AUTHENTREND

-The trend of Authentication-

KEY. Card

User Guide *rev: 1.1*

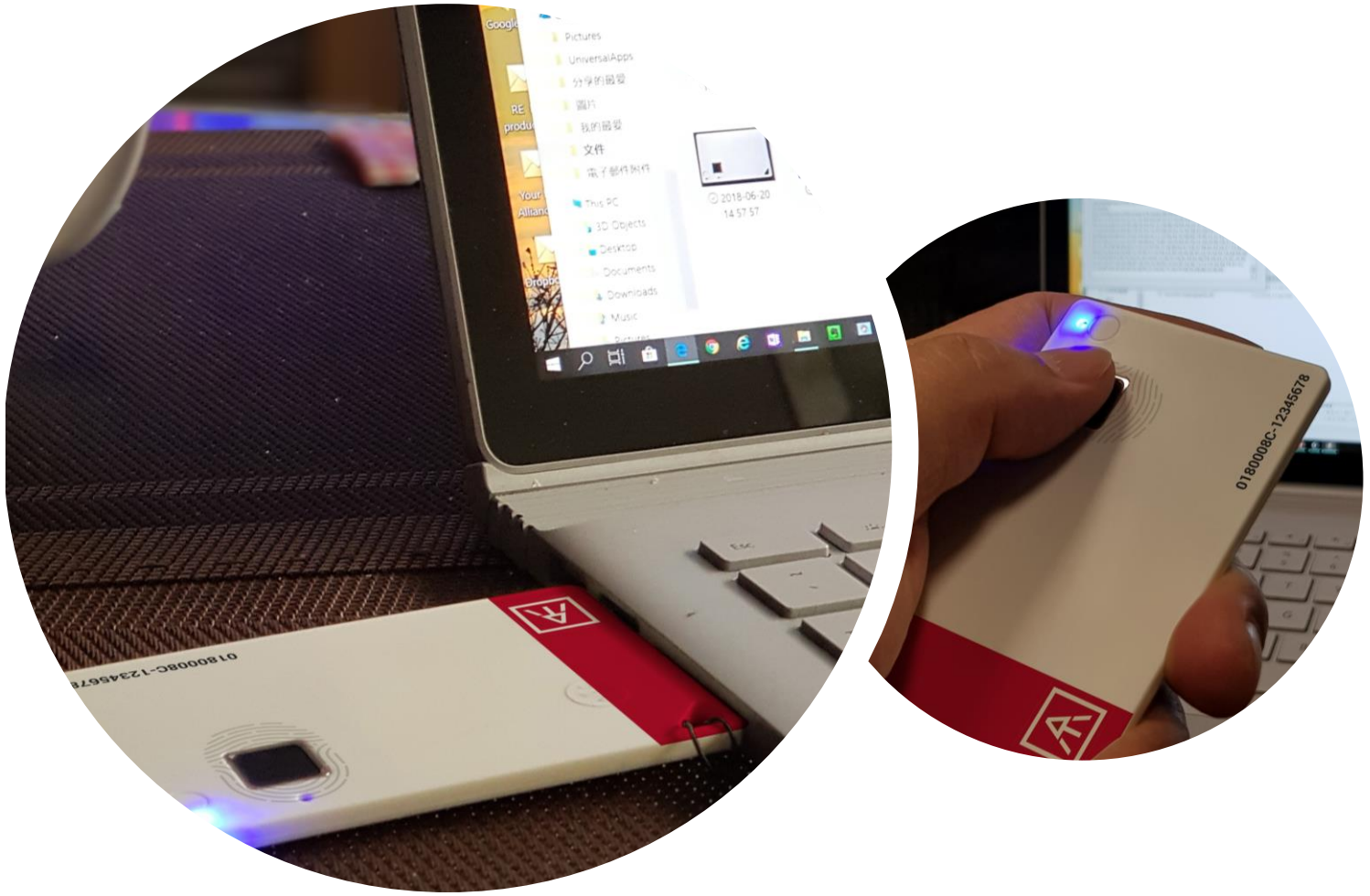
Fingerprint enabled Security key + Smart badge

NFC for Access Control
BLE for location tracking
USB for authentications

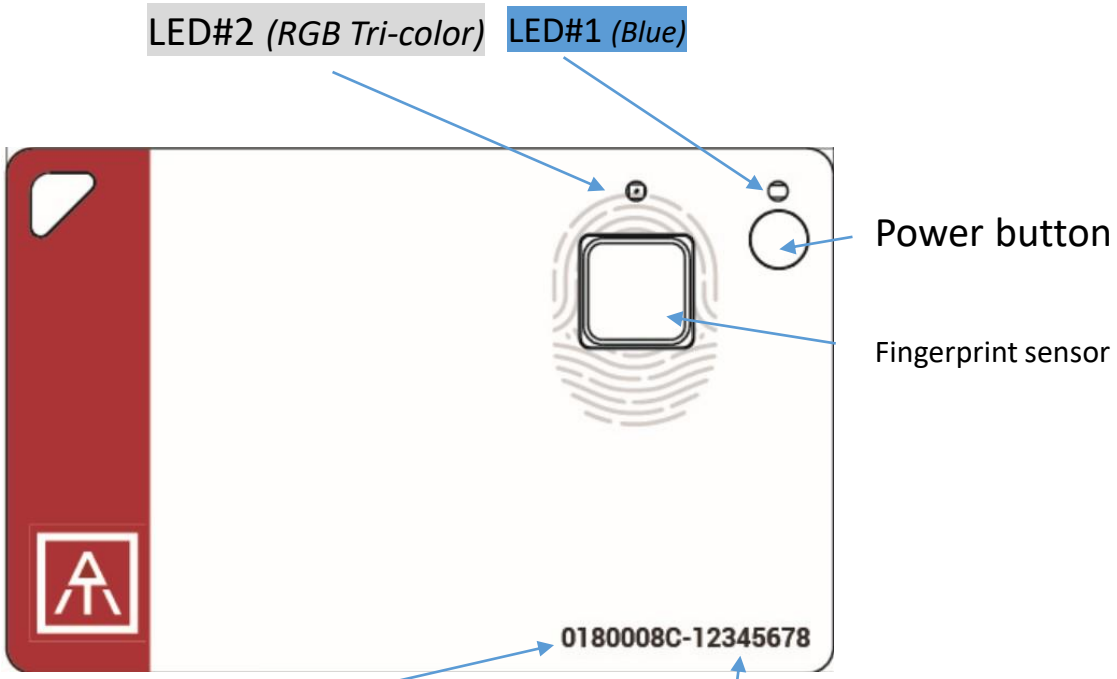
fido CERTIFIED L1 FIDO2

- About ATKey.Card Page 3
- Outlook Page 4
- Highlights Page 5
- USB Page 6
- BLE Page 7
- NFC Page 8
- LED Page 10
- Functionalities Page 11
- Fingerprint enrollment Page 12
- APP – ATKey for Windows Page 16
- APP – ATKey for Mac Page 18
- Windows Hello Page 20
- Mac Companion Page 22
- FIDO2: Azure AD Page 23
- FIDO2: Microsoft account Page 25
- FIDO U2F Page 27
- NFC Access Control Page 32
- Regulations Page 33

KEY. Card

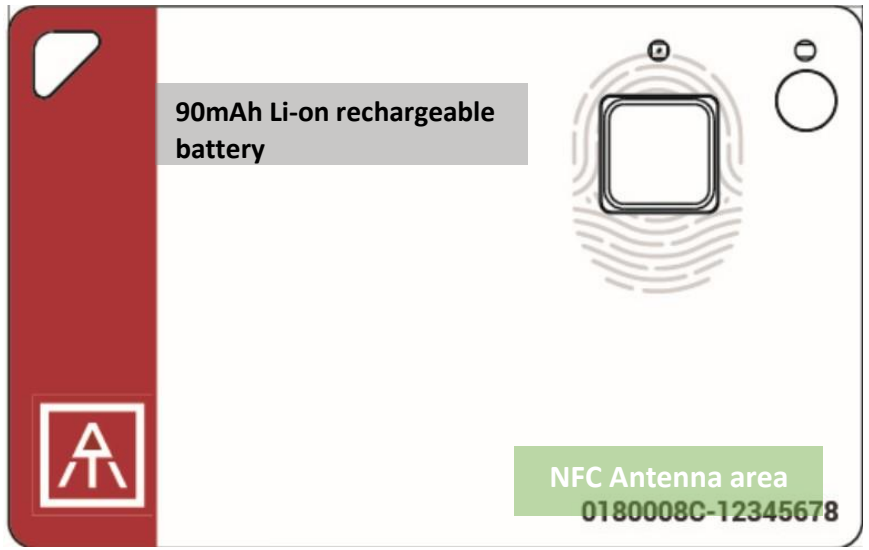


- USB HID + BLE + NFC device, no driver needs
- Portable key for any Windows, Mac or Chromebook
- Up to 8x fingerprints, matching < 1 sec., FAR < 1/50,000, FRR < 2 %
- FIDO2 certificate

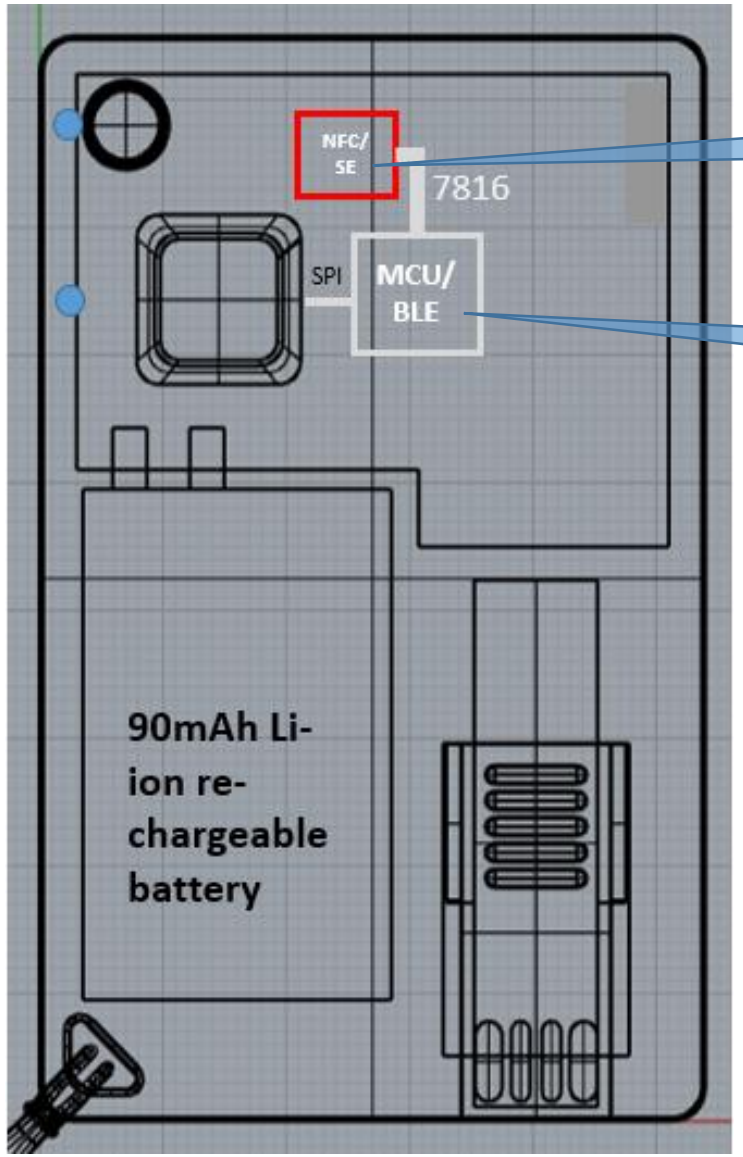


Keycode

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



USB Connector (back side)



JavaApplet

* JavaApplet needs to sync with firmware version; recommended by 2.0.1

firmware

- Recommended firmware version 3.00.21.37 or later version
- You can do **firmware/JavaApplet upgrade** through ATKey app

Before Starts:

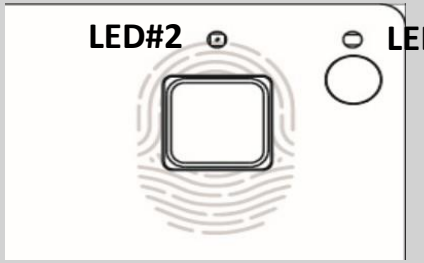
- Please do battery charging before you use the card – insert card to USB port or any USB power adaptor
  - If ATKey.card connected to USB port but nothing happened (no LED ON), please wait for a while since there is protect circuit to make sure the battery voltage is not lower than 3.0V
  - USB port of PC: USB mode, ATKey.card can work as USB key
  - USB power adaptor: BLE mode, ATKey.card can work as BLE key
- ATKey.card will be OFF automatically if it's in idle state for 60 seconds (no any operations, not insert to USB port, no BLE device connected)
- NFC is off, only when fingerprint matched, NFC is ON for 15 seconds (not is USB mode, not in BLE mode)

- USB 2.0 Type A
- USB HID device
- USB for data and also battery charge
- 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 protect circuit to make sure the battery voltage is not lower than 3.0V
  - If it's USB port of PC: USB mode, ATKey.card can work as an USB key
  - If it's USB power adaptor: BLE mode, ATKey.card can work as a BLE key

What we can do through USB:

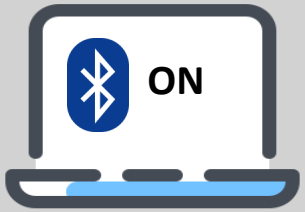
- Add/Delete fingerprint
  - through ATKey for Windows
  - through Windows Settings
- Firmware version and upgrade
  - through ATKey for Windows
- FIDO2
  - USB security key for Windows, Mac and Chromebook via Edge, Chrome, Firefox browsers
  - Azure AD Passwordless login
- FIDO U2F
  - USB security key for Chrome browser for Windows, Mac and Chromebook
- Windows Hello
- Battery charge
- OTP (options)

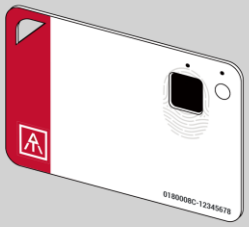
LED indicator in USB mode:



LED#1	LED#2	
ON	OFF	USB mode, battery is 100% charged
ON	flashing	Battery charging
flashing		Wait 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

- Bt4.2 BLE mode
- 1st thing: pair target device & 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)

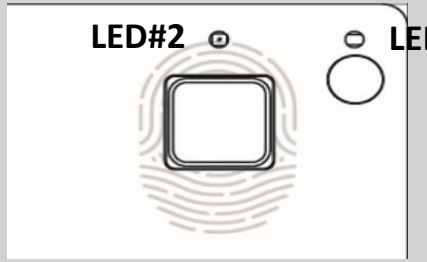
- Scan and find specific card – check the keycode to identify the card
- Select it to pair

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

What we can do through USB:

- Add/Delete fingerprint
  - through ATKey for Windows
  - Through ATKey for Mac
  - through Windows Settings
- Firmware version and upgrade
  - through ATKey for Windows
  - Through ATKey for Mac
- FIDO2
  - BLE security key for Windows, Mac and Chromebook via Edge, Chrome, Firefox browsers
  - Azure AD Passwordless login
- FIDO U2F
  - BLE security key for Chrome browser for Windows, Mac , Chromebook, Android, IOS (app Smart Lock needs)
- Windows Hello via BLE
- Mac login via BLE

LED indicator in BLE mode:



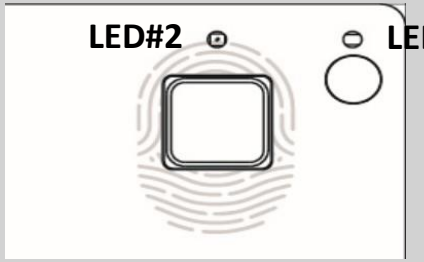
LED#1	LED#2	
ON	Flashing	BLE broadcasting
ON	ON	BLE connected to device
flashing	ON	BLE connected and wait for fingerprint verification
ON	flashing	BLE secure pairing mode
ON	flashing	Touch fingerprint sensor to confirm the pairing
ON	Slow flashing	Battery low – please do battery charging via USB

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

What we can do through NFC:

- FIDO2 (via JavaApplet) – by demands
  - NFC security key for Windows, Mac and Chromebook via Edge, Chrome, Firefox browsers
  - Azure AD Passwordless login
- FIDO U2F (via JavaApplet)
  - NFC security key for Chrome browser for Windows, Mac , Chromebook AND Android
- NFC access control or door locker (via MiFare ID)
  - Power on ATKey.card, verify fingerprint to turn NFC ON, then it's same as normal NFC card to touch/touchless to reader to unlock; NFC is ON for 15 seconds
- But if ATKey.card is in USB mode or BLE connected mode, NFC won't be enabled

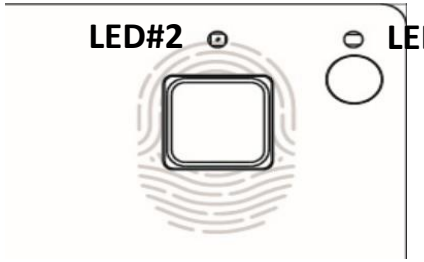
LED indicator in NFC mode:



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

	BLE	USB	NFC
Enroll fingerprint	√	√	
Azure AD logon (FIDO2)	√	√	by demands
Windows 10 build 1903 or later version • FIDO2 (Edge, Chrome, Firefox) • U2F (Chrome)	√	√	√
Windows 10 build 1809 … • FIDO2 (edge, Chrome, Firefox) • U2F (Chrome)		√	
Windows logon via Windows Hello (CDF)	√	√	
Android: • FIDO2 (Chrome browser on Android) • U2F (Chrome browser on Android)			√
iOS: • U2F (Chrome browser on iOS via Smart Lock)	√		
Mac OS X logon	√		
Mac OS FIDO2 and U2F via Chrome browser	√	√	√
Chromebook FIDO2 and U2F via Chrome browser	√	√	√
NFC door locker (Mifare typeA)			√

- *For FIDO2, FIDO U2F or Windows Hello, you can just register by one interface (USB or BLE), then you can use the card via any interface (USB, BLE, NFC) for authentications*

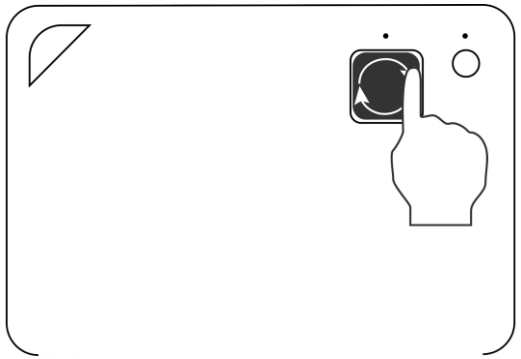


LED#1	LED#2	
ON	ON	• ATKey.card is locked (due to continuous 5 times fingerprint mismatching). • Please wait for 1 (1st time) or 12 hours (from 2nd time) to unlock
ON	ON	• Normally this is BLE issue (BLE connected, fingerprint verified, but still waiting response from Host) • Please re-boot the card (long-press power button to power off, then click power button to power ON)
-	Slow flashing	• Battery low, please do battery charge via USB
flashing (waiting for fingerprint matching)	ON for 1 sec. ON for 1 sec.	• Fingerprint matching failed • Fingerprint matched, and NFC is ON (if it's not in USB or BLE connected)
ON	flashing	• Request to confirm the BLE pairing • Touch fingerprint sensor to confirm the pairing
		• 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	• 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	• Battery charging • Battery charge full, stop charging
OFF	OFF	• (power on but no LED ON) very low battery, please do battery charge and wait till LED is ON

Step 1
Enroll fingerprint to ATKey

Step 2
Register ATKey to device or Service

Step 3
Fingerprint matching for authentication



Standalone enrollment (patent filing)
https://youtu.be/BdF_1jbowXw

or through Windows Settings (build 1903)

or through "ATKey for Windows" app

FIDO2

- **Azure AD Passwordless logon**
- **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/

FIDO U2F

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

Windows Hello (option)

- **Windows Logon (via CDF)**

** If your Windows joined Azure AD, don't enable this one*

OTP (option)

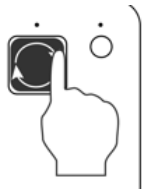
- **2FA via OTP**

** This is only for customization projects or customers*

KEY.Card | Step1: Fingerprint Enrollment (up to 8x fingerprints)

Standalone enrollment

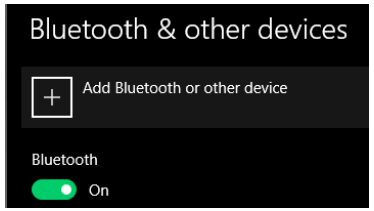
- Power on ATKey.Card
- Check Youtube video here for the detail: *https://youtu.be/BdF_1jbowXw*
- LED#1 is BLUE ON, quick click power-button 3x times to go into enrollment mode:
  - If there is no any fingerprint enrolled, LED#2 turns to WHITE
  - If there are any enrolled fingerprints, LED#2 is GREEN 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



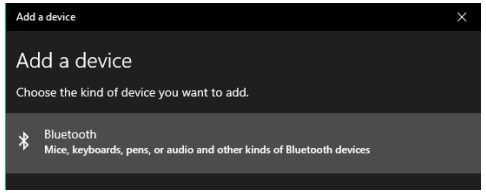
- If you want to quit from standalone enrollment, click power button once, LED will turn to Blue, back to normal state.

Enroll from Windows Settings

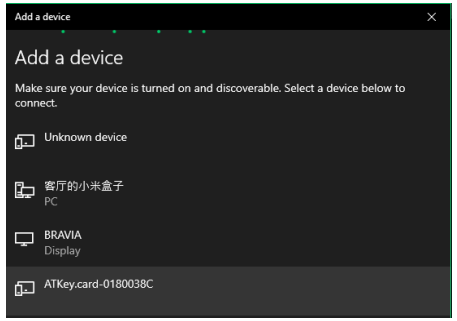
- If your OS is Windows 10 build 1903 or later versions, you can manage ATKey as security key through Windows Settings
- **(BLE) Pair ATKey with your Windows first**
  - Through Windows Settings => Device => ADD Bluetooth or other device



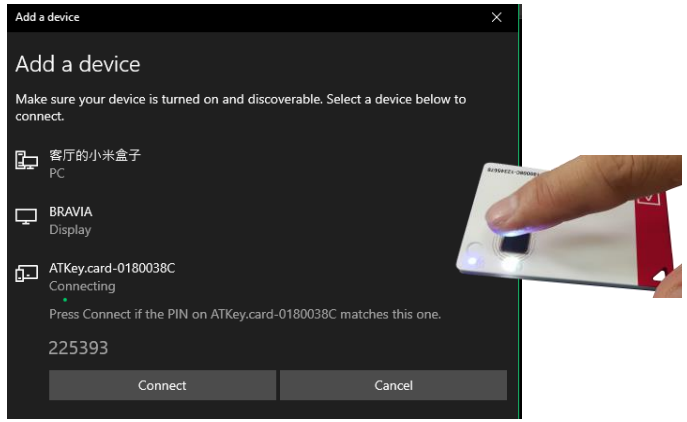
  - Add a device - Bluetooth



  - 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

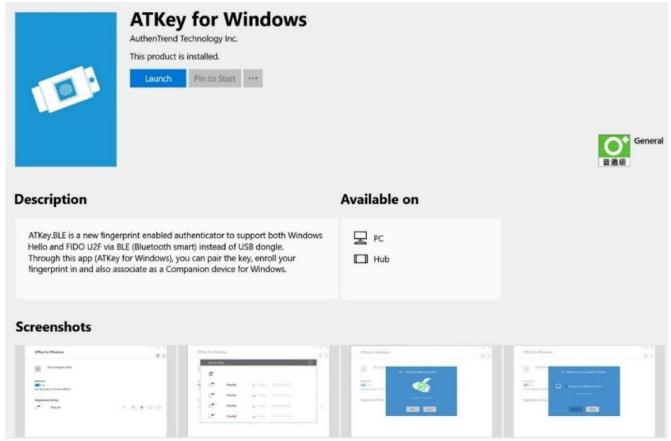


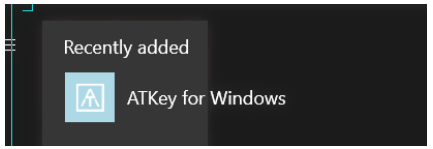
- Then ATKey is paired with battery indicator *(OS 1903 build or later version)*

