



FIDO2 Fingerprint Security Key



Fingerprint-enabled Security Key + Smart Badge

- * Passwordless Login to Azure AD or FIDO2 Services
- * Standalone Enrollment + Card Lock Mechanism
- * Keep Badge Personal- Fingerprint Matching to Boost NFC for Permission to Door Locker and No Need to Upgrade Equipments





3-Way Authentication

App

About ATKey.Card

Page 2

Outlook

Page 3

3 Steps Quick Start

Page 5

USB

Page 6

BLE

Page 7

NFC

Page 8

LED

Page 10

Fingerprint Enrollment

Page 11

App – ATKey for Windows

Page 15

FIDO2: Azure AD

Page 19

FIDO2: Microsoft Account

Page 21

NFC Access Control

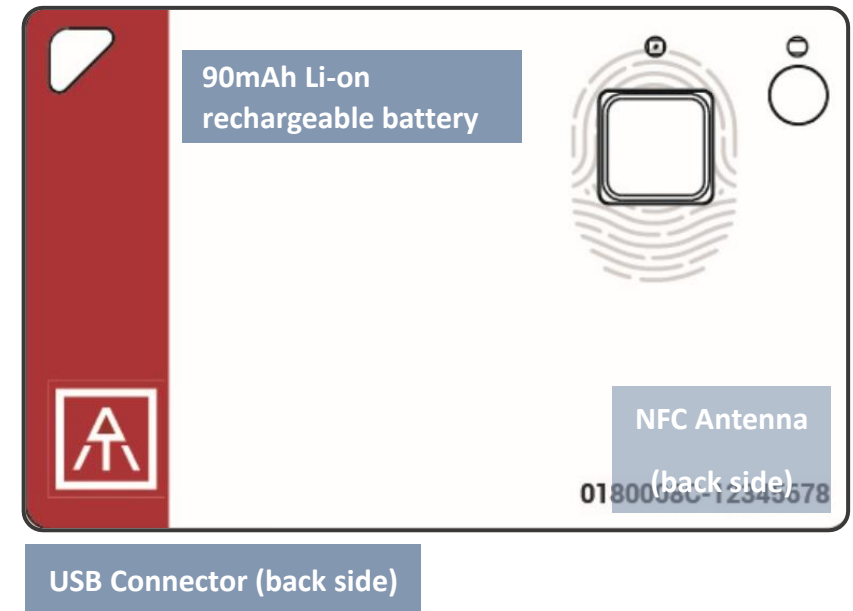
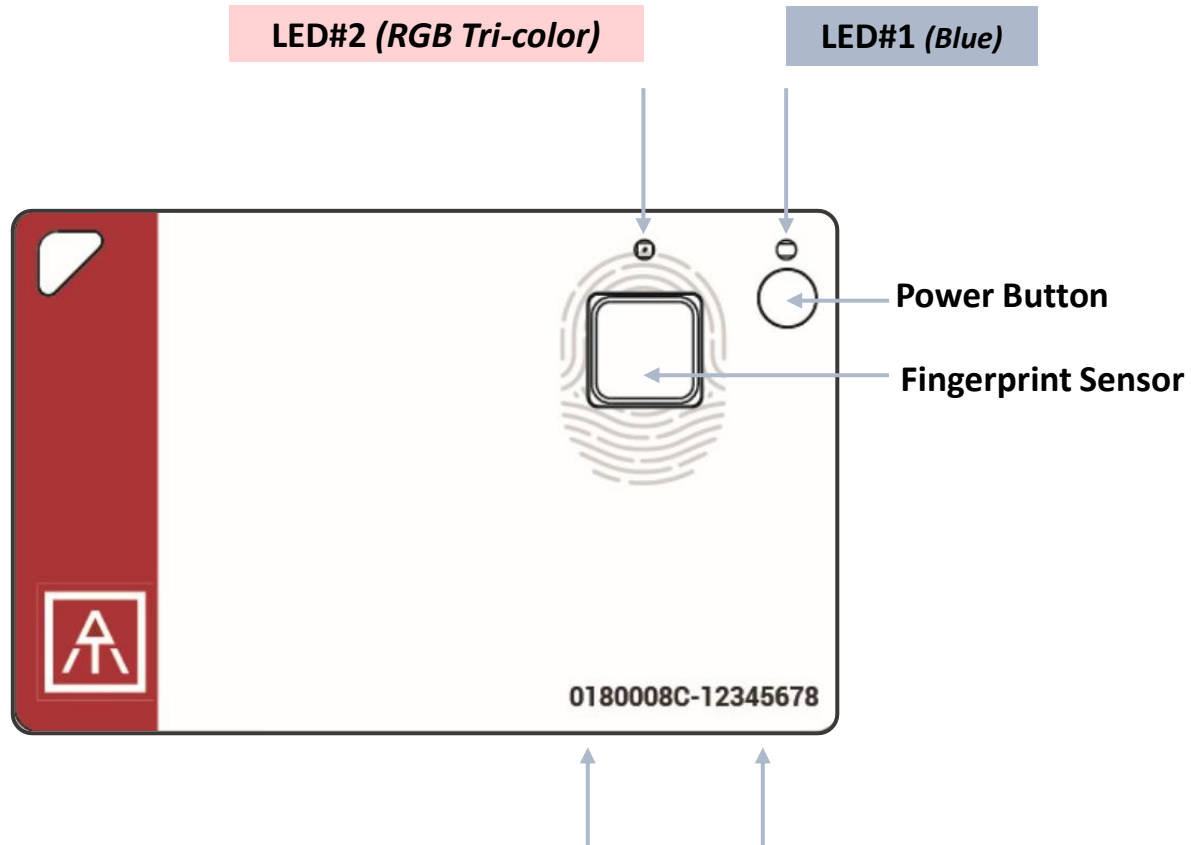
Page 27

Regulations

Page 28

- USB HID + BLE + NFC device, no driver needed
- Portable key for any Windows, Mac or Chromebook
- Up to 8x fingerprints, matching < 1 sec., FAR < 1/50,000, FRR < 2 %
- FIDO2 certificated





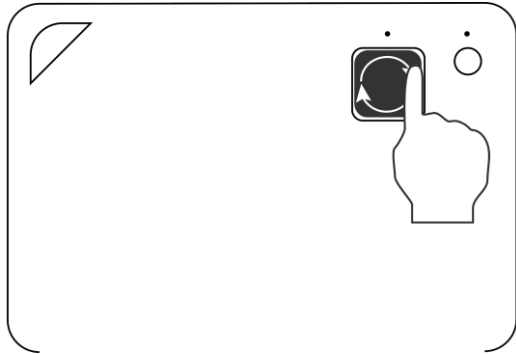
- Each key has his own unique keycode
- It's equal to serial number
- Check keycode for production records, customer service and also warranty

Keycode **Mifare ID,** (ISO14443 Mifare TypeA)
8 Digits



Step 1

Enroll Fingerprint to ATKey



1. Standalone Enrollment (Patent Filing)
<https://www.youtube.com/watch?v=wyxdFyRYcog>
2. Windows Settings (build 1903)
3. "ATKey for Windows" app

-Please check from page 12

Step 2

Register ATKey to Device or Service

FIDO2

Azure AD Passwordless login

Passwordless login Microsoft account or other
FIDO2 authentication via Browsers on Windows ,
Mac and Chromebook

You can find FIDO security key readiness services from here:
<https://www.dongleauth.info/>

Login Google, Facebook, Dropbox, Salesforce,
Gitlab via Chrome browser as 2nd factor

Check here for ATKey compatible FIDO enabled services
<https://authentrend.com/compatible-with-atkeys/>

Step 3

Fingerprint Matching for Authentication

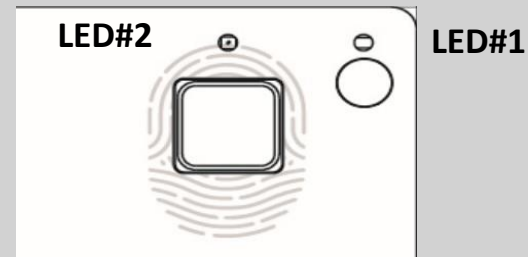


- USB 2.0 Type A (HID) is both for data transfer and charging functions.
- Plug USB connect out from backside, insert it into USB port.
 - If ATKey.card connected to USB port but nothing happened (no LED ON); Please wait for a while since there is a protect circuit to make sure the battery voltage is not lower than 3.0V.

What we can do with USB:

- **Add/Delete fingerprint**
 - “ATKey for Windows” App
 - Windows Settings
- **Firmware version**
 - “ATKey for Windows” App
- **FIDO2**
 - USB security key for Windows, Mac and Chromebook via Edge, Chrome, Firefox, etc.
 - Azure AD Passwordless login
- **Battery charge**

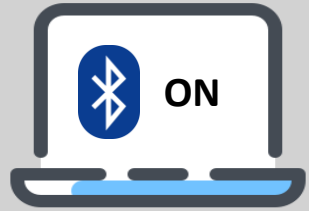
LED indicator in USB mode:



LED#1	LED#2	
ON	OFF	USB mode Battery is 100% charged
ON	flashing	Battery charging
flashing		Waiting for fingerprint verification
OFF	OFF	Battery voltage is lower than 3.0V, please wait for a while doing battery charges until LED#2 showing yellow flashing



- BLE mode:
Pairing your target device with ATKey.Card



Device (Windows, Mac, Chromebook, iOS, Android) or App is ready for pairing



- Power on ATKey.card
- Double-click power button to secure pairing mode (LED#2)

- Scan and find specific card – check the keycode to identify the card
- Select it to pair

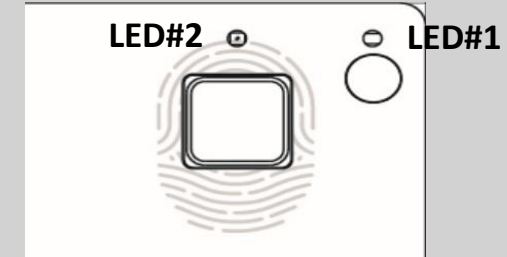
- Touch fingerprint sensor to confirm the pairing (LED#2)

What we can do with BLE:

- Add/Delete fingerprint**
 - “ATKey for Windows” App
- Firmware version**
 - “ATKey for Windows” App
- FIDO2**
 - BLE security key for Windows, and Chromebook via Edge, Chrome, Firefox, etc.
 - Azure AD Passwordless login

**** Mac and Safari are not enabled BLE FIDO2 key support**

LED indicator in BLE mode:



LED#1	LED#2	
ON	Flashing	BLE broadcasting
ON	ON	BLE connected to device
flashing	ON	BLE connected and wait for fingerprint verification
ON	flashing	BLE secure pairing mode
ON	flashing	Touch fingerprint sensor to confirm the pairing
ON	Slow flashing	Battery low – please do battery charging via USB



- Work with Mifare Type A (ISO 14443 / for 13.56MHz NFC reader)
 - NFC card reader
 - Android Phone
 - NFC access control
 - NFC door locker
- NFC default is off, only boost after fingerprint matching for 15 seconds.
 - 8-digits unique Mifare ID
 - App is running on JavaApplet

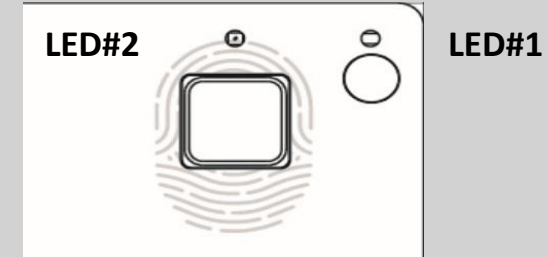
What we can do with NFC:

- FIDO2 (via JavaApplet) – by demands
 - NFC security key for Windows, Mac and Chromebook via Edge, Chrome, Firefox browsers
 - Azure AD Passwordless login
- NFC access control or door locker (via MiFare ID)
 - Power on ATKey.Card → Verify fingerprint to turn NFC ON → Approach reader to unlock; NFC will be ON for 15 seconds

If ATKey.card is in USB mode or BLE connected mode, NFC won't be enabled

**** Mac and Safari are not enabled NFC FIDO2 key support**




LED indicator in NFC mode:



LED#1	LED#2	
flashing	Flashing	Verify fingerprint to enable NFC
ON	ON	NFC is ON

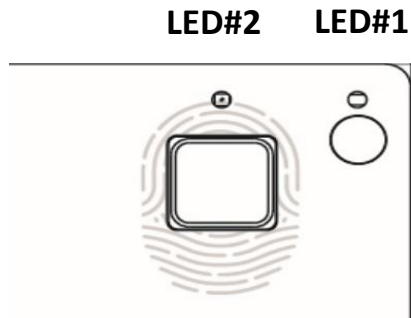
Note:

After Power ON, BLE will start to broadcast. It needed you to verify fingerprint, NFC will then be turned ON for 15 sec.; BUT if BLE connected, fingerprint matching is for BLE; if your host is PC (Windows or Chromebook), we recommend turning off your Bluetooth of PC to avoid BLE/NFC conflicts to Card.

			
	BLE	USB	NFC
Enroll fingerprint	✓	✓	
Azure AD logon (FIDO2)	✓	✓	✓
Windows 10 <u>build 1903</u> or later version	✓	✓	✓
• FIDO2 (Edge, Chrome)			
• FIDO2 registration	✓	✓	
• FIDO2 authentication	✓	✓	✓
Android:			
• FIDO2 (Chrome browser on Android)	✓		✓
• U2F (Chrome browser on Android)			
iOS:			
• FIDO2 (Safari)			✓
Mac OS FIDO2 and U2F via Chrome browser		✓	
Chromebook FIDO2 and U2F via Chrome browser	✓	✓	✓
NFC door locker (Mifare TypeA)			✓

For ATKey.Card, we recommend to register fido services via USB or BLE interface on Windows (or Mac via USB), then you can do authentication via

- USB/BLE on Windows,
- USB on Mac,
- NFC on iOS and Android.

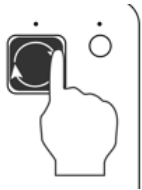


LED#1	LED#2	
ON	ON	<ul style="list-style-type: none"> Normally this is BLE issue (BLE connected, fingerprint verified, but still waiting response from Host) Please re-boot the card (long-press power button to power off, then click power button to power ON)
-	Slow flashing	<ul style="list-style-type: none"> Battery low, please do battery charge via USB
flashing (waiting for fingerprint matching)	ON for 1 sec. ON for 1 sec.	<ul style="list-style-type: none"> Fingerprint matching failed Fingerprint matched, and NFC is ON (if it's not in USB or BLE connected)
ON	flashing	<ul style="list-style-type: none"> Request to confirm the BLE pairing Touch fingerprint sensor to confirm the pairing
		<ul style="list-style-type: none"> If this happens on "standalone mode" (click power button 3x times), please enroll your fingerprint (there is no fingerprint template inside the card)
ON	flashing	<ul style="list-style-type: none"> If this happens on "standalone mode" (click power button 3x times), please do fingerprint matching first (fingerprint already enrolled into card), then you can start to enroll new fingerprint
ON	flashing OFF	<ul style="list-style-type: none"> Battery charging Battery charge full, stop charging
OFF	OFF	<ul style="list-style-type: none"> (power on but no LED ON) very low battery, please do battery charge and wait till LED is ON



Standalone enrollment

- Power on ATKey.Card
- Check Youtube video here for the detail:
<https://youtu.be/RmBJXXVXXH8>
- LED#1 is BLUE ON, quick click power-button 3x times to go into enrollment mode:
 - If there is no any fingerprint enrolled, LED#2 turns to WHITE
 - If there are any enrolled fingerprints, LED#2 is GREEN flashing, please verify enrolled fingerprint to start enrolling new finger
- Put your specific finger on sensor, touch fingerprint sensor circle and slow (LED is WHITE flashing, from slow to faster), till LED shows GREEN, then your fingerprint is enrolled



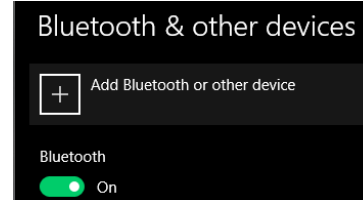
- If you want to quit from standalone enrollment, click power button once, LED will turn to Blue, back to normal state.

Enroll from Windows Settings

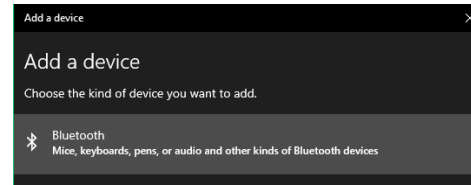
- If your OS is Windows 10 build 1903 or later versions, you can manage ATKey as security key through Windows Settings

(BLE) Pair ATKey with your Windows first

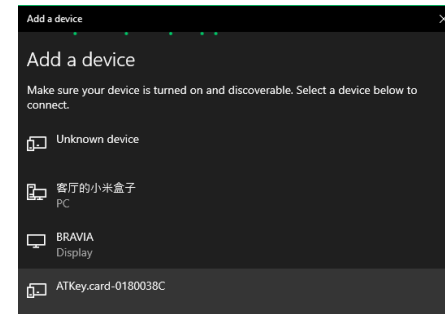
- Through Windows Settings => Device => ADD Bluetooth or other device



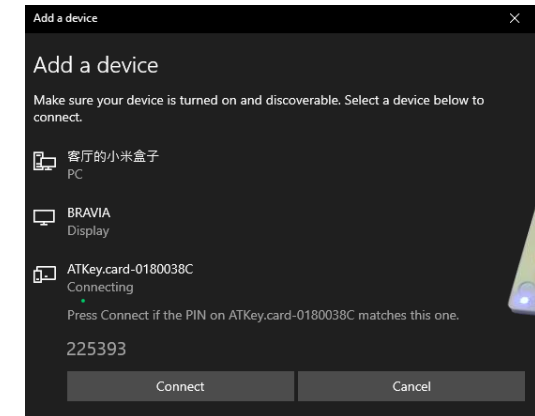
Add a device - Bluetooth



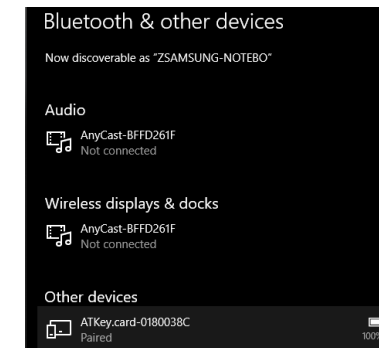
- Power on ATKey, double-click power button to BLE secure pairing mode (LED#2 is cyan flashing), then you will see the ATKey.card showing (ATKey.card-keycode)



- Click target ATKey.card, click "Connect" from UI and touch fingerprint sensor (LED#2 is white flashing) to confirm the pairing



- Then ATKey is paired with battery indicator (OS 1903 build or later version)



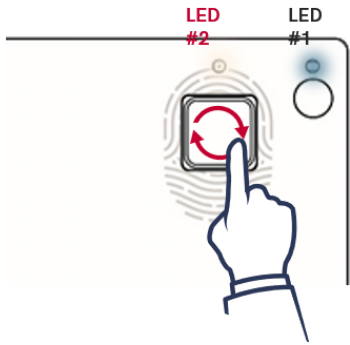
- **Or you can skip BLE pairing, just using USB for fingerprint enrollment**
- Go to **"Windows Settings (OS build is 1903 or later version) – Enroll fingerprint"** page for the detail



With no need for any device or application download.

- Please enroll a fingerprint at the same place If you have already set up a PIN using any previous method.
You can enroll your fingerprint directly using this method only if you have not yet set up a PIN or you want to add more fingerprints.

Standalone enrollment



- Power on your ATKey.Card.
- LED#1 Blue ON.
- Press the side button 3 times quickly.
- LED#2 turns WHITE.
- Touch the sensor in a circular motion,
LED#2 will change from slowly flashing to faster flashing.
- LED Green ON, enrollment is complete.

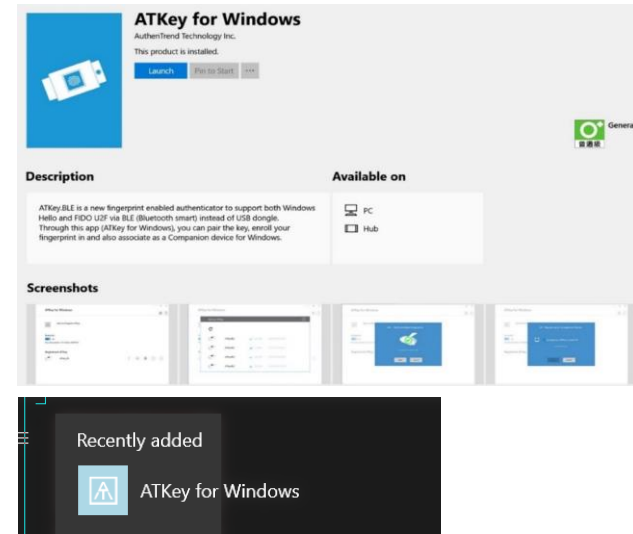


Tutorial video

- If you want to quit "standalone enrollment", press the button and the LED will turn to Blue, back to the normal state.
- If there are any enrolled fingerprints in your ATKey.Pro, LED#2 will Green flash first on step 4, that you need to verify registered fingerprint to start enrolling new finger.

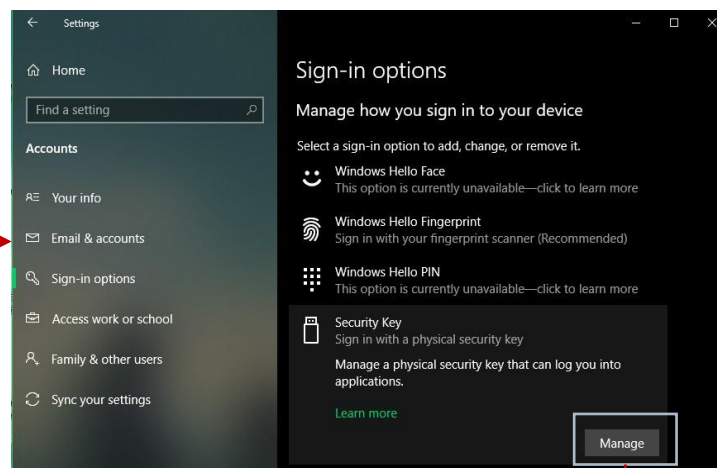
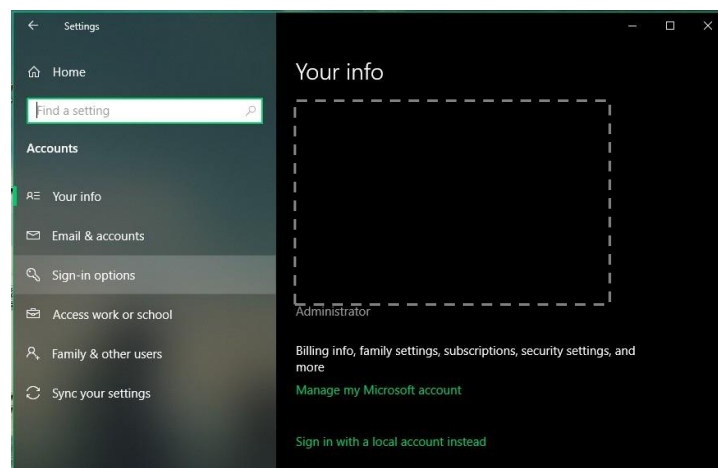
Enroll from ATKey for Windows App

- Download "ATKey for Windows" app from Windows Store to manage ATKey:
 - Enroll fingerprint
 - Add/delete fingerprint
 - ATKey information
 - Companion ATKey to Windows (Windows Hello login)
- Search "ATKey" or "AuthenTrend" from Windows Store to find the app, download and install

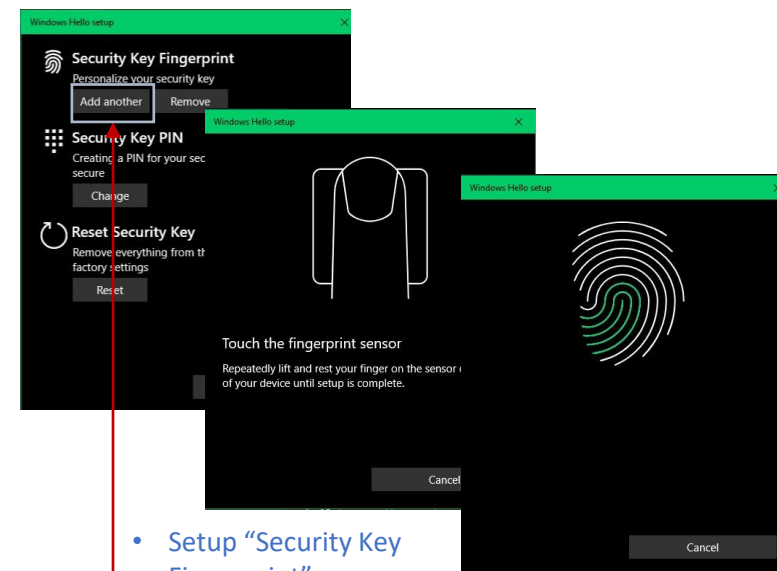


- Jump to ["ATKey for Windows" for the detail](#)

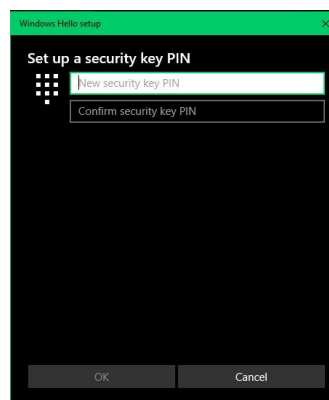
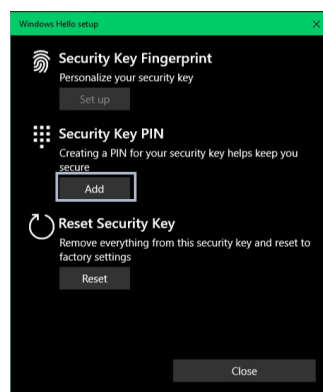
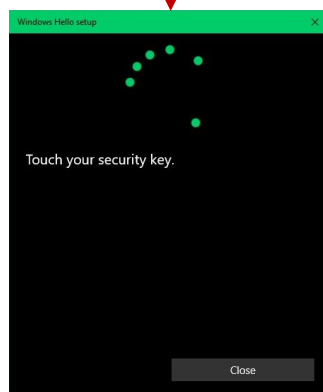
- Windows Settings => Account => Sign-in options => Security Key => **add “PIN code” and enroll “Fingerprints”**
- It works for both USB and BLE interface (for BLE, please double-click power button to BLE pairing mode to pair with Windows)



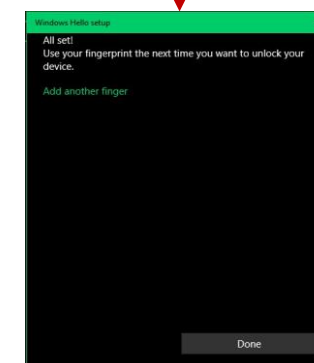
Click “Manage”,
touch fingerprint sensor to setup



- Setup “Security Key Fingerprint”
- Type-in PIN code, following screen hint to enroll fingerprint, until “All Set!”

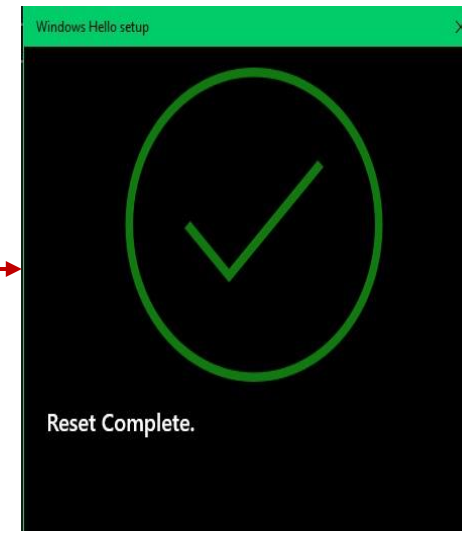
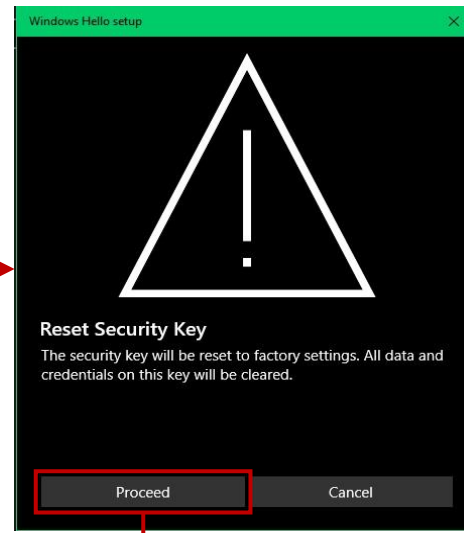
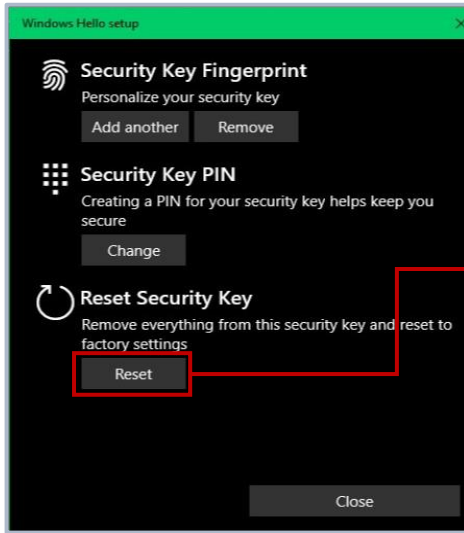


Add “Security Key PIN”
first; this PIN code will
write into ATKey.Pro





- Windows Settings => Account => Sign-in options => Security Key => **Reset Security key (Delete PIN code and erase all fingerprints)**



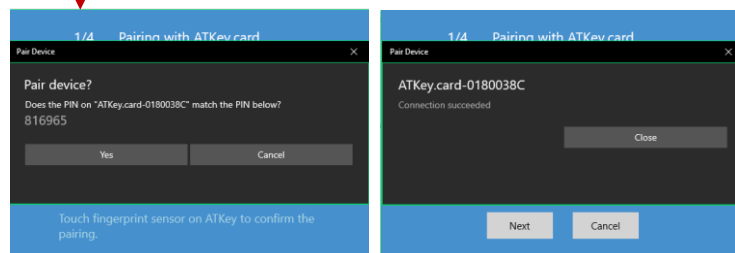
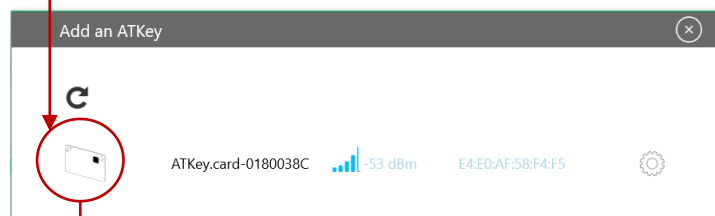
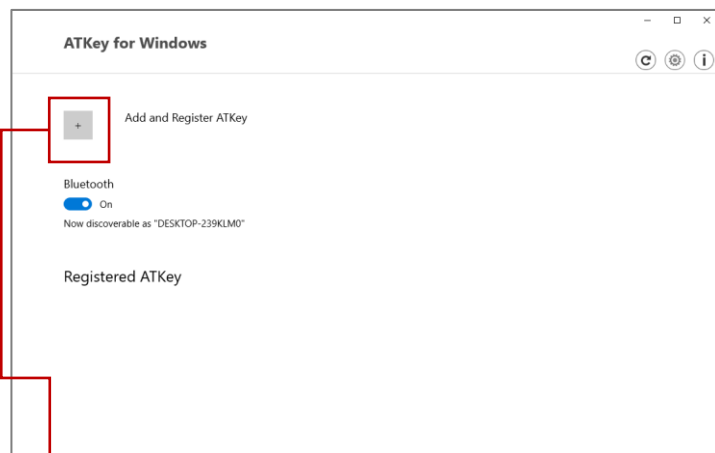
Power on ATKey.card, doing “reset” within 10 seconds (after card booting), this is Microsoft rule

Touch fingerprint to confirm reset;
Not verified enrolled fingerprint to rest, this designed for IT Administrator

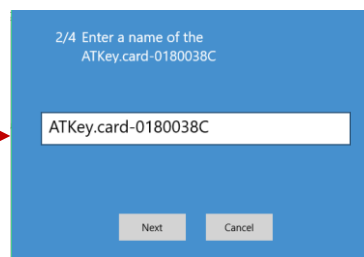
Microsoft required spec.- for authenticator reset: in order to prevent accidental trigger of this mechanism, user presence is required. In case of authenticators with no display, request MUST have come to the authenticator within 10 seconds of powering up of the authenticator.



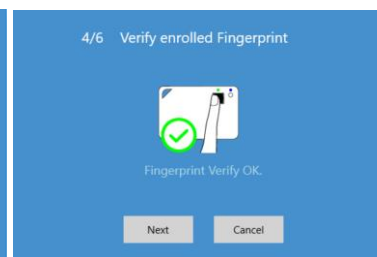
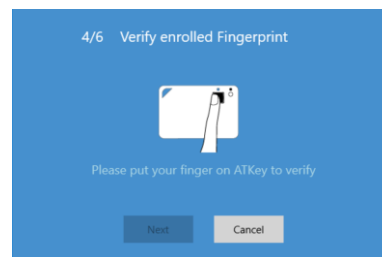
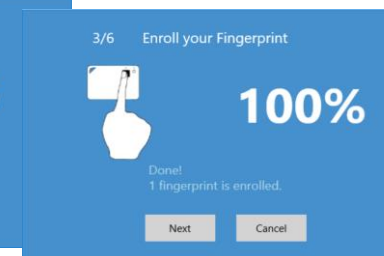
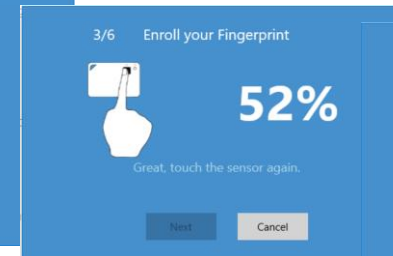
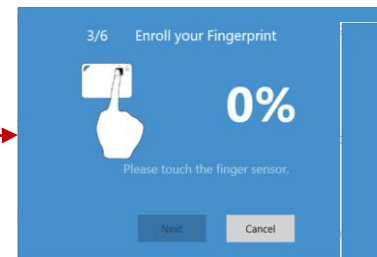
- Launch “ATKey for Windows” App (version 2.0.55.0 or later version)
- Click “Add and Register ATKey” – please make sure ATKey is ON (LED#1 blue ON, LED#2 blue flashing)
 - **Double-click power button** to secure pairing mode (LED#2 is cyan flashing)



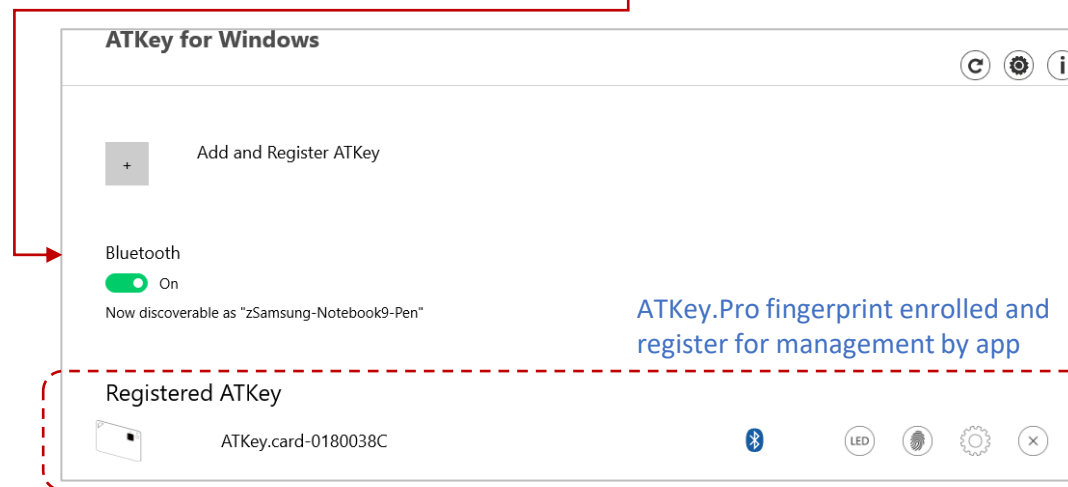
LED#2 is WHITE flashing, touch fingerprint to confirm the pairing, and also click “Yes” from UI.



Default name is -: ATKey.card + Keycode



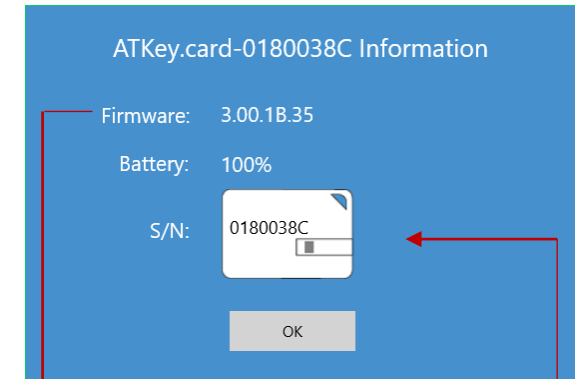
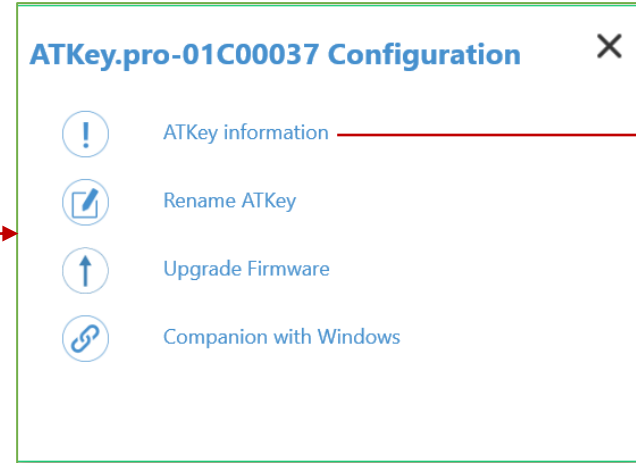
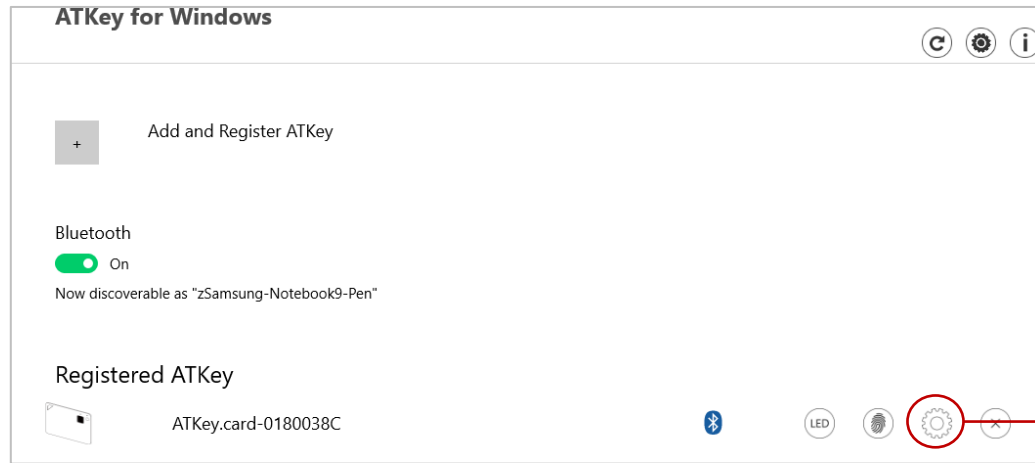
Verify enrolled fingerprint to confirm



