 WebRTC 技术进行实时音频和视频通信。

WebRTC 使用安全实时传输协议（DTLS-SRTP）来建立和加密媒体流。

在两个或多个用户之间建立点对点呼叫之前，一些信令被完成以交换某些信息并建立呼叫。

这个信令是通过现有的Chat / XMPP 通道完成的，并且如上所述，也使用与AES / RSA 的消息交换相同的加密方案进行端对端加密。

原生Android 和iOS 应用程序

Android 和iOS 应用包含与Web 客户端相同的收件箱，聊天，群聊和通话功能，并与系统紧密集成，并将接收各种事件（例如新收件箱，聊天消息和来电）的推送通知。

点对点加密的设计和开发使用与浏览器客户端相同的强大加密和算法。 对于iOS 和Android 应用程序，端到端加密层已经被开发成一个单一的跨平台库，使用最新的OpenSSL 发行版在C ++中编写，并在两个应用程序中使用。

网页数字货币API

网页浏览器实现最新的浏览器功能，并使用万维网联盟（W3C）定义的Web 标准Web 密码API（Web Crypto API），该标准允许在Javascript Web 客户端应用程序中进行加密操作。

使用网页数字货币 API 使得加密设计及其实现在执行各种加密操作时高度稳定且高效，因为它利用了浏览器自己的加密栈实现，并使得可靠的加密算法可用，与其他纯粹的Javascript 加密实现相比。

网络安全

跨站点脚本攻击（XSS）可能是Web 应用程序中最广泛传播的攻击类型，当将恶意脚本注入到网站以将攻击目标定位到最终用户时，就会发生这种攻击。

XSS 攻击的目标是在受感染站点的受害者浏览器中执行一些浏览器脚本，并从经过身份验证的用户窃取诸如会话cookie 之类的敏感信息，然后将其发送回攻击者的服务器。 然后，攻击者可以使用这个会话cookie 访问受害者在特定网站上的帐户。 这样的攻击可以在受害者不知情的情况下完成。

这种攻击已经在WhatsApp 等知名服务上进行过，攻击者可以完全窃听某个受害者的WhatsApp 账户，并能够控制受害者的账户。

通常，当用户输入未被正确过滤时，网站和Web 应用程序容易受到XSS 攻击。

FortKnoxster 实施了多种安全措施，确保我们的用户免受任何类型的XSS 攻击，确保用户输入内容（例如收件箱或聊天消息）在显示之前在接收者的浏览器中被转义和消毒。 此外，我们的Web 应用程序和服务器配置已经过优化，以设置**HTTPOnly** cookie 标志，**X-XSS-Protection** 和 **Content-Security-Policy** 响应头。

我们对**内容安全策略（CSP）**的研究已经导致了非常严格的CSP 配置，因为不允许任何外部源在FortKnoxster 环境中加载。

所有现代浏览器均支持CSP，并且在访问网站时，将允许使用的脚本，样式，媒体和其他资源列入白名单，以抵御XSS。

为了实现这种保护，CSP 配置需要在Web 服务器配置中完成，并且是一个特殊的响应头（Content

-安全策略），当请求页面时，从服务器发送回浏览器。

我们已经采取了这些额外的安全措施，通过仅将内部资源列入白名单，从而确保我们的CSP 配置尽可能的严格，从而在访问我们的网站和使用我们的服务时将客户浏览器中的任何外部资源加载列入黑名单， 我们用户的隐私。

跨站点请求伪造（CSRF / XSRF）是一种特殊的攻击方式，攻击者可以诱骗受害者执行不必要的行为，例如授权银行转账。

FortKnoxster 通过在每个HTTP 请求和一个特殊的XSRF cookie 中包含一个唯一的会话标记来防止CSRF 漏洞。

此外，FortKnoxster 会话cookie 使用AES-CBC 256 位和使用HMAC 功能的mac 进行加密，将服务器密钥作为输入。

网络钓鱼是一种社会工程攻击。 攻击者伪装成可信站点，欺骗受害者执行不必要的操作，如窃取登录凭据，信用卡详细信息和其他敏感数据。

FortKnoxster 实施了多种安全措施，以防止这种类型的攻击。

账户安全

为了保护用户免受任何帐户攻击，FortKnoxster 强制执行各种安全措施并提供以下帐户安全功能：

- 使用 TOTP，SMS 和 FIDO U2F 的双因素身份验证。
- Restrict account access by IP and country.限制IP 和国家的账户访问。
- 安全审计日志。
- Web 应用程序防火墙（WAF）过滤Web 请求。
- 当检测到暴力攻击或其他滥用行为时自动帐户阻止。

