ePass FIDO® -NFC
MultiPass FIDO®
Security Key

User Manual

For Google 2-Step Verification &
Advanced Protection Program

FEITIAN
WE BUILD SECURITY

Overview

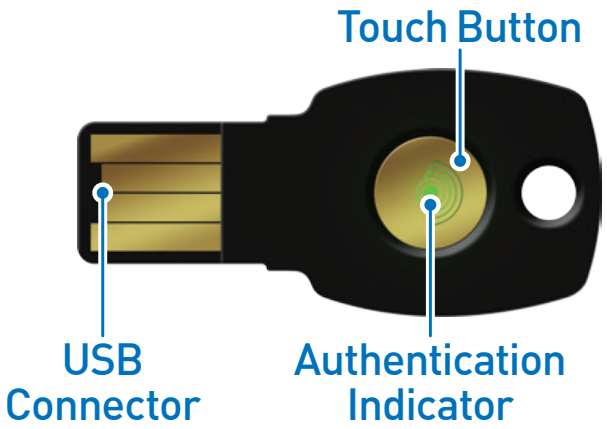
FEITIAN ePass FIDO® Series Security Key is a FIDO® U2F certified authenticator. Unlike traditional second-factor authentication devices, FIDO® U2F provides a much more convenient solution to replace or be a plus of traditional password. A single FEITIAN ePass FIDO® Security Key can protect an unlimited number of applications. Each application will be assigned an independent key pair.

FEITIAN ePass FIDO® Series Security Key employs high-performance secure element. All credentials are physically protected by the hardware security chip. The confidential information and credentials will never be revealed under any type of attacks such as phishing and man-in-the-middle.

Users' accounts will always be secure even though the whole server of the application you are using is hacked. The public keys stored in the application server might be revealed under attacks while however, your private key is always under protection.

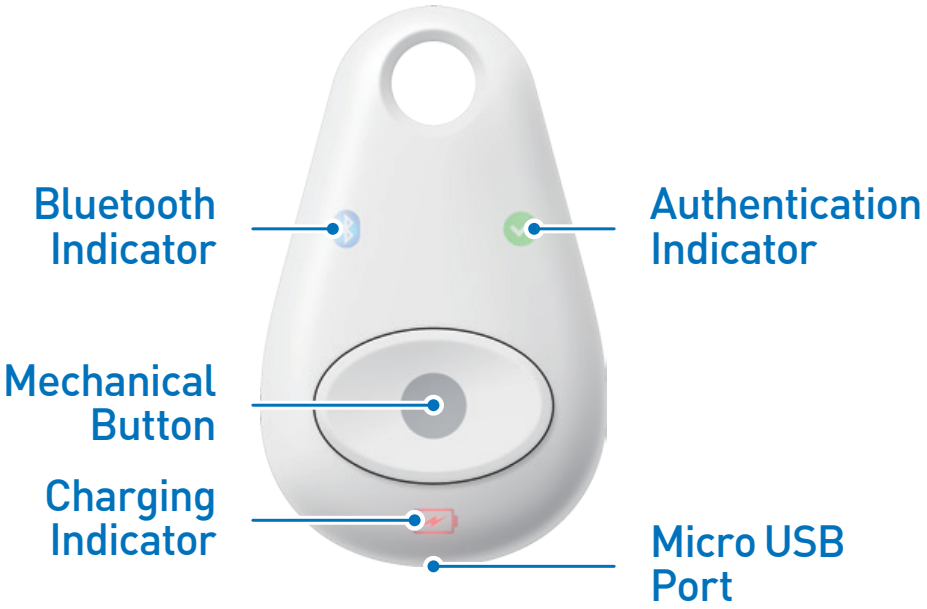
FEITIAN ePass FIDO® -NFC and MultiPass FIDO® Security Key are devices to go beyond the traditional two-factor authentication systems, the built-in BLE (MultiPass FIDO® only), NFC, and USB communication interfaces empower users to select the desired channel and complete a secure FIDO® U2F authentication across any of your client devices in contact or wirelessly, including desktop, notebook, tablet, and smartphone.

