IDENATI

Security Guide

At Idenati, security is our #1 priority, and it's important to us that you understand how the app works. Please take a few minutes to review this security document and learn how your information is kept secure and private using military-grade encryption.

The Master Password.

When you create an Idenati account, you will also create a new Master Password. Think of your Master Password as the key that unlocks all your other passwords. And what's great about Idenati is that we never store your Master Password on our servers, or in our database. In other words:

Your Master Password never leaves your computer or your phone.

This will be the last password you have to remember, so make it a good one!

Protecting Your Passwords.

After you've created an Idenati account, you will have the ability to save all your passwords inside the app. Each time you do this, the app will immediately lock and hide the password using your Master Password as the key; this process is known as encryption. In simple terms, the encryption process scrambles your password in a way that can only be undone using your Master Password.

Idenati uses military-grade encryption and decryption algorithms that ensure you are the only one who can view your passwords.

In fact, other sensitive items like your usernames or notes are encrypted as well.

You can also let Idenati generate a secure password for you. When you select this option, a new and unique password will be created for the website you choose. The app will then display this password so that you can set or change the password on the intended website. There are a couple advantages for letting Idenati create a secure password for you. This type of password:

- will be completely new and randomly generated.
- will be unique to you and the website.
- will NOT be stored anywhere, even in its encrypted form. It's like magic!

Using Your Passwords.

When you need to access your passwords again in the future, just sign in to Idenati (at idenati.com) with your email address and Master Password.

This process will temporarily unlock (or decrypt) your password information.

This is the exact opposite of the encryption process, and the final step in keeping your information safe.

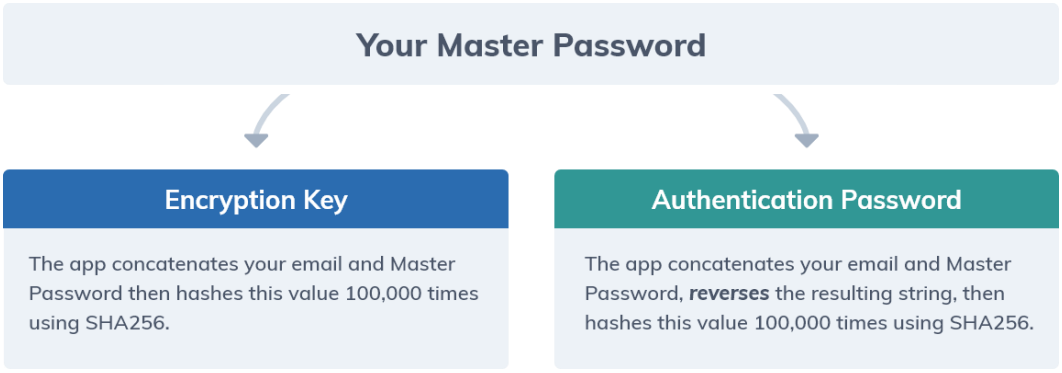
Idenati's Encryption Process.

Idenati's encryption process is designed to hide your passwords from everyone (including Idenati employees) except you. An example of encryption might be:

- Encrypt **abc** with **password-key** to get **KVdHpjkAmFrTQ**
- Decrypt **KVdHpjkAmFrTQ** with **password-key** to get **abc**.

The random string KVdHpjkAmFrTQ has no meaning to anyone, nor does it say anything about abc. Thus, the information is kept secure. The following sections explain Idenati's use of standard encryption functions, specifically the Advanced Encryption Standard (AES) and the Secure Hash Algorithms (SHA). Both functions are approved by the US National Security Agency (NSA) for Top Secret use.

Perhaps the most critical piece of keeping your information safe is the Encryption Key. It was noted previously that your Master Password is the Encryption Key, however it is technically a cryptographic derivative of your Master Password. This considerably strengthens the security of your information. Furthermore, the password that is used to authenticate and retrieve your data from our servers is also a cryptographic derivative, although an entirely different one.



Upon signing in, the Authentication Password is securely transmitted to Idenati's servers to retrieve your data, and the Encryption Key is kept locally on your device (never transmitted) for encryption and decryption operations using AES256.

Cryptographic Password Management.

The Idenati app uses your Encryption Key from the previous section to encrypt your account data (passwords, usernames, etc.) before sending it to our servers for secure storage. When you sign back in, the app decrypts your account data, but keeps any custom passwords in their encrypted form, until you ask to retrieve them.

Regarding auto-generated passwords, Idenati has invented a unique mix of cryptographic functions that allows the app to create strong passwords without storing them. To accomplish this, the app compiles a unique "Password Recipe" for you behind the scenes, using your Encryption Key (this time the resulting hash is converted to number format) and a third cryptographic key called the Offset (also in number format). The Offset is randomly generated during account creation and securely stored on our servers. The Password Recipe is defined as:

```
"domain.version."+(EncryptionKey+Offset)
domain.version.856702100443002523189910591442690028727876356427827 92...
```

To retrieve an auto-generated password, Idenati replaces "domain" and "version" with the target website's corresponding values, and then hashes the Password Recipe using SHA256 in hexadecimal form. The app adds "aA@0" to the beginning of these passwords, replacing "@" with any special character that you define. It then truncates the entire passwords to the desired length.

```
"aA"+specialChar+"0"+sha256(passwordRecipe).substring(0,passwordLength)
aA@0a45c92bd786acd7f3ee048ef01
```

This operation takes places locally, once all three keys have been activated: Authentication Password, Encryption Key, and Offset.

In the event of a Master Password change, you have the option to recalculate the Offset so that your current Idenati generated passwords stay intact and do not change (otherwise they will change as result of a new Encryption Key and Password Recipe).

Additional Features & Final Notes.

You have the option to setup Multi-Factor Authentication (MFA) for your Idenati account, and this will require a second secure code from an authenticator app (e.g. Google Authenticator, Authy) when signing in.

You also can add a Secret Phrase (e.g. PIN) to your Password Recipe, through the "App Settings" panel. If active, the app will hash your Secret Phrase using SHA256 (output in integer format) and add this to Encryption Key and Offset.

There is an alternative configuration that allows you to use a Custom Recipe (this setting is off by default). If activated, you will override the previously defined Password Recipe with your own Custom Recipe upon starting the Idenati app, and this Custom Recipe is never transmitted to our servers or database.

The Idenati application is hosted on Amazon Web Services (AWS) in the United States, noting that we use Heroku and MongoDB services for application and database management. The following links will direct you to the security documentation for these products: AWS, Heroku and MongoDB. We are in the process of obtaining a certified third-party security and compliance audit for Idenati and will update this document once completed. Idenati holds technology and cyber liability business insurance.

As a final note on the Secure Hash Algorithms (SHA): these algorithms receive an input and produce a unique scrambled output that is collision resistant (i.e. two different input values will not result in the same output). The SHA functions are also considered one-way; they are practically impossible to reverse engineer.

info@idenati.com