



User Guide for



AUTHENTREND



Index

- ATKey.Card NFC briefing
- Initial ATKey.Card NFC via APP “SecurityKey NFC”
 - iOS or Android
 - Activation
 - Reset
 - Set PIN code
 - Enroll fingerprints
 - Check sign-in data
- Register to Passkey enabled services
- Authentication as a Passkey

**Please check PC (Windows, Mac) user guide separately!*

https://authentrend.com/atkeycardnfc_user_guide_pc/



- ISO/IEC 14443 Mifare Type-A 13.56MHz contactless Smart card, without battery.
- Dimension: 85 x 54 x 0.8mm, meet ISO/IEC 7810 spec.
- FIDO2 CTAP2.1 certified: Device-bound (Hardware) Paskey.

Unique ID

Fingerprint sensor, allow max. 2 fingers

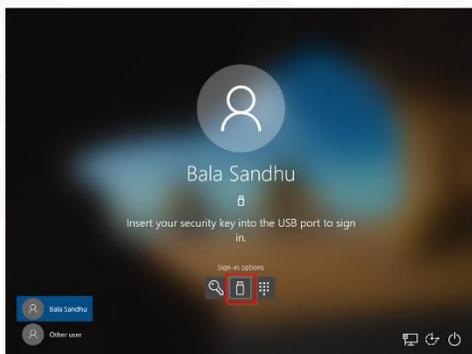
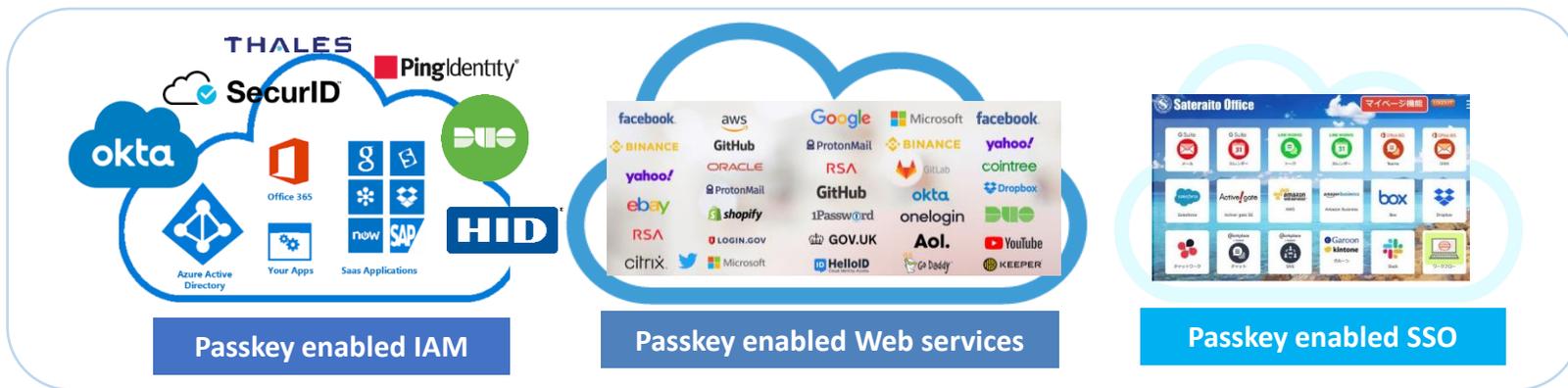
NFC antenna area
Built-in Mifare Type-A UUID

For 7816 smart card reader
the reader must be full support for short APDU and extended APDU commands.

back-side is blank, reserve for badge printing



Applications



Windows Passwordless login joined Entra ID (Azure AD) PC
https://authentrend.com/download/ATKey_for_MSFT_AzureAD_guide.pdf



Go Passwordless for Your Personal Computer Authentication.

Windows Passwordless login to any Windows Account via ATKey.Login
<https://authentrend.com/atkey-login/>



For security reason,
 • if PIN code continuous failed 8 times, or
 • fingerprint continuous failed 15 times,
 the card will be locked, user needs to reset it.