传输层安全

客户端（网络浏览器，Android 应用程序，iOS 应用程序）和服务器之间的所有通信都采用额外的单独严格加密通道进行分层。 只支持TLS 1.2，并且配置最强密码套件可用，包括DHE 的4096 位Diffie-Hellman 参数密码套件。

强大的TLS 配置可实现HTTP 严格传输安全性（HSTS），OCSP 装订，前向保密以及针对所有已知攻击（如Beast，Heartbleed，Poodle 等等）的防护。

算法概述

以下是FortKnoxster 端到端加密加密设计中使用的加密算法和加密操作的概述。

Algorithm	Encrypt	Decrypt	Sign	Verify	Derive	Digest	Wrap	Unwrap
RSASSA-PKCS1-v1			✓	✓				
RSA-OAEP	✓	✓						
ECDSA			✓	✓				
ECDH					✓			
AES-CBC	✓	✓						
AES-GCM	✓	✓					✓	✓
AES-KW							✓	✓
HMAC			✓	✓				
PBKDF2					✓			
BCRYPT					✓			
SHA-256						✓		

附录2：即将发布GDPR 法

下面是对即将到来的GDPR 法的简短描述。 FortKnoxster 是符合严格的GDPR 法则的一个好的和相关的工具，并且易于在任何规模和行业的组织中实施。

“一般数据保护条例”（GDPR）（欧盟法规 2016/679）是欧洲议会，欧盟理事会和欧盟委员会打算加强和统一欧盟内所有个人的数据保护的条例 （欧洲联盟）。

企业迫切需要使其运营符合新的数据保护制度。 这里是GDPR 最重要的部分。

什么时候

该法于2018 年5 月25 日生效，之后将对不合规的实体开始执行。 在此之前，现行的国家数据保护法适用，包括国家安全法，就业法和言论自由。

谁

新的“欧洲数据保护条例”适用于任何业务，不论其业务活动或经济部门如何：

在欧盟建立业务或受欧盟法律约束。

在欧盟之外建立业务，但是a）向欧盟提供服务或货物居民；b）监测欧盟居民的行为。

例如，追踪其欧洲用户的“Runkeeper 应用程序”即使是在欧盟没有办公室的北美公司，也是有责任的。

“欧洲数据保护条例”引入了负责任企业的重大扩张，现在适用于处理欧洲居民私人数据的非欧洲实体。

这也意味着Google，Facebook，雅虎和微软等科技巨头将不得不遵守。 否则，其影响包括巨额罚款。

罚款

违反欧盟数据保护条例将导致罚款。 单次违约的最高罚款为2000 万欧元，即全球年营业额的4%，以较高者为准。 这个数字是故意设置的高，以吸引高管们关注数据保护和遵守新法规的问题。

加密是解决方案

GDPR 法规为什么样的安全提供了具体的建议行动可能被认为是“适当的风险”，包括：

个人资料的加密。

能够确保处理个人数据的系统和服务的机密性，完整性，可用性和灵活性。

在发生物理或技术事件时及时恢复数据的可用性和访问能力。

定期测试，评估和评估技术和组织措施的有效性以确保加工安全的过程。

“欧洲数据保护条例”主要给最终用户带来好消息，但这并不是坏消息，更多的工作和更大的开支。 在规定中有一个特别有价值的部分规定，公司应该满足用户对数据隐私的“合理期望”。这个规则表明加密，匿名和授权令牌满足了这些期望。 如果贵公司在休息和运输过程中对公司数据和用户数据进行加密，那么在与第三方承包商打交道时，也要将公司密钥放在安全且加密的地方，这样就能够有效证明您符合“个人隐私的合理期望”。

