

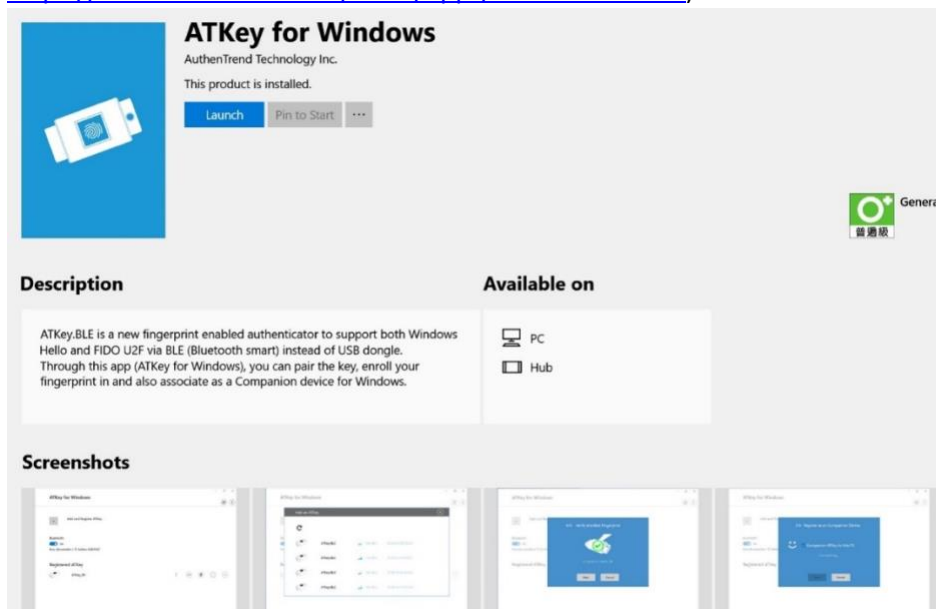
ATKey.BLE Quick Guide (Windows 10)

2018.01 rev1.2

- Preface
 - ATKey.BLE

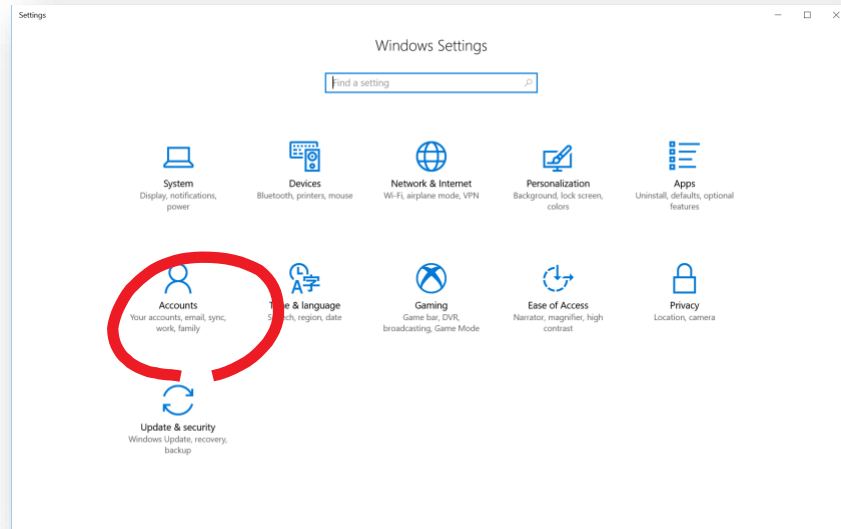


- Windows 10 RS2 (Creators Update, build 1703) or later version
- ATKey app (download from Windows Store:
<https://www.microsoft.com/store/apps/9P7GR8W9SJD3>)

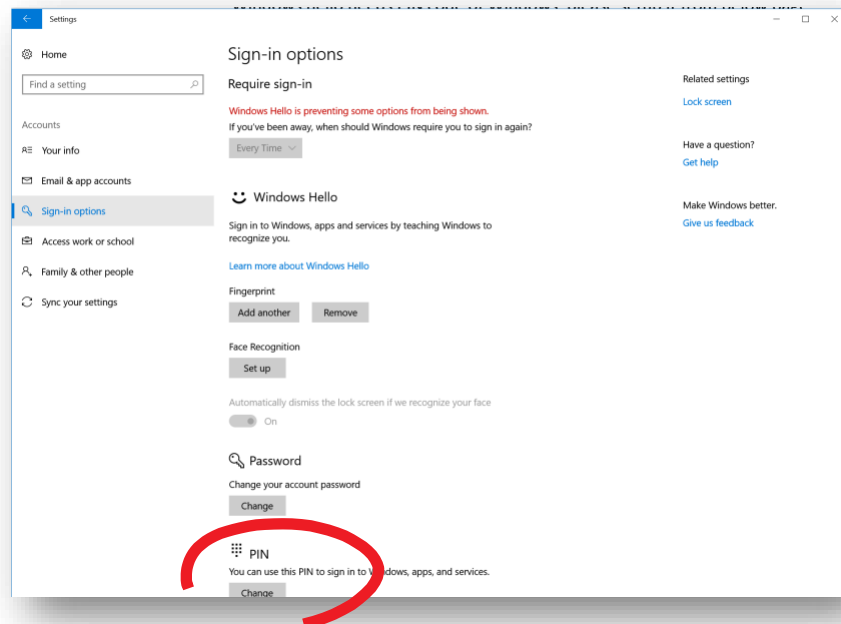


- Note 1: One host device (Windows or Mac) can just pair one BLE key, but one BLE key can work for multiple host devices (Windows and Mac).
- Note 2: to support FIDO U2F, it needs to download extra U2F plug-in for Chrome browser to enable it

- **Before install app**
 - Enable PIN
 - Windows hello needs PIN code of Windows, please setup it from below page:
 - Windows Settings => Accounts

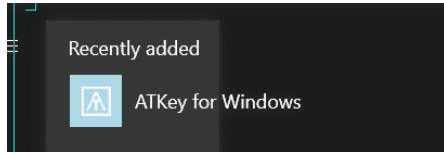


- Accounts => Sign-in Option



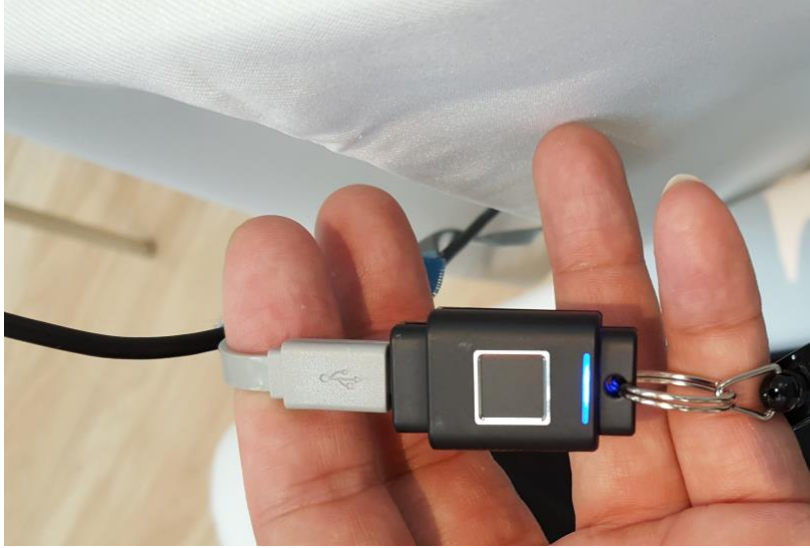
- PIN
 - SETUP your PIN code following Windows instructions