• iOS needs Safari browser for NFC Paskey



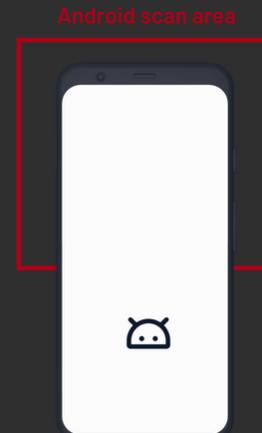
Physical access (Mifare TypeA UUID); but w/o fingerprint matching



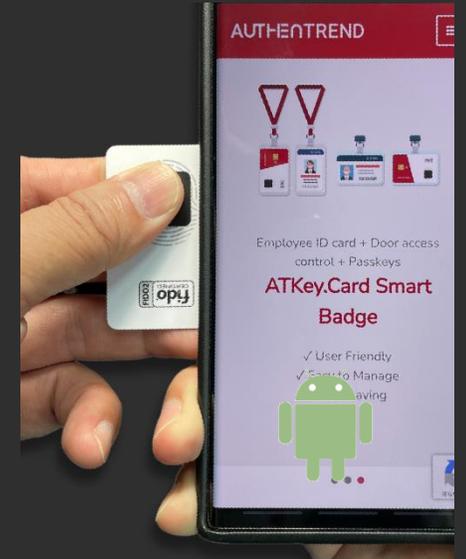
back-side is blank reserve for badge printing



Take the card by “enrolled” thumb finger (on fingerprint sensor sear) and index finger (on back)



iPhone is fixed location



For Android, please turn NFC ON from settings, and normally MFC Antenna is on back side, please check your Android Phone brand and model to make sure the NFC antenna location



Download APP: "SecurityKey NFC"



SecurityKey NFC

Manage your ATKey.Card NFC



Please apply Android App public testing below to get "SecurityKey NFC" app for Android:

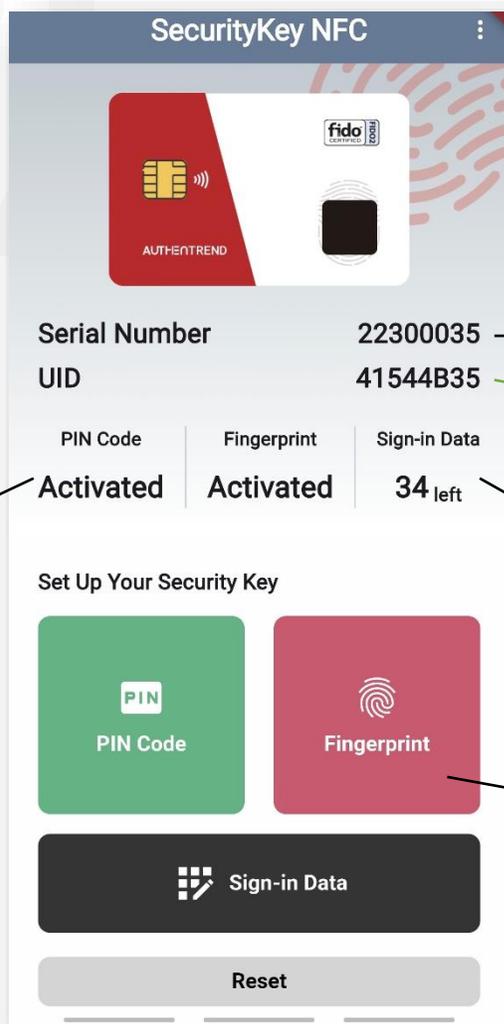
- Join through your Android device:
https://play.google.com/store/apps/details?id=com.authentrend.security_key_nfc
- Join through network:
https://play.google.com/apps/testing/com.authentrend.security_key_nfc

We recommend to check video here as step-by-step guide:

<https://www.youtube.com/watch?v=2APP6j7Tlrg&t=4s> (iOS version)



App Briefing



Unique ID, inked on Card surface and also inside card itself, not changeable.