ATKey.Pro fingerprint enrolled and register for management by app

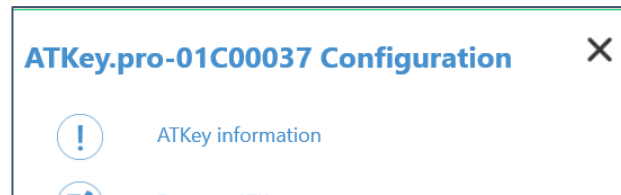
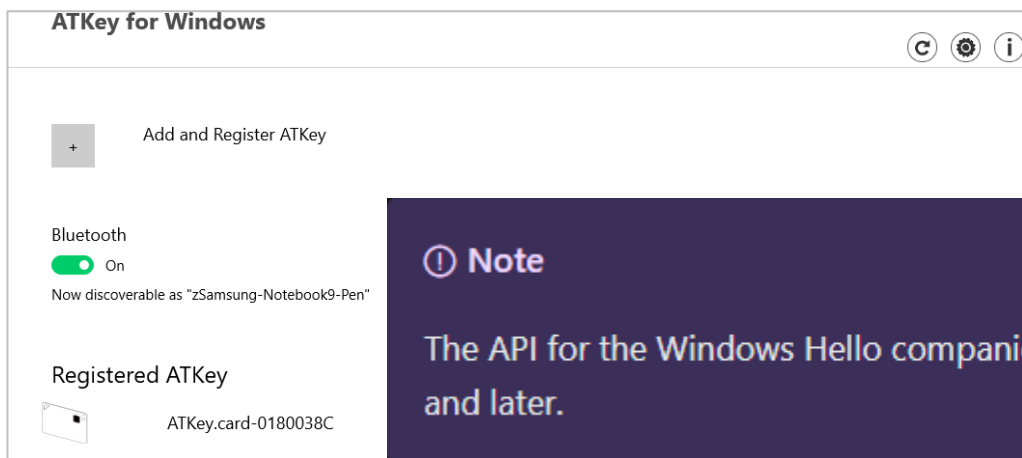


- ATKey management – information, rename



- read firmware version here
- Read “keycode” here

- ATKey management – Companion with Windows (Windows Hello login via CDF)
- *If your Windows 10 joined Azure AD, please ignore this page since FIDO2 is ready for Azure AD login, it may conflict with Windows Hello*



Guidelines for Windows Hello:

- [Windows Unlock with Windows Hello companion devices](#)
- [How to Enable or Disable users to use Companion device to sign in to](#)

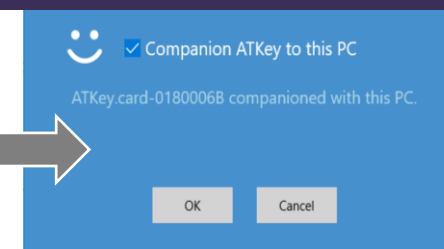
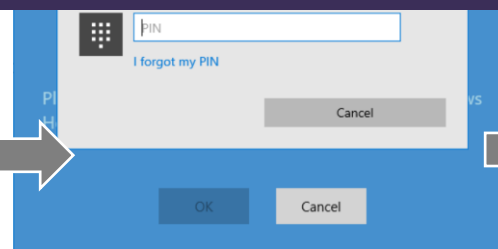
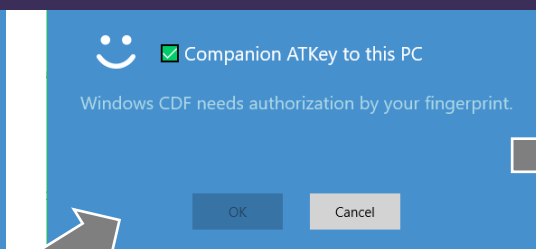
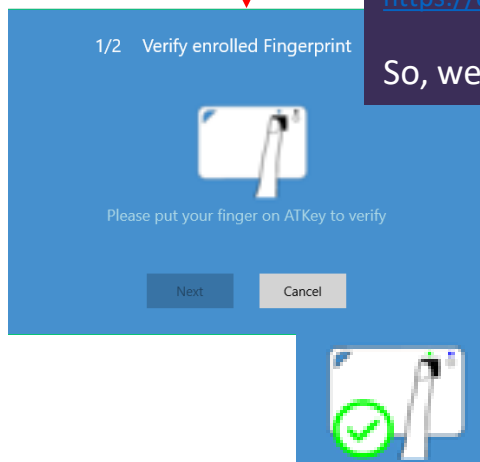
[How to Enable Domain users to use Companion device to sign in to Windows 10](#)

Note

The API for the Windows Hello companion device framework is deprecated in Windows 10, version 2004 and later.

<https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-companion-device-framework>

So, we won't continue support this feature due to it's relative to your OS build and also environment!!



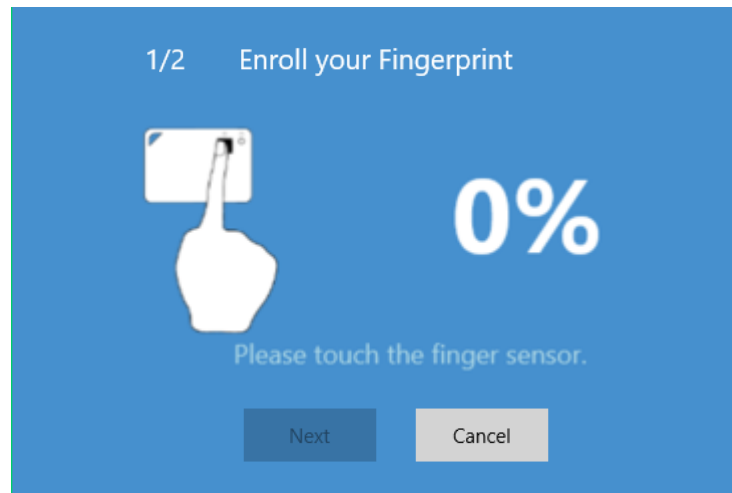
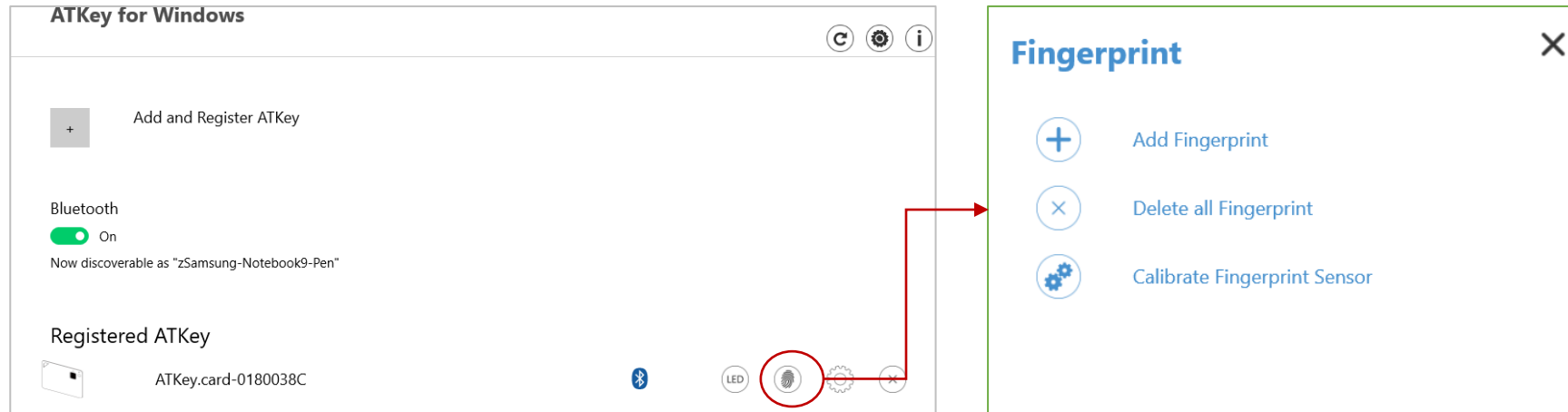
- **Type in “Windows Hello PIN” to allow the companion;**
- *Some Corp. or Org. may disable this group policy by IT Admin, if you saw the message, please contact your IT.*



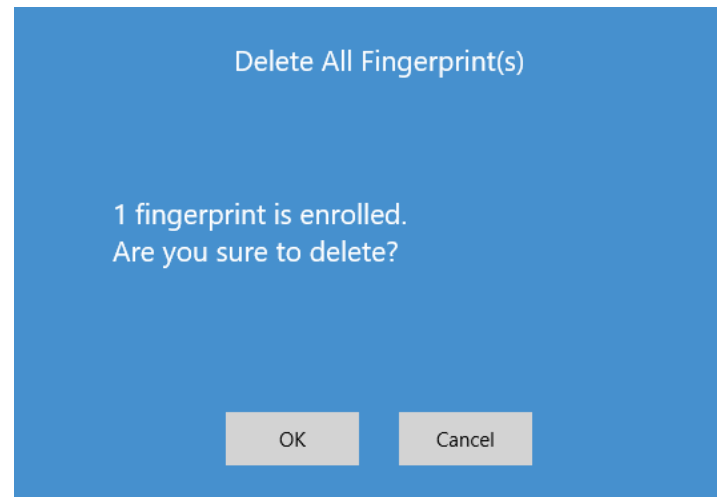
This icon means it's a companion key for Windows Hello via CDF (Companion Device Framework)



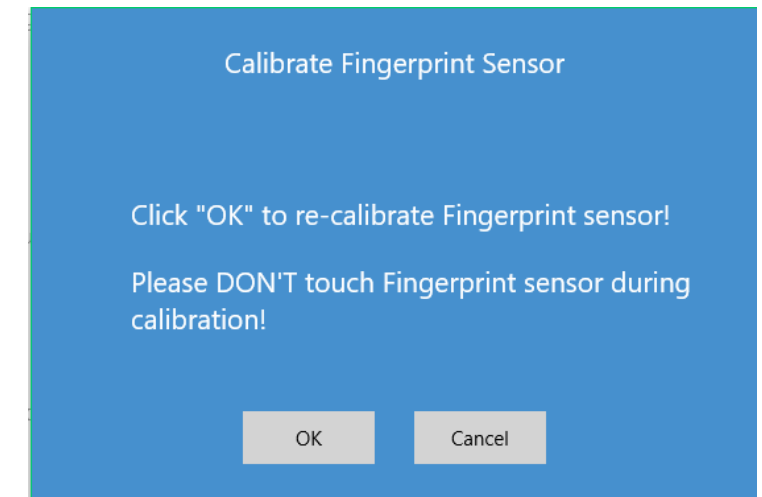
- ATKey management – Add/Delete fingerprints, fingerprint sensor calibration



- Enroll new fingerprint in by ~12 times touch, following UI message; up to 10x fingerprints



- Here will delete all enrolled fingerprints, "OK" to delete them
- It needs Windows PIN code to authorize.