附录3： 服务条款

服务条款

生效日期：2017 年8 月1 日

这些服务条款（以下简称“条款”）涵盖您使用和访问由FortKnoxster Ltd. 提供的名为“FortKnoxster”（“服务”）的服务。通过使用我们的服务，您同意受这些条款的约束 还请查看我们的隐私政策。 如果您将我们的服务用于组织或其他法律实体，则代表该组织同意这些条款。 FortKnoxster Ltd. 保留随时更改本协议的权利。

FortKnoxster 服务

FortKnoxster 服务提供的系统允许用户访问我们的FortKnoxster 安全通信平台。 为了获得服务，您需要创建一个包含电子邮件地址和密码的帐户。

访问

为了访问您的帐户，您必须首先使用您的FortKnoxster 用户名和密码登录，然后通过验证过程。 在此之后，您可以使用该服务。使用本服务需要您访问互联网。您可以从计算机或移动设备进行访问。

帐户安全

通过完成本服务的注册，即表示您同意遵守这些条款和条件以及FortKnoxster 的隐私政策，您保证您至少年满18 周岁，或者您已经获得同意向父母开立和维护一个帐户。 您同意维护您的密码和身份证明的安全，您将完全负责FortKnoxster 服务的所有使用。您应立即通知FortKnoxster 有限公司任何未经授权使用您的密码或帐户，任何丢失或盗用您的密码或任何其他违反安全的行为。

允许使用

您可以根据这些条款和条件访问和使用服务，并遵守网站上出现的任何操作规则/合同或公布的政策。 任何使用本服务的风险和责任由您自行承担。

没有非法使用

您声明并保证，作为使用本服务的一个条件，您不会将本服务用于任何非法，非法或禁止的目的。 您不得使TEP 系统遭受任何垃圾邮件，拒绝服务攻击，病毒或任何干扰系统正常运行的行为，活动或代码。

赔款

您同意捍卫并保护FortKnoxster 有限公司及其附属公司和联营公司及其董事，高级职员，代理人，承包商，股东，合伙人和雇员免受任何诉讼，索赔，要求或责任的伤害， 您违反本协议的任何条款和条件，任何第三方的权利或您对本服务的使用或连接。 本服务按“原样”提供，您同意不承担由于与本服务的性能有关的使用，数据，信息或利润的损失而导致的任何损害。 此外，如果由于安全故障，脆弱性或不可抗力而无意发布任何材料，您将不会承担FortKnoxster 有限公司的责任。

密码

由于我们无法访问您的帐户或数据，因此我们不会保留您的密码记录。 如果您忘记密码，除了为您提供新帐户之外，我们无法为您提供帮助。

付费帐户

开票。 我们将自动激活用户帐户的日期和每次定期更新直到取消为止。 您需要负责所有适用的税收，并且我们会在需要时收取税款和增值税。

不能退款。 任何时候您都可以取消您的FortKnoxster 升级账户时间，但是你不会得到退款。

降级。 根据这些条款，您的升级账户将一直有效，直至被取消或终止。 如果您没有按时支付升级帐户，我们保留暂停或将您的帐户降至免费帐户的权利。

变化。 我们可能会更改有效的费用，但会通过与您的帐户关联的电子邮件地址的消息提前通知这些更改。

知识产权

FortKnoxster Ltd. 对本服务中的所有版权，商标，商业机密，专利或任何其他知识产权拥有所有权利，所有权和利益，并且这些权利的名称和利益受到 根据瑞士和国际法律最充分的程度。 未经FortKnoxster 有限公司事先书面同意，您不得使用或允许任何第三方使用任何商标或商品名称，本服务中的任何内容不得以任何形式或以任何方式复制，复制或复制。

整个协议

这些条款和条件规定了有关本标的整个协议，并取代您和FortKnoxster 公司之间所有以前或同期的通信和建议，无论是电子的，口头的还是书面的。

放弃

如果FortKnoxster 有限公司没有行使或执行这些条款和条件的任何权利或条款，则不构成对该权利或条款的放弃。

适用法律

本协议受直布罗陀法律的管辖和解释。 依照此处开始的所有行动应送交直布罗陀法院。

变化

如果FortKnoxster 有限公司涉及未来的兼并，收购，重组或出售我们的资产，则您的信息可能会作为其中的一部分转移。 我们会通知您（例如，通过与您的账户相关的电子邮件地址的消息）任何此类交易和大纲的详细信息。