- ***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**

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)
  - Firmware upgrade
- Search “ATKey” or “AuthenTrend” from Windows Store to find the app, download and install





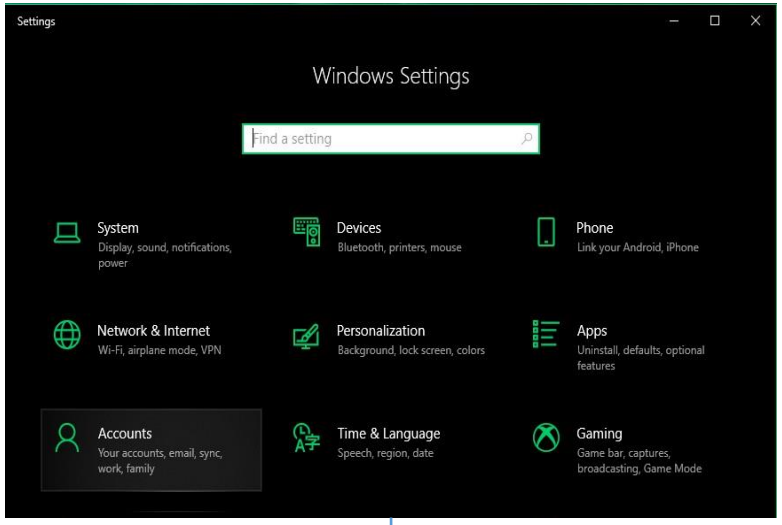
- Jump to “ATKey for Windows” for the detail

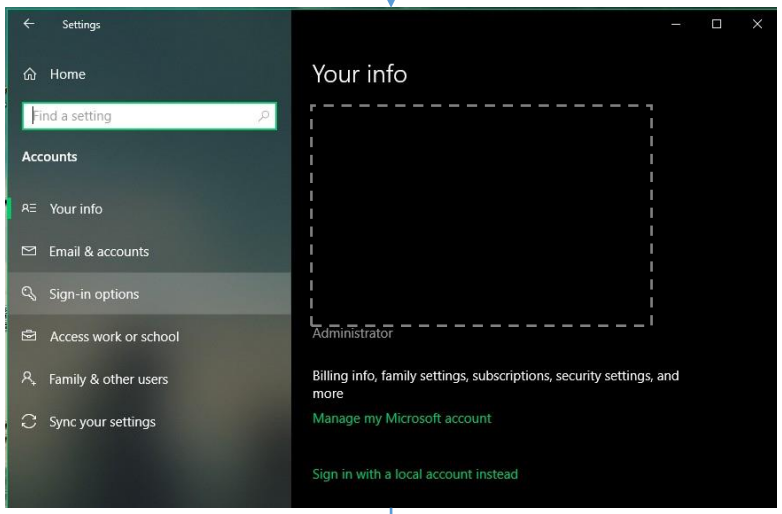
Enroll from ATKey for Mac app

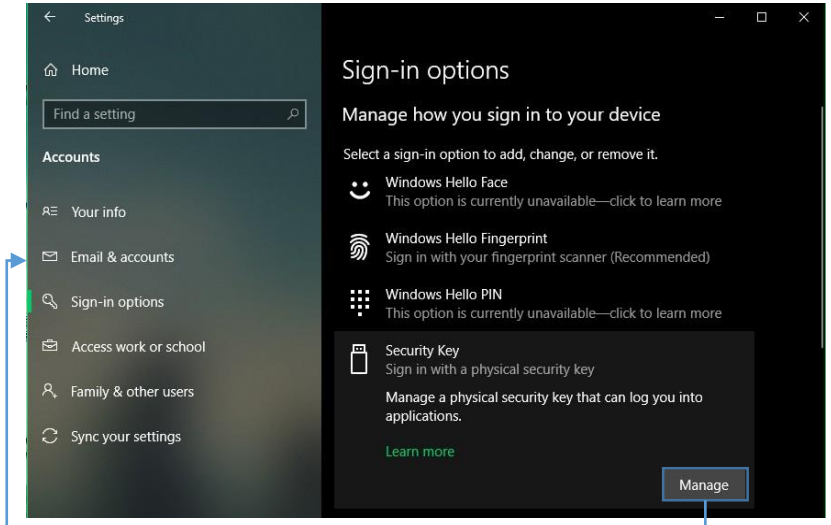
- Download “ATKey for Mac” app from *https://authentrend.com/download/ATKeyForMac.zip* to manage ATKey:
  - BLE mode only
  - Enroll fingerprint
  - Add/delete fingerprint
  - ATKey information
  - Companion ATKey to Mac (Mac login, password replacement)
  - Firmware upgrade
- Jump to “ATKey for Mac” for the detail

Mac OS X

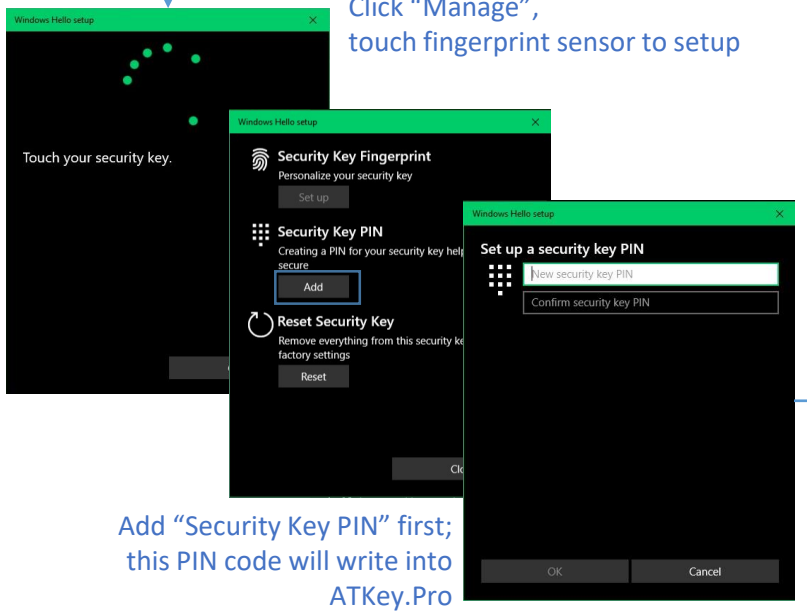
- Windows Settings => Account => Sign-in options => Security Key => **add “PIN code” and enroll “Fingerprints”**
- It works for both **USB** and **BLE** interface



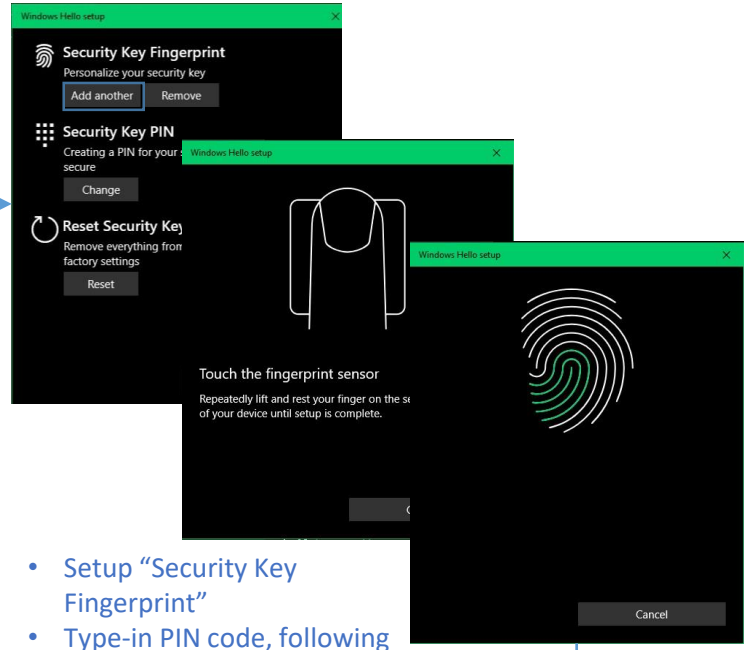




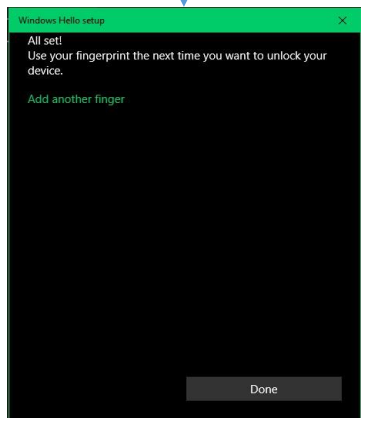
Click “Manage”,
touch fingerprint sensor to setup



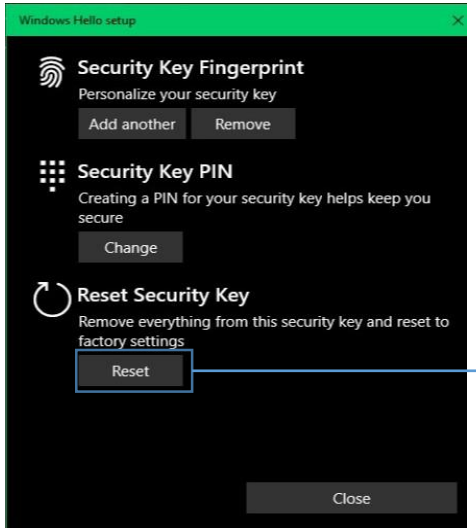
Add “Security Key PIN” first;
this PIN code will write into
ATKey.Pro

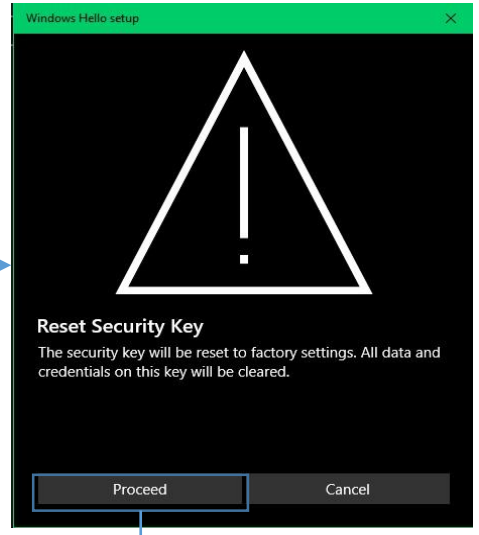


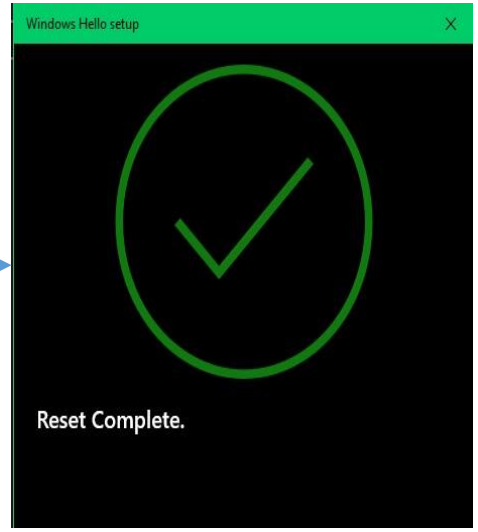
- Setup “Security Key Fingerprint”
- Type-in PIN code, following screen hint to enroll fingerprint, until “All Set!”