- After installed, find “ATKey for Windows” icon



- **Start your ATKey.BLE**

- Plug micro-USB power cable in to wake up Key first – LED Blue ON



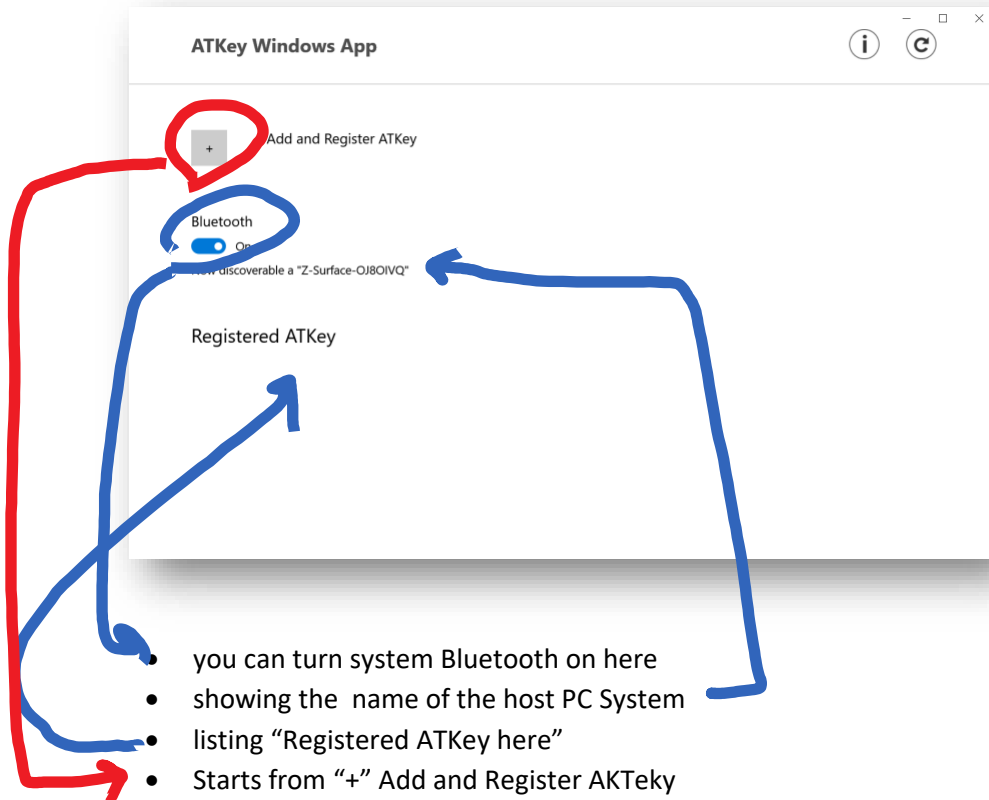
- Then, LED RED ON, power is charging



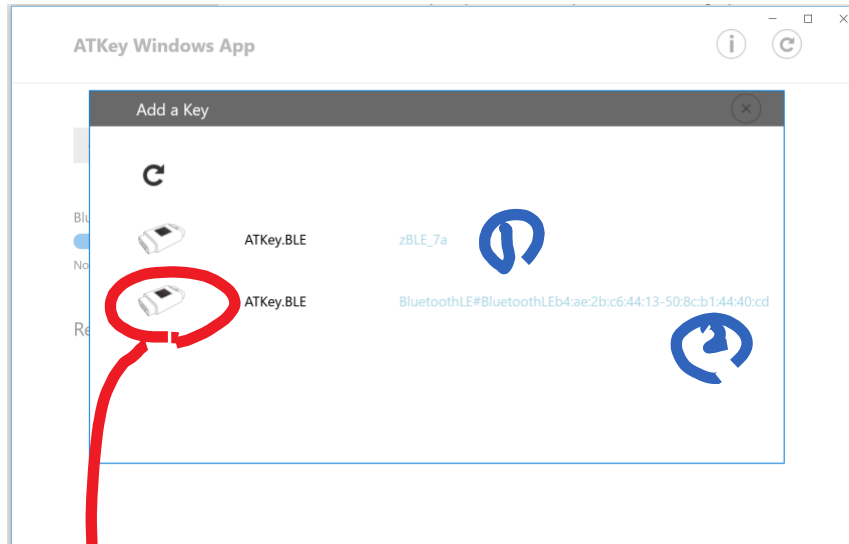
- You can continue power charging, or remove the micro-USB cable (if LED is flash RED, it means low power state, please re-charge it)
- Battery full charge – LED will be off
- Low battery (20% or lower) – the KEY won't work, RED LED is flashing, please do battery charge by Micro USB cable

- **Pair ATKey.BLE to your PC and APP**

- Click to run app (ATKey for Windows)



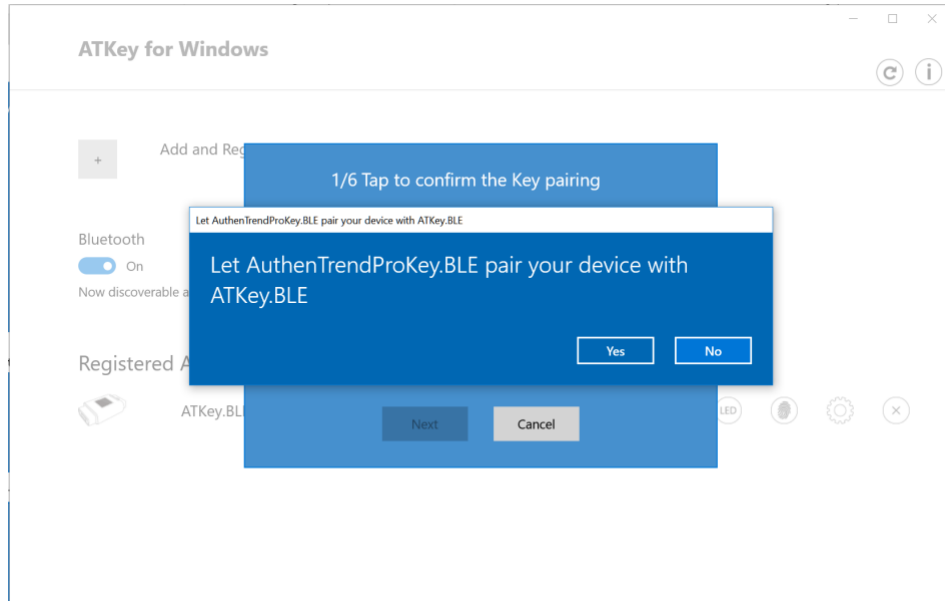
- Discover ATKey (base on RSSI) around the host PC



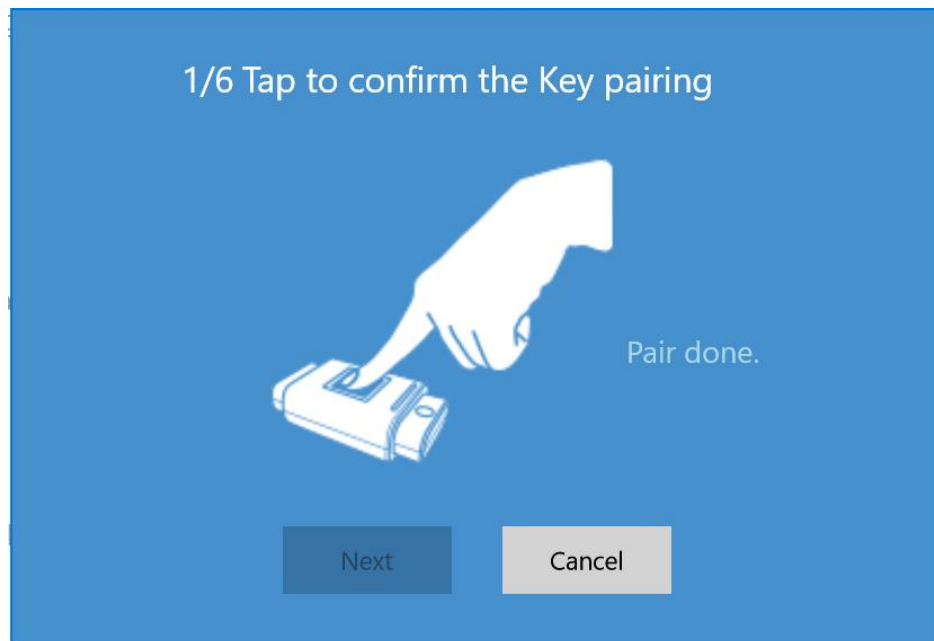
- Showing discovered ATKey
 - 1st example, ever registered and also rename the key
 - 2nd example, find a new ATKey, showing BLE ID (last 2 digits we noted on label sticker)
 - Click "icon" to connect the specific ATKey ...

- **Wizard mode: 1/6**, pair the device

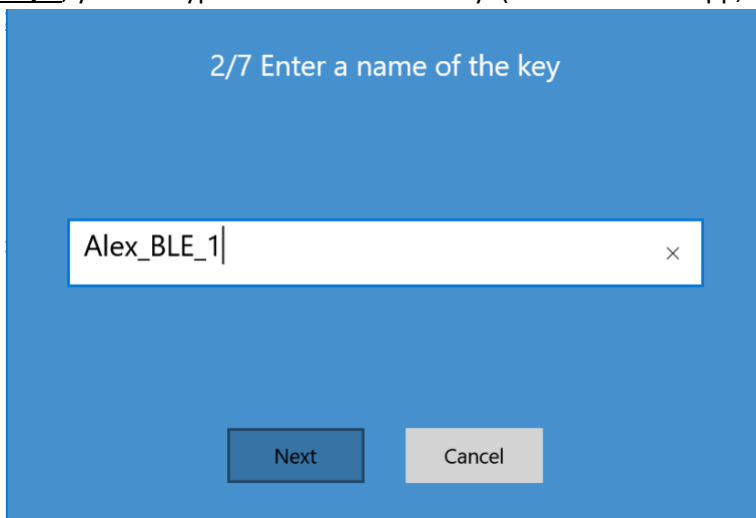
- “Yes” to pair



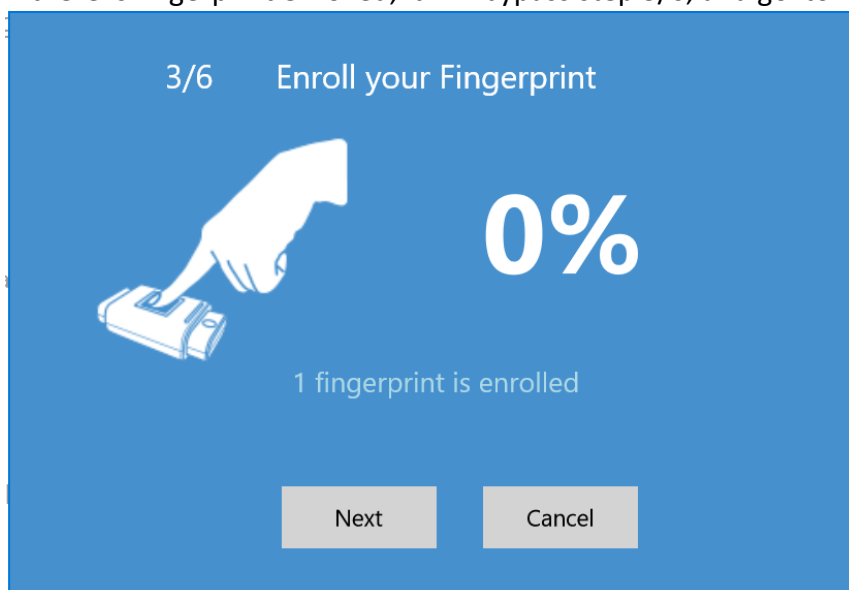
- Target ATKey LED is flashing (Blue), please tap the fingerprint to confirm the pairing (within 10 sec); if you did not touch the fingerprint to confirm within 10 sec. (timeout), please re-do it by Cancel first. “Yes” to pair