- If you feel something wrong of fingerprint, doing Calibration to re-calibrate the sensor
- Don't put your finger on during calibration; LED will be WHITE flashing then back to Blue



- Does your company/org. license Azure AD?
- If yes, does your authentication policy allow “add method” including “security key”?
- Please check below links to learn how to enable security key for Azure AD:
 - [Passwordless Security Keys](#)
 - [Passwordless Windows 10](#)
 - [Passwordless On-premises](#)
 - [Passwordless authentication options – Security Key](#)

1. A new Authentication methods blade in your Azure AD admin portal that allows you to [assign passwordless credentials](#) using FIDO2 security keys and passwordless sign-in with Microsoft Authenticator to users and groups.

METHOD	TARGET	ENABLED
FIDO2 Security Key	1 user, 1 group	Yes
Microsoft Authenticator passwordless sign-in	All users	Yes

FIDO2 Security Key settings

ENABLE: ☒ Yes ☐ No

TARGET: ☒ All users ☐ Select users

USE FOR:

- Sign in
- Strong authentication

GENERAL

Allow self-service set up: ☒ Yes ☐ No

Enforce attestation: ☒ Yes ☐ No

KEY RESTRICTION POLICY

Enforce key restrictions: ☒ Yes ☐ No

Restrict specific keys: ☒ Allow ☐ Block

Add AAGUID

2. Updated capabilities in the converged Registration portal for your users to [create and manage FIDO2 security keys](#).

Wingtip Toys My Profile

Overview

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

+ Add method

Method	Device	Action
Microsoft Authenticator	Libby's iPhone 7	Delete
Microsoft Authenticator	iOS Demo Device	Delete
Security key		Delete

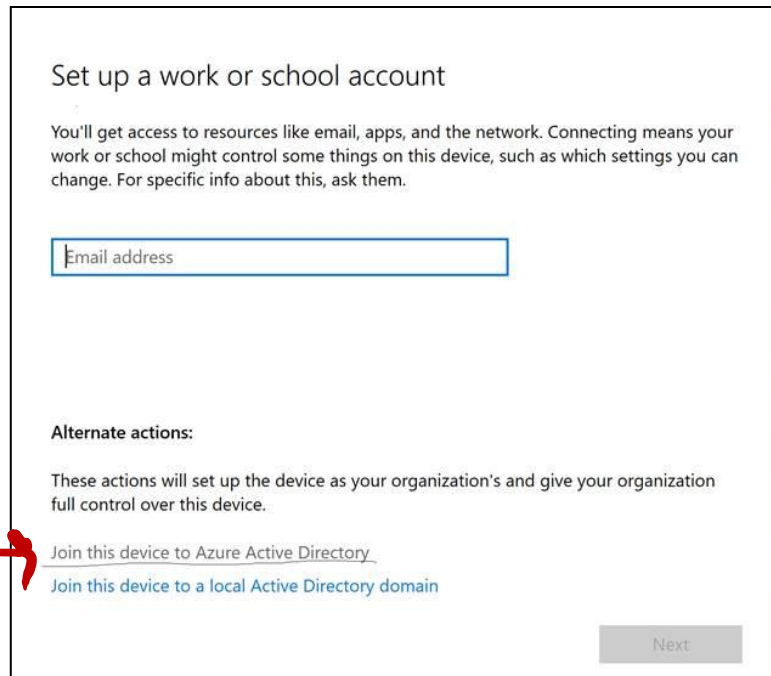
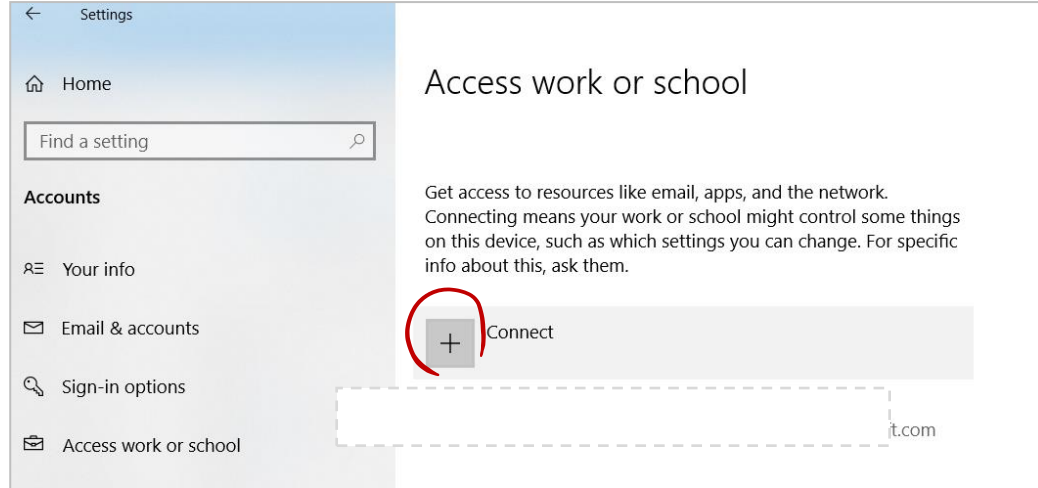
Lost a device? Require sign in

Add a method

Which method would you like to add?

Security key

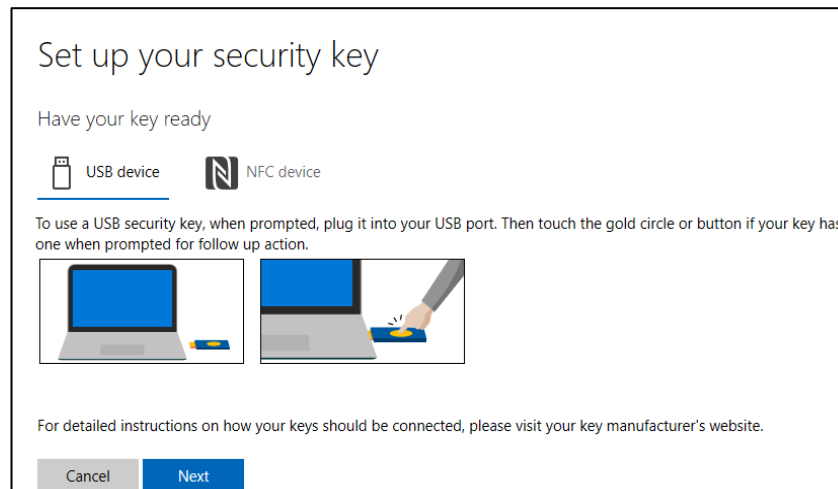
Cancel Add



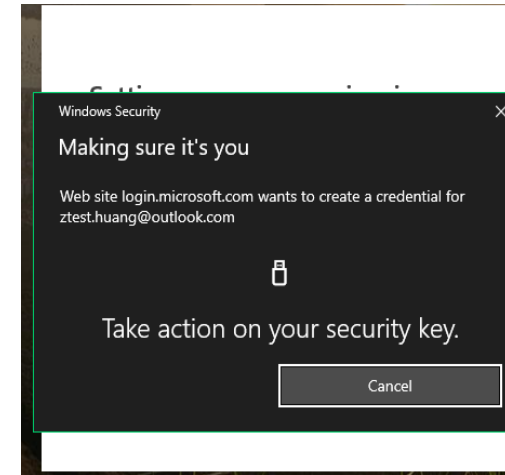
User registration and management of FIDO2 security keys

1. Browse to <https://myprofile.microsoft.com>
2. Sign in by ID/Password or app
3. Click **Security Info**
 - If the user already has at least one Azure Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key.
 - If they don't have at least one Azure Multi-Factor Authentication method registered, they must add one.
4. Add a FIDO2 Security key by clicking **Add method** and choosing **Security key**
5. Choose **USB device** or **BLE device**
6. Have your key ready and choose **Next**
7. A box will appear and ask you to create/enter a PIN for your security key, then perform the required gesture for your key either biometric or touch.
8. You will be returned to the combined registration experience and asked to provide a meaningful name for your token so you can identify which one if you have multiple. Click **Next**.
9. Click **Done** to complete the process

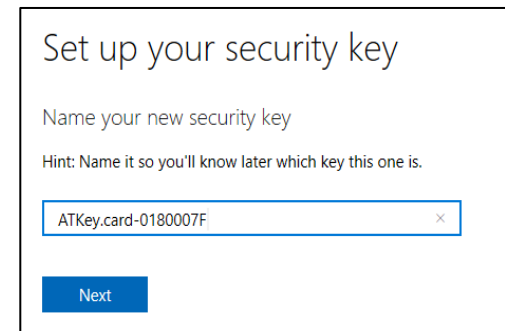
- Passwordless login Microsoft account by security key:
 - For Password-less login to Microsoft account - **Windows 10 build 1809** or later version via **Edge/Chrome browser, USB/BLE** mode:
 - You can login to add ATKey.Card as security key for your Windows account from here: <https://account.microsoft.com/account>
 - Login by ID/Password first
 - Step by step to setup security key (or check video: https://youtu.be/aSnJ8W_Oya4 to setup)
 1. Click “Security” from banner bar
 2. Click “**more security options**” from bottom
 3. From “Windows Hello and security keys” section, click “**Set up a security key**”



