

KeepYouSafe.Com Technical Overview - White Paper

At Information Survival, LLC we believe in transparency when it comes to Security. We believe that our customers have a right to know how their important data is being protected. This document is a technical overview relating to the security and survivability of KeepYouSafe.Com's Online Safe Deposit Box™ service. It is intended for a more technical audience.

For a more general description of the service please visit <http://www.KeepYouSafe.com>

Passwords & Login

When you sign up, you create a password. We have a "Password Strength" feature to help people select a strong password that is difficult to guess or crack by including a variety of types of characters (upper case, lower case, numbers and special characters such !@#\$%^&*). Having multiple classes of characters and longer passwords drastically increases the strength of the password, making it much more difficult to guess or crack using software tools.

Box-holders have the option of using single-factor authentication (User ID & password pair) as well as two factor authentication (User ID & password pair PLUS a Security Token[1]). While using a strong password offers a high level of protection, we recommend using the Security Token to minimize the risk that a lost or guessed password will expose your data.

The Security Token features a changing six digit number that you enter in addition to your valid User ID and Password. Thus, the "two factors" that you must have to log in are something you KNOW (your password) and something you HAVE (the token, with whatever six digit number is displayed at login time). Without both pieces, access is denied. If someone watches you type in your password and the security token code, and walks back to their computer to re-enter that information they will be denied access – the code displayed on your token is only valid ONCE, and changes every sixty seconds for extra security.

In addition, multiple systems monitor login attempts in real-time. These monitoring systems will temporarily or permanently lock out an account and notify our Security Team if the monitoring system believes that attempts to log in seem to be fraudulent in nature. These could take the form of multiple failed logins, password guessing attempts and geo-correlation of logins across multiple accounts.

Data Encryption

We use the Secure Hash Algorithm 512 bit (SHA-512) to calculate a mathematical representation of your password called a "hash" so that when you log in we can verify you. This hash, and NOT your password is stored in our secure database. We do not store a copy of your password. When you log in,

KeepYouSafe.Com Technical Overview - White Paper

we use SHA-512 to hash the password you submit, and look to see if it matches the hash that we have on file for your User ID.

The hash cannot be used to decrypt your data, nor can the hash be easily "reversed" to help guess your password. For example, if your password was "@K33pY0uSaf3!" the SHA-512 hash would be:

```
1039f68dba557bcbbfe2f29ddb649d32e2cf061ff234a13c038ecf0051f6966de213
66c64a86bfab9ac4bf7528b855634bce8ed47353c5b12574a23d7b40a35.
```

The US Government has approved SHA-512 for all applications using Secure Hash Algorithms[2].

Once you successfully log in, your password is associated with your session in secure memory. We use that password as the "key" for 256 bit Advanced Encrypted Standard (AES) encryption to both encrypt new data and decrypt existing data that you wish to view or download. Your password is "shredded" from this secure memory area when you log out or when your session expires due to inactivity, currently set to 10 minutes.

We also use AES to encrypt the sensitive personal data we store about you, including your address and billing information such as your credit card number.

The AES key for that encrypted customer data is stored in an bytecode-level encrypted file on the server to further protect it.

256 bit AES is so strong that the US Government has approved it to protect top secret classified data.[3]

Security of Data In-Transport

Between the browser and our servers, we use industry standard SSL encryption from 128 bit up to 256 bits if your browser supports it. SSL is required to log in and access your box. This is the same SSL that your bank, online shopping sites, brokers and other large companies use to protect your data.

Between our servers and for maintenance, everything is done via SSL or Secure Shell (SSH) version 2. Customer data is never transmitted or stored "in the clear".

Network-Level Protection

We utilize both hardware (network based) and software (server based) firewalls, access rules and intrusion detection systems to protect our systems and your data. Our security systems are designed, monitored and maintained by Certified Information Systems Security Professionals (CISSP's).

KeepYouSafe.Com Technical Overview - White Paper

System Administration & Patching

There are trained system administrators available 24x7x365 to address any immediate issues, and to respond to real-time notifications by our systems. We maintain clusters of machines in multiple cities across the world, and each system undergoes a vigorous lock-down procedure before they are placed on our network. In addition, regular patching and maintenance are performed to ensure every server and storage system maintains the highest levels of security and reliability.

Data Backups

First, we maintain a live "always on and ready" backup site in Europe (with a third backup site in the Southern Hemisphere in the works). As our global backup management system notices the contents of your encrypted box changing, your box is scheduled for a backup to the alternate site(s). This happens throughout the day, 7 days a week, 365 days per year. This way you can be sure, that if anything happens to our primary secure site, there are systems with your current data, secure and ready to serve you. No human intervention is required for our Europe backup systems to "take over" in the event that our US systems are unavailable or destroyed. In addition, daily and weekly onsite and offsite tape backups are performed.

Audit & Security Testing

We take audit and testing very seriously, and have split this important function into three segments:

1) Self assessment and continuous improvement. Our founders are both CISSPs. We have another CISSP Bank Technology Auditor on staff that spent the last 15 years testing and evaluating the security and controls at some of the largest banks in the world. We monitor public, private and government security alerts to ensure we manage new security threats before these threats have a chance to affect us. We regularly assess the security of our systems using manual and automated methods. Any relevant issues are promptly remediated. We are working hard towards ISO27001 certification.

2) We have put together a "Security Advisory Board" including current and past members of the Local and Federal Law Enforcement community, Computer Security Experts, and Technical Professionals to regularly review our ideas, designs, code, systems, network and databases to help ensure maximum security and privacy for our customers.

3) Finally, we have contracted with ScanAlert to perform a full external penetration test on our service EVERY DAY. We are proud to say that we have earned their "Hacker Safe" certification.

KeepYouSafe.Com Technical Overview - White Paper

More Information

If you have a technical question about our service that was not answered here, please e-mail support@keepyousafe.com.

References

[1] http://en.wikipedia.org/wiki/Security_token

[2] "The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms." <http://csrc.nist.gov/CryptoToolkit/tkhash.html>

[3] "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use." http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf