2024

MYSTSAFE

KEEP YOUR SECRETS PRIVATE

mystsafe.com

Problem

No tools exist that allow users to store and transfer their personal and business secrets privately, anonymously, with crypto-grade security and undeniable accessibility.

Traditional password managers and secret vaults require users to disclose their personally identifiable information. User identity, secrets, and activity history can be stolen by hackers or subpoenaed by governments. Access can be denied or blocked by corporations.

To protect their identity, data, and activities, users must maintain multiple accounts and use fake names, disposable email addresses, burner phones, VoIP numbers, VPN services, or hardware devices which come with an extra cost and inconvenience.

Solution

We offer an app with zero identification and zero activity tracking where users can manage their personal, family, and business secrets in a single account:

- **Password manager** (a primary feature) to store any personal and business secrets such as crypto wallets, website passwords, credit card numbers, or database credentials.
- **Private chat** (a bonus feature) to transfer the secrets privately to other users and send confidential messages.
- **Secret vault** (a business feature) to configure any app to access secrets without encryption keys or additional software, from any cloud or on-prem location.

Product

MystSafe app stands out in the crowded field of digital security with its unique blend of standard features and innovative differentiators.

Key Differentiators

These are not found in traditional solutions and therefore are unique and exclusive to MystSafe users:

- **Anonymous Profiles**: Account registration does not require providing any personal data such as name, phone number, email, or address. Payments for premium plans are decoupled from the user accounts so there is no link between user identity and account activities.
- **Unbreakable Database**: While traditional password managers rely on a cryptographically weak "master" password, MystSafe adopts a cryptocurrency-inspired approach.
  It utilizes a blockchain-like *permissionless database* where secrets and messages are encrypted end-to-end using a 12-word security phrase, which ensures that even if the database is compromised, the data remains secure against unauthorized access.
- **Untraceable Activities**: MystSafe employs technology found in privacy-preserving cryptocurrencies that hides the owner of the secret records as well as the sender and the recipient of the chat messages.
- **Undeniable Service**: MystSafe's design ensures that no corporation or government can block accounts or restrict user services, providing continuous access to essential data such as cryptocurrency wallet secret phrases. This feature guarantees that users can always access and manage their funds, reinforcing their autonomy and financial freedom.
- **Inclusive Access**: MystSafe offers unrestricted and equal access to all, ensuring no discrimination based on location, nationality, or financial history. This commitment allows anyone to use the app, with premium features payable via cryptocurrency for those without traditional banking means.
- **Built-in Chat**: MystSafe enables users to share secrets directly from the secret screen and send instant direct messages securely and discreetly through its integrated chat interface.
- **Offline Mode**: MystSafe stores secret and chat data locally on the user’s device and syncs with the network only when updates are made, enabling read-only access without internet communication and thereby reducing the online footprint.
- **TOR Support**: The MystSafe app can work through the TOR network which enables an extra layer of security and privacy protection while eliminating the need for a paid VPN service.
- **Unlimited Accounts**: MystSafe users can open as many accounts as they want, for free, which allows them to differentiate their interactions with users from different groups and separate public and private affairs.
- **Open Source**: MystSafe source code is open for anyone to examine the cutting-edge algorithms used to protect user privacy and security.

Standard Features

These are the standard features found in traditional solutions, but also very important:

- **Unlimited Devices**: The users can sync their data between multiple devices, with any hardware platform or operating system, while preserving the security of their data and the privacy of their actions.
- **End-to-end Encryption**: All data (no exceptions) is encrypted/decrypted by default end-to-end within user devices.
- **Fingerprint and Face ID**: Instead of using passwords to protect the app on a user device, MystSafe uses a passkey authentication that supports biometric, passwordless access.

Market

In today's digital landscape, the growing concern for privacy and security is evident from the increasing number of individuals adopting tools designed to protect their personal information. These trends not only validate the market for privacy-centric products but also highlight the vast potential for new entrants in this field.