影响

本协议自您完成FortKnoxster 有限公司注册或首次付款之日起生效，FortKnoxster Ltd. 可随时终止本服务。 使用本服务即表示您同意本协议的条款。

客户支持

我们将在一个工作日内通过电子邮件回复支持请求。 如果您对我们的服务有任何问题，想法或疑虑，请与我们联系 info@FortKnoxster.com.

附录4：隐私政策

2017 年8 月1 日生效

隐私是我们的业务

FortKnoxster 有限公司尊重并尊重所有用户的隐私和匿名性，并坚定地致力于根据本隐私政策保护任何信息的机密安全性和完整性。

本隐私政策解释了FortKnoxster 有限公司处理您的信息。

保护您的信息

通常。 您的信息的安全对我们来说是必不可少的，实际上这是我们或商业模式的核心，保护我们用户及其数据的隐私。 在技术和法律的范围内，我们将不断创新，不断推陈出新，保持最佳的私密和安全的沟通平台。

技术上。 我们使用物理，电子和复杂的安全方法来防止未经授权的访问，维护数据隐私并确保正确保护信息。 我们使用强大的加密技术，包括AES 256，RSA 2048，密钥认证算法，安全套接字层（SSL）等。我们的整个用户数据以加密形式存储，甚至FortKnoxster Ltd. 员工也无法访问。 另外，用户帐户受多因素身份验证（可选）的保护。

我们的服务器托管在瑞士高度安全的数据中心。 此外，我们的安全套接字层（SSL）也是瑞士的起源，因此受到严格的瑞士隐私法律的保护，这意味着FortKnoxster 有限公司不能被迫对隐私进行任何合法的拦截或其他攻击。 同样，即使数据被泄露，由于所有数据都是高度加密的，所以这是没有用的。 我们也参考下面的不披露部分。

数据采集

FortKnoxster 有限公司收集和使用匿名用户信息用于以下有限的目的:

1. 发送和接收的消息：我们无法访问任何消息内容，因为它是高度加密的。我们可以访问以下记录：发送的消息数量，使用的存储空间，消息总数，上次登录时间和国家代码登录。
2. 电子邮件：在帐户创建过程中提供给我们的所有电子邮件，是机密信息，您的电子邮件永远不会被出售，分享，给予，租赁或披露给任何第三方。 由于额外的安全问题，您的电子邮件需要向您发送帐户创建过程中的初始链接。

管理你的数据

您的数据属于您，您可以随时将其删除。 您的帐户信息可以随时通过登录到您的帐户，并更改或删除信息进行更改。 如果您想要删除您的帐户，我们将从我们的服务器中清除您所有剩余的加密帐户数据。 任何超过12 个月的闲置帐户可能会被自动删除。

数据存储

所有数据在任何给定时间以加密格式存储。 临时备份也完全加密。 我们无法访问您的加密数据，因此无法恢复您的密码，如果您丢失了密码。

非公开

FortKnoxster Ltd. 拥有零披露政策。 对于有关用户，日志，数据或类似信息的任何请求，我们将不予回复。 任何当局都必须向有关当局提出要求，然后可能会按照有关法律规定的协议与我们联系。 我们不会比任何法律要求更高的要求。

支付

这仅适用于使用我们的“升级”服务的用户。 第三方处理所有电子支付交易，FortKnoxster Ltd. 不保留任何客户支付信息。 为了管理目的，我们确实需要存储关于哪个帐户由特定交易支付的数据。

客户支持

我们将在一个工作日内通过电子邮件回复支持请求。 如果您对我们的服务有任何问题，意见或评论，请与我们联系 info@FortKnoxster.com.

谢谢你的兴趣

更多资料请前往:

www.fortknoxster.com

或者发邮件到

tokensale@fortknoxster.com

FORT

KNOXSTER