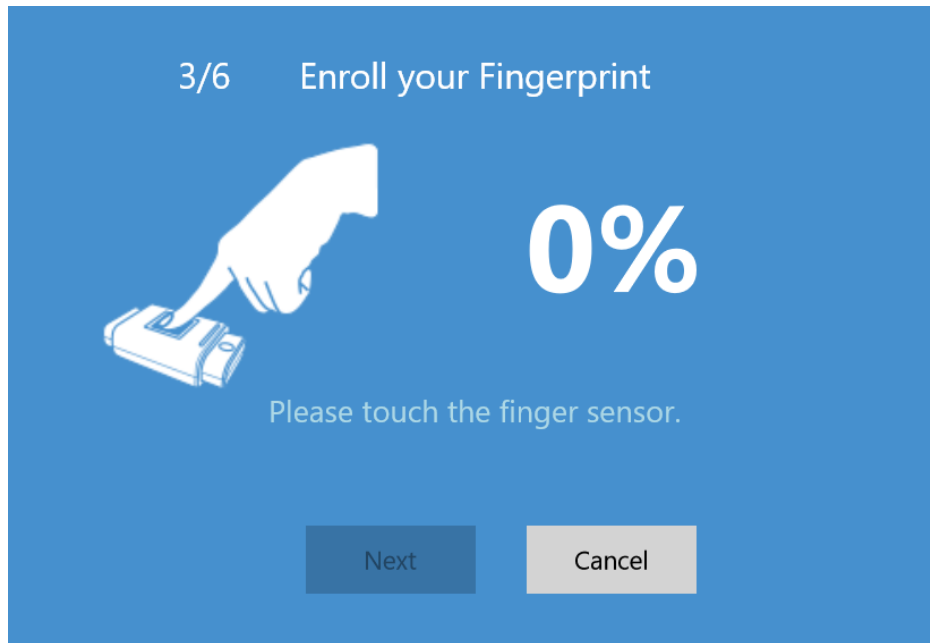
- **Next to 2/6**, you can type in a name for the key (store inside PC app, not inside the Key)



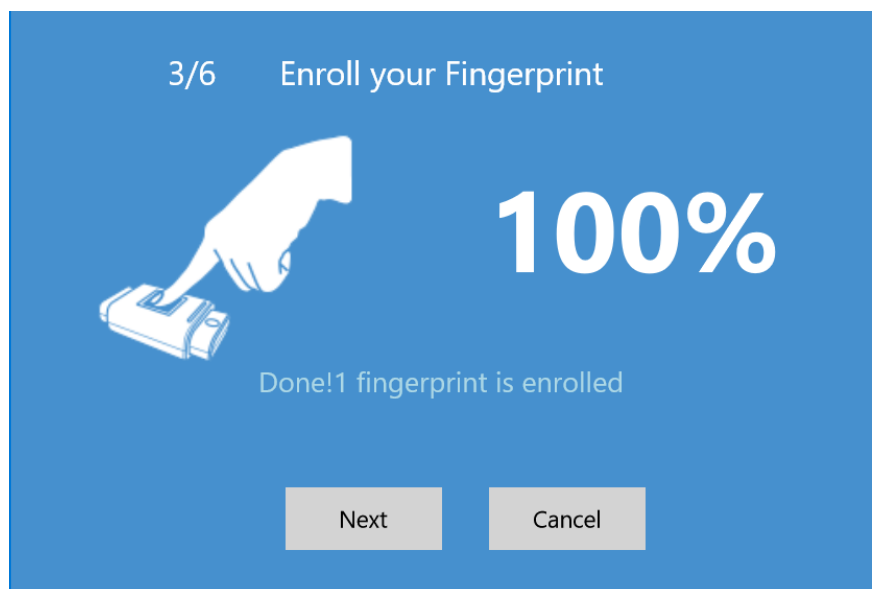
- **Next to 3/6**, enroll fingerprint (ATKey BLE LED is flashing by BLUE color)
 - If there is fingerprint enrolled, it will bypass step 3/6, and go to 4/6



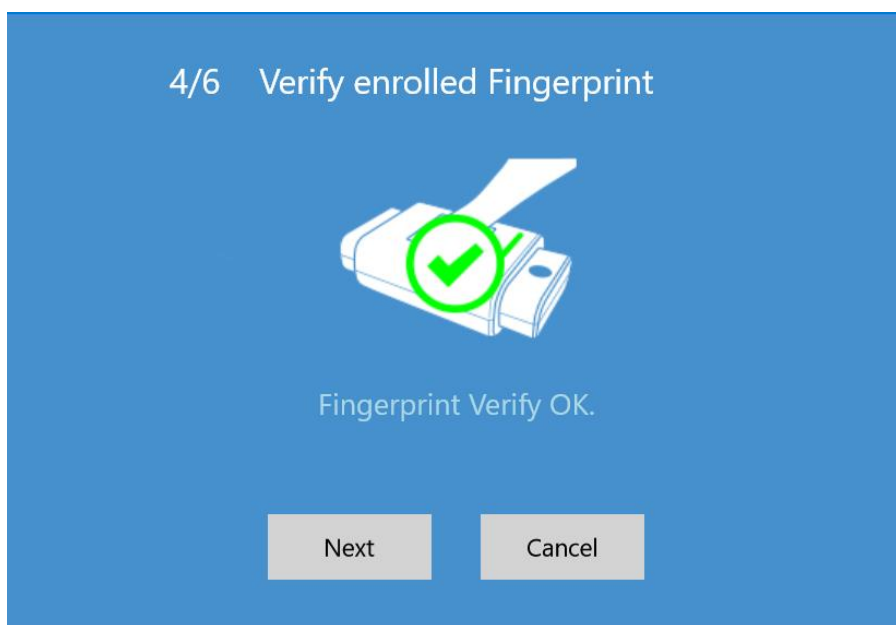
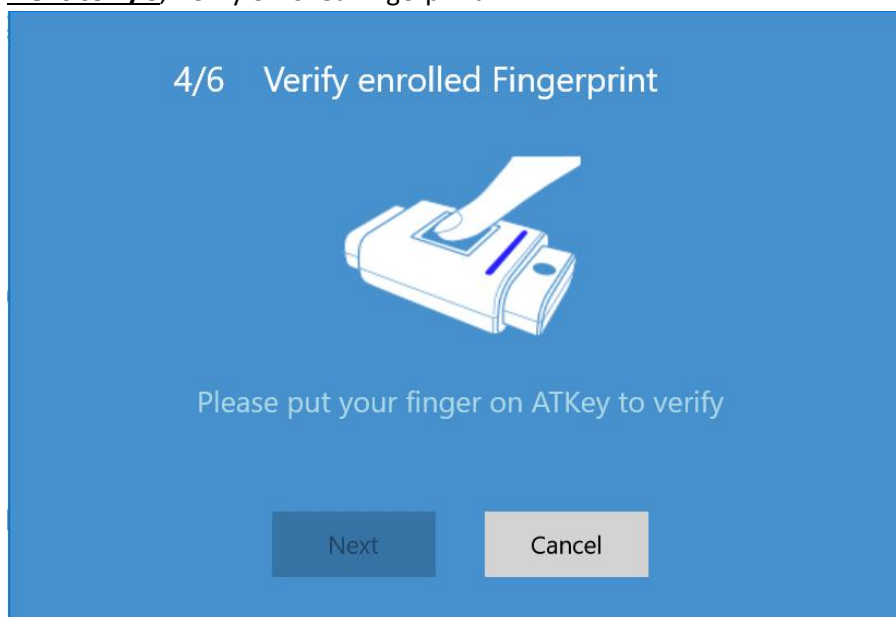
- If there is NO fingerprint enrolled:



- Please enroll your fingerprint following screen message (*touch and lift, slightly move finger for more locations of the specific fingerprint to be enrolled, but don't just change the angle during your fingerprint enrollment*), till 100% showing
 - Please enroll your fingerprint by the same direction; after enrolled, you can touch by any 360 degrees to verify (but don't do 360 degree enrollment)
- Just touch the fingerprint by your specific finger
- during the enrollment, the % is increasing like 8%, 16%, ..., normally it need 8~10 times enrollment

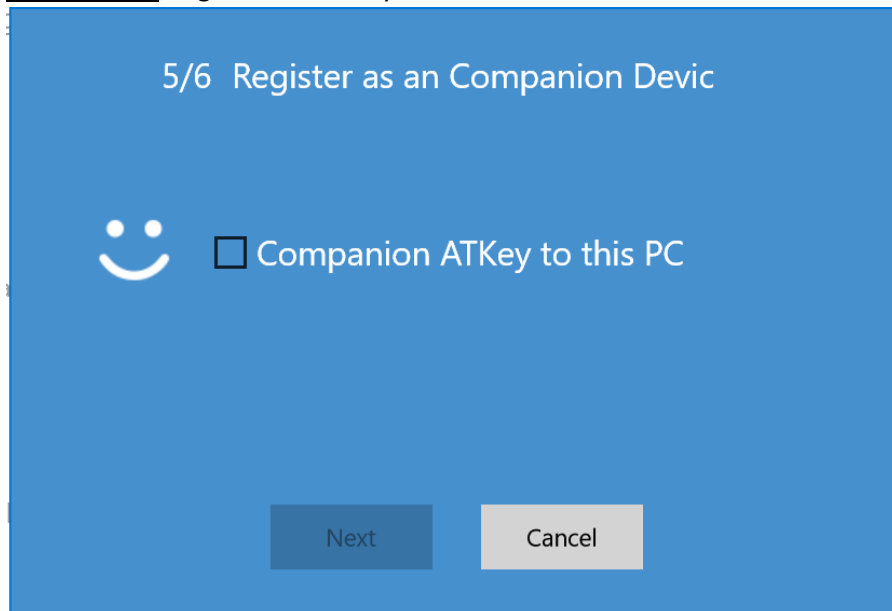


- **Next to 4/6**, Verify enrolled fingerprint

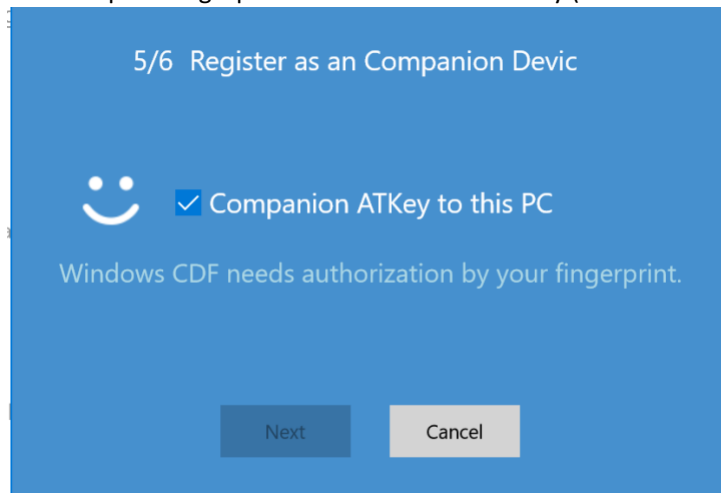


Verify "Success" (ATKey LED is **Green**), then go to 5/6;
Verify "Fail" (LED is **RED**), then LED continue flashing (**Blue**), try again; if it continues failed, please "Cancel" to stop it.

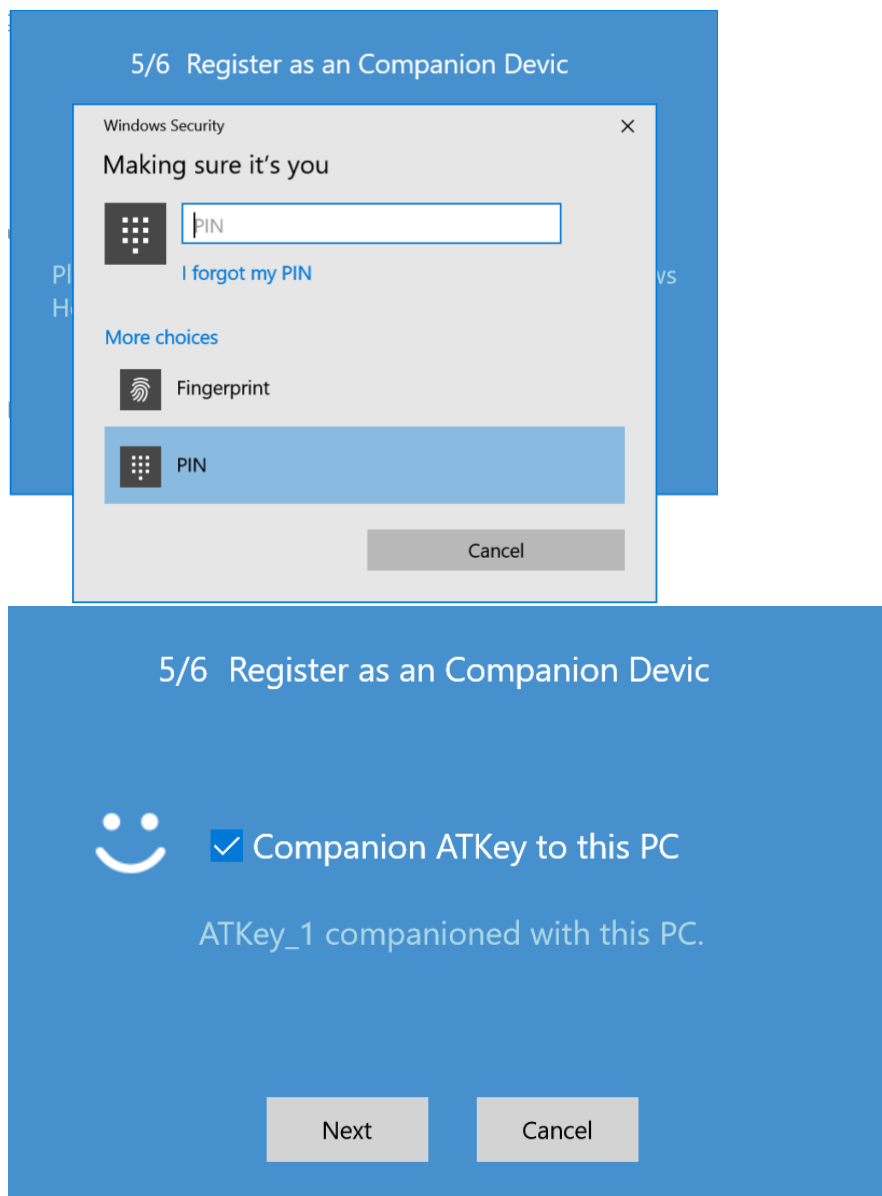
- **Next to 5/6**, register this ATKey to Windows CDF



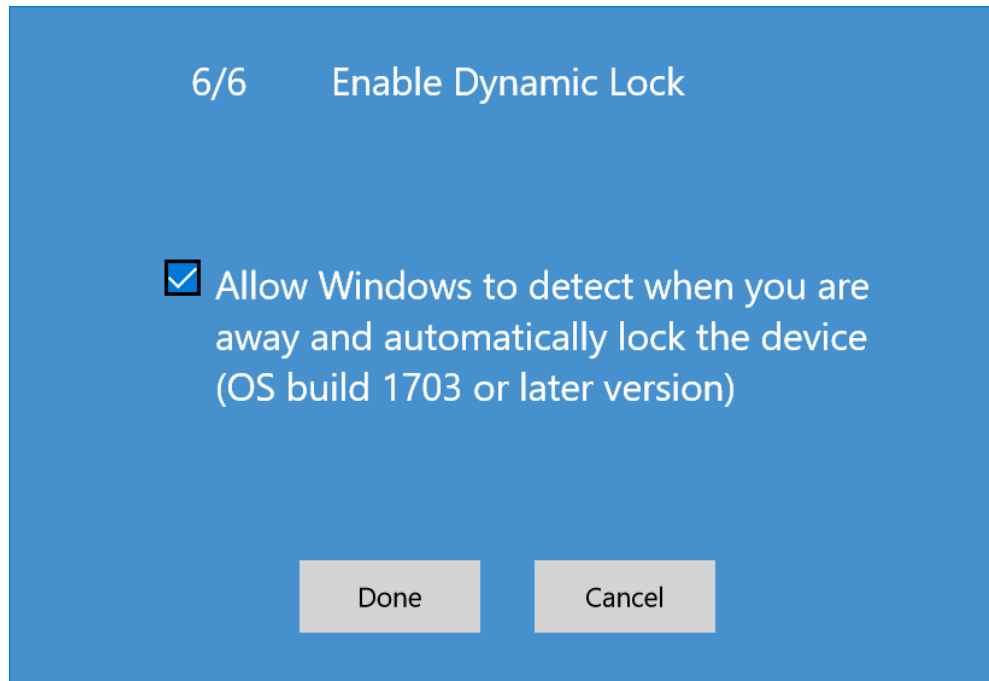
- “Check” the check box to enable it
 - It will request fingerprint verification from ATKey (LED is flashing BLUE)