- Touch your enrolled fingerprint to verify



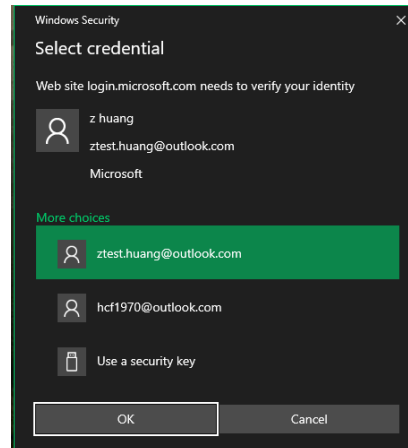
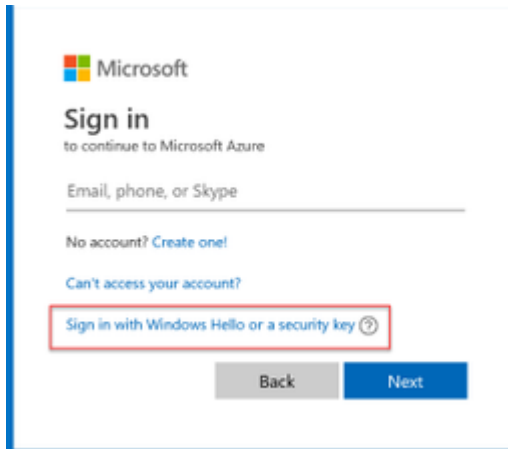
- Fingerprint matched, type in name of the key (default name following keycode)



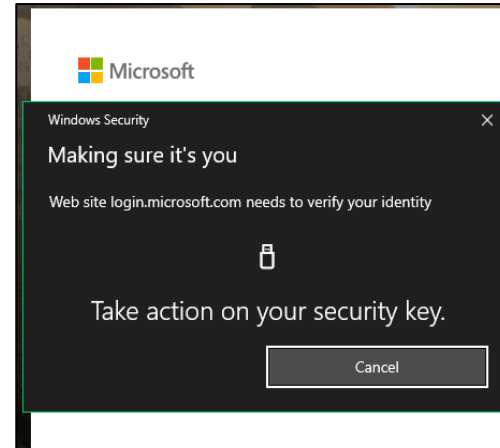
- You can find all your registered keys, click “**Manage your sign-in methods**”

Manage your sign-in methods			
NAME	SIGN-IN METHODS	ADDED ON	LAST USED
ATKey.card-0180007F	 Security key	1/16/2019 8:40 AM	1/16/2019 8:40 AM

- Sign-out to logon by security key (password-less)



Use security key



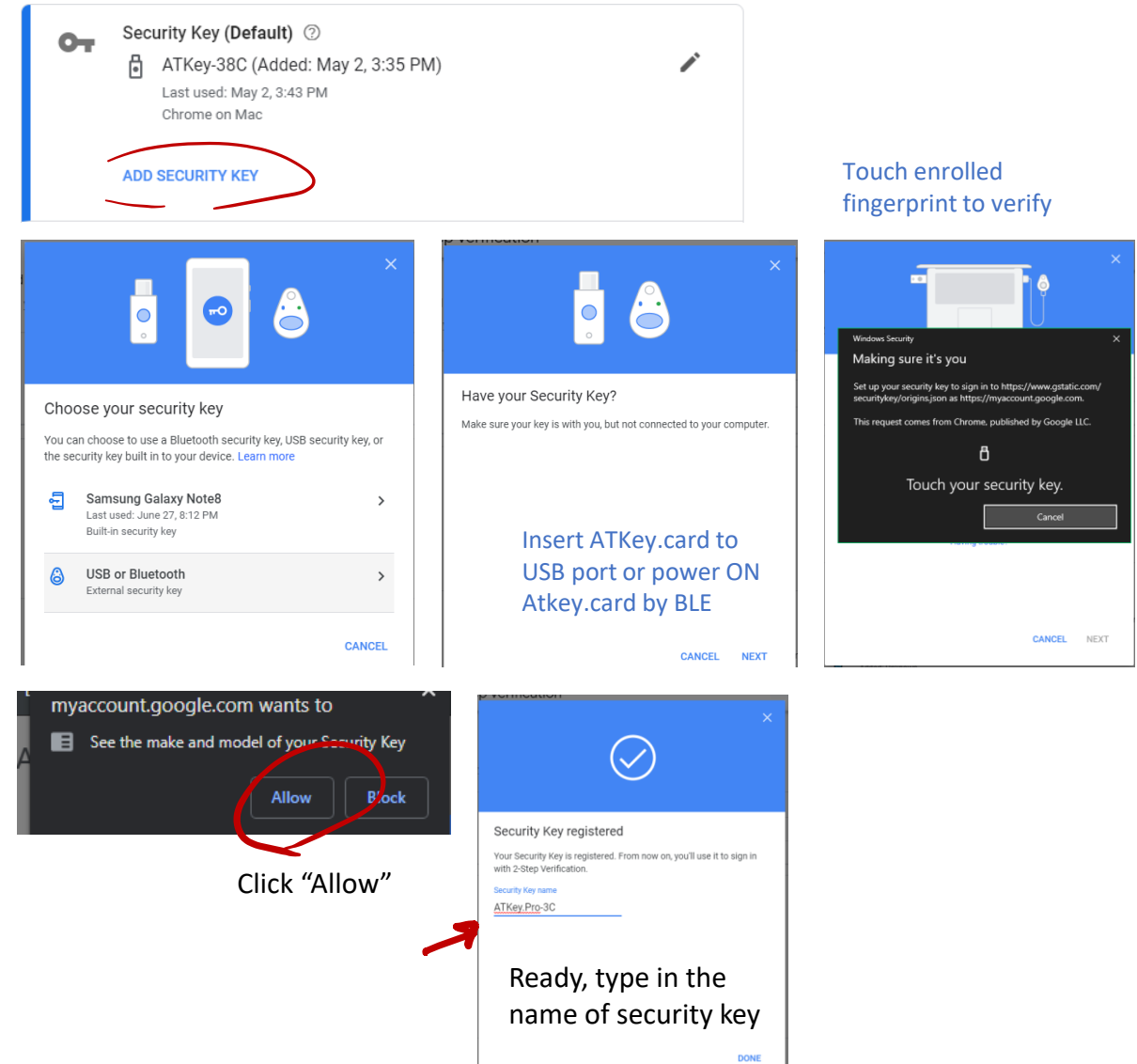
Fingerprint verified to login

- ATKey.Card is FIDO U2F ready, it can be a security key for 2nd factor authentication.
- Here are FIDO2 U2F ready service:

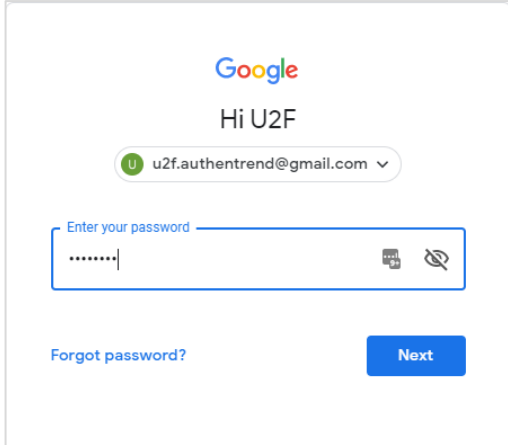


- Or you can search and find available FIDO U2F certified server here: <https://fidoalliance.org/certification/fido-certified-products/?appSession=8YT7Z25V0DOH6M41OQG26WI22N0F6D5MF9W19F58545OZWKJPBOH5XMB874A6596S8432G491GGF12B5Y7PIAM6PKR09S5G9Z3Q9T0FLK91C5445079DO1NWZFP8714Q>
- **But, Chrome browser only**
- **Google:**
 - Turn on 2-Step Verification, <https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en>
 - Use a security key for 2-Step Verification, <https://support.google.com/accounts/answer/6103523?co=GENIE.Platform%3DAndroid&hl=en>
- **Facebook:** <https://www.facebook.com/help/148233965247823>
- **Gitlab:** Enable 2FA via U2F device, https://docs.gitlab.com/ee/user/profile/account/two_factor_authentication.html
- **Salesforce:** https://help.salesforce.com/articleView?id=security_u2f_enable.htm&type=5
- **Dropbox:** <https://help.dropbox.com/teams-admins/team-member/enable-two-step-verification>

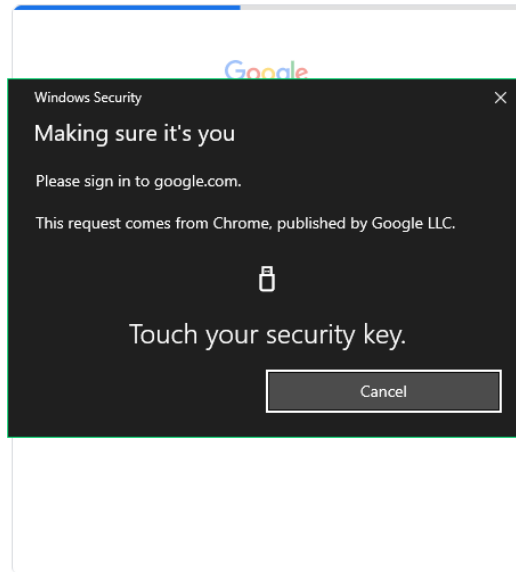
- (e.g.) Google account – add ATKey.Card as security to Google account:



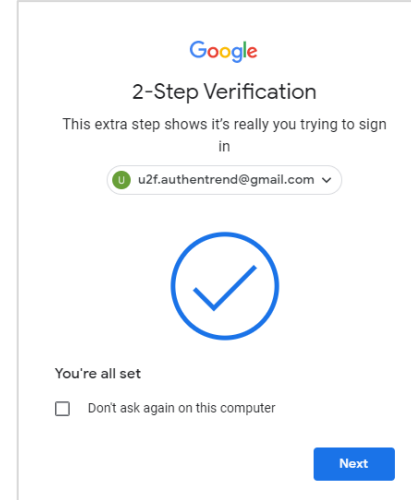
- (e.g.) Google account – login via ATKey.Card



1st factor: ID and password still



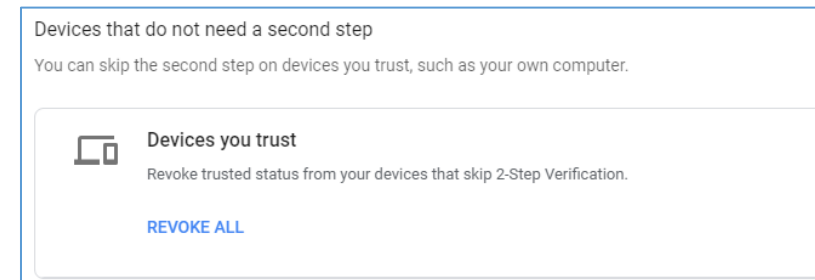
2nd factor: verify your enrolled fingerprint



Done and login!