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



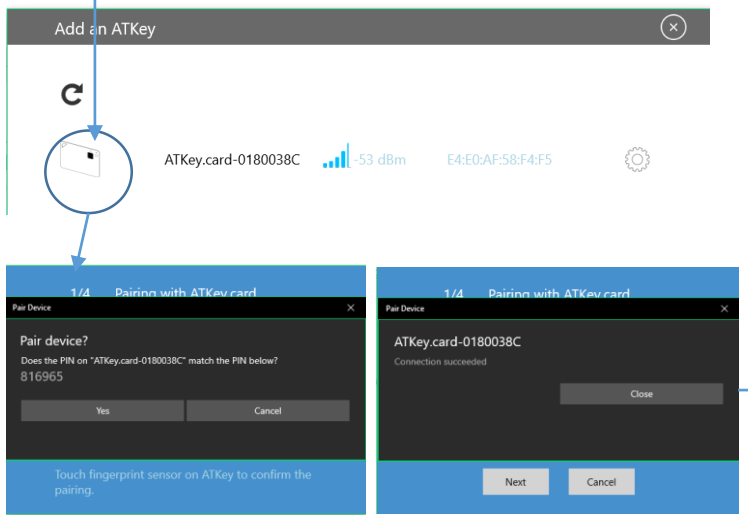




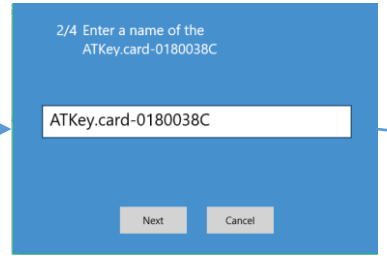
Power on ATKey.card, doing "reset" **within 10 seconds** (after card booting), this is Microsoft rule

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

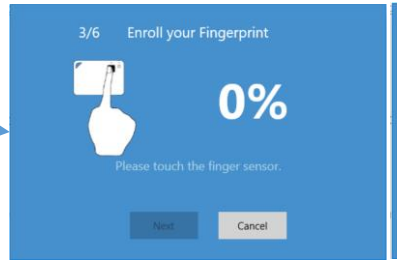
- Launch “ATKey for Windows” app *(version 2.0.55.0 or later version)*
- Click “Add and Register ATKey” – please make sure ATKey is ON (LED#1 blue ON, LED#2 blue flashing)
  - Double-click power button to secure pairing mode (LED#2 is cyan flashing)

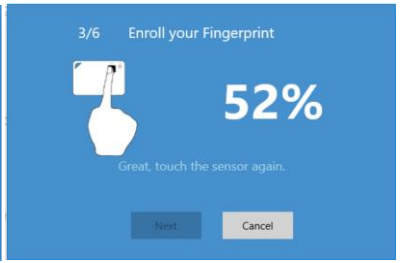


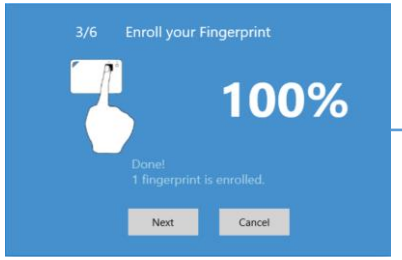
LED#2 is WHITE flashing, touch fingerprint to confirm the pairing, and also click “Yes” from UI.



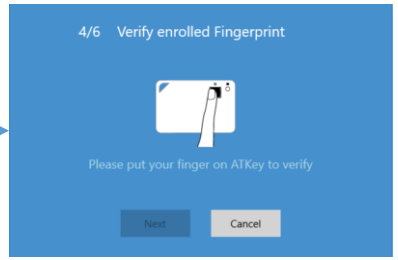
Default name is -: ATKey.card + Keycode

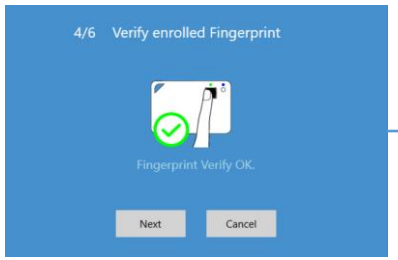




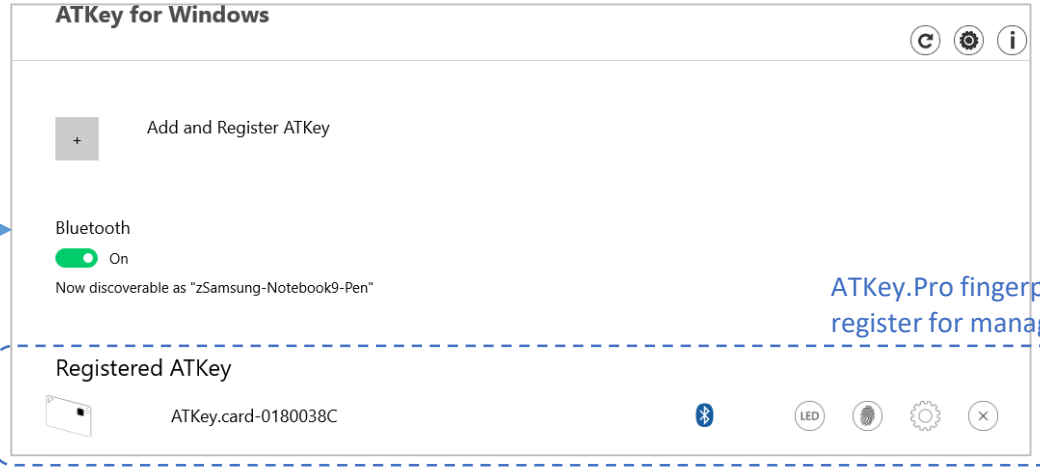


Circle enroll your fingerprint



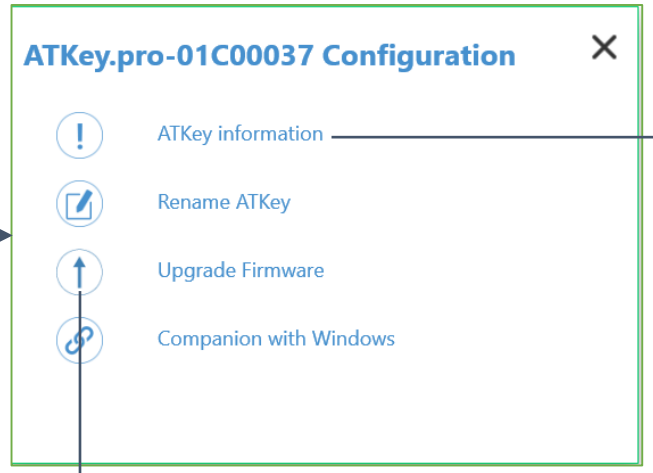


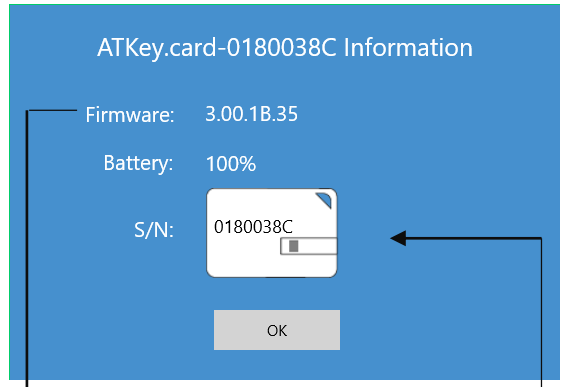
Verify enrolled fingerprint to confirm



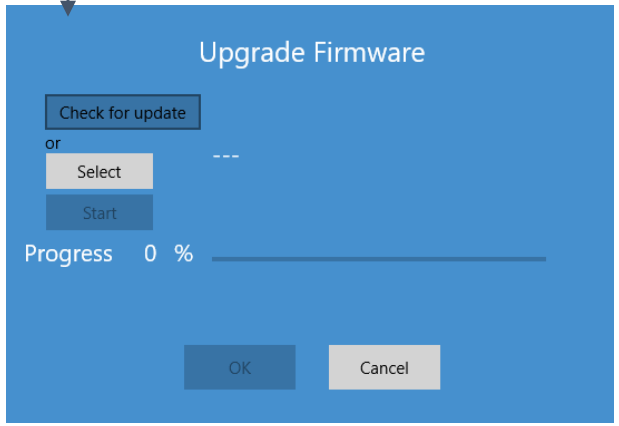
ATKey.Pro fingerprint enrolled and register for management by app

- ATKey management – information, rename, firmware upgrade





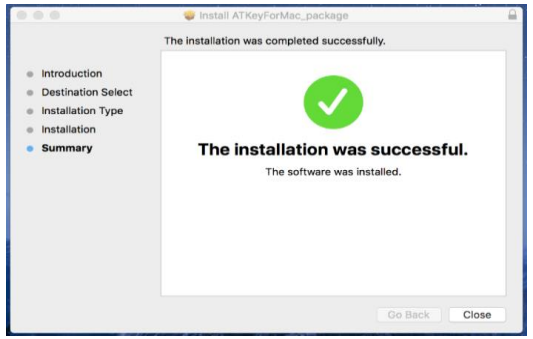
- read firmware version here
- Read “keycode” here



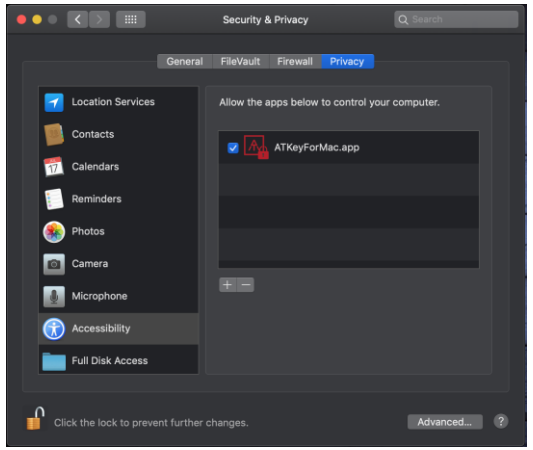
- “Check for Update”
- Select encrypted firmware image to upgrade manually
- Please wait till 100% done, power off ATKey.Card, then power on again, LED#2 starts WHITE flashing for a few seconds, then back to Blue flashing, it means firmware is upgraded.

Mac OS X

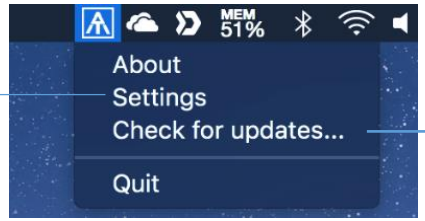
- Download app from: https://authentrend.com/download/ATKeyForMac.zip
- Please make sure your app is v1.2.5 or later versions, or you can upgrade version from “Check for updates” from app
- Install app “ATKey for Mac”



- Please unlock “ATKeyforMac.app” from Security & Privacy

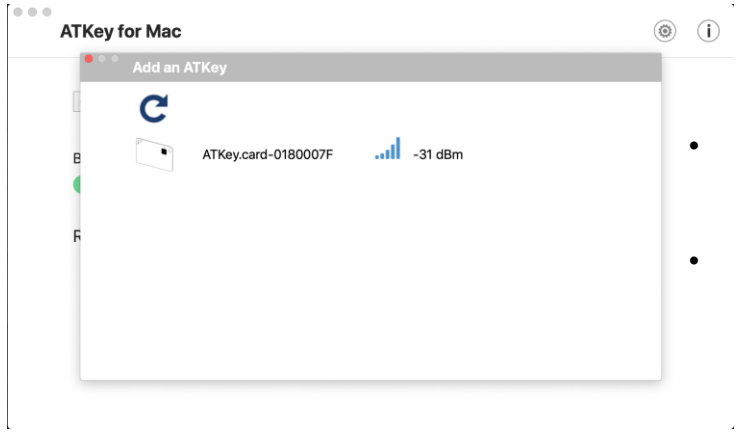


- App is working now, please enable Bluetooth of Mac also



App auto updates, not ATKey

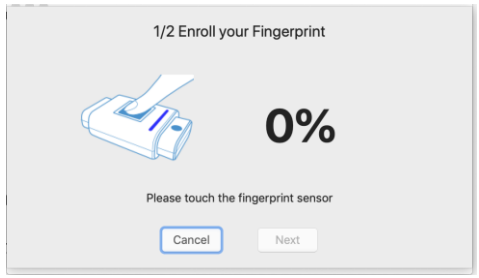
- Add ATKey – pairing to Mac (BLE only)

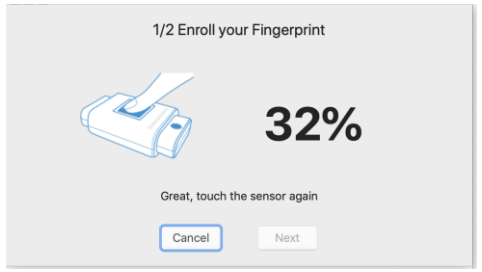


- Double-click power button to secure BLE pairing mode (LED#2 is cyan)
- Touch fingerprint sensor to confirm paring (LED#2 is WHITE)