12M

users of Threema, a **paid** privacy-focused messenger

33M

people used LastPass password manager before they disclosed the security breach

40M

users of Signal, a privacy focused messenging app

90M

users **pay** for password management tools

113M

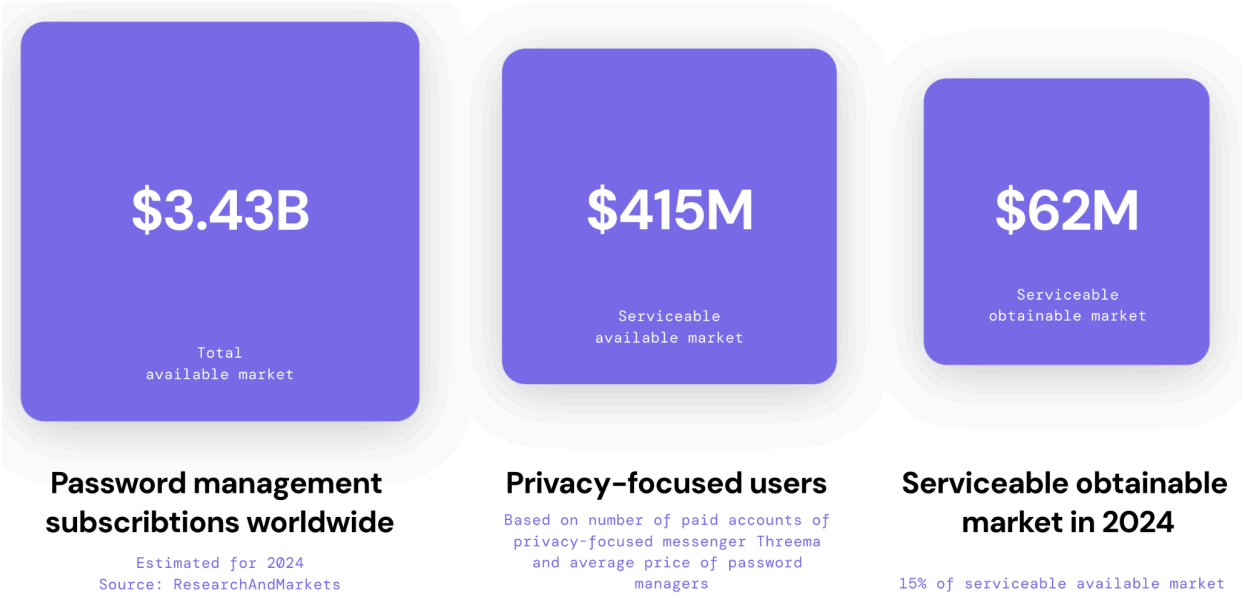
Americans use password management tools

420M

people worldwide use cryptocurrencies and are familiar with services that do not require identity and do not track activities

Market Size

The following visualization reflects a significant opportunity for MystSafe within the privacy-focused digital tools sector. The figures underscore the increasing demand and potential revenue, positioning the product as a strong contender in the industry.



Password management subscribtions worldwide

Estimated for 2024
Source: ResearchAndMarkets

Privacy-focused users

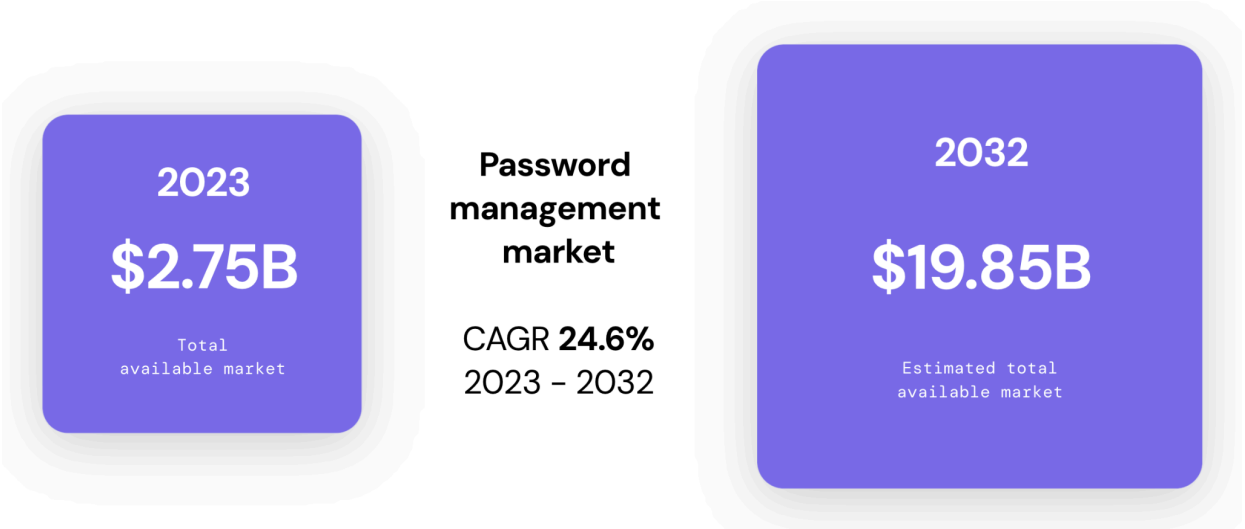
Based on number of paid accounts of privacy-focused messenger Threema and average price of password managers