Mifare Type A UID

Allow 38 FIDO2 credentials, here means we already registered 4, so remaining 34

Enroll fingerprint here, but following FIDO2 spec., PIN needs to setup first

- It's totally new card, or after reset, here is "Inactive" state;
- If PIN code set, it's activated state;
- If Fingerprint enrolled, it's Activate state.

Step1: Activate Card



- Launch “SecurityKey NFC” app
 - Click “Manage”, then tap card on Phone NFC Antenna area
 - iOS: NFC ON is automatically
 - Android: NFC ON/OFF is manually, please turn it on from Settings

- 1 Unique serial number inside each card; it may also prints on card surface (beside FIDO logo)
- 2 Mifare Type A UUID, for Mifare reader (door access control)
- 3 Remaining sign-in data you still can register (to those Passkey enabled services); *here only records registered as “FIDO2 Security key”*, U2F is not recorded to counter.

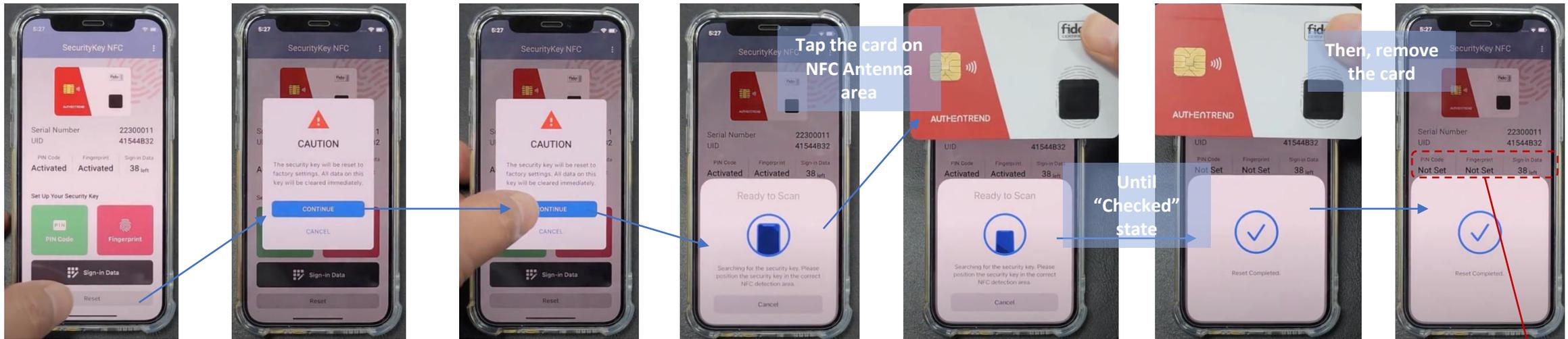




Step2: Reset



- Reset to factory state, it does not need user's PIN code or Fingerprint authentication
 - Click "Reset", then tap the card on NFC Antenna area

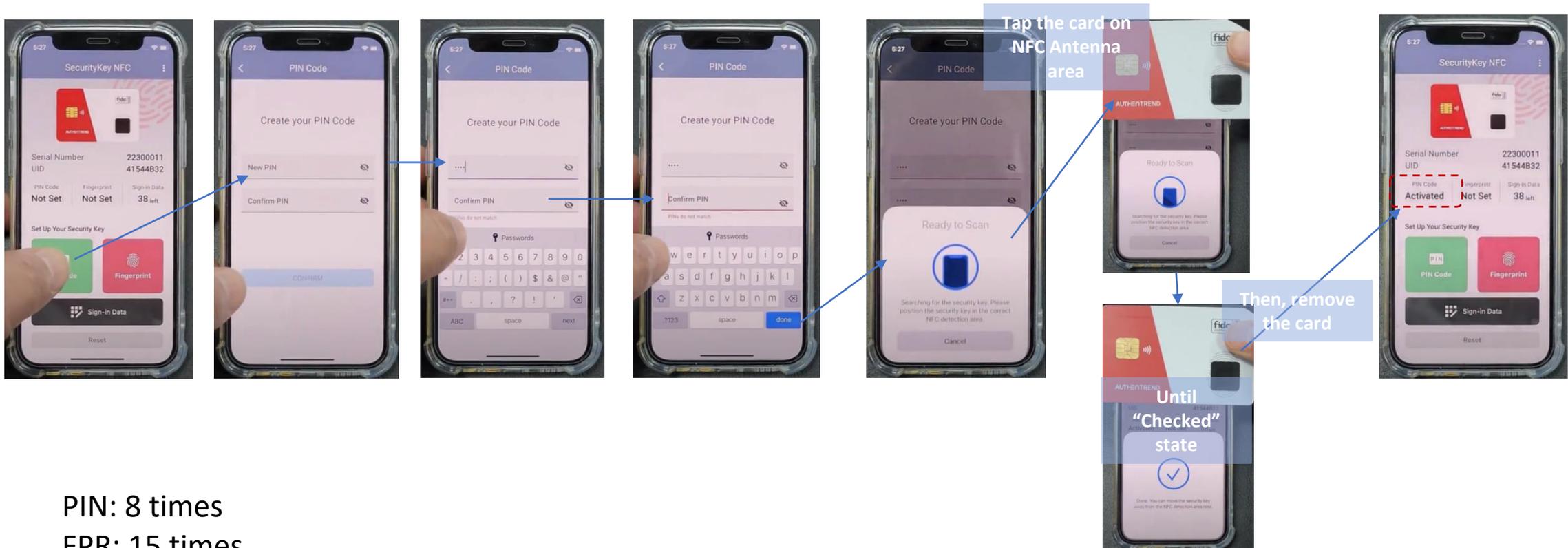


PIN code, fingerprints are all reset, and sign-in data is back to max.



Step3: Setup PIN code

- Setup PIN code to the card, then you can enroll fingerprint
 - PIN is only for card management, not for authentication
 - Fingerprint failed continuously, user can't login by typing PIN code instead of biometrics verifications.

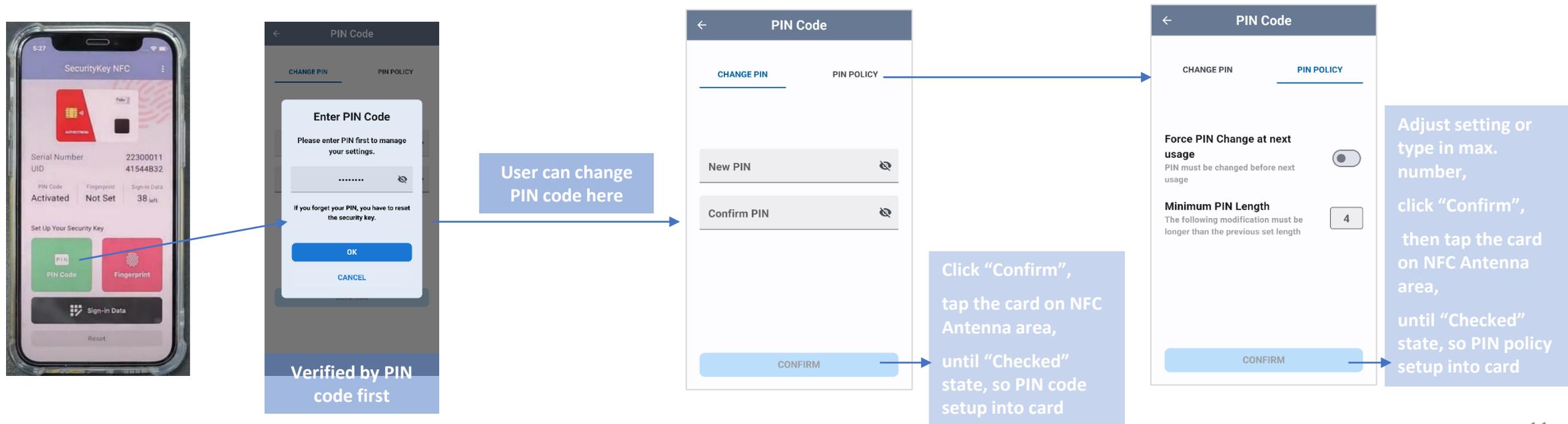


PIN: 8 times
FPR: 15 times



Step3-1: Configure PIN Policy

- We allow user to configure the PIN code policy
 - Change PIN code
 - User can change PIN code (after PIN verified), or the card setup by Admin (with PIN code) but force to change at 1st time use
 - PIN Policy
 - Force PIN Change at next usage –normally this is admin feature to avoid any unexpected modification during delivery or transportation to employees
 - Admin can request minimum PIN length for security

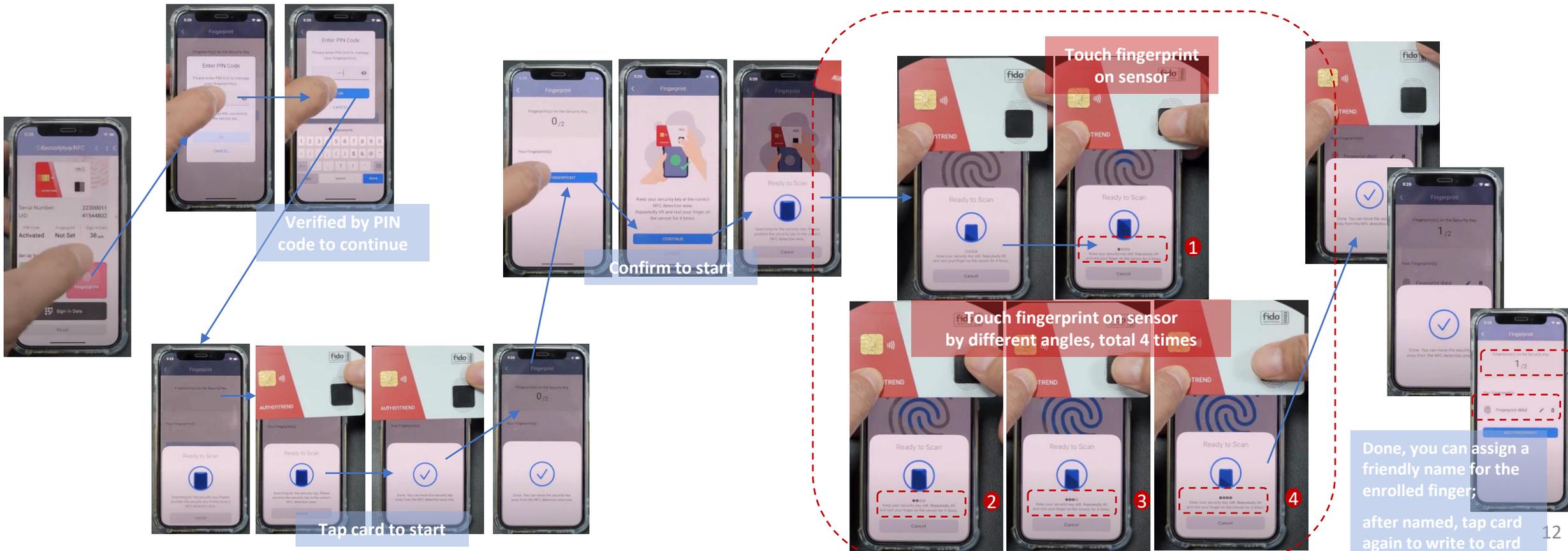




Step4: Enroll Fingerprint



- Click “Fingerprint”
 - If it’s new card w/o fingerprint enrolled, type in PIN code to enroll fingerprint
 - If the card with fingerprint enrolled, verified by fingerprint or type-in PIN code to continue

