

HIDEEZ

Hideez Key



USER MANUAL

Version 1.1

Firmware 1.2.0
Hideez Safe for Windows 1.3.15
Hideez Safe for Android 0.8.30

© Hideez Technology, 2016

The Context

Common information	3
Safety measures.....	4
Technical details.....	4
Requirements	5
Warranty	5
Compliance.....	5
What is Hideez Key	5
Principles of operation	6
Getting started	7
Device layout	7
Hideez Safe software installation.....	8
Cancellation of use and private data erasing from Hideez Key ...	9
Firmware update.....	9
Working with Hideez Key	10
Protecting of PC, tablet or smartphone.....	13
Several users on the same PC	15
Password manager.....	15
Android version of password manager	16
Windows version of password manager	18
One-time passwords (OTP) and two-factor authentication	22
Backup	23
Hideez Safe for Android enhanced mode	25
Touch guard	25
Remote control (selfie, voice recorder, etc.)	26
Panic button.....	27
Alarm clock.....	28
Troubleshooting	29
Annex 1. Hideez Key signals and states.....	30
Annex 2. Frequently asked questions and answers.....	31

Common information

Disclaimer of Warranties; Exclusion of Liability

Except as set forth in the express warranty contained on the warranty page enclosed with the product, the purchaser takes the product "as is", and Hideez Inc. makes no express or implied warranty of any kind whatsoever with respect to the product, including but not limited to the merchantability of the product or its fitness for any particular purpose or use; the design, condition or quality of the product; the performance of the product; the workmanship of the product or the components contained therein; or compliance of the product with the requirements of any law, rule, specification or contract pertaining thereto. Nothing contained in the instruction manual shall be construed to create an express or implied warranty of any kind whatsoever with respect to the product. In addition, Hideez Inc. shall not be liable for any damages of any kind resulting from the purchase or use of the product or arising from the breach of the express warranty, including incidental, special or consequential damages, or loss of anticipated profits or benefits.

Modification of Software

Hideez Inc. is not liable for performance issues or incompatibilities caused by your editing of registry settings, or your modification of operating system software.

Using custom operating system software may cause your device and applications to work improperly. Your carrier may not permit users to download certain software, such as custom OS.

Trademarks

© Hideez Technology LTD., Belize, internet Address: www.hideez.com

©2015 Hideez, Hideez Key are all trademarks of Hideez Technology. Bluetooth is a registered trademark of Bluetooth SIG. Microsoft® Windows™ is registered trademark of Microsoft Corporation. Google, Android, YouTube are trademarks of Google, Inc. Other companies and product names mentioned herein may be trademarks of their respective owners. Screen images simulated. Appearance of device may vary.

Legal information

The online version of the User manual guide for your device can be found at: www.hideez.com/download

The online version of the End User Licensing Agreement for your device can be found at: www.hideez.com/Legal.

Safety measures

The device is NOT water and dust resistant and may be damaged if exposed.

The next tips are given to maintain long term operation and prevent the malfunction:

- Do not immerse the device in water.
- If the device become wet occasionally, please open the case, pull out the battery and dry them thoroughly by hair dryer.
- Do not expose the device to extremely high or low temperatures.
- Note: the operating temperature ranges from -10 ° C to 40 ° C.
- Protect it from direct sunlight for a long time to prevent plastic parts from wearing out.
- Do not expose the device to open fire.
- Do not apply extensive force when pressing the button.
- Do not expose the device to strong electromagnetic fields.
- Keep the device away from children under 3 years.

The device does not contain harmful substances, and can be disposed of as household waste. The battery should be disposed of separately according to the local rules.

The device radio module operates in 2.4GHz band according to Bluetooth 4.0 specification. It does not require be turned off in an aircraft, according to FAA press-release from 10.31.2013.

If you use personal medical devices (e.g. pacemakers and hearing aids), consult with your doctor or the manufacturer about compatibility.

Technical details

CPU	Nordic NRF51 based
Radio	Bluetooth 4.0 LE
Battery:	1xCR2032
Battery life-cycle:	up to 6 month
Dimensions:	31x31x7,5 mm
Weight:	8 gr.
Operation temperature:	-10 °C - +40°C
Buttons quantity:	1
LEDs quantity:	2 (Red & Green)
Sound:	loud buzzer

Requirements

Hideez Key is designed for work with devices that comply with

- Bluetooth adapter ver. 4.0 Low Energy
- OS Microsoft® Windows™ 8.1, Microsoft® Windows™ 10, Android 4.3 and above, MacOS X.

Warranty

Unless otherwise stated in the warranty card, warranty period is 12 months.

Compliance

FCC compliance statement

The device fits requirements of part 15 of FCC rules.

This device may not cause adverse effects.

This device may accept any interference signals, including signals that could cause it to malfunction.

The equipment complies with FCC RF exposure guidelines in an uncontrolled environment. The transmitter must not be co-located with any other antenna or transmitter, and should not take them signals.

What is Hideez Key

Electronic key (another term is "label") Hideez Key is designed for user identification working with PC, tablets, smartphones; storing personal digital keys and passwords, data encryption and digital signing.

Hideez Key functionality allows:

- To lock/unlock PC, a tablet, smartphone.
- To keep user passwords for applications and web-services and enter it with the Hideez Key button (Hideez Safe software must be installed). To make one-time passwords for services with two-factor authentication like Google Mail.
- To keep private key for data encryption.
- To provide data encryption and digital signage
- To serve as a backup information store for another Hideez Key device.
- To prevent the loss of personal belongings, controlling their presence.

- To serve as a remote control for smartphone, e.g. taking photo (selfie).
- To serve as "panic button", sending geodata and an urgent message to the predefined phone number.
- To run a preliminary programmed action sequences (scripts) by pushing Hideez Key button.
- To specify a place on a Google map where connection with Hideez Key was lost (Last seen place).
- To solve similar tasks.

Principles of operation

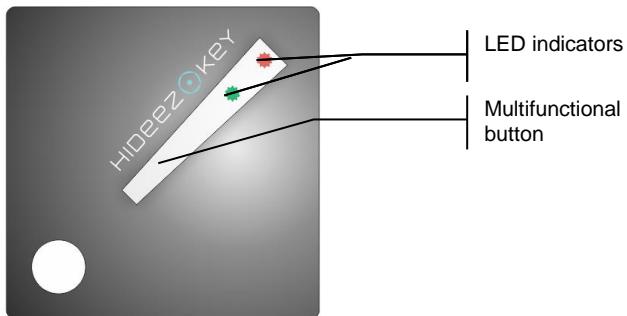
Electronic device Hideez Key interacts with the similar devices, tablets, PCs, via RF signals according Bluetooth 4.0 Low Energy specification. This connection can be established on the distance up to 100 meters (open space) or up to 25 meter indoors. In fact, RF signal strength level depends on: the distance, surrounding objects, obstacles on the signal way, including human bodies. All of these impacts on the range of communication between the Tag and host device.

The device can measure received signal strength (RSSI) and in this way estimate the distance between connected devices. This ability is a basic for considerable part of guard and signaling functionality.

Note: For normal operation of Bluetooth it may be need to disable some of smartphone/tablet power saving features.

Getting started

Device layout



Hideez Key is made as a key fob with one multifunctional button. Two LED indicators (green and red) are situated under this button/

There is a buzzer inside the Hideez Key case.

Set up a battery

Open Hideez Key case and insert CR2032 battery with "+" side up, "-" side down to the board. Hideez Key will give a beep after some seconds.

Hideez Key initialization and connecting

In a normal life Hideez Key interacts with paired devices only and is hidden for any another. Connecting to other devices, Hideez Key stores connection context (bonding data) and put in a "device whitelist". Whitelist size is limited to eight devices (firmware 1.1.59). When nine devices coming, the oldest device is deleted.

After power is on (the battery is inserted) Hideez Key checks if any saved bonding data are present in nonvolatile memory. If yes, the Hideez Key starts advertisement for devices from whitelist. If no, Hideez Key starts advertisement for all available devices around. That mode is indicated by slow flashing green light. The advertisement period is 60 seconds. If no connection was established during this period, the device will go to power down mode to minimize the power consumption. To start advertisement again, press the button one more time.

On the connecting device Hideez Key is seen as Hideez-XXXXXX in Bluetooth environment, where XXXXXX – last digits of serial number.

Connection procedures for Android and Windows based devices are described below.

Connect to the next device.

Mentioned devices are considered as hosts for Hideez Key. According to Bluetooth 4.0 specification the only one host-connection allowed at the same time, so to pair new host device you have to disconnect Hideez Key from currently connected host device by switching off Bluetooth adapter on host device side or distance the host device enough to lose the connection with Hideez Key. Than Hideez Key could be paired with new host device. When the connection is not active, pressing the button takes Hideez Key in the communication mode (advertisement).

For the pairing procedure, place Hideez Key as close as possible to the device to be connected.

Switching between paired devices.

If there are saved bonding data, Hideez Key can be switched between the relevant devices. To do this, press and hold the button for time from 2 to 4 seconds. Hideez Key will disconnect from the current device and send an invitation (advertisement) to other devices from the "whitelist". If these no device responds or whitelist contain one device only, Hideez Key will reconnect back after advertising period finished (approximately 30s).

Hideez Safe software installation

For Android devices – install Hideez Safe from Google Play.

For Windows PC download Hideez Safe application <http://hideez.com/download> and run it (you may need administrator rights). After the installation  icon appears in the system tray.

Attention! The Hideez Safe has a functionality of downloading and installing of updates from Hideez.com site. Some anti-virus software considers that functionality can be malicious and gives danger warning

Registering my.hideez account.

For security reasons, Hideez Key and its data are “bonded” to the user's account on my.hideez.com service. This binding does not allow the device to connect to the “alien” computer / tablet without the user permission.

My.hideez account (login and password) must be entered on the first time the user starts the program. If this account is not created yet, there is option to create it. To do that, click on “Sign up”. In the opened web page, enter your actual email address as your login and type the password. A confirmation email will be sent to your email. Check it and click on the link this email to complete the registration procedure.

When new Hideez Key is connected to the computer / tablet at the first time, it gets the secret key of your my.hideez account. This secret key will be checked next time you connect the Hideez Key to any other computer.

Connecting to Android-devices.

Connection should be done from Hideez Safe app.

Turn on Bluetooth on the tablet, launch Hideez Safe app and follow the instructions on the screen. When it will be asked, enter you're my.hideez credentials.

The app starts connection wizard. Place Hideez Key close to the tablet and press the button once. A signal sounds, Hideez Key will be connected and registered in your my.hideez account within a few seconds.

Connecting to Windows PC.

On the Windows PC launch Hideez Safe app by click on  in the system tray, then follow the connection wizard instructions.

Cancellation of use and private data erasing from Hideez Key

Before giving Hideez Key away to another person, it is necessary to execute the command "Unregister". This command wipe all of the data from device and clear binding to your my.hideez account.

This procedure must be done to ensure that new users will be able to activate the device in their my.hideez account and connect it to their PC.

Firmware update

Hideez Key firmware is constantly improved. New features are coming with firmware update procedure by Hideez Safe app. The application checks for firmware and software update regularly. The user also can check it when it is needed.

Hideez Technology recommends to check firmware and software updates immediately after setting it up and devices connection.

To do it:

1. Connect Hideez Key to Android tablet or Windows PC.
2. Check whether the Hideez Key battery is full.
3. Connect the tablet or Windows PC to the Internet
4. In Hideez Safe go to "Devices", choose Hideez Key, click "Check for updates" and follow on-screen instructions.

Working with Hideez Key

Finding and guarding of belongings

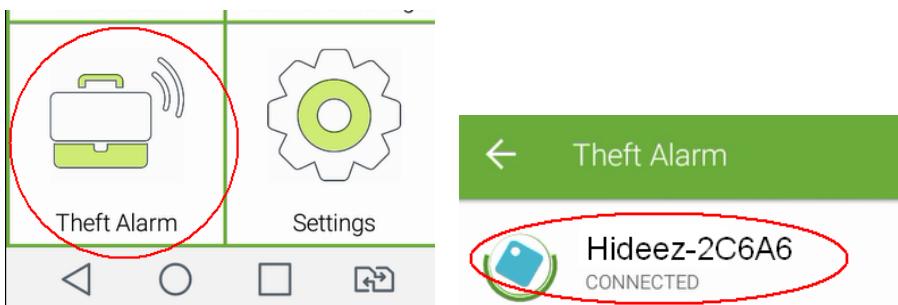
If Hideez Key is secured on any object, it helps to prevent loosing belongings like keys, wallet or portfolio.

It also depends on whether you are in a safe ("trusted") place like home, your office or in other place.

Guard mode worked in Hideez Safe for Android.

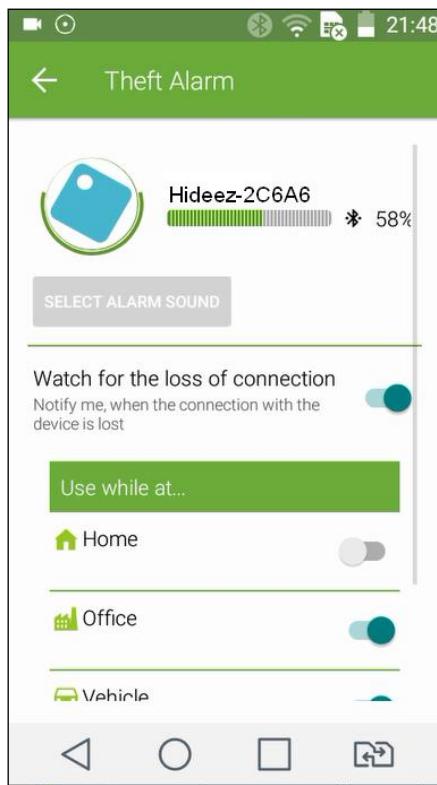
To turn it on do the next steps.

1. Connect Hideez Key to an Android tablet.
2. Place Hideez Key to a wallet, portfolio or key ring.
3. In Hideez Safe open menu "Devices", choose Hideez Key.



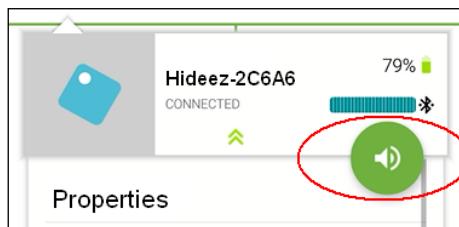
4. Go to "Theft Alarm" menu, then

- Turn on "Watch for communication loss" switch and choose melody which will warn you if the device will be forgotten.
- Turn on the switches "Use while at..." of appropriated profile "Home", "Office" or "Car".
- The program is set to trigger when the signal level is about 10%.
- To change signal level, turn on 'advanced mode' in program settings. After that you will have detailed tuning functions in Theft Alarm, (e.g. signal level)



Finding of objects.

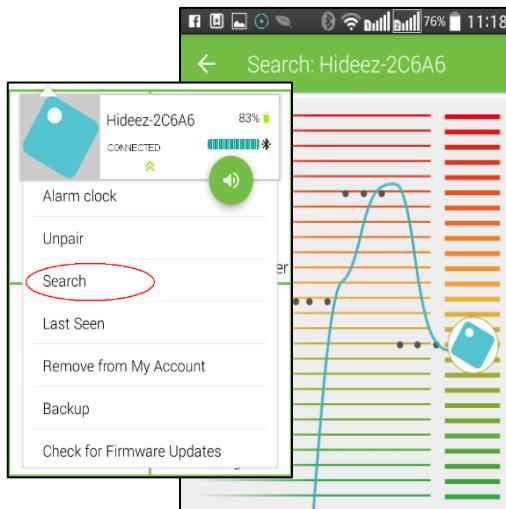
Use signal icon to the fast search connected Hideez Key "by ear".



Note, this feature works if the Hideez Key connection is already established (the device is on signal reception area).

Finding by RSSI.

Sometimes object with Hideez Key is within radio signal reception area, but you can't hear its sound. In this case use radio signal graph (point "Find" in the drop down menu).



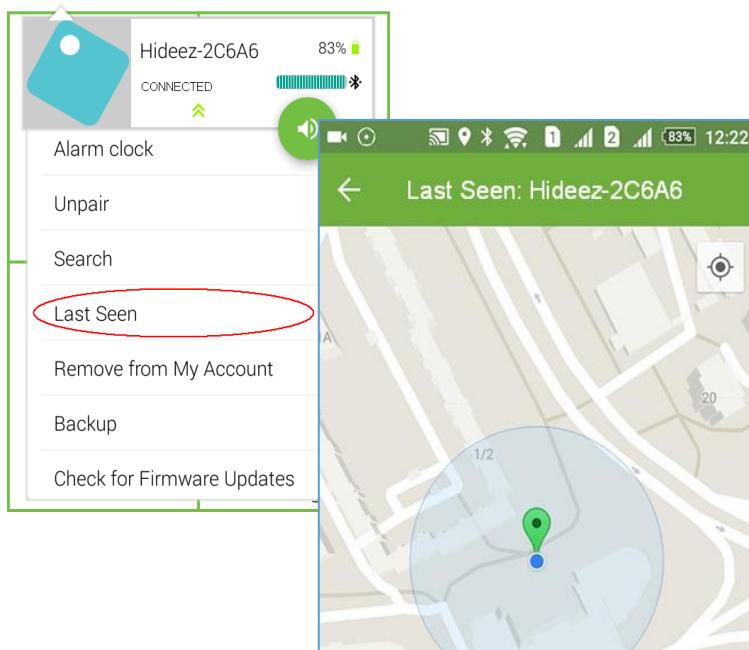
The bottom of graph means the minimal distance between the tablet and Hideez Key. Moving with the tablet, define the place with the best signal strength, this way you will find the object.

Finding objects with Google Maps.

Hideez Safe app is constantly watching Hideez Key connection status.

If Hideez Key connection is lost, app memorize place coordinates when it happened. So convenient to find abandoned items, such as a car on the big parking lot.

In device drop down menu choose "Last seen" item:



The last seen point will be shown on the Google Maps.

Protecting of PC, tablet or smartphone

The most common method to prevent computer unauthorized access is a login/password pair.

Hideez Key facilitates electronic devices access by identifying their owner. Being next to paired device, Hideez Key allows using it without entering password or PIN-code. This Hideez Safe feature has the name "SmartLock".

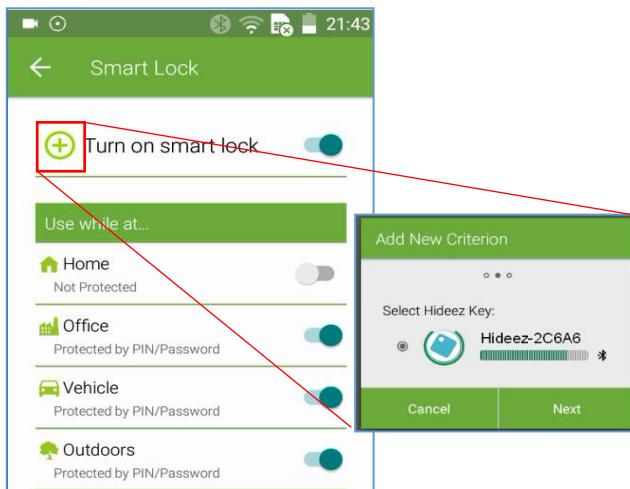
Working with Android device

Hideez Safe app is an administrator of Android device.

For a tablet protection you need set up blocking system according to location profiles, and choose the Hideez Key device which will serve as an owner ID.



1. Go to “Smart Lock” in main screen and click the switch “Turn the Smart Lock on”. At the first time the app will ask for the tablet administration permissions.
2. Enter a password or PIN-code for screen unblocking. It also will be necessary to access to this section.



3. Add the Hideez Key, which will act as unlock criterion, as shown in the figure. The tablet will not require password before the signal level exceeds the predefined one. By default, the signal level is set at 10%. To change the level, you should turn on the advanced mode.
4. For each of trusted location profile (Home, Office, Vehicle) define whether the tablet should be blocked when Hideez Key is out of range. E.g. “Home” is a safe place, so you don’t need protect your tablet from unauthorized access.

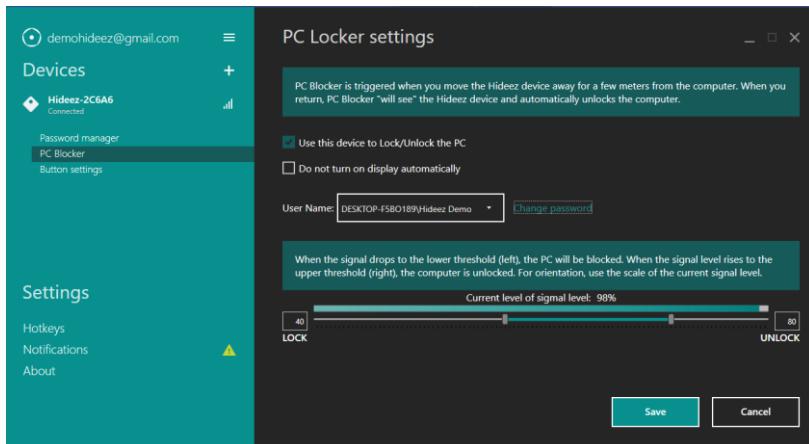
By default, each of location profiles assumes that the tablet is protected by PIN/password.

Windows PC protection

Microsoft Windows uses login/password pair as usual for the local PC or Active Directory user authorization.

Hideez Safe installs its own Credential Provider service into operation system.

To activate the locking feature, go to PC Blocker item in the Hideez Key settings as shown on the figure below.



- 1) Set checkbox " Use this device to Lock/Unlock the PC "
- 2) Type the user name. To choose one from PC local users click triangle on the right.
- 3) Enter the user password. This password will be stored in Hideez Key only.
- 4) If it is necessary, open enhanced settings to change the default upper and lower signal level at which the computer will be locked / unlocked.

Several users on the same PC

It is possible to use some Hideez Key's owned by different users. In this case, each Hideez Key "opens" the Windows user session of the appropriate user.

Password manager

Hideez Key keeps up to thousand passwords. The list size is limited by available internal memory only. Passwords are entered to password field directly via virtual keyboard. Of course, the user can type password manually any time.

Hideez Safe keeps an applications list; the corresponding passwords are stored in the Hideez Key encrypted. Matching passwords to the actual running application is performed by the active window title.

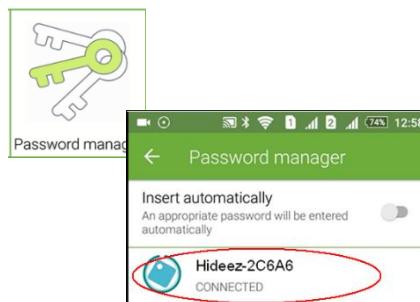
The main item of stored record is “account”, which includes elements of credentials. For firmware ver. 1.1.55 they are:

- Account name
- Login
- Password
- OTP secret key (see point. “One-time passwords” below)

Length of each item is not limited.

Android version of password manager

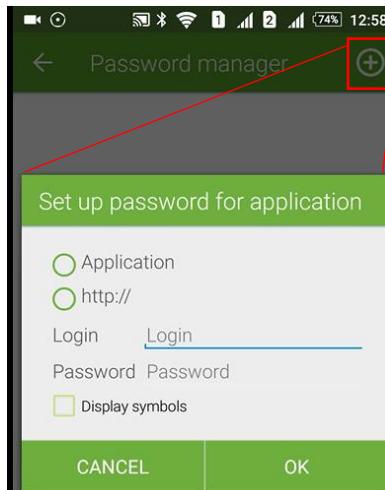
Tap the Password Manager icon on the main window and select Hideez Key device that stores passwords.



For the first time the program will ask for permission to access to password entering. To confirm it, tap the appropriate checkbox in Android dialog box opened.

In Android 5.0 and higher Hideez Safe can enter passwords into applications and web pages automatically. To use this feature, turn on the switch “Insert automatically”.

To add a password, press the "+" at the top, as shown in the figure.

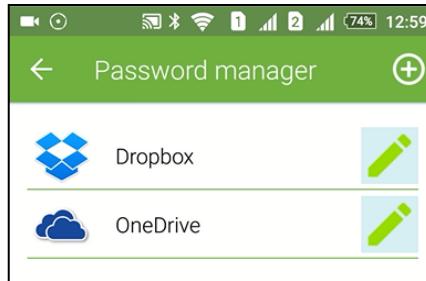


If "Application" selected, the list of Android applications will be opened. Choose one and then enter login and password for it.

If a web-site (http // ...) selected, you can enter a site domain. The password will be applicable to the pages on this domain and its sub-domains.

Please note, login may be empty for some sites or applications. If the program uses a PIN-code (4 digits) - enter it into the password field.

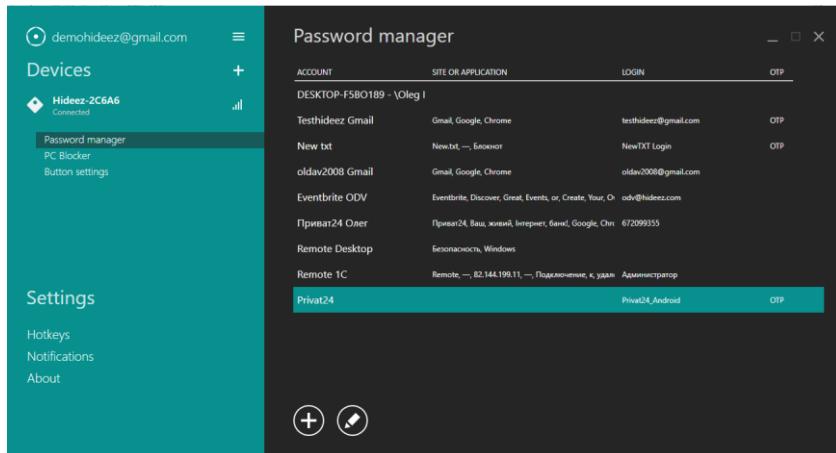
Filled password list looks like the image below, and can include hundreds of entries.



The entries can be edited by clicking or, deleted by "swipe" gesture. The stored password can't be read while editing.

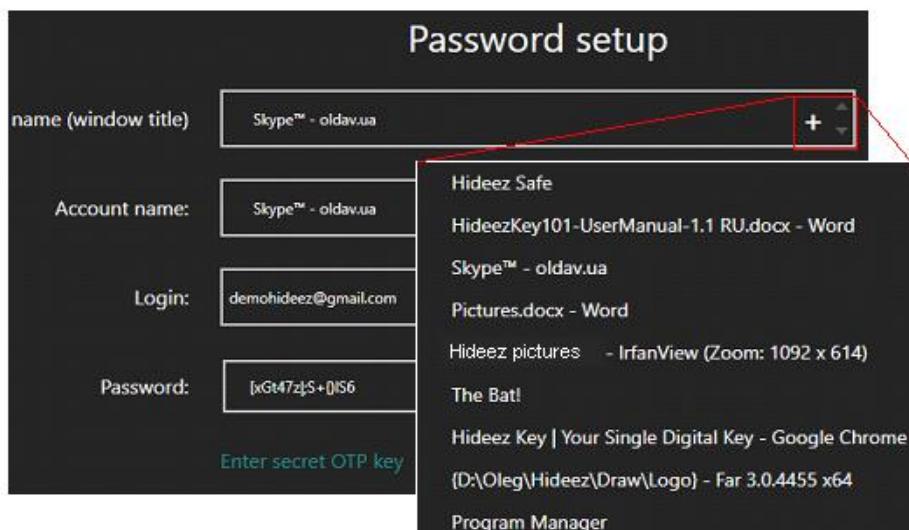
Windows version of password manager

A common view of the password manager screen is shown below.



Adding a new password.

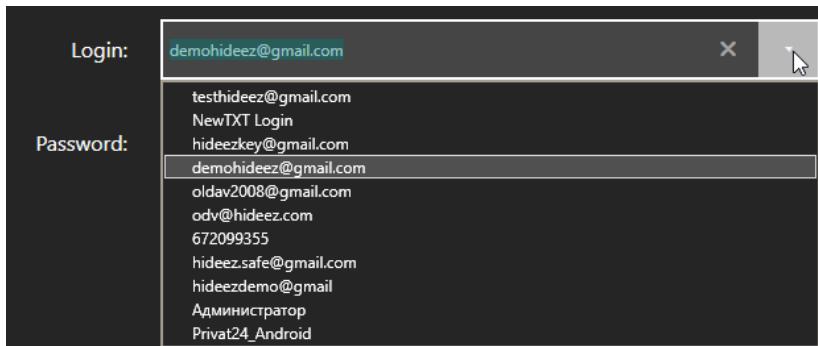
To add new entree in the list, click icon on the bottom of password list. In dialog form opened type an application window title in “Application or website” field. Or, use drop down list of running program, as it shown below.



Hideez Key. User Manual

Into “Account name” type the account name convenient for you, e.g. “Gmail home star”.

Into “Login” field you can type login text, or select one of existing logins from the list as it shown below



Fill “Password” field. Typed symbols are hidden, click icon  to reveal them.



To create a new complex password, click “Generate”. The app will offer a unique password from letters, digits and special symbols.

For accounts of services with two-factor authentication, secret OTP key is needed. Click on “Enter secret OTP key” and insert key sequence into field opened.



To save the changes click “Save” button on the bottom.

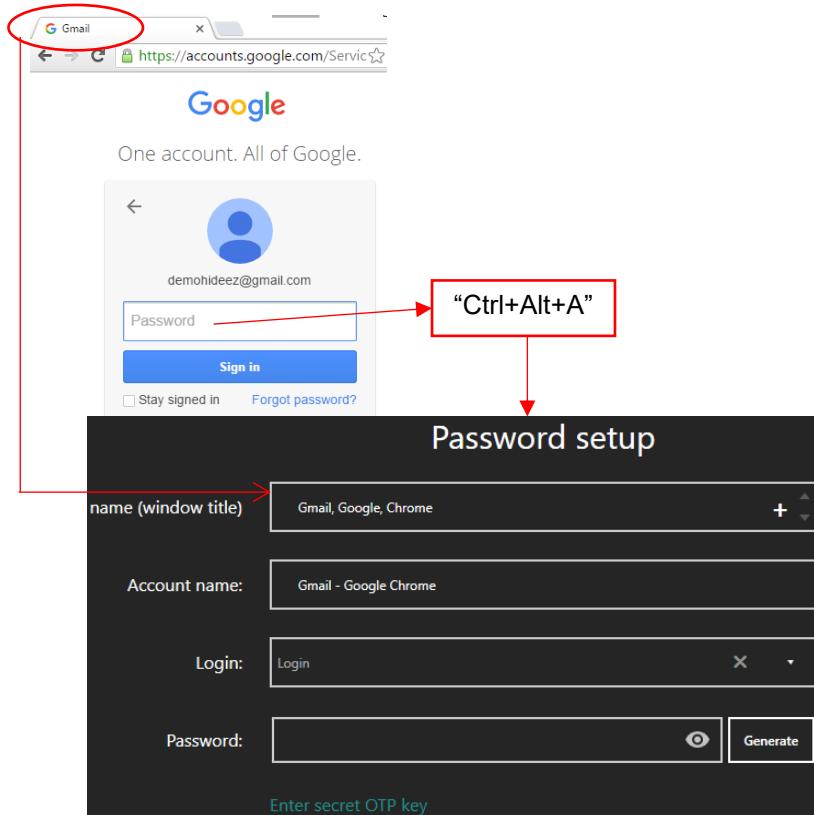
Adding a new password with hotkeys

Hideez Safe for Windows use several hotkeys to speed working with the keyboard.

You can create a new password item from the target application directly. Do that this way:

- 1) Place the text cursor into login or password field of the target app/web-site.
- 2) Press hotkey «Ctrl+Alt+A».
- 3) In the dialog form opened, some fields are filled automatically. Type the login and password ad save the changes.

The figure below illustrates the process of creating password manager item for the existing user Gmail account.



Using of Hideez Key for passwords input

When the Password manager accounts are stored in the Hideez Key, they can be entered into appropriate fields with Hideez Key button or keyboard hotkeys.

Place the text cursor into an appropriate field and do an action from the table below.

Action	Hideez Key button	Hotkey
Enter login	Once	Ctrl+Alt+L
Enter password	Twice	Ctrl+Alt+P
Generate OTP	Triple	Ctrl+Alt+O
Add new item in the password list	-	Ctrl+Alt+A
Enter default password	-	Ctrl+Alt+D

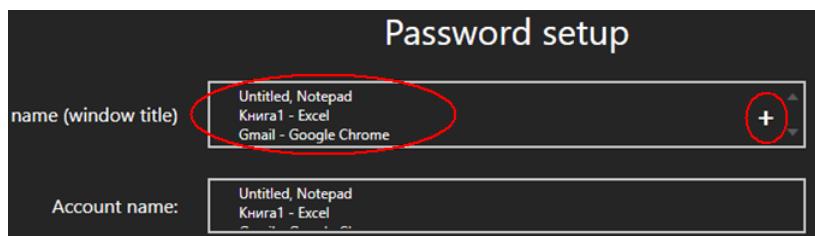
How Hideez Safe for Windows works

When a user run a command from the table above, Hideez Safe detects the active window of the current application.

The program searches the active window title in the table for corresponding password. If there is only one appropriate record, the credentials are read from Hideez Key and entered into the input field via the "virtual keyboard".

If there are multiple entries that correspond to the window title, a list of these records will appear in pop-up window. User will be prompted to choose one of the list. A good case is multiple email accounts on mail service with the browser access.

If the same credentials are used for several programs, no needs to create multiple entries. Password manager can match a record to several programs. Just list them in the "Program or site" field manually or by clicking the "+" as shown in the figure below.



Removing entries from Password manager

To remove credential record from Password manager, open the record and click “Remove account” on the bottom of the dialog.

Note: To quick all data removing use the “Unregister” command in the device settings.

One-time passwords (OTP) and two-factor authentication

Hideez Key supports one-time passwords (OTP) according to RFC 6238 standard. Each entries of password manager can keep secret OTP key for OTP passwords generating.

The following information shows how to use Hideez Key for Google two-factor authentication (TWA).

To enable two-factor authentication, you should create private key (Private OTP-key) and store it to the device.

1. Go to your account security settings <https://accounts.google.com/b/0/SmsAuthConfig>
2. Turn on TWA for your account (corporate clients may need corporate admin confirmation).
3. Google may ask your mobile number. Specify it and put a special code, received from Google via SMS.
4. Choose “Get codes via our mobile app instead”, and check “Android”.
5. In dialog “Set up Google Authenticator” click on link “Can't scan the barcode?” and find 32-symbols secret key as it shown on a picture below.

Can't scan the barcode?

1. In Google Authenticator, touch Menu and select “Set up account.”
2. Select “Enter provided key”
3. In “Enter account name” type your full email address.
4. In “Enter your key” type your secret key:

yk5e pz7w kz73 klee ucfn jc6n zapy

z5c4

Spaces don't matter.

5. Key type: make sure “Time-based” is selected.
6. Tap Add.
6. Copy the secret key into clipboard.
7. Open Password manager entries, click “Enter secret OTP key”, paste copied data and save the changes.

Now, one push of Hideez Key button will generate actual OTP-password and enter it into current input field on PC.

Note. Each new secret code generation on Google web-service makes previous code invalid, so you need to install private key in all the devices simultaneously, e.g. Hideez Key and Google Authenticator on your smartphone.

Backup

Hideez Key device can keep a thousand passwords. To prevent losing it and all the inconveniences, Hideez Safe can do backup and restore of user data.

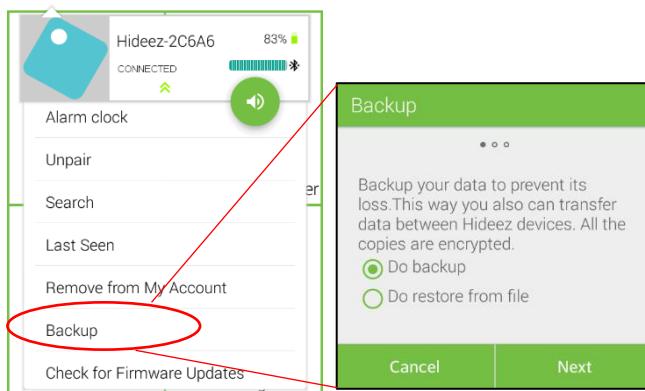
The backup file is kept on local PC/tablet storage only. The file is encrypted by my.hideez password according to AES-256.

The device should be connected while backup/restore procedure is running.

Each restore procedure asks for the password of my.hideez account, the backup procedure was done for.

Hideez Key backup on Android.

On the Hideez Key drop down menu tap “Backup” and follow the screen instructions.

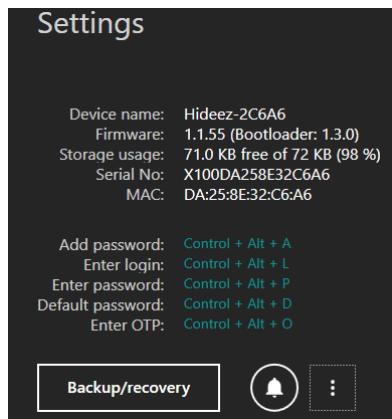


Backup file has the extension *.hb and the file name which includes device name, date and time of backup.

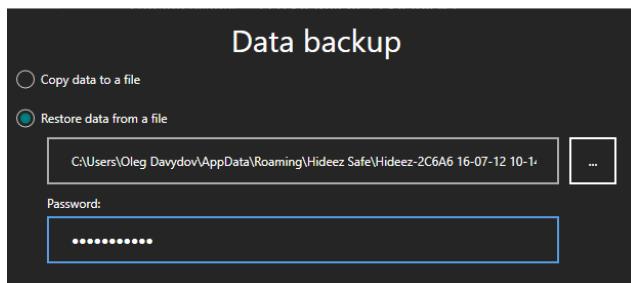
To restore the data select “Restore” radio-button and choose file with backup data.

Hideez Key backup on Windows.

On Hideez Key settings screen click “Backup/recovery”.



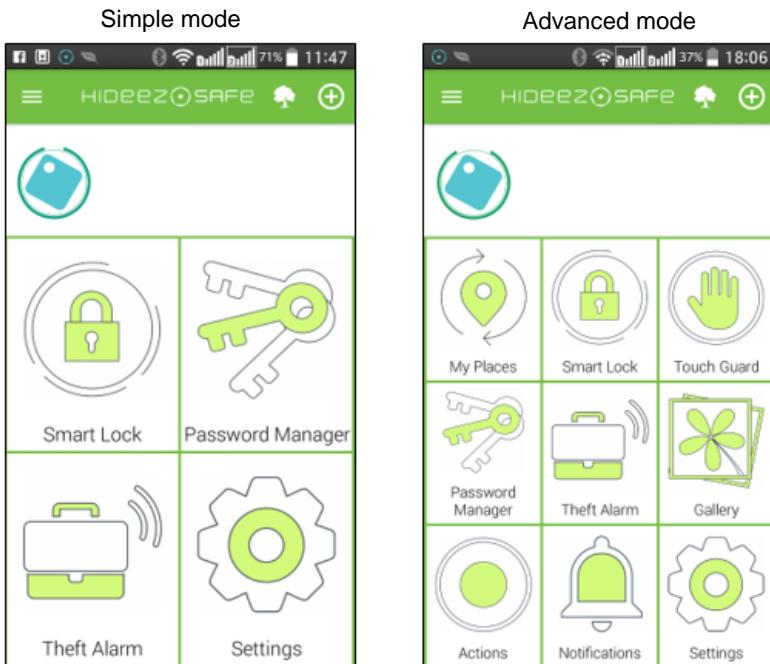
The data saving procedure is similar to described above.



The backup/restore procedure can be used for data transfer between one user Hideez Key devices, as well as between different user devices, if the users trust each other and knows both of my.hideez account credentials.

Hideez Safe for Android enhanced mode

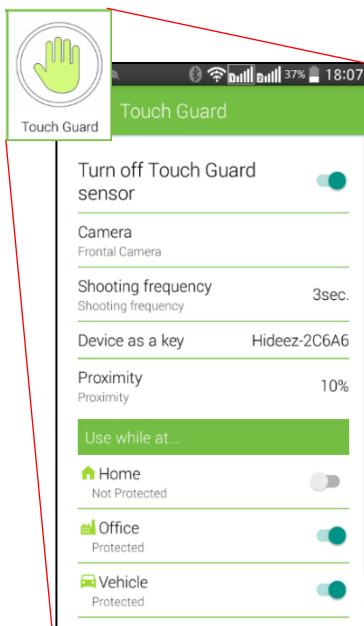
Some Hideez Safe functionality is hidden and appears only “Advanced mode”. To turn on this mode, go to Settings and turn on the appropriate switch. The main screen will be changed:



Touch guard

Hideez Safe for Android can take a photo series silently, when somebody picks up unattended smartphone (or tablet). The pictures will be made under following conditions:

- 1) Touch Guard mode is on and smartphone is in a waiting mode.
- 2) Hideez Key is paired with smartphone and RSSI is lower than defined in settings.
- 3) Accelerometer shows the activity (smartphone moves)



On the “Touch guard” section the user can define cameras (front, rear, or both) which should be activated, shooting period, signal level, as well as any location profiles should use this mode.

Remote control (selfie, voice recorder, etc.)

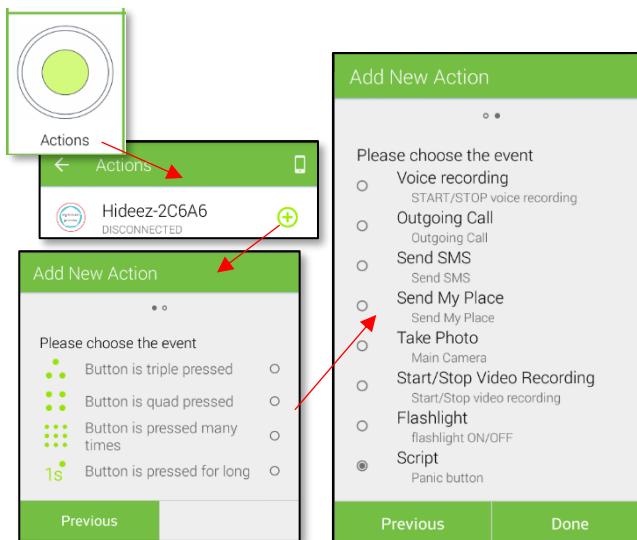
Hideez Safe for Android provides the ability to perform action on smartphone by pushing Hideez Key button. You may assign different events to the three-, four-, and multi button pressing and long press (more than 1 second).

As an example let's consider Hideez Key as a remote control for shooting selfie and voice recorder.

Go to “Actions” in main menu.

1. Add new action by clicking , select the device for what it will perform.
2. Choose button pressing amount.
3. Choose the action “Take photo”
4. Choose camera (front, rear or both)

Taken pictures may be seen later in Gallery



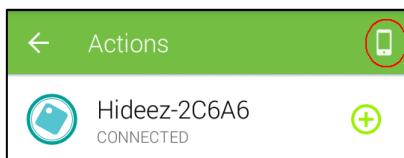
The same way you can assign start/stop voice recording to other button pressing event or choose another actions that you consider useful.

Panic button

Hideez Safe for Android may perform not only the single actions, but also action sequences (scripts) on the smartphone by pressing Hideez Key button.

Let's create sequence for sending SMS as a script example.

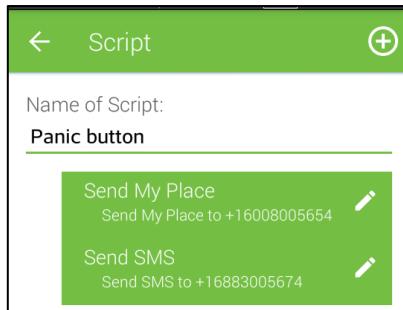
1. Go to "Actions" in the main screen as it specified above.
2. Tap the icon on top right corner.



3. Add a new script by click , then enter the action name "Panic button".
4. Add a new action by click  then select "Send SMS".
5. Enter mobile phone number in international format and the SMS text (e.g. "I need help").
6. Add new action by  and select action "Send my coordinates".
7. Enter the same phone number.

8. Click “Done” for script saving.

The approximate result is shown below.



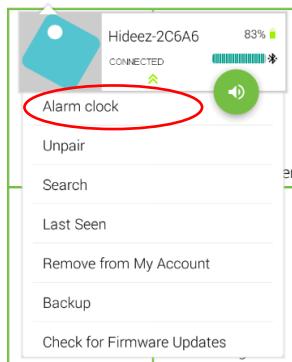
9. Go to “Actions” point and add a new action to double press of the button. Note, the created script “Panic button” was added to the standard list of action. Choose it and save the new action

You can edit created actions and scripts by pushing . To remove unnecessary entries - just swipe them and confirm the deletion.

Alarm clock

Hideez Key supports up to three built-in alarm. Use Hideez Safe for Android to set them up.

Go to Main Menu - Devices, select “Alarm clock” from the context menu of the chosen device.



There are some points can be set up for every alarm clock:

- Alarm time
- Day of week

Troubleshooting

1. Hideez Key does not work, does not respond to button presses

You should replace the battery as described in "Getting Started".

2. You can't find Hideez Key in Bluetooth-environment

The Hideez Key device, as usual, is not in the Bluetooth-visibility mode. After establishing the connection with the specific tablet or PC, Hideez Key only works with it. To connect Hideez Key to other device, you need to turn off Bluetooth on the first one, or just bring Hideez Key away from radio signal range. Then press the device button. Hideez Key will start advertising mode and you will be able to pair it with other device.

Note. On some devices advertisement doesn't work when geolocation settings are off in Android settings.

3. The device has been in the water and stoped working.

Water may cause permanent damage to the device, but it is reasonable to do "rescue actions" in any case.

Remove the device from the water as soon as possible, open the case, remove the battery and dry the mainboard with household hair dryer.

After drying, install a new battery and test the functionality.

Annex 1. Hideez Key signals and states

Sound and light signals of Hideez Key.

Sound signals:

1. Alarm – an alternating sound 6000Hz, 2680Hz, 1080Hz for about 5s
2. Single beep – short beep 480Hz * 80ms
3. Double beep – two short beeps 2680Hz *80ms
4. Roger beep - two short beeps 480Hz * 80ms
5. Error beep - three beeps 200Hz *200ms
6. Connected beep - 960Hz * 80ms, 1360Hz * 80ms
7. Disconnected beep - 960Hz * 80ms, 800Hz * 80ms, 800Hz * 80ms
8. Peripheral beep - 3400Hz * 160ms, 3600Hz * 80ms, 3800Hz * 160ms
9. Roger beep in menu - 1480Hz * 80ms, 1880Hz * 80ms, 3200Hz * 160ms

Light signals:

1. Connected – indicates active BT connection established, 100ms on, 3900ms off. (cycled)
2. Fast blink - 100ms on, 100ms off. (cycled)
3. Slow blink - 500ms on, 500ms off. (cycled)
4. Double blink - 100ms on, 100ms off,100ms on, 800ms off (single)
5. Single Blink - 100ms on, 100ms off. (single)

Signals description

Signal		Event, state
Sound	LED	
Single beep	Single Blink green	accompanies single button push; counts seconds when the button is held
Double beep	Double blink green	Ready to work after power is on
Roger beep	Double blink green	Confirm command from the button is accepted; Confirm command from the menu is run
Error beep	Double blink red	Command or scenario execution error
Connected beep	Double blink green	At the moment BT connection is established
Disconnected beep	Double blink red	At the moment BT connection is broken
	Connected, green	Hideez Key is currently connected to BT device
Peripheral beep	Fast blink red	Enter to menu mode
	Slow blink green	Hideez Key is broadcasting to connect (advertisement) for any device (whitelist is ignored)

Annex 2. Frequently asked questions and answers

How long do the Hideez Key work before battery change?

The estimated operation time of Hideez Key at minimal power consumption (e.g. constantly connected or constantly advertising) is up to 6 months if the new CR2032 battery.

How do I change the battery? Will the data be lost?

User data, including passwords, signatures private keys are stored in the nonvolatile memory encrypted, so they will not be lost. However, Hideez recommends to do backup of the important information. Backup file is encrypted by AES 256 protocol can be stored on your computer or on another Hideez Key device.

Will Hideez Key work with the iPhone?

Yes, it will work after Hideez Safe for iOS is issued. However, the function lock / unlock the iPhone are not available due to the peculiarities iOS.

How can I use the Hideez Key with my office computer and my Android smartphone simultaneously?

The computer and the smartphone are host-devices for Hideez Key. Bluetooth 4.0 specification does not allow simultaneous connections to several hosts. So the only concurrent operation is possible at one moment. Hideez Key can be paired with 8 devices (e.g. Windows PC and smartphone). To switch between them, press and hold the Hideez Key button for 2 seconds.

How can I update Hideez Key firmware?

Firmware update procedure is performed with Hideez Safe. You need connect the Hideez Key to the PC/tablet and check for updates.

How the user can be identified on the device?

Hideez Key don't assume any owner authentication procedure at the moment. Hideez Band bracelet can be configured to require user authentication in Hideez Safe for Android on connected smartphone. Authentication methods are that: PIN-code, password, biometric method – eye recognition via smartphone camera.

How I can clean my Hideez Key if I want pass it to somebody?

Each Hideez Key is registered in my.hideez account of its owner. To pass it to anyone, the owner should run “Unregister” procedure. It will clean the device registration and wipe all the user data.

How to backup of my personal information?

Backup of all the user information can be done by Hideez Safe on PC or tablet. Actually, another Hideez Key can serve as safe backup storage.

What physical conditions are dangerous for the Hideez Key?

The Hideez Key is made of plastic and doesn't provide extra resistance. Electronic components retain their characteristics in the domestic environment (direct sunlight, electromagnetic radiation) that are safe for humans. It is not recommended to expose the device prolonged sunlight to avoid aging of the plastic housing.

Is the Hideez Key allowed on a flying plane?

Yes, it is. The device receives and transmits radio frequency according to the Bluetooth 4.0 standard for a short distance, and does not require off in an aircraft, according to FAA instructions from 10.31.2013. If you use personal medical devices (such as pacemakers and hearing aids), consult with your doctor or the manufacturer to find out whether they are protected against external RF signals.

Is it possible to integrate with our corporate information system? Is there any API for such integration?

Yes, it is possible, ask Hideez for developer's guide and API documentation.

FCC Caution:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.