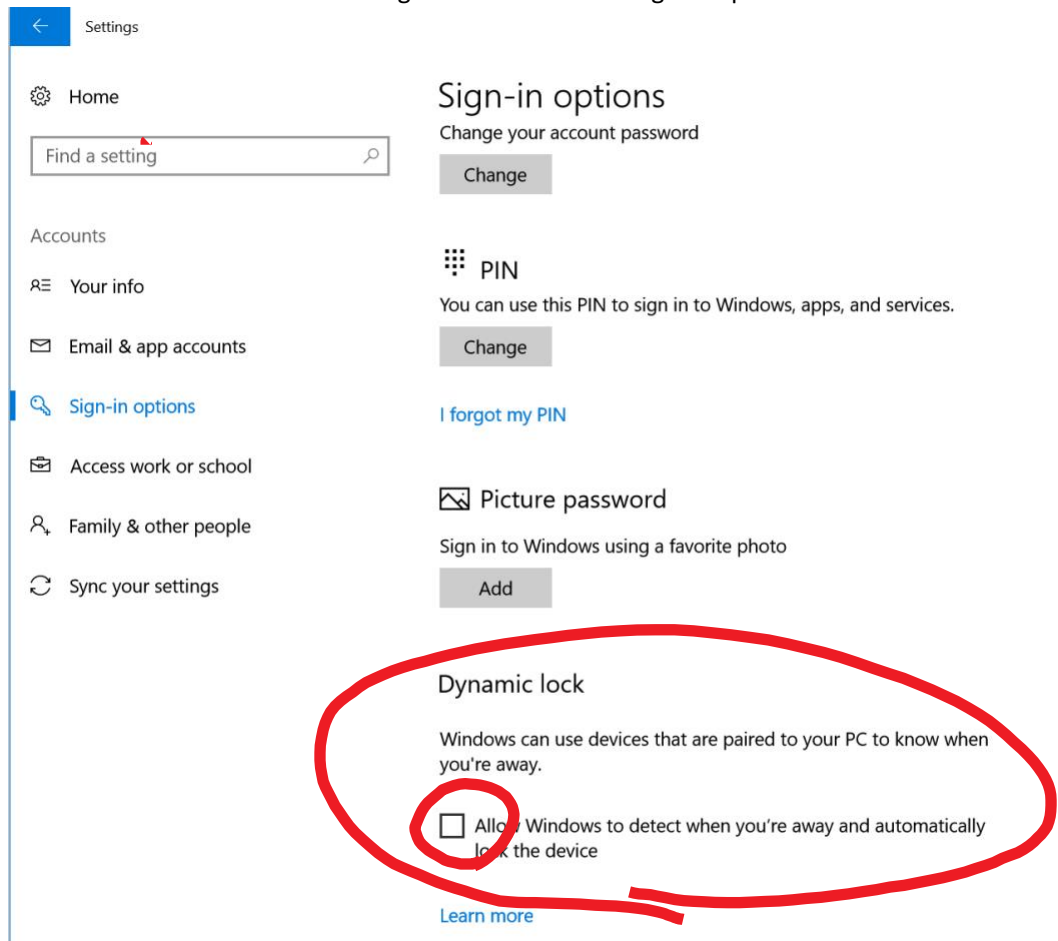
- And also request “PIN” code verification (Windows behavior)



- **Next to 6/6**, enable “Dynamic Lock” (*OS must be build 1703 or later version*)

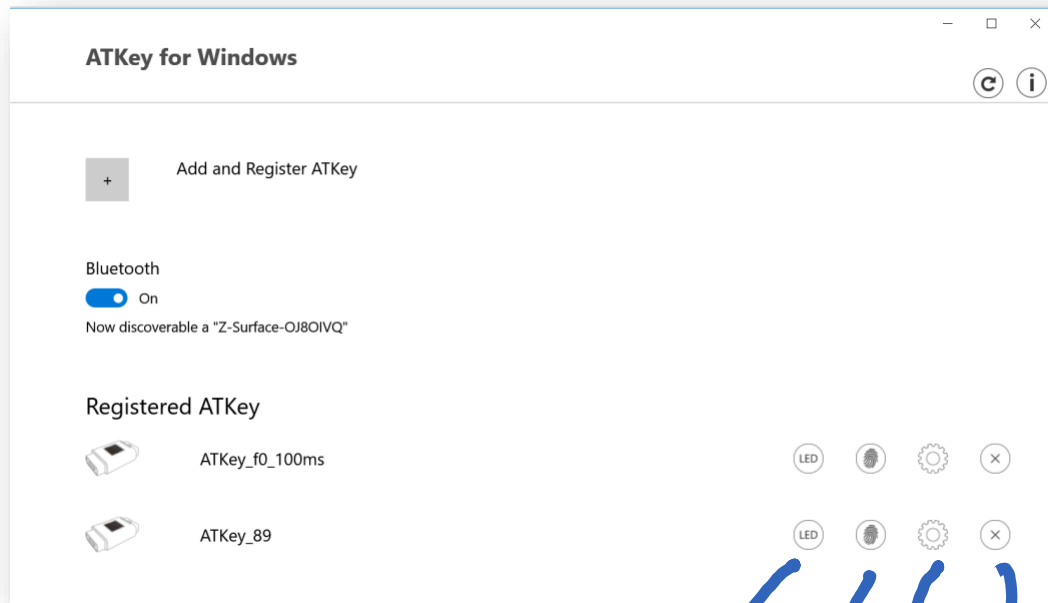


- This is relative to “Windows Setting” => “Account” => “Sign-in options”



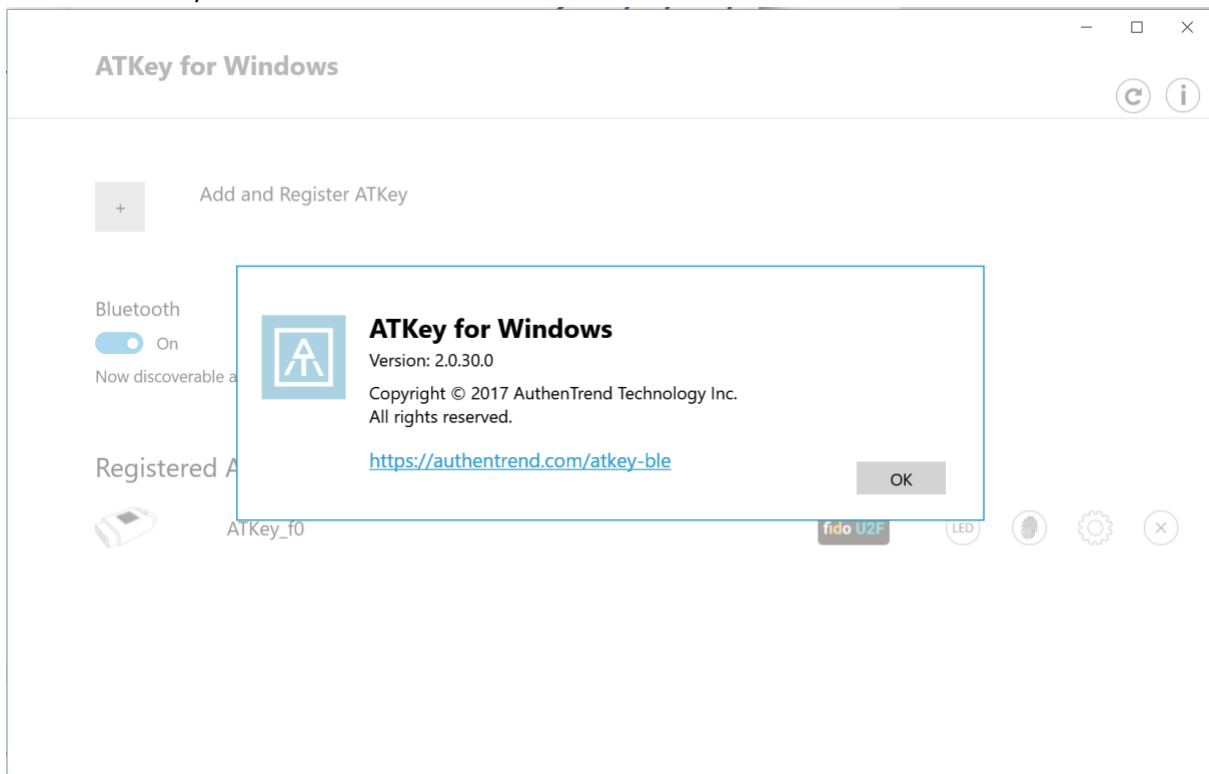
- Design concept of “Dynamic Lock”
 - Windows API - if there is NO operations for 30 sec., ATKey app is aware from Windows API, then we are checking the RSSI value of the companioned ATKey for 10 sec., if RSSI value is lower than -70, then lock the PC to Logon screen

- Wizard is done, you can see the Registered ATKey listing as below



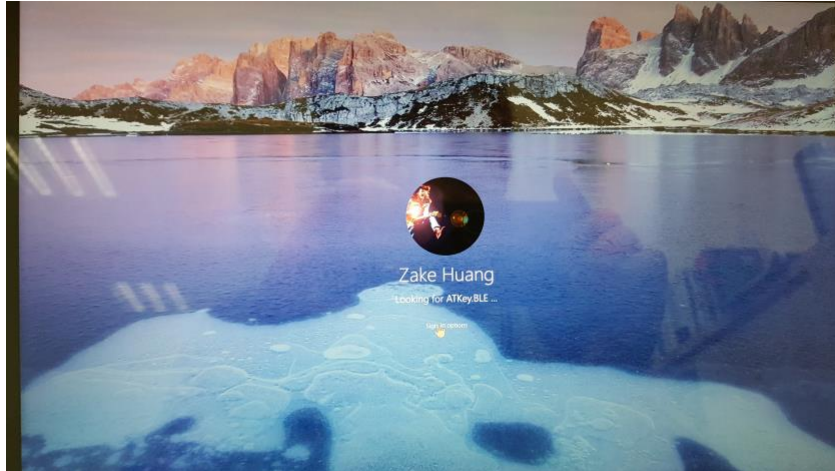
- Buttons of the ATKey:
 - “LED”: click it, BLUE LED of the ATKey will enable, and flashing for 5 sec. - this is helpful to identify the registered ATKeys if you have a lot of ATKeys there.
 - Fingerprint(s): add (up to 3), delete (delete all), Calibration (re-calibrate fingerprint sensor if you found FRR getting worse or slow response)
 - “Configure”:
 - Key information
 - BLE information
 - Rename
 - Dynamic Lock
 - “Remove”: Remove this ATKey from this PC (not paired, not companion)