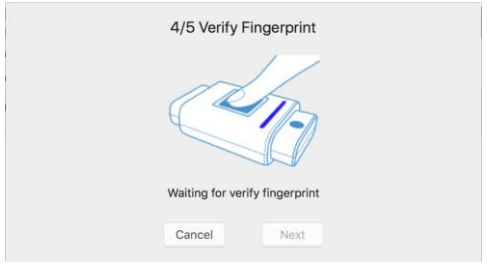
Mac OS X

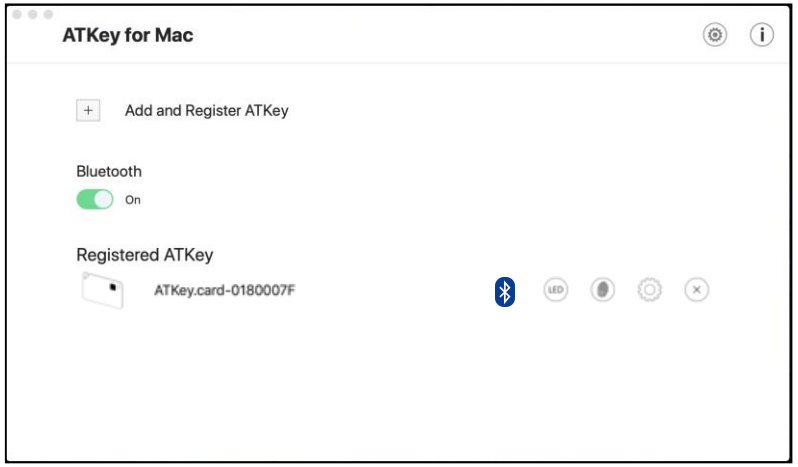
- Circle enroll your fingerprint into card until 100%



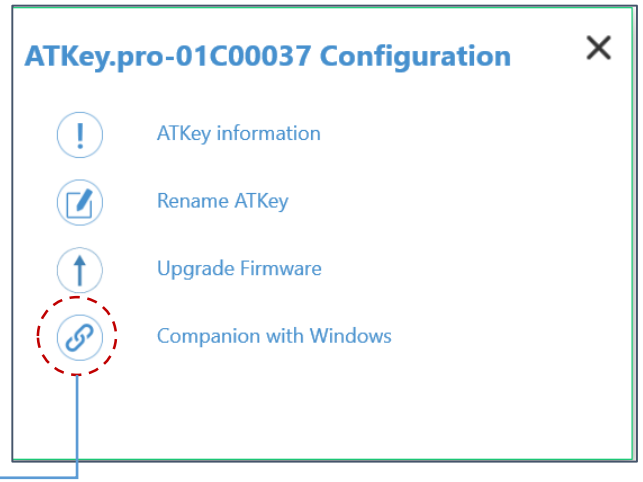


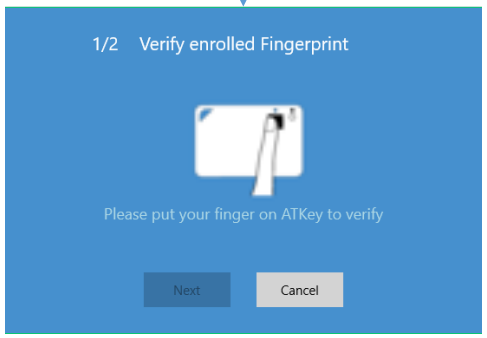
- Verify enrolled fingerprint

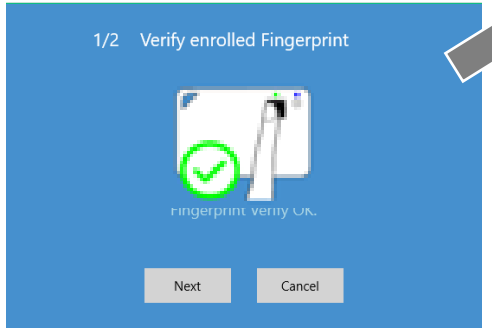


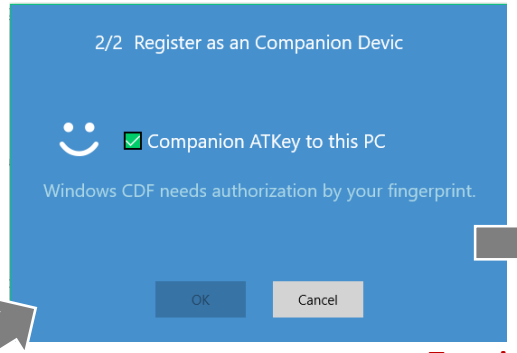


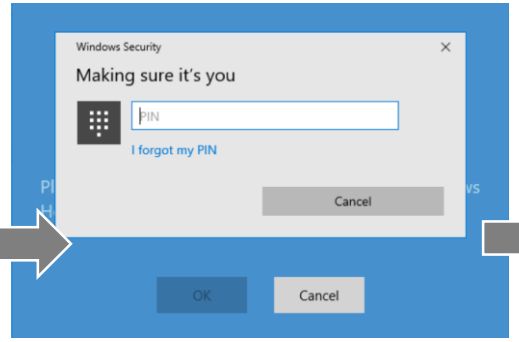
- ATKey management – Companion with Windows (Windows Hello login via CDF)
- *If your Windows 10 joined Azure AD, please ignore this page since FIDO2 is ready for Azure AD login, it may conflict with Windows Hello*

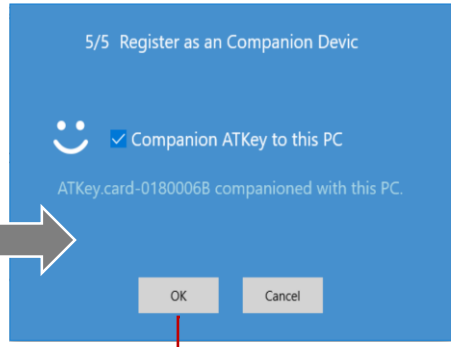




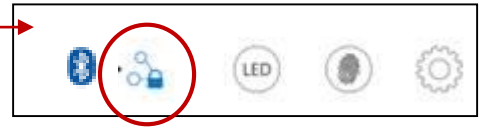






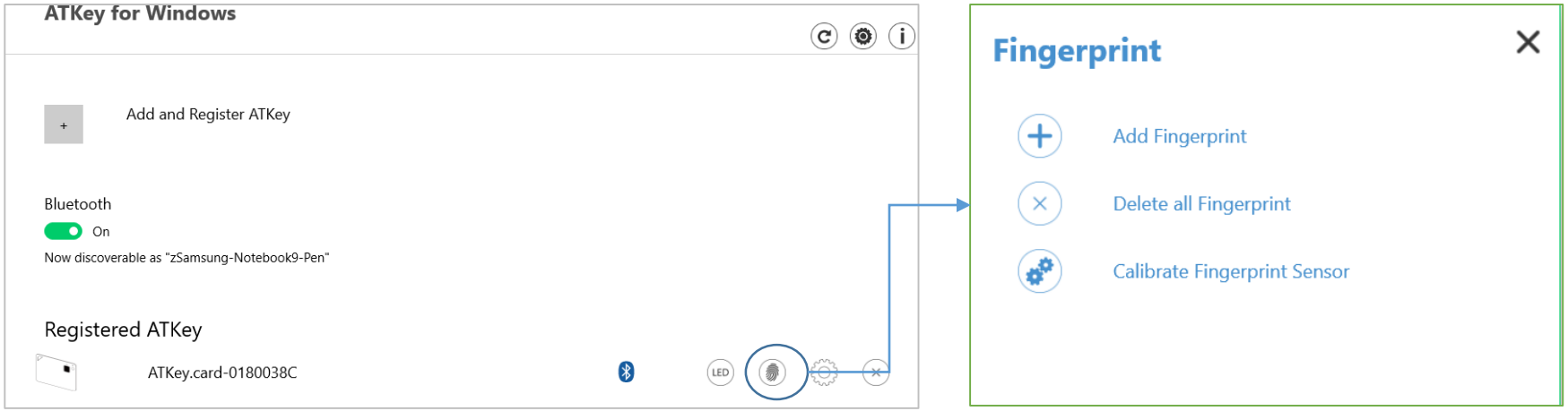


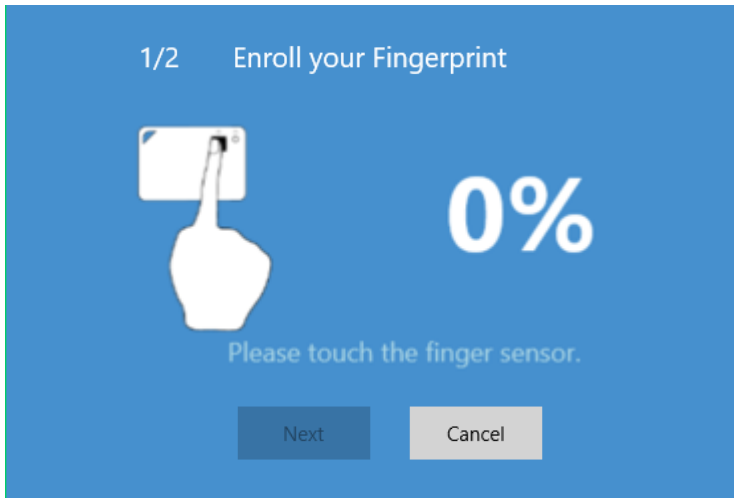
- **Type in “Windows Hello PIN” to allow the companion;**
- *Some Corp. or Org. may disable this group policy by IT Admin, if you saw the message, please contact your IT.*



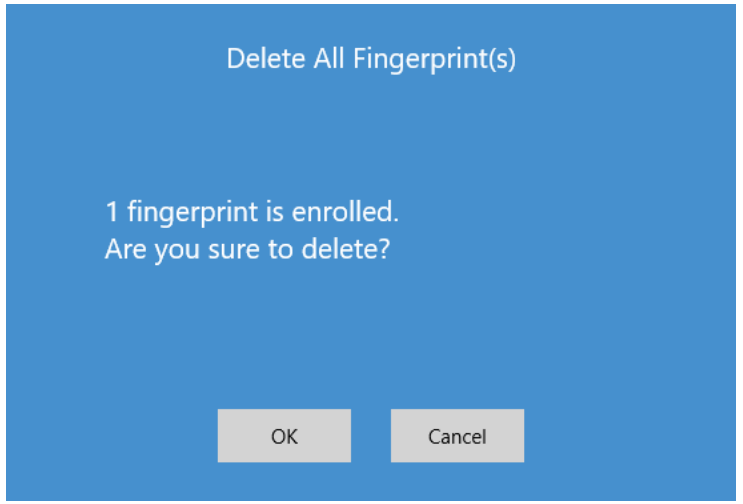
This icon means it’s a companion key for Windows Hello via CDF (Companion Device Framework)

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

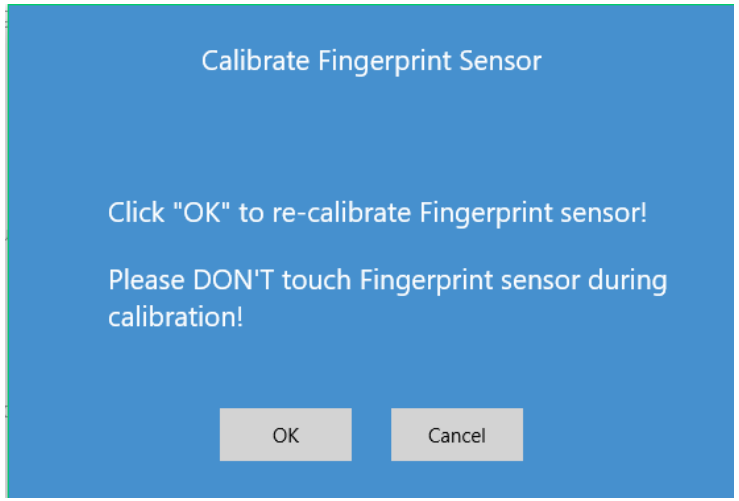




- Enroll new fingerprint in by ~12 times touch, following UI message; up to 10x fingerprints



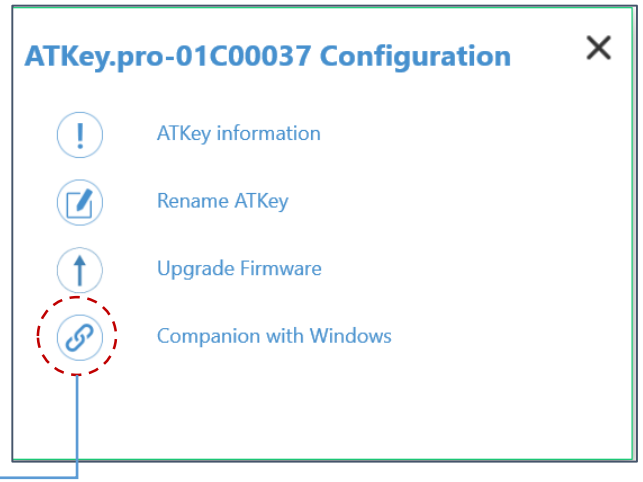
- Here will delete all enrolled fingerprints, “OK” to delete them
- It needs Windows PIN code to authorize.