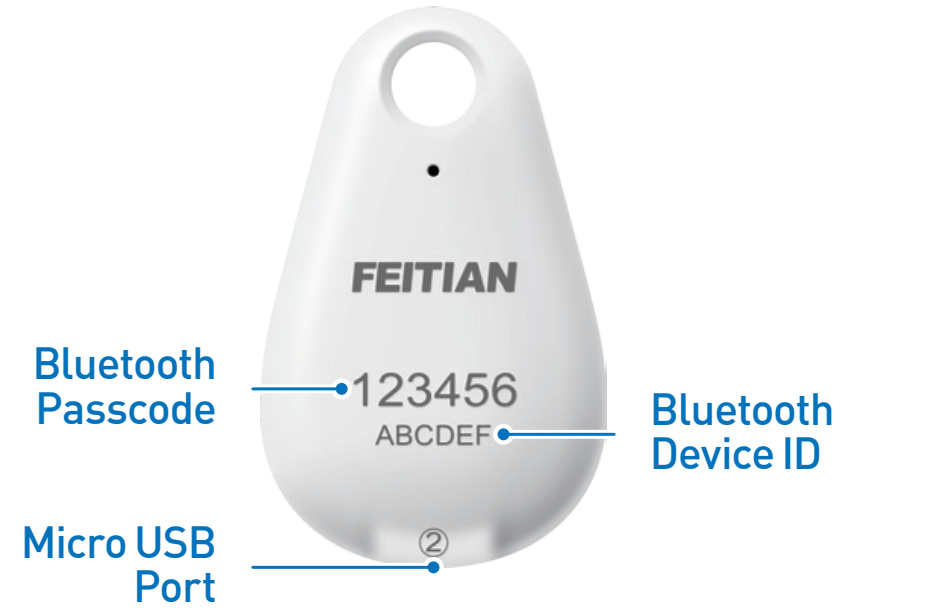
Diagram

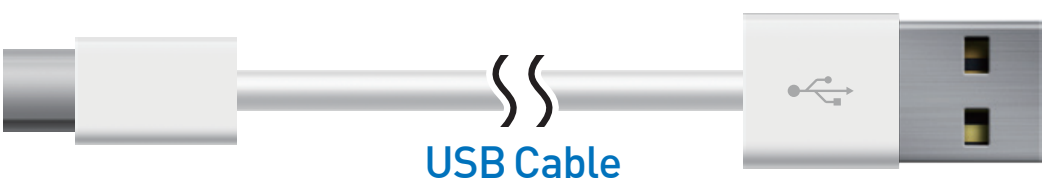


ePass FIDO® -NFC

Diagram

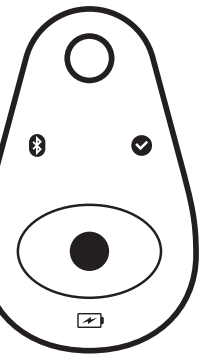






MultiPass FIDO®

Compatibility



	android	iOS	mac OS / Windows / Linux (Using Chrome browser)
USB	✗	✗	✓
NFC	✓	✗	✗
USB	✗	✗	✓
NFC	✓	✗	✗
Bluetooth	✓	✓	✗

Note: Please keep updating to latest operating system(s) / software for maximum compatibility.

Registration

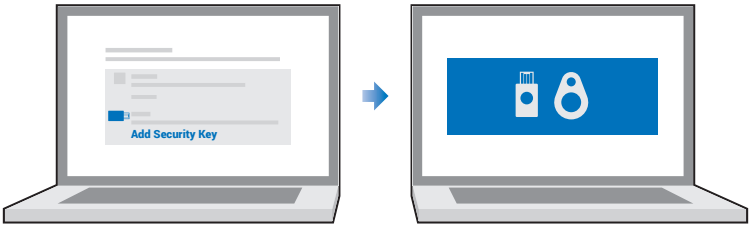
Google 2-Step Verification

Note: The following registration process can only be done on PC over USB connection.

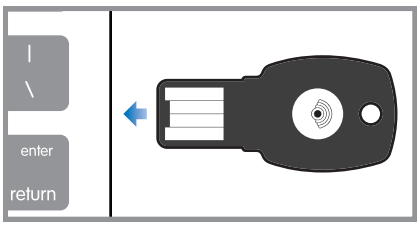
❶ **Log in** to your **Google account** with a **Chrome core based browser** on a **computer**;

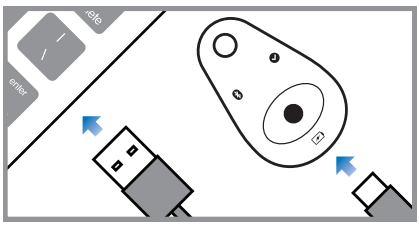
❷ Click **“My account” -> “Sign-in & Security” -> “2-Step Verification”**;

❸ Click **“Add Security Key”** and follow the instruction to complete the registration;

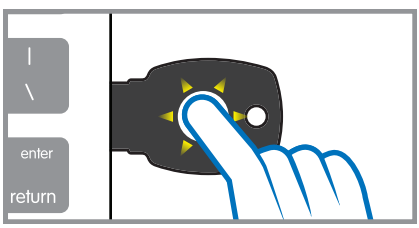


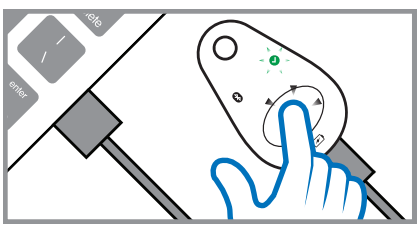
❹ You will be informed to **insert** your ePass FIDO® Security Key during the registration process;





❺ **Click / touch** the button to proof the user presence when the authentication indicator blinks. Your registration will complete in a moment.





Registration

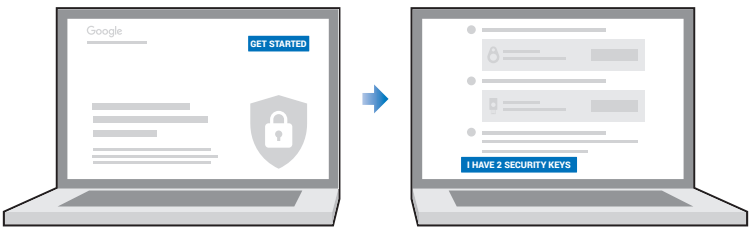
Google Advanced Protection Program

Note: The following registration process can only be done on PC over USB connection.

❶ **Access** the home page of **Advanced Protection Program** with a **Chrome core based browser** on a **computer** at:

https://landing.google.com/advancedprotection/

❷ Click **"GET STARTED"** and you will see a page as shown below;



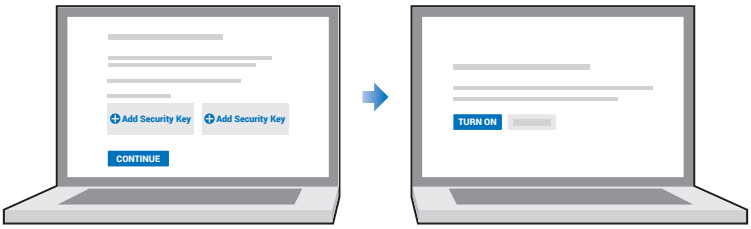
❸ Get 2 security keys ready and click **"I HAVE 2 SECURITY KEYS"**;

Note: The brand and token model recommended in this page are not mandatory. Any FIDO® U2F certified security can be used for Google Advanced Protection. However, to maximize the compatibility, using the token shown in the page is highly recommended.

❹ You will be required to enter your **password** again;

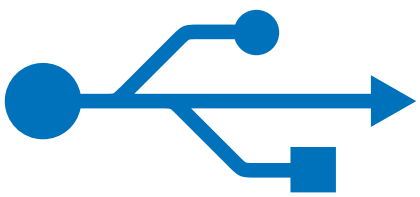
❺ The registration process starts as shown below. **Register** the security key one by one and click **"CONTINUE"**;

❻ Read and confirm the notifications about Advanced Protection Program and click **"TURN ON"**. Your registration will complete in a moment.



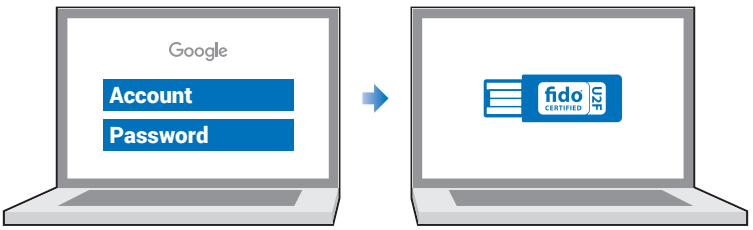
Authentication

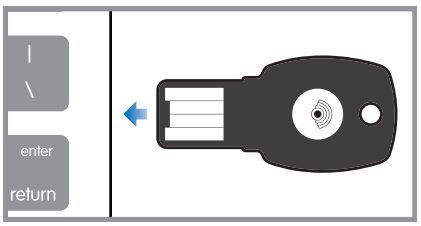
Via USB

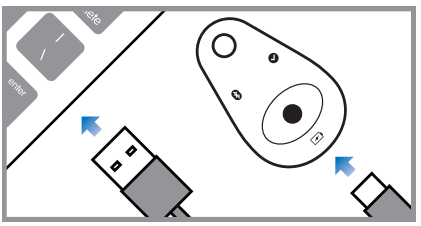


❶ **Log in** to your Google account with a **Chrome core based browser** on a computer using your account and password.

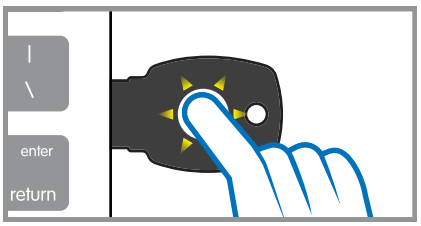
You will be informed to **insert** your registered ePass FIDO® Security Key during the authentication process;

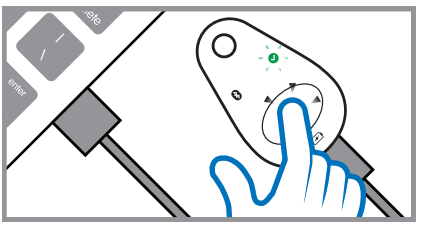






❷ **Click / touch** the button to proof the user presence when the authentication indicator flashes;



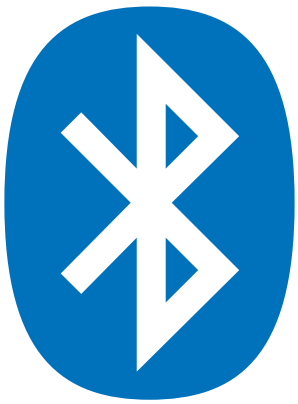


❸ Your authentication will complete in a moment.

Note: Please do take your ePass FIDO® Security Key with you all the time in case you're asked to do the authentication procedure again.

Authentication

Via Bluetooth



Note: Bluetooth authentication only works for MultiPass FIDO®.

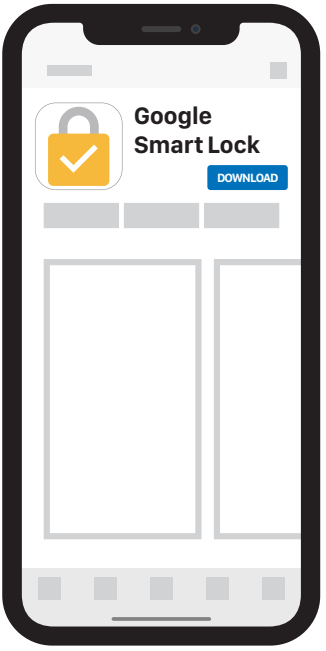
android

Make sure your Google Play services is up to date, then go to **“Settings” -> “Account” -> “Add Account” -> “Google Account”**;

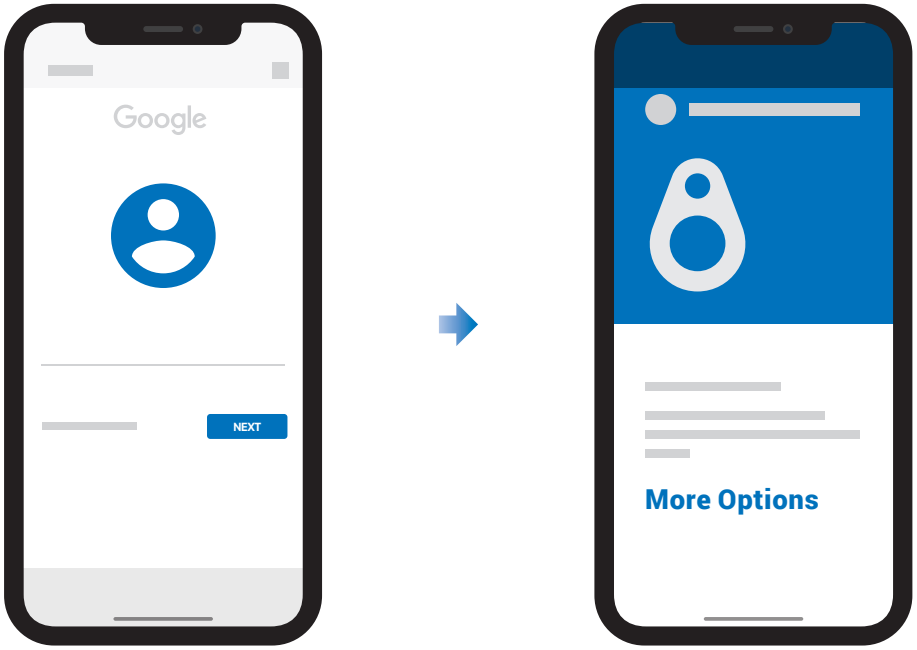
1

iOS

Download “Smart Lock” app from App Store, then launch the app and **add** your **Google Account**;

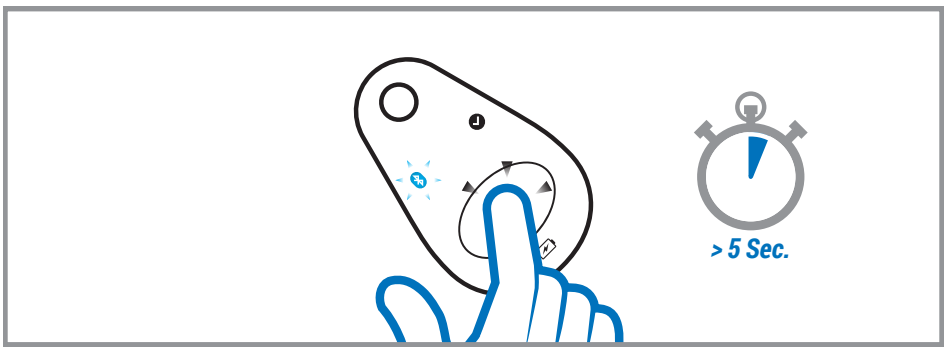


❷ Follow the instruction on your mobile device. You will be asked to **present** your registered MultiPass FIDO® Security Key. Please make sure Bluetooth of the mobile device is turned on;

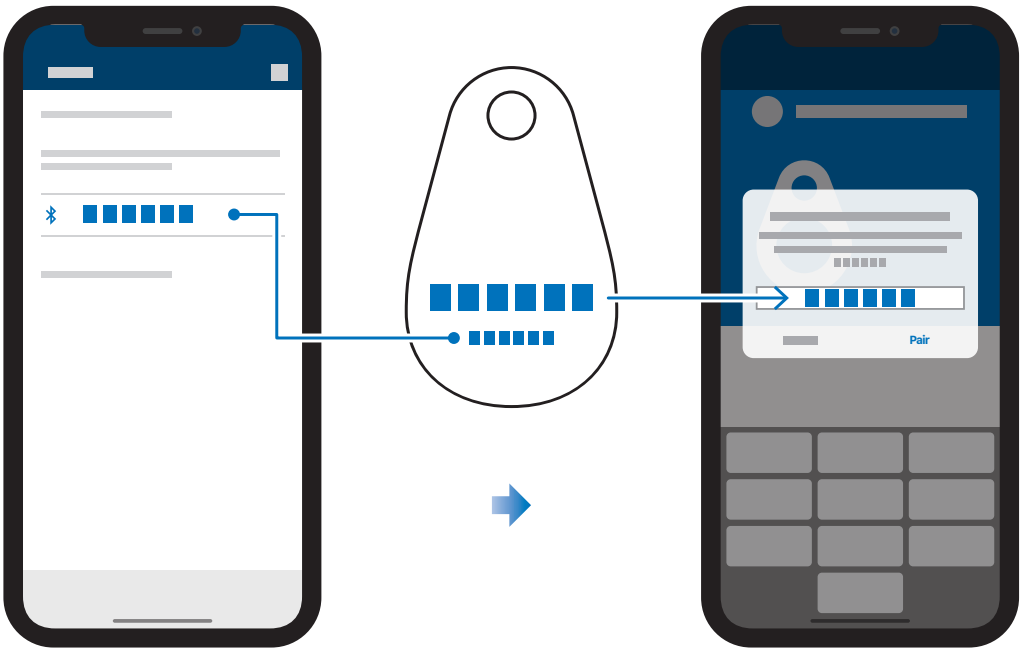


❸ You need to **pair** your registered MultiPass FIDO® Security Key first when using it on your mobile device for the very first time. Click **"More options" -> "Pair a new security key" -> "Next"** to start pairing procedure;

❹ **Press and hold** the button on your registered MultiPass FIDO® Security Key for **over 5 seconds** to active Bluetooth Pairing Mode, a blue indicator shall flash;



❺ **Select** your registered ePass FIDO® Security Key from the Bluetooth Device List. The Bluetooth Device ID of your Security Key is a 6-letter alphabetic name printed on the back of it;

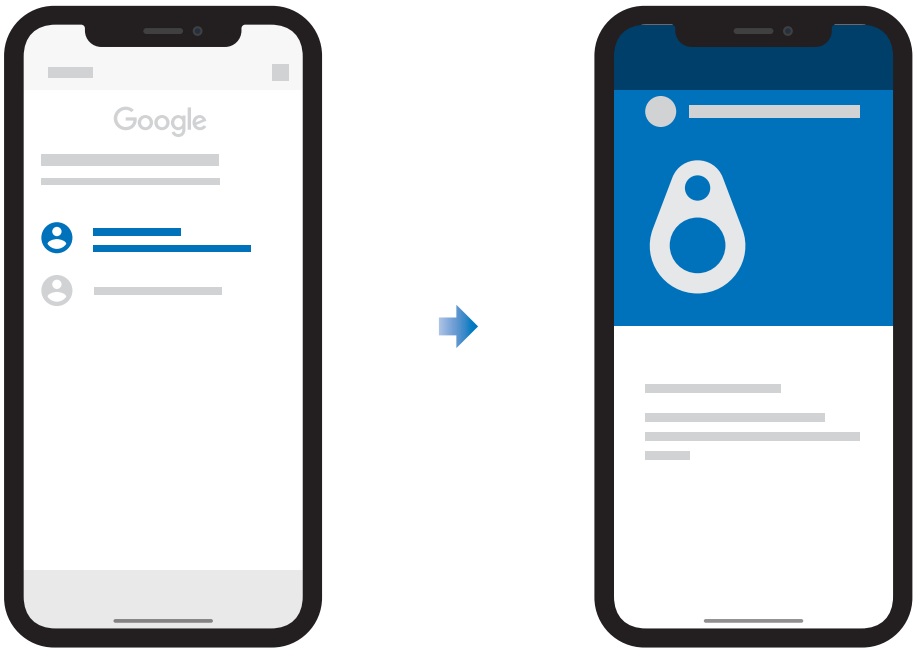


❻ **Input** the 6-digit muneric **Passcode** printed on the back of your Security Key and click **"Pair"**;

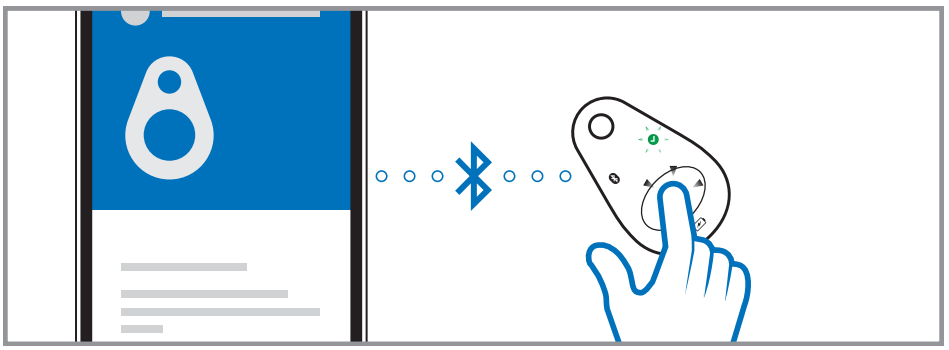
❼ Pairing procedure and your first-time authentication on this mobile device will complete in a moment. Now you can login to any Google Service app on this mobile device with your account for a certain period wihout being asked to do the authentication procedure again.

Note: After this certain period, you will be asked to authenticate you to this mobile device again. Please do take your MultiPass FIDO® Security Key with you all the time in case you're asked to do the authentication procedure again.

❽ When you're asked to authenticate yourself on a paired mobile device again, **present** your registered ePass FIDO® Security Key. Please make sure Bluetooth of the mobile device is turned on;



❾ **Click** the button on your MultiPass FIDO® Security Key to complete the authentication, a green indicator shall flash;



❿ Your authentication will complete in a moment.

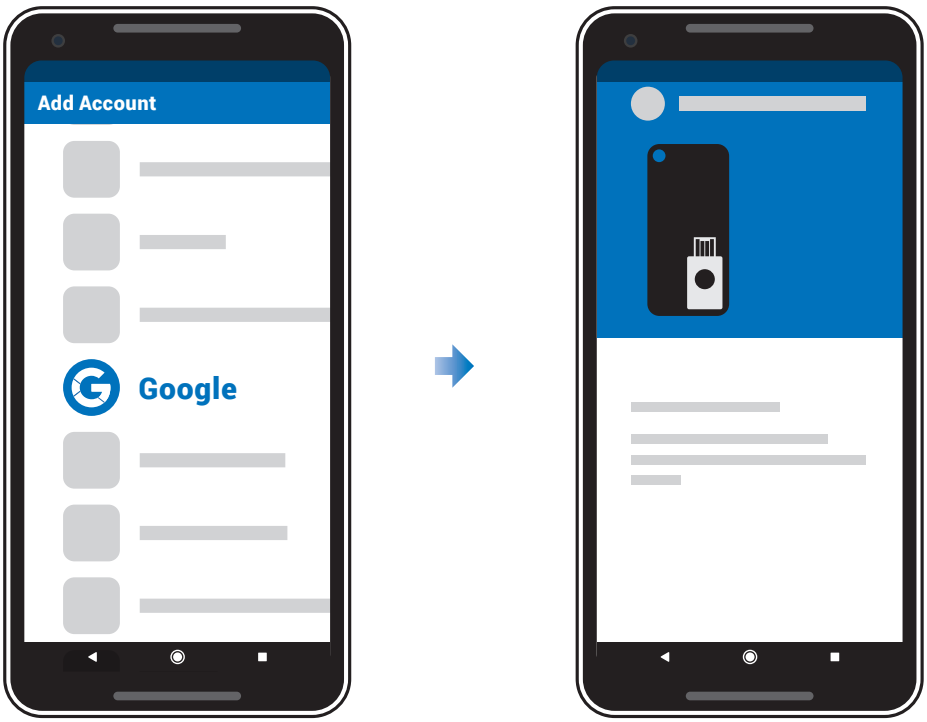
Authentication

Via NFC

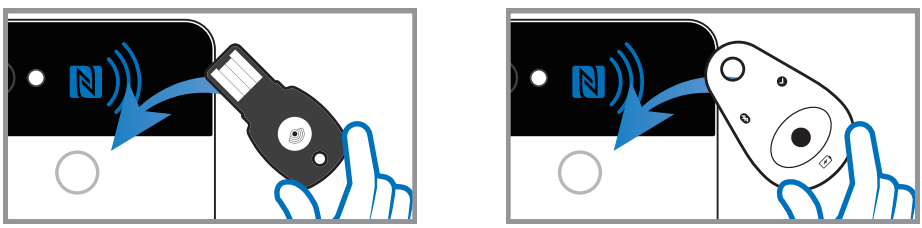
Note: NFC authentication only works on android devices.

❶ Make sure your Google Play services is up to date, then go to **“Settings” -> “Account” -> “Add Account” -> “Google Account”**;

❷ Follow the instruction on your mobile device. You will be asked to **present** your registered ePass FIDO® Security Key. Please make sure NFC of the mobile device is turned on;



❸ **Tap** your registered ePass FIDO® Security Key to the mobile device’s NFC sensor to complete the authentication;



❹ Your authentication will complete in a moment.

Note: After a certain period, you will be asked to authenticate you to this mobile device again. Please do take your ePass FIDO® Security Key with you all the time in case you’re asked to do the authentication procedure again.

FAQ

Q ***How can I pair MultiPass FIDO® Security Key with my iPhone?***

A iPhone does not allow the Security Key to be paired over the Bluetooth setting page directly. You need to download the application "Smart Lock" from app store and use the "Smart Lock" to pair the Security Key.

Q ***Can I use MultiPass FIDO® Security Key on PC over Bluetooth?***

A Most of the FIDO® U2F PC applications rely on HID interface which Bluetooth is not compatible with that. Please use the token on PC over USB interface. A U2F Bluetooth adapter will be released soon. This adapter will allow you to use the MultiPass FIDO® on PC over Bluetooth.

Q ***What browsers support FIDO® U2F Security Key?***

A Chrome and Chrome core based browsers (Such as Epic browser), Firefox. The support of other browsers will come soon.

Q ***Can I install my own applet into the JAVA Smart Card inside MultiPass FIDO® Security Key?***

A Standard product does not allow modification on the JAVA Smart Card. Installing customized application will need placing a customization order to FEITIAN.

Q ***What applications support FIDO® U2F Security Key?***

A The applications support FIDO® U2F include but not limited to: Google, Facebook, Dropbox, GitHub, Dashlane, DUO, StrongAuth etc.

Q ***How long is the battery life?***

A The MultiPass FIDO® Security Key can be used for around 3 months for each full charging (Assuming using Bluetooth authentication 10 times / day).

FAQ

Q ***What to do if I lost my Security Key?***

A Different applications provide different solutions for key recovery. Such as Google is using SMS OTP as alternative 2-step verification method while Facebook is using recovery codes. Please kindly check with your service provider about the security key recovery methods.

Q ***Can I register a Security Key over my smart phone?***

A You can always authenticate the security key with your mobile devices, but registration can only be done from a non-mobile device with Chrome and other U2F supported browsers.

Q ***What app do I need to install for using the MultiPass FIDO® Security Keyon my Android phone?***

A

Nothing. Just be sure that the google play services and chrome browser are up to date.

Q ***How can I know the battery is fully charged?***

A Charging process starts automatically when USB cable is plugged in. A red indicator will be lit during charging process, and goes off when the Security Key is fully charged.

Q ***Why the key is not working properly in Linux?***

A In Linux, there should be a rules file for using U2F keys.

Follow the following step to setup the rules file:

1. Download "70-u2f.rules" from https://ftsafe.com/services/Resources.

2. Copy the downloaded file into /etc/udev/rules.d/ (You may need to use sudo mode).

3. Restart the system

Specification

ePass FIDO® -NFC

Supported Operating Systems	Chrome OS, Windows, Linux, macOS,
Certifications	FIDO® U2F
Embedded security algorithm	ECDSA, SHA256
Size	43.9 × 20.8 × 3.1 mm
Max number of keys	No limit
Interface type	USB
Data storage life	At least 10 years
Programming cycles	100,000 times
Communication protocol	HID
Working voltage	5.0V
Working current	22mA
Power	0.11W
Working temperature	-10ºC ~ 50ºC
Storage temperature	-20ºC ~ 70ºC
Button	Touching type; Green LED light
Casing Material	ABS, Calcium carbonate

Specification

MultiPass FIDO®

Supported Operating Systems	Chrome OS, Windows, Linux, macOS,
Certifications	FIDO® U2F
Embedded security algorithm	ECDSA, SHA256
Size	47.3 × 29.3 × 8.3 mm
Max number of keys	No limit
Interface type	USB
Data storage life	At least 10 years
Programming cycles	100,000 times
Communication protocol	HID
Working voltage	5.0V
Working current	22mA
Power	0.11W
Working temperature	-10°C ~ 50°C
Storage temperature	-20°C ~ 70°C
Button	Physical type; Green, red and blue LED lights
Casing Material	ABS, Calcium carbonate
Battery capacity	35mAh
Rechargeable	Yes

FEITIAN ePass FIDO® Series Security Key can also be used for 2-Step Verifications on the following service(s):

For further informations, please contact world.sales@ftsafe.com, or your service provider.

This manual was released on February 12, 2018.
For further update, please check on:
http://download.ftsafe.com/files/FIDO/Manual/ePass%20FIDO-Multi-Interface%20Manual.pdf,
or scan the QR code.

Feitian Technologies Co., Ltd.

www.ftsafe.com

FEITIAN
WE BUILD SECURITY