- Info of the ATKey:

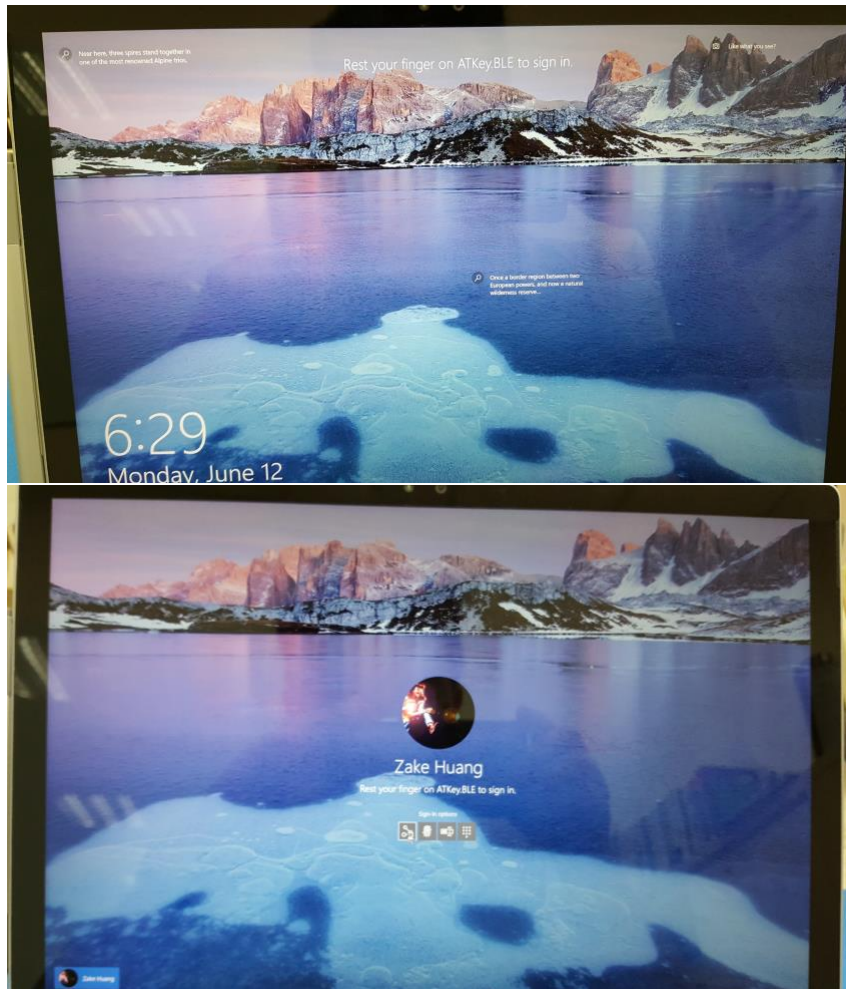


Here is app version number, and also URL of ATKey.BLE

- Try “Windows +L” to Windows Lock screen
 - Message showing on screen: **“Looking for ATKey.BLE...” “See ATKey.BLE for Sign-in instruction”,** and LED Is Blue for a second, then off (it means PC broadcasting to find the key)



- Message showing on screen: **“Rest your finger on ATKey.BLE to sign in”,** and LED is flashing Blue, please put your fingerprint on, till Green LED shows (or Red); then it will auto-unlock to Windows.



- Limitation from Windows 10: CDF device can't logon at cold boot or Windows reboot since it needs password or PIN code by design; but from Windows 10 build 1709 (RS3), it can support CDF login even at cold boot or reboot.

- **FIDO U2F (2nd Factor)**

- If you want to get more ideas of FIDO and U2F, please visit this URL:

<https://fidoalliance.org/specifications/overview/>

- ATKey for U2F

- **Read these items first:**

1. Please download and install Chrome Browser, we are doing U2F base on Chrome plug-ins
2. Here are FIDO U2F enabled online services



i.

- b. If you are using Google ID or Facebook ID as other online login, you can leverage ATKey as 2nd factor still for higher security

3. Please make sure you already paired and companioned your ATKey for Windows

- This is generic FIDO U2F:

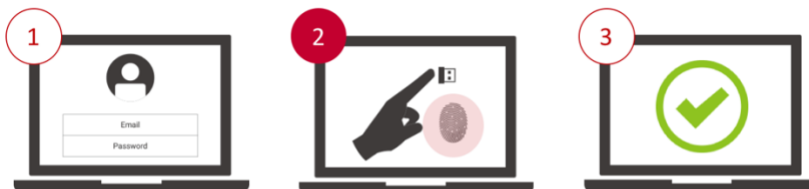
- 1st factor: something you know (ID/Password),
- 2nd factor: something you have (authenticator)

SECOND FACTOR EXPERIENCE (U2F standards)



- AuthenTrend brings biometrics into FIDO as 3rd factor combining with 2nd factor, high secure even you lost the authenticator, no one can use it except fingerprint verified

- 1st factor: something you know (ID/Password)
- 2nd factor: something you are (fingerprint) + something you have (ATKey)



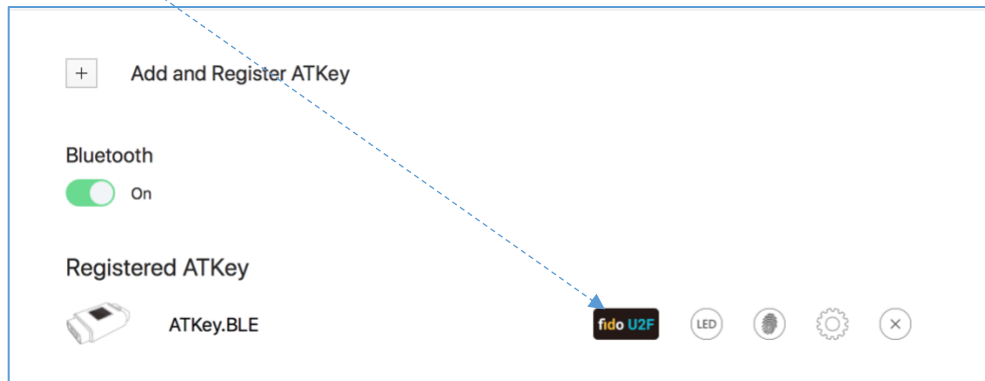
1st factor: Something you know (ID/Password)

2nd factor: Something you have + Something you are!

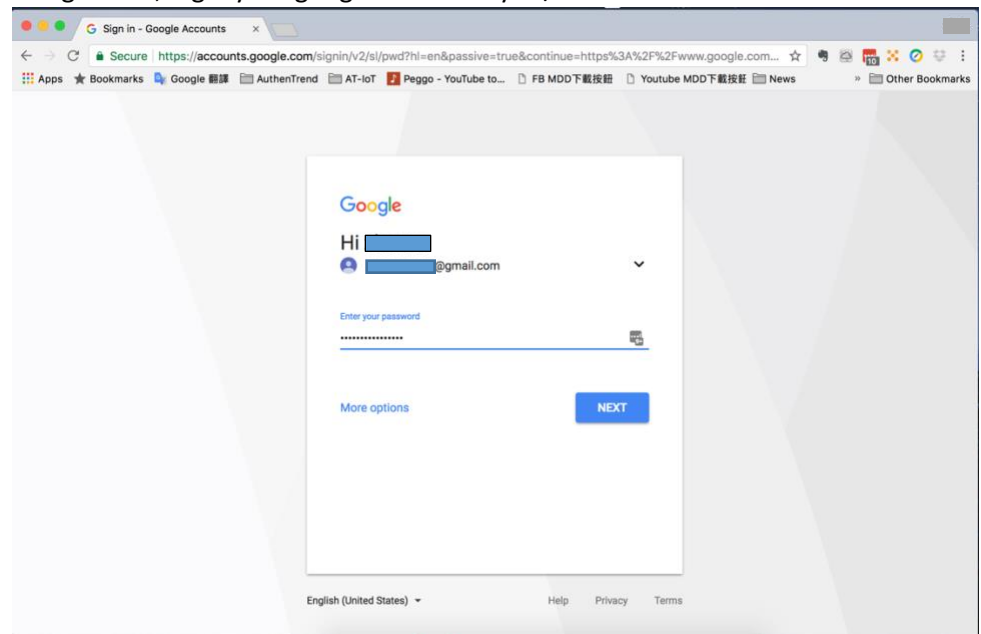
- Install and enable U2F:
 - Download and install “ATKey U2F Plug-in” from AuthenTrend web site; after installation, you should see below program icons from Start Menu