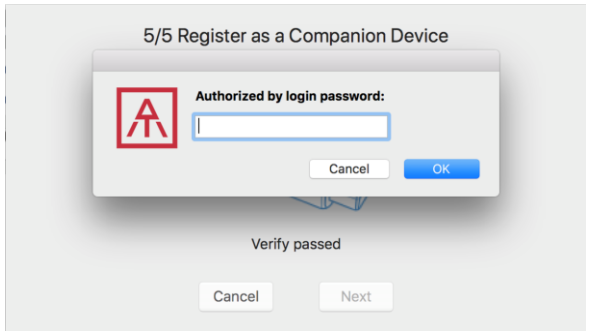


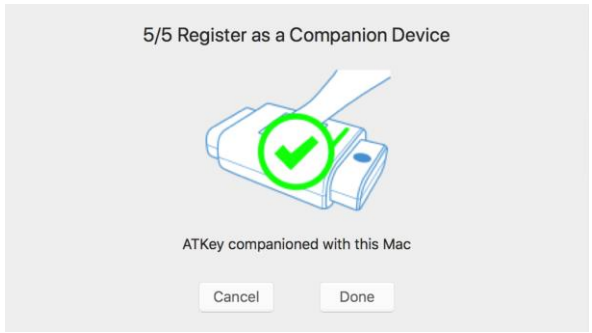
- If you feel something wrong of fingerprint, doing Calibration to re-calibrate the sensor
- Don’t put your finger on during calibration; LED will be WHITE flashing then back to Blue

Mac OS X

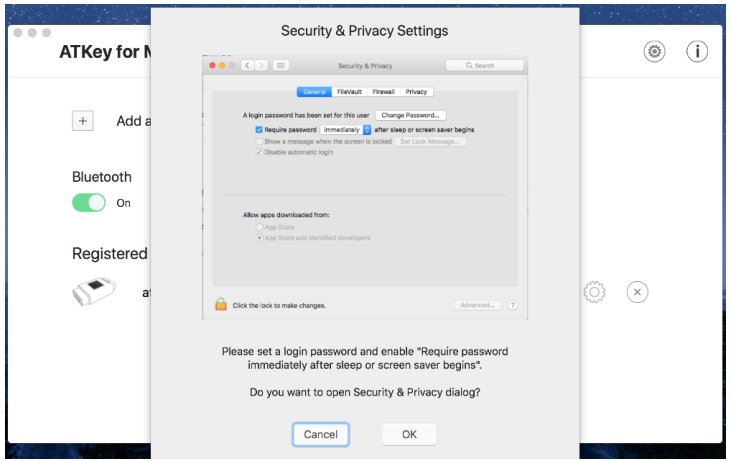
- ATKey management – Companion with Mac to login without typing password



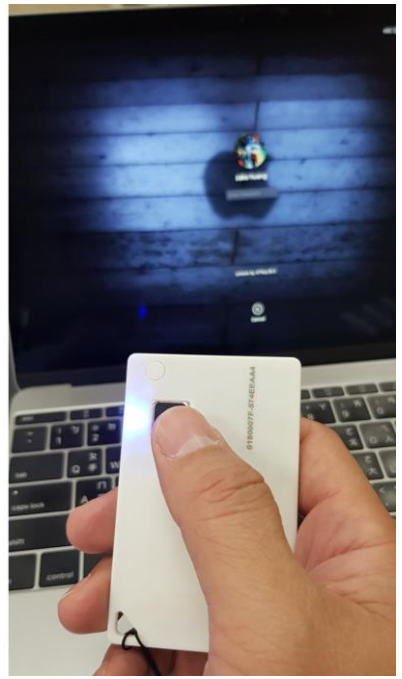




we need your password to authorize it; in addition, we will leverage this password at every login (when fingerprint verify passed!);
so if you change your login password, please remember to re-companion the card



Then, we will guide you to the setting as reminding – enable “Require password: immediately” from “Security & Privacy Settings”

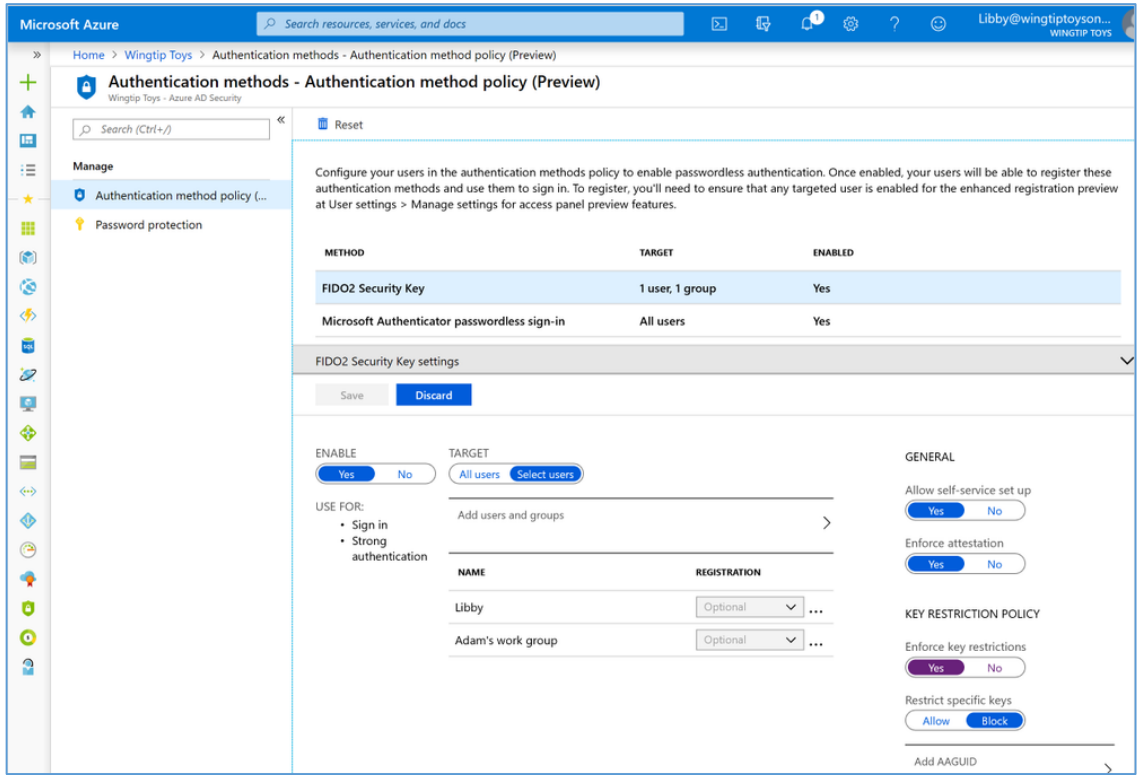


- Does your company/org. license Azure AD?
- If yes, does your authentication policy allow “add method” including “security key”?
- Please check below links to learn how to enable security key for Azure AD:
  - https://cloudtotal.blog/2019/07/tutorial-configure-fido2-passwordless-authentication-in-azure-ad/
  - https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Announcing-the-public-preview-of-Azure-AD-support-for-FIDO2/ba-p/746362
  - https://www.bleepingcomputer.com/news/microsoft/microsoft-azure-ad-fido2-passwordless-sign-in-in-public-preview/

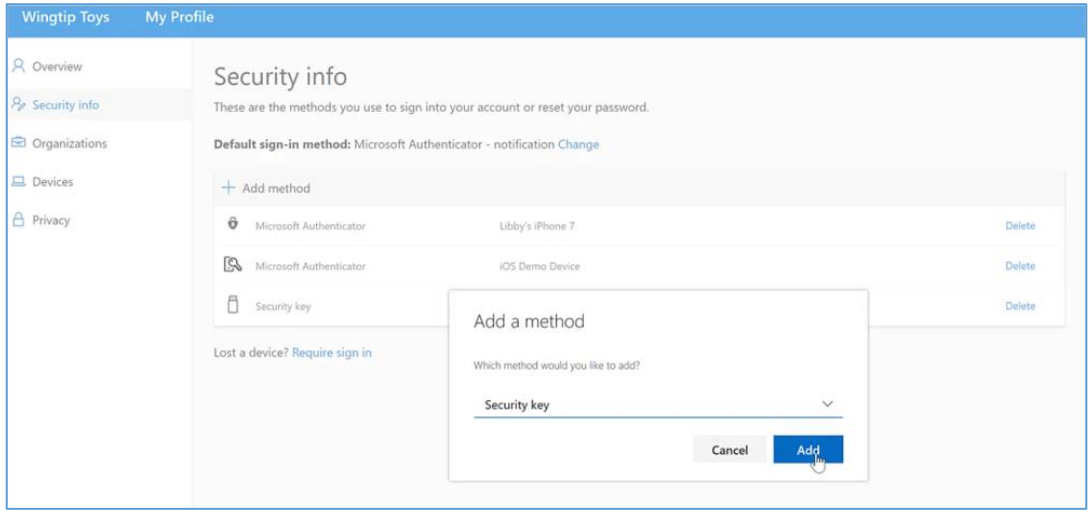
What you’ll need:

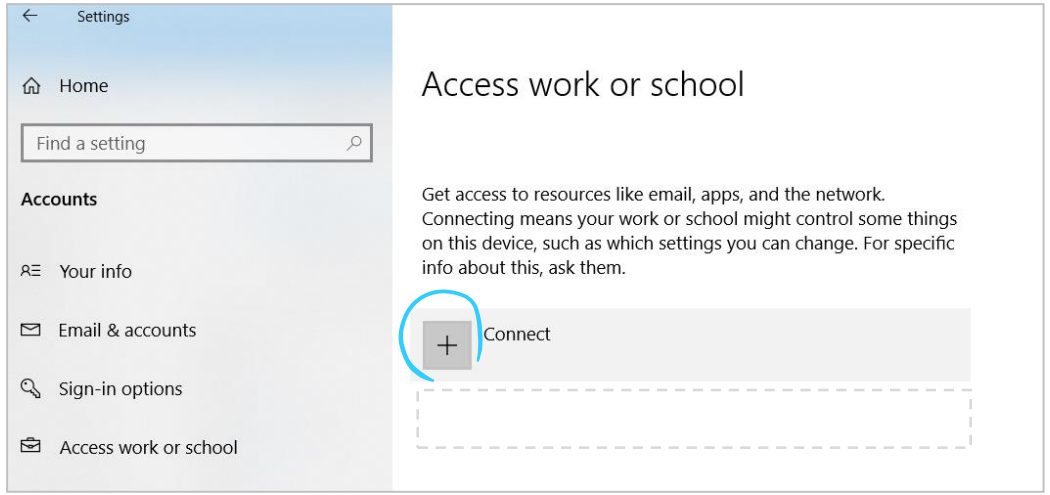
- An active Azure AD tenant which is able to leverage Azure MFA functions.
- A global admin account in Azure AD
- A test account with normal privileges in Azure AD
- ATKey.Pro - FIDO2 compatible security key.

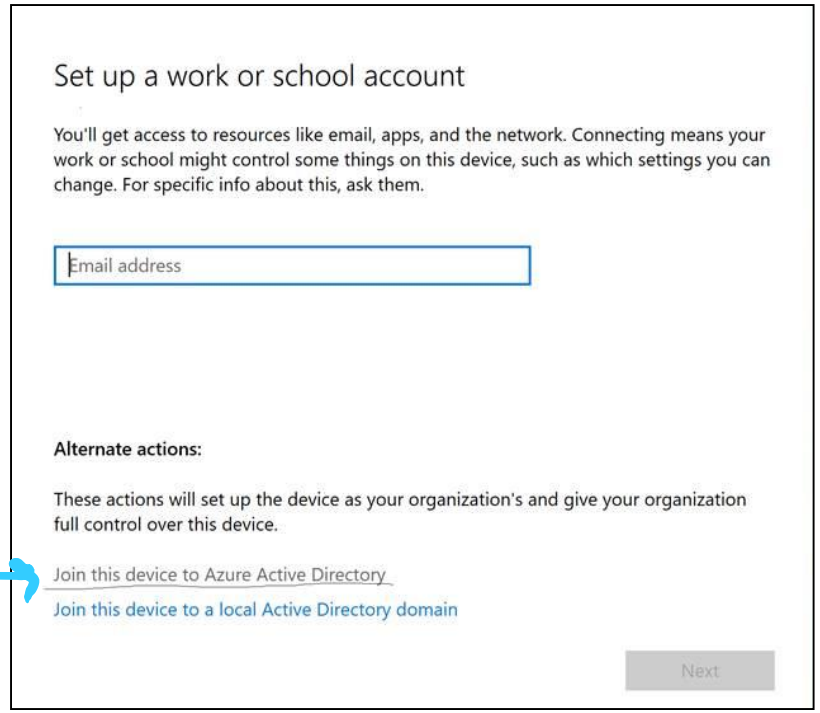
1. A new Authentication methods blade in your Azure AD admin portal that allows you to assign passwordless credentials using FIDO2 security keys and passwordless sign-in with Microsoft Authenticator to users and groups.



2. Updated capabilities in the converged Registration portal for your users to create and manage FIDO2 security keys.



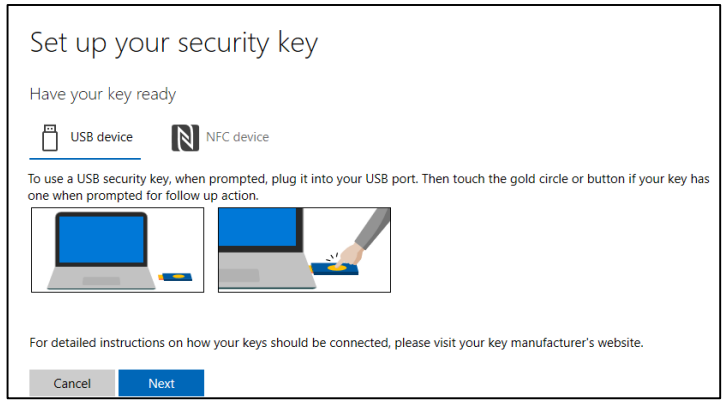




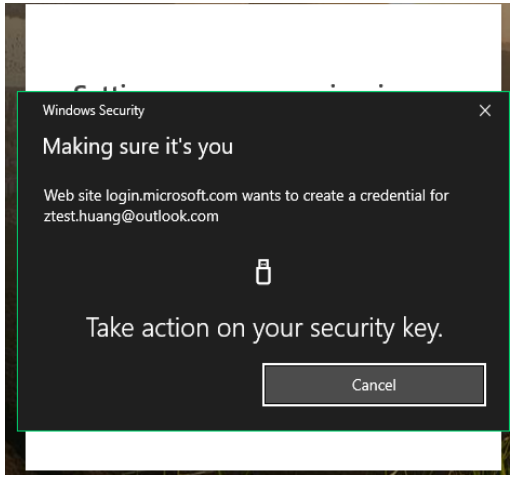
User registration and management of FIDO2 security keys

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

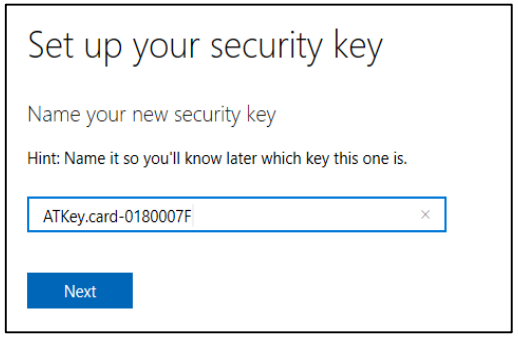
- Passwordless login Microsoft account by security key:
  - For Password-less login to Microsoft account - **Windows 10 build 1809** or later version via **Edge/Chrome browser**, **USB/BLE** mode:
    - You can login to add ATKey.Card as security key for your Windows account from here: https://account.microsoft.com/account
      - Login by ID/Password first
      - Step by step to setup security key (or check video: https://youtu.be/aSnJ8W_0ya4 to setup)
        - Click “Security” from banner bar
        - Click “**more security options**” from bottom
        - From “Windows Hello and security keys” section, click “**Set up a security key**”



- Touch your enrolled fingerprint to verify

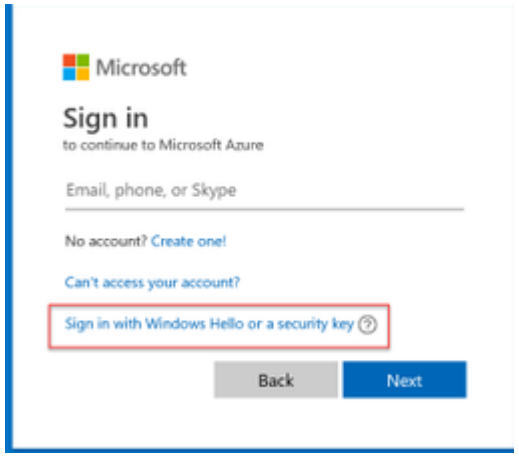


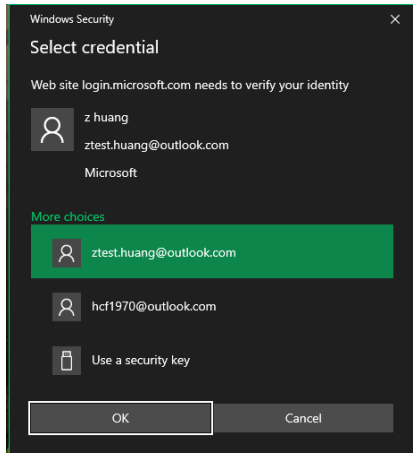
- Fingerprint matched, type in name of the key (default name following keycode)



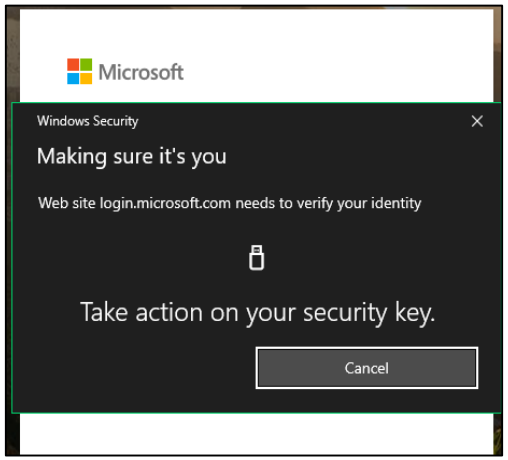
- You can find all your registered keys, click "**Manage your sign-in methods**"

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





Use security key



Fingerprint verified to login

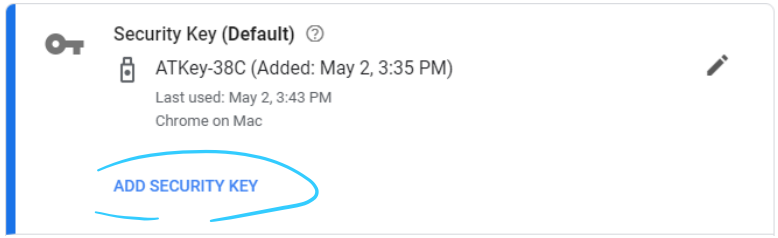
- ATKey.Card is FIDO U2F ready, it can be a security key for 2nd factor authentication.
- Here are FIDO2 U2F ready service:

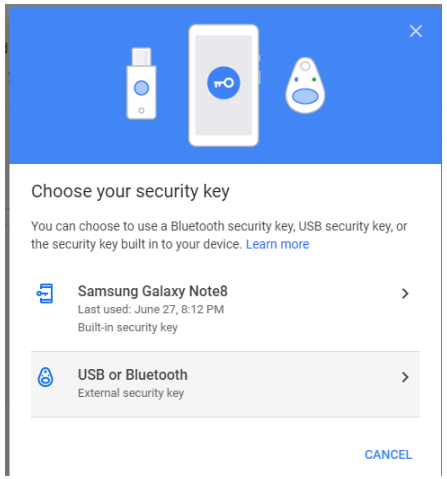
Google Gmail Google Docs YouTube GitHub FastMail Dropbox salesforce

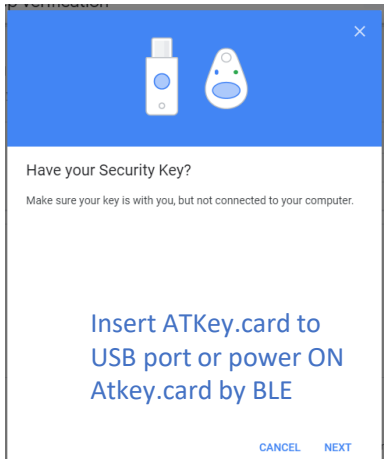
- Or you can search and find available FIDO U2F certified server here: *https://fidoalliance.org/certification/fido-certified-products/?appSession=8YT7Z25V0DOH6M41OQG26WI22N0F6D5MF9W19F58545OZWKJPBOH5XMB874A6596S8432G491GGF12B5Y7PIAM6PKR09S5G9Z3Q9T0FLK91C5445079DO1NWZFP8714Q*
- **But, Chrome browser 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

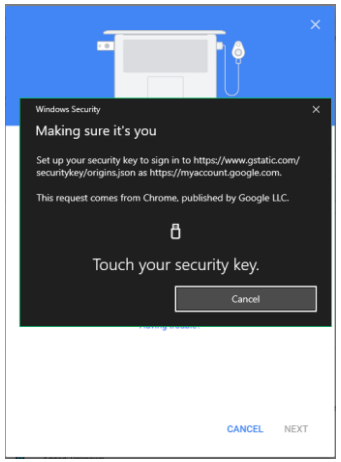
- **(e.g.) Google account – add ATKey.Card as security to Google account:**



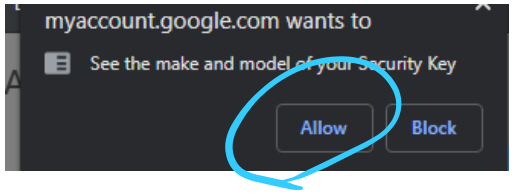




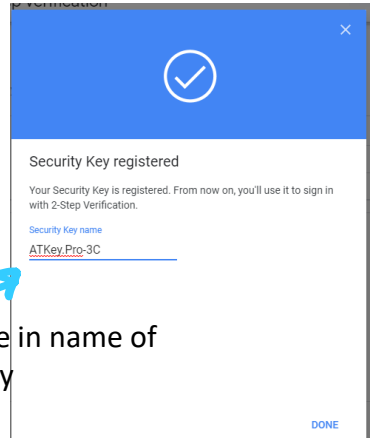
Insert ATKey.card to USB port or power ON Atkey.card by BLE



Touch enrolled fingerprint to verify

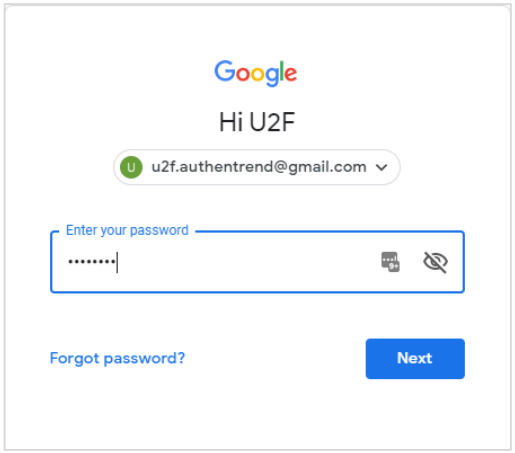


Click “Allow”

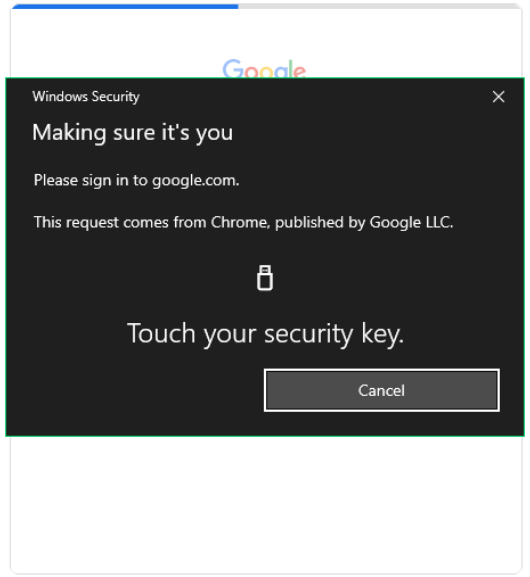


Ready, type in name of security key

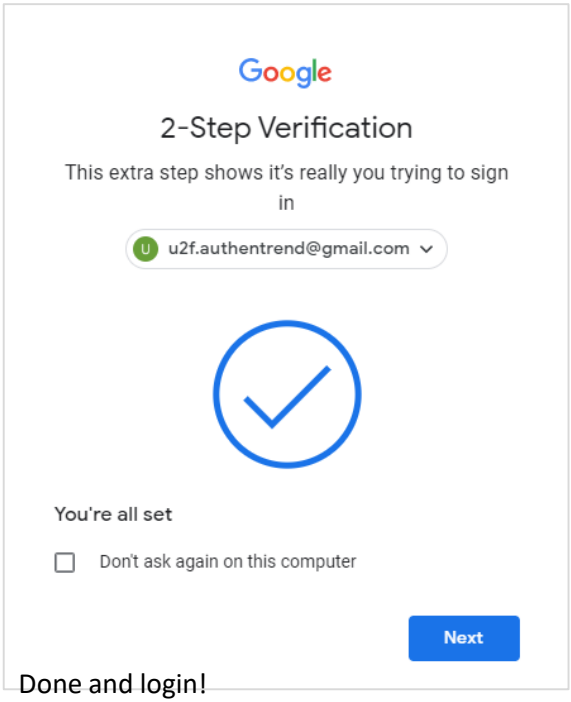
- **(e.g.) Google account – login via ATKey.Card**



1st factor: ID and password still



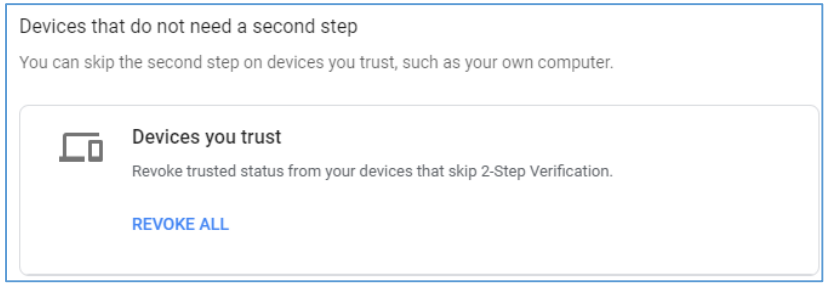
2nd factor: verify your enrolled fingerprint



Done and login!

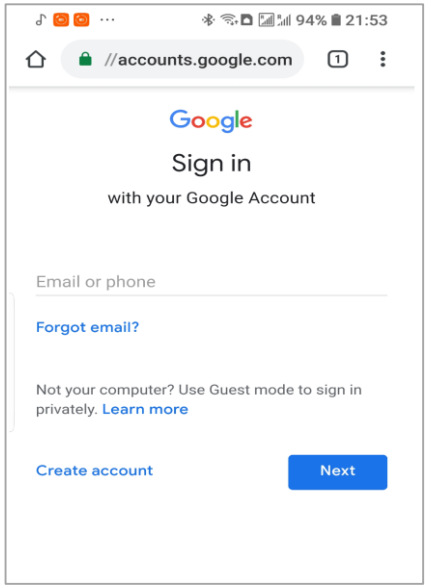
*If you want to login your google account with ATKey later, please **uncheck** "Don't ask again on this computer" (default is checked).*

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:

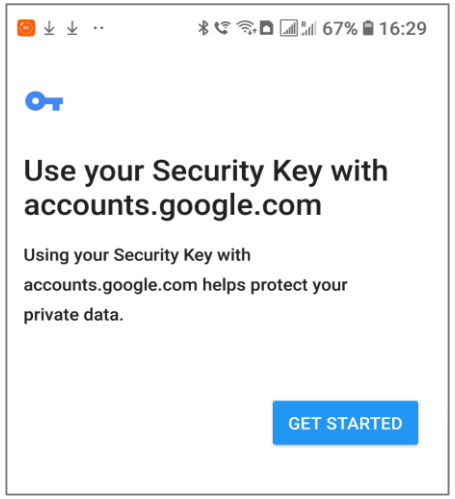


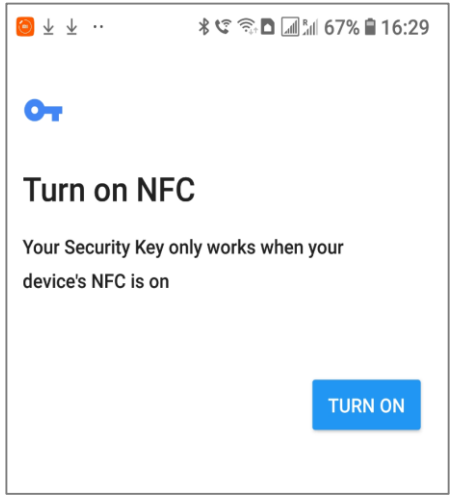
FIDO U2F via Android phone/tablet – Chrome browser

- Sign in Google account via Chrome browser

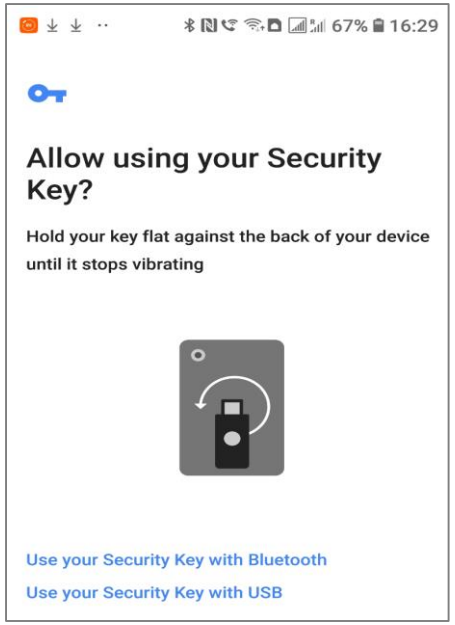


- Request Security Key and turn on NFC



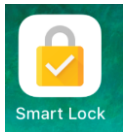


- Authenticate via ATKey through NFC

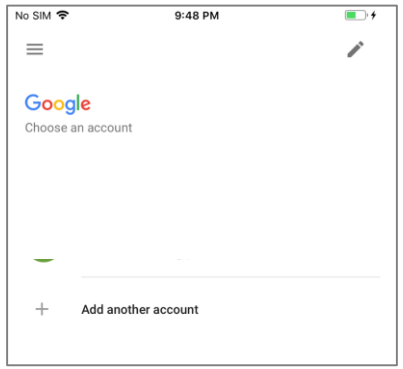


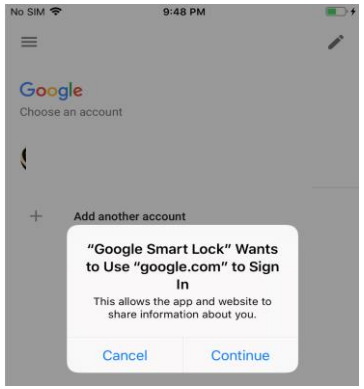
- Power on ATKey.card
- LED#1 is flashing, just touch fingerprint to verify to enable NFC (for 15 sec.)
- ATKey.card contacts Android Phone (back side) to send U2F token via NFC (JavaApplet) to Phone to server for authentication

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

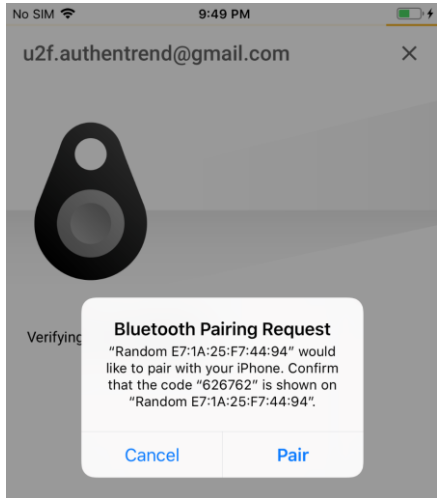


- Add your google account in

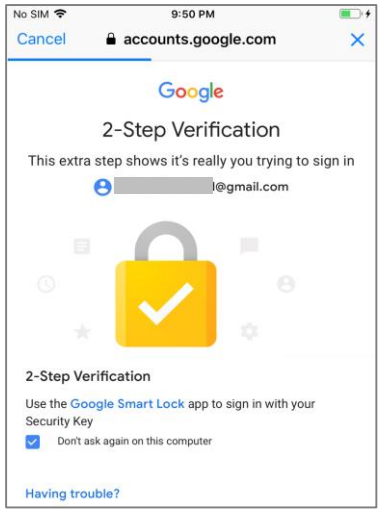


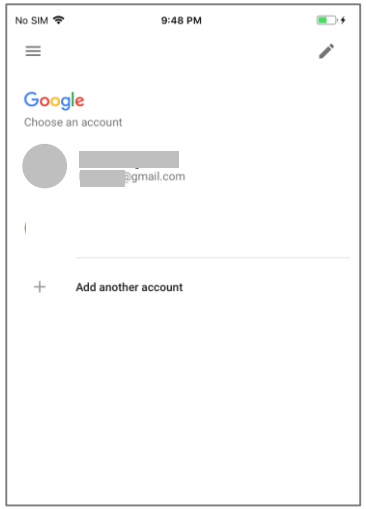


- Pair ATKey

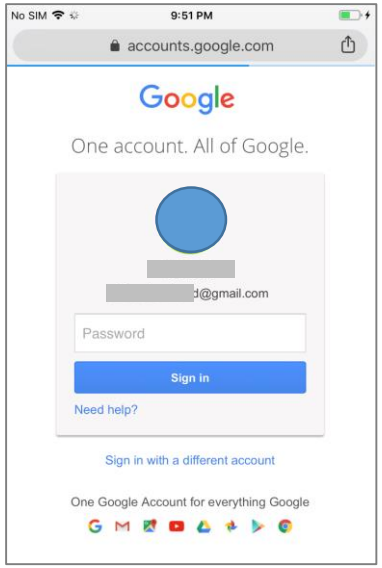


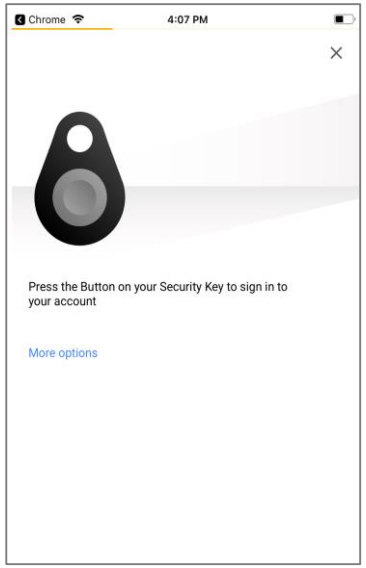
- Double-click power button to secure BLE pairing mode (LED#2 is cyan)
- Touch fingerprint sensor to confirm paring (LED#2 is WHITE)





- 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

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.

209-J00349 CCAO18LP122OT8

FCC ID: 2AOPY-ATKEYCARD1

R-C-Ath-ATKycard
M/N: ATKeycard

THANK YOU!

www.authentrend.com

contact@authentrend.com

AuthenTrend

AuthenTrend

AUTHENTREND