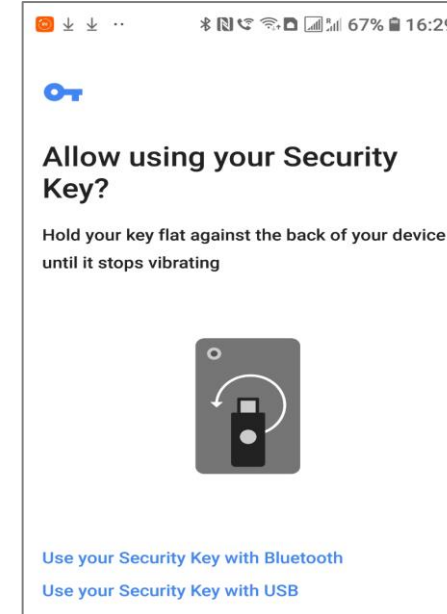
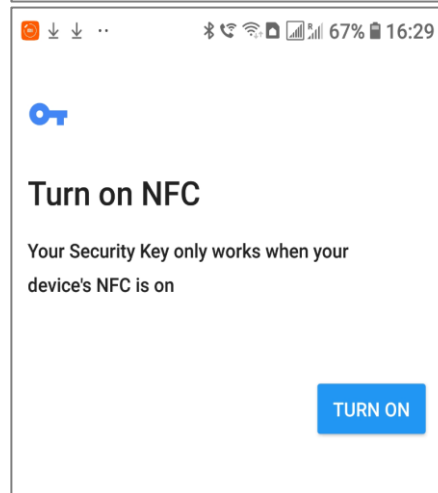
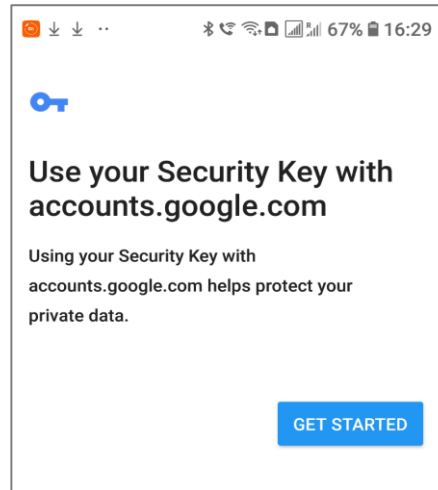
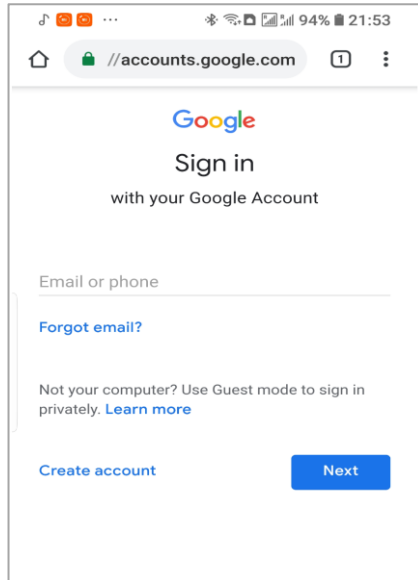
If you want to login your google account with ATKey later, please uncheck "Don't ask again on this computer" (default is checked).

But if you checked and login, but you want to use ATKey as 2nd factor to login again, please revoke all "device you trust" as below:



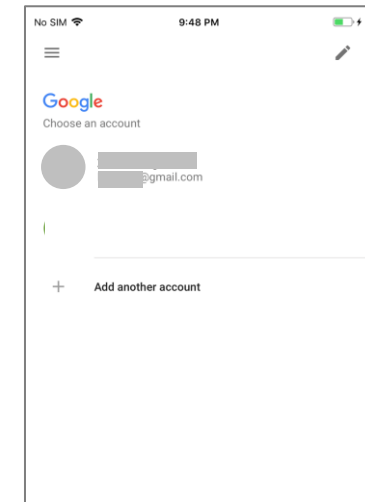
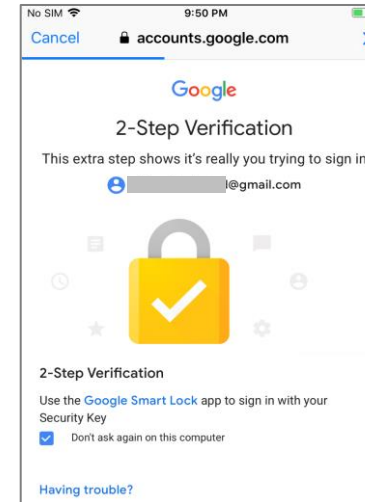
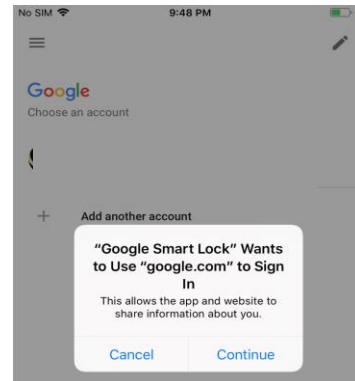
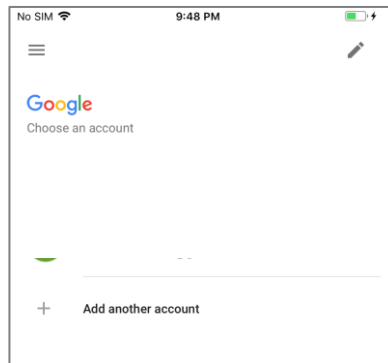
FIDO U2F via Android phone/tablet – Chrome browser

- Sign in Google account via Chrome browser
- Request Security Key and turn on NFC
- Authenticate via ATKey through NFC

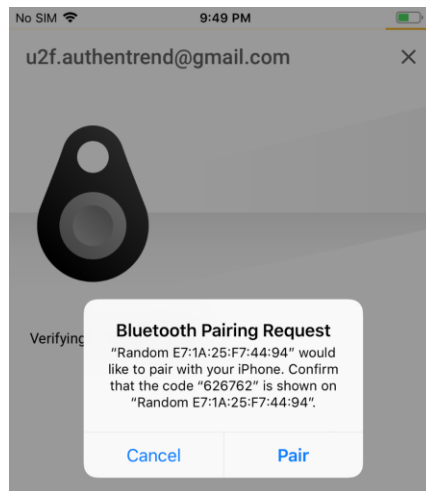


- Power on ATKey.card
- LED#1 is flashing, just touch fingerprint to verify to enable NFC (for 15 sec.)
- ATKey.card contacts Android Phone (back side) to send U2F token via NFC (JavaApplet) to Phone to server for authentication

- **FIDO U2F via iPhone/iPad (iOS) – app “Smart Lock” and Chrome browser**
- Download Smart Lock app from store
- Add your google account in

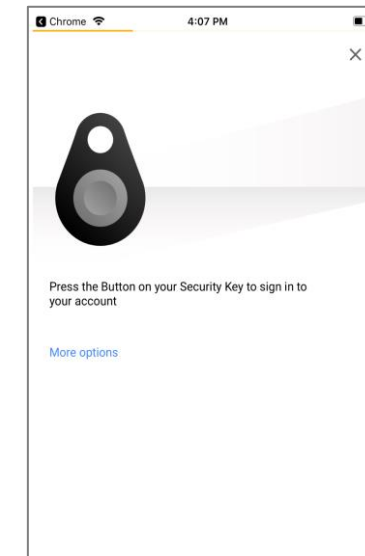
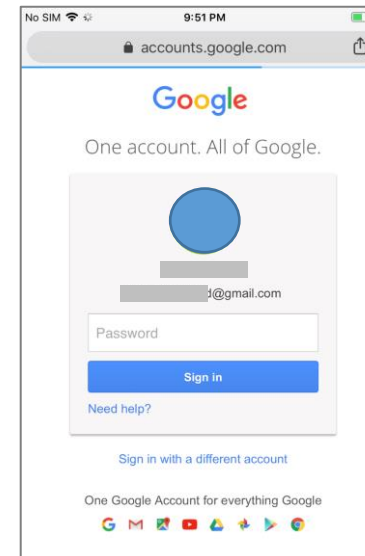


- **Pair ATKey**



- Double-click power button to secure BLE pairing mode (LED#2 is cyan)
- Touch fingerprint sensor to confirm pairing (LED#2 is WHITE)

- **Chrome browser – login your google account by U2F**



ATKey.card is a NFC tag type for ISO14443 & Mifare Type A NFC reader

- ATKey.card works for **13.56MHz** NFC reader
- Mifare ID is resident and unique ID inside SE/NFC chip
- For NFC door locker
 - If there is a “Mifare ID table” in the backend of NFC card reader (Door NFC reader), just need to copy Mifare ID of those specific cards
 - Or register ATKey.card to Mifare Type A NFC door locker



Mifare ID



FCC Label Compliance Statement:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

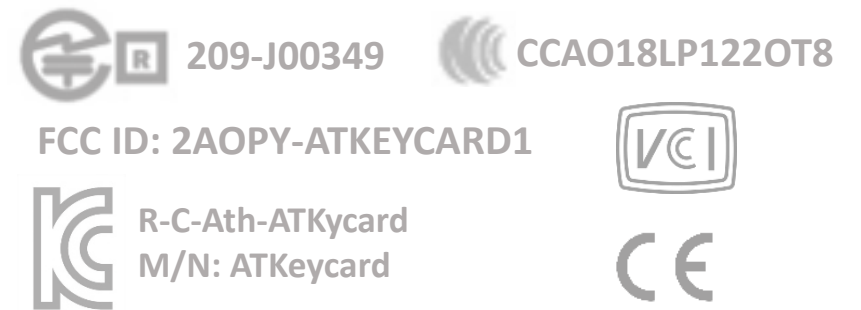
(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

To assure continued FCC compliance:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

Exposure to Radio Frequency Radiation:

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.



THANK YOU!



www.authentrend.com



contact@authentrend.com



[AuthenTrend](#)



[AuthenTrend](#)

AUTHENTREND