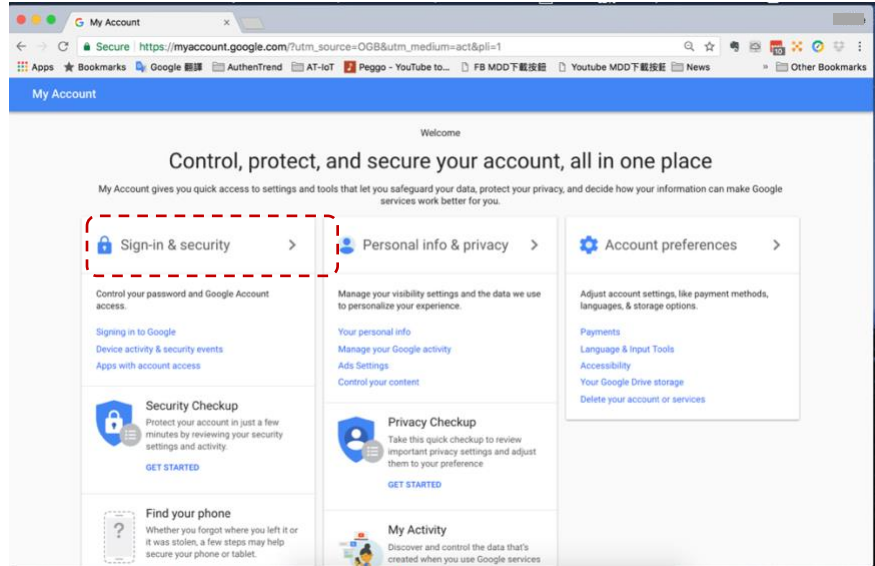
And “fido U2F” icon is enabled as below:



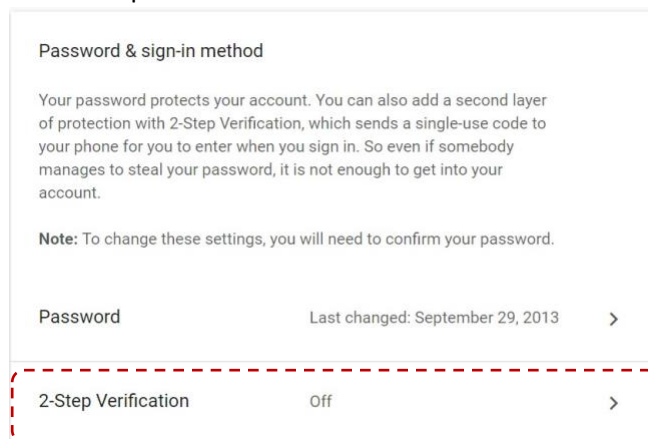
- Take example from Google
 - a) Google.com, login your google account by ID/Password first as usual:



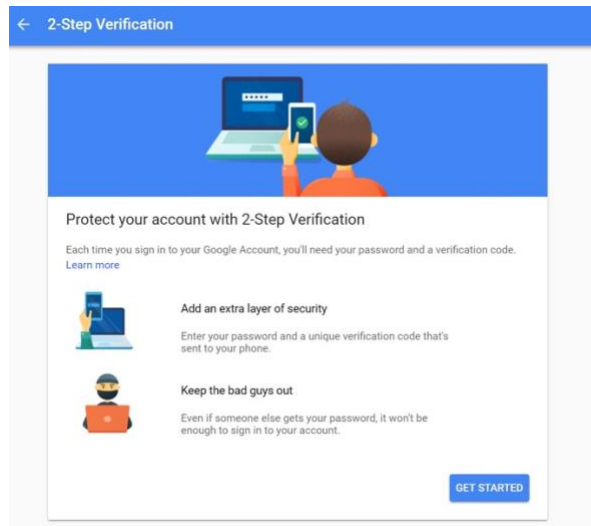
- b) Enabled U2F
 - Start from “Sign-in & Security”:



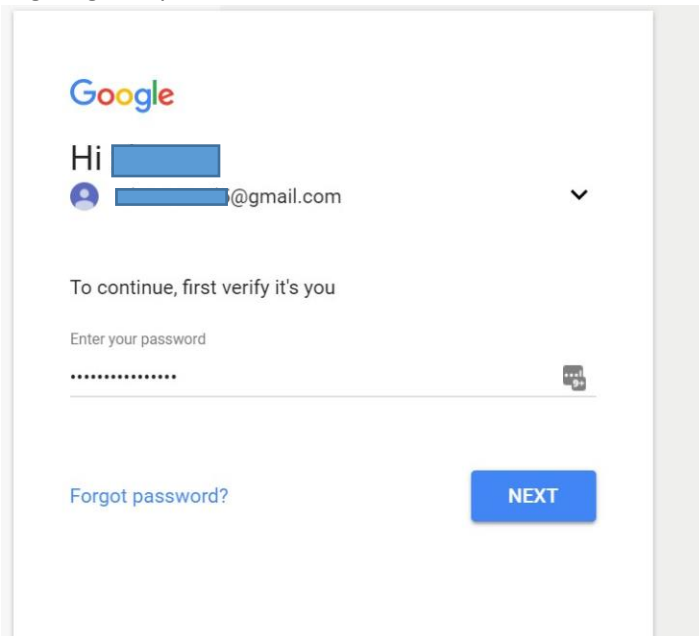
○ Turn 2-step Verification ON



○ Get Start



- Login again by ID/Password:



Google

Hi [redacted]

[redacted]@gmail.com

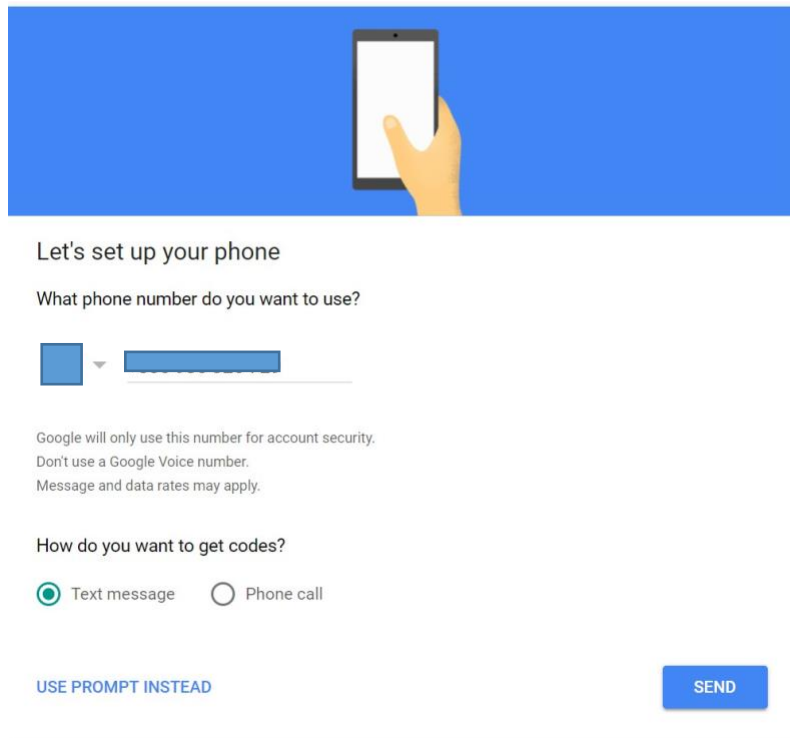
To continue, first verify it's you

Enter your password

.....

[Forgot password?](#) **NEXT**

- You must get SMS code from your mobile phone first – select your country, type in your phone number, click “SEND” to receive SMS code



Let's set up your phone

What phone number do you want to use?

[country code] [phone number]


Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

☒ Text message ☐ Phone call

[USE PROMPT INSTEAD](#) **SEND**

- Type in SMS code



Confirm that it works


Google just sent a text message with a verification code to **0936 326 729**.

[Enter the code](#)

Didn't get it? [Resend](#)

[BACK](#) [NEXT](#)

- Confirm to turn on 2-step verification (default is voice or SMS)



Turn on 2-Step Verification?

Second step: **Voice or text message (default)**

You'll stay signed in to [redacted]@gmail.com on these devices: [redacted].

You'll be signed out of your other devices. To sign back in, you'll need your password and second step.

[TURN ON](#)

- Page down to find "Security Key" and "add security key"

2-Step Verification

2-Step Verification is ON since Feb 6, 2018

TURN OFF

Your second step

After entering your password, you'll be asked for a second verification step. [Learn more](#)

Tired of typing verification codes?

Get a Google prompt on your phone and just tap Yes to sign in.

ADD GOOGLE PROMPT

Voice or text message (Default)

Verification codes are sent by text message.

Set up alternative second step

Set up at least one backup option so that you can sign in even if your other second steps aren't available.

Backup codes

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.

SET UP

Google prompt

Get a Google prompt on your phone and just tap Yes to sign in.

ADD PHONE

Authenticator app

Use the Authenticator app to get free verification codes, even when your phone is offline. Available for Android and iPhone.

SET UP

Backup phone

Add a backup phone so you can still sign in if you lose your phone.