Serviceable obtainable market in 2024

15% of serviceable available market

Market Growth

The password management market is demonstrating a robust growth trajectory, as evidenced by the compelling projections detailed in the following graph. This growth underscores the increasing value and necessity of password management solutions in safeguarding digital identities across diverse sectors, reflecting an escalating demand that MystSafe product is well-positioned to meet.



Total available market in 2023

Source: ResearchAndMarkets

Estimated total available market in 2032

Source: ResearchAndMarkets

Business Model

MystSafe is offered as a service via an app that is downloaded to the user's device and runs locally in a browser. There are both free and premium plans available.

Free Plan

The free plan serves as a trial that does not require payment or money-back concerns. However, unlike most solutions, MystSafe's free plan can be used indefinitely beyond the trial period. This is enabled through a blockchain-like architecture where data records and their modifications are represented by individual blocks with timestamps. Once the trial period expires, the network deletes the expired blocks, effectively freeing up the resources.

Users can still add new secrets and start new chats, which remain valid for another trial period. Additionally, editing an existing record effectively resets its expiration date, allowing users to perpetually refresh their data.

Premium Plan

The premium plan allows users to maintain their records indefinitely by attaching a license proof block to every data block. MystSafe will roll out different types of licenses for premium plans in phases:

Premium License

The license will be purchasable via the MystSafe license portal (https://checkout.mystsafe.com) for one, two, or three years. Users receive *Reward points* with every premium plan purchase, which are non-expiring even after the license itself expires.

Go to Market Schedule

The project is structured into several phases:

First Phase: Initial Design and Building MVP

This phase introduced the fully functional MystSafe beta app available at https://app.mystsafe.com.

Current Phase: Enhancement and Crypto Licensing

Currently underway, this phase includes the addition of various new product features and the implementation of the crypto licensing model.

Next Phases: Expansion and Rewards

Future features such as group chats and a business-oriented secret vault will be added. Users will have the option to trade their licenses for reward tokens and vice versa.

Technology

The MystSafe system, designed to ensure robust privacy and security, consists of three primary components: the App, Relay Node, and Database. The App operates as a client application executed solely in a user's browser across various devices, ensuring that all private keys remain confined to the client device. On top of default end-to-end data encryption, the communication between the App and Relay Nodes is secured with TLS encryption, and can be supplemented by optional VPN or/and *TOR* use for added anonymity.

The Database itself is a *permissionless*, noSQL, *directed acyclic graph* that stores encrypted user secrets and messages, accessible through Relay Nodes that facilitate outdated records deletion using specialized *garbage collection* protocols. Data within the database is structured in interconnected *blocks* and *blockchains*, masking any direct associations between users and their data.

Stealth addresses and end-to-end encryption obscure sender and recipient identities, ensuring only the intended parties can access the secret records and message content. Additional security measures include double digital signatures and optional *ring signatures* and *key images* for transactions, particularly when using non-private payment methods, to maintain payment anonymity and disconnect user identity from payment

details. The system also employs *proof of work* (PoW) to safeguard against potential DDOS attacks.

These components collectively establish a secure and private secret management and communication platform, analogous to a container ship that carries data containers without knowledge of their origins, contents, or destinations.

Conclusion

MystSafe is dedicated to redefining privacy and security in the digital age, leveraging blockchain technology to deliver a robust, user-centric service that respects and protects individual anonymity. By continually evolving and expanding its offerings, MystSafe is poised to set new standards in secure digital communication and data storage.

Additional Information

Website: https://mystsafe.com

App: https://app.mystsafe.com

Product details and manuals: https://docs.mystsafe.com

Pitch Deck: https://www.mystsafe.com/_files/ugd/d224ea_13af2893e620411d86d10fec514bd661.pdf

Technical details: https://docs.mystsafe.com/cryptachat/technical-reference

License portal: https://checkout.mystsafe.com