FEITIAN
WE BUILD SECURITY

ePass FIDO K13
PRODUCT MANUAL

V1.0

2016-02

FEITIAN Technologies Co., Ltd.

Website: www.FTsafe.com

Content

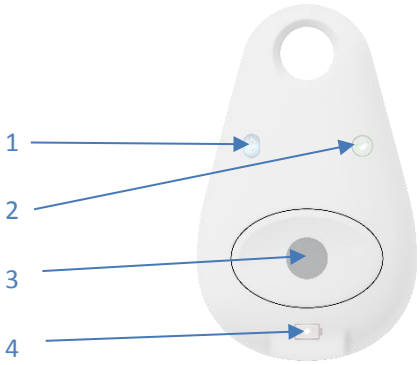
1. Overview

Feitian FIDO K13 is a FIDO alliance certified U2F security key. Feitian FIDO K13 is a Top Gear in the Feitian FIDO U2F Security Key family. NFC, BLE and USB, K13 employees three interfaces for conducting communications with authenticating devices. Users are allowed to use any of these interfaces to complete the FIDO U2F registration and verification. FIDO K13 brings the most stable and compatible experiences to the users.

2. Product Views

a) Casing Views

b) Casing Introduction



1	BLE indicator. This LED indicator lights up while the key is in pairing mode.
2	Authentication indicator. Any authentication request received will be passed while this LED is on.
3	Control button. Short press to power on. Long press for 5 seconds for entering pairing mode.
4	Battery indicator.

3. User Guide

3.1 BLE Pairing

1. Press and hold the button for 5 seconds till the BLE indicator is blinking, then release pressing. This authenticator keeps blinking for 15 seconds if there is not pairing request received.
2. ScanBLE devices on your client side (e.g. a smart phone). Connect the BLE device which has the same alphabetic name as printed on the back of the authenticator (As shown in the figure "TCQWLA").
3. Input 6-digits PIN as printed on the back of the authenticator(As shown in the figure " 440620

**For security purpose, the authenticator will be forced to shut down after 60 seconds after powered on.*

3.2Authentication

3.2.1 BLE mode

1. Short press the button to power on and enter BLE mode.
2. Make sure this authenticator has been paired with the client. The authentication indicator should start blinking. Any authentication request received will be responded automatically within a limited time (20 seconds). Pressing the button to refresh the timer.
   ** Using FIDO U2F with BLE mode on mobile devices requires middle ware. Using Chrome browser and Google authenticator is a good example.*

3.2.2 NFC mode

1. Make sure the device is off.

2. Request authentication from the client device.

3. Attach the key to the NFC sensor.

** Using FIDO U2F with NFC mode on mobile devices requires middle ware. Using Chrome browser and Google authenticator is a good example.*

3.2.3 USB mode

1. Connect the authenticator with your client PC by using the attached USB cable.

2. The authentication indicator will blink when an authentication request is received.

3. Press the button to confirm this authentication.

4. Specification

ePass FIDO K13	
Specification	Value
OS	Windows, Linux, OS X
Certifications	FIDO U2F
Embedded security algorithm	ECDSA, SHA256
Size	47.29mm*29.32mm*8.34mm
Max number of keys	No limit
Interface type	USB, NFC (Receiving), Bluetooth
Data storage life	At least 10 years
Erasing times	100,000 times
Communication protocol	HID
Working voltage	5.0V (USB)
Working current	22mA (USB)
Power	0.11W (USB)
Working temperature	-10℃ — +50℃
Storage temperature	-20℃ — +70℃
Button	Physical type; Green, red and blue LED lights
Case Material	ABS

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.

The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

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.

Radiation Exposure Statement

This equipment complies with FCC Radiation exposure limits set forth for an uncontrolled environment.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.