ADD PHONE

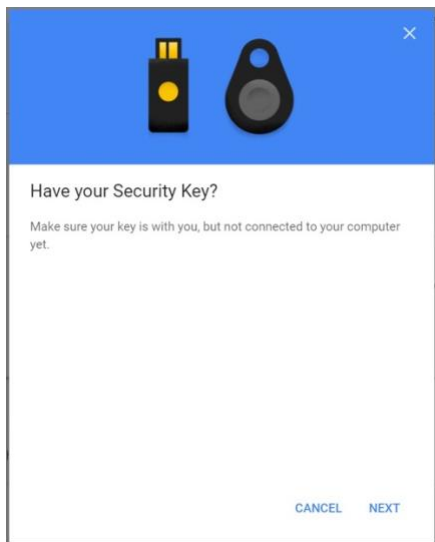
Security Key

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. [Learn more](#)

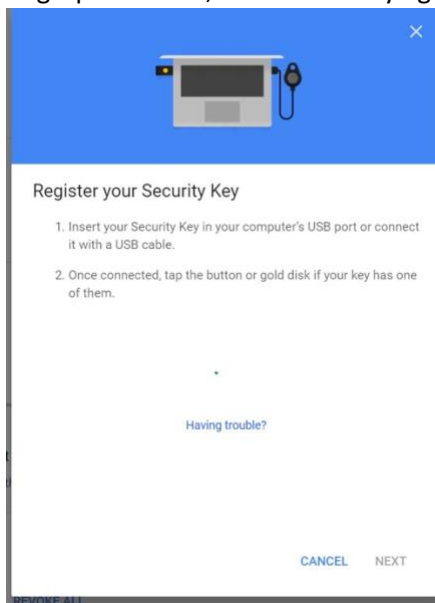
ADD SECURITY KEY

- Prepare your ATKey

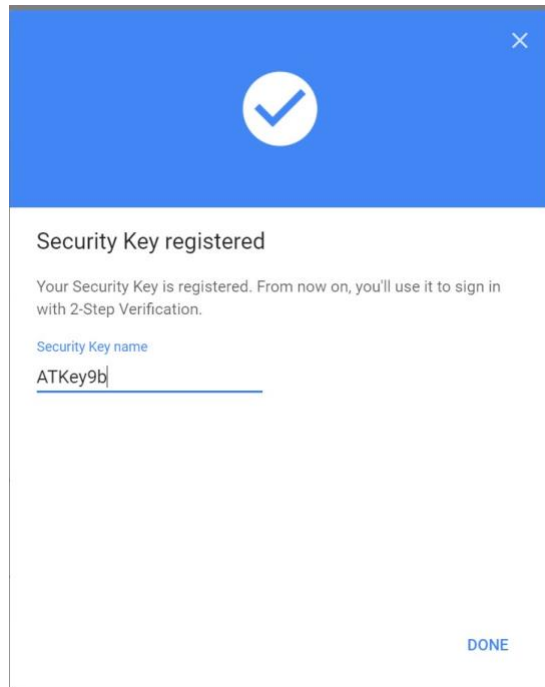
22



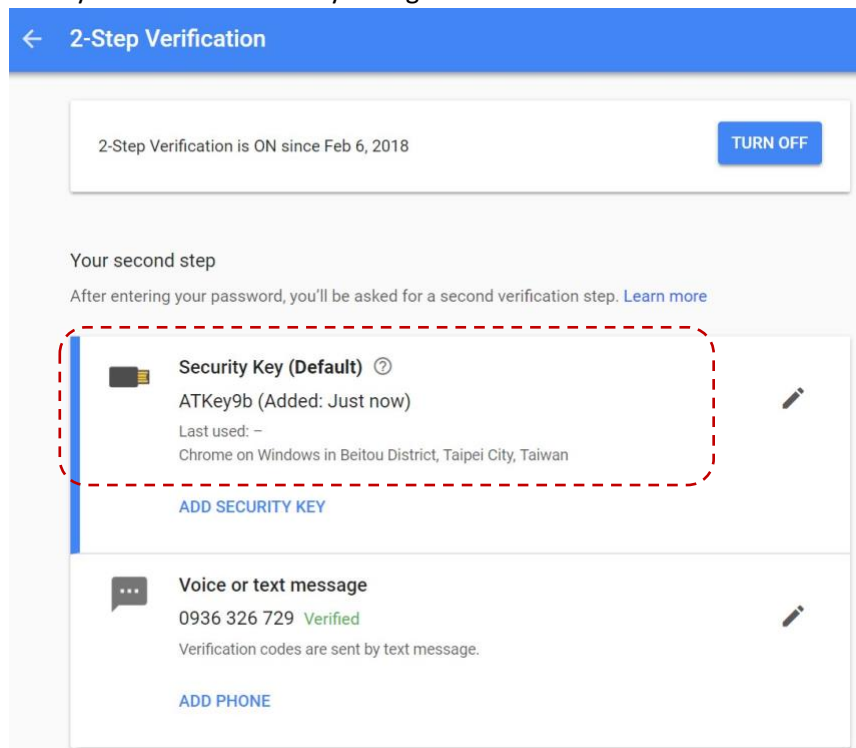
- Register ATKey here – when Blue LED is flashing (ATKey), touch by your registered finger, when Green LED is ON, it means fingerprint verified and register this ATKey to Google U2F server; if Red LED is on, it means fingerprint failed, wait and verify again



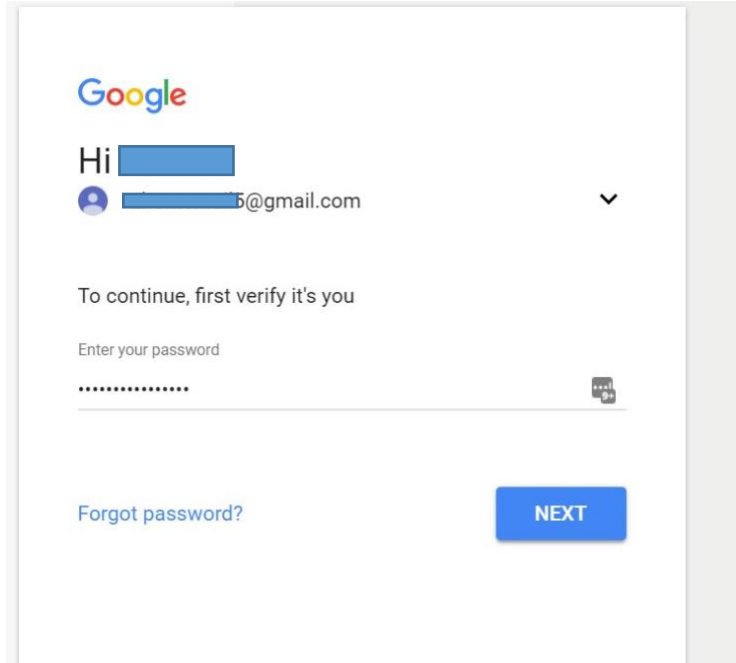
- Fingerprint verified, type in the name of ATKey, then “Done”



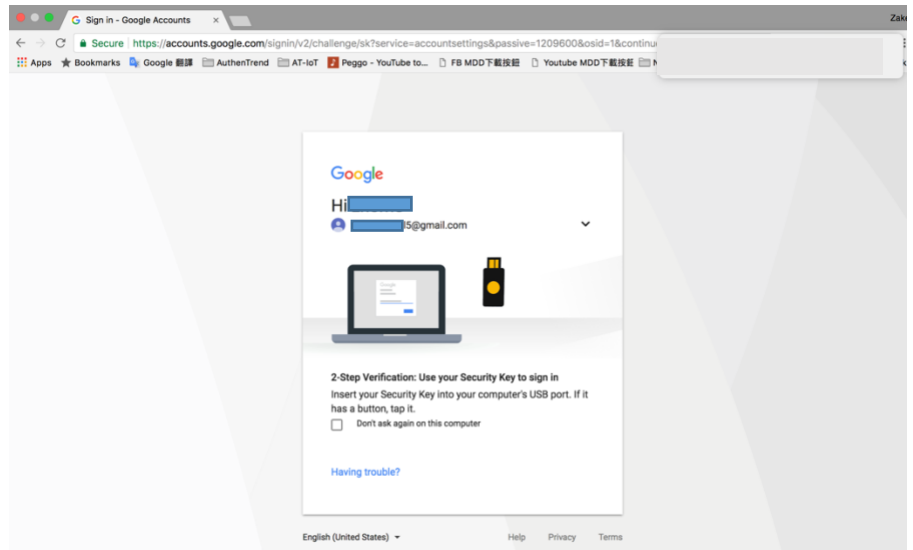
- Then you can see the ATKey listing as a 2nd factor



- c) Logout and login your Google account again:
 - 1st factor: ID/Password still



- 2nd factor: when the blue LED is flashing (ATKey), touch your fingerprint to verify (Green LED on), then it passed 2nd factor to login your google account



- For other U2F enabled services:
 - Dropbox: <https://www.dropbox.com/help/security/enable-two-step-verification>
 - Facebook: <https://www.facebook.com/notes/facebook-security/security-key-for-safer-logins-with-a-touch/10154125089265766/>
 - Github: <https://help.github.com/articles/configuring-two-factor-authentication-via-fido-u2f/>
 - Salesforce: https://help.salesforce.com/articleView?id=security_u2f_enable.htm&type=5

- **Trouble Shooting**

- ATKey.BLE can't work if the battery is lower than 20%
 - Battery consuming:
 - Fingerprint matching (major)
 - BLE broadcasting (this is background task to consume battery, and it won't stop) for better BLE connection and actions
- One ATKey.BLE for multiple devices
 - If you have more than 1 device (Windows PC, Mac, ...) paired with your ATKey.BLE, it will connect to demanding one (by BLE broadcasting); but if there are 2 or more devices are broadcasting and requesting the ATKey.BLE, it may connect to closet one (depending on BLE RSSI)
 - After login (fingerprint matched and login device), we will disconnect it, so another device can broadcast to find ATKey.BLE to connect
- If your target device can't find ATKey.BLE (from app, from login screen)
 - The Key should be connected by other device, you need to disconnect it first
- Maximum: 3 x fingerprints
 - It may take more seconds for fingerprint matching if you have more than 1 fingerprint registered
- Rename of ATKey.BLE
 - The name will just keep inside app, not inside the ATKey; default name is "ATKey.BLE"
- "Reset" – when you plug the power source in (Micro USB port), ATKey.BLE will be reset (Blue LED), then charging
- U2F support
 - We will release separated "U2F Plug-in" to download
 - We will provide another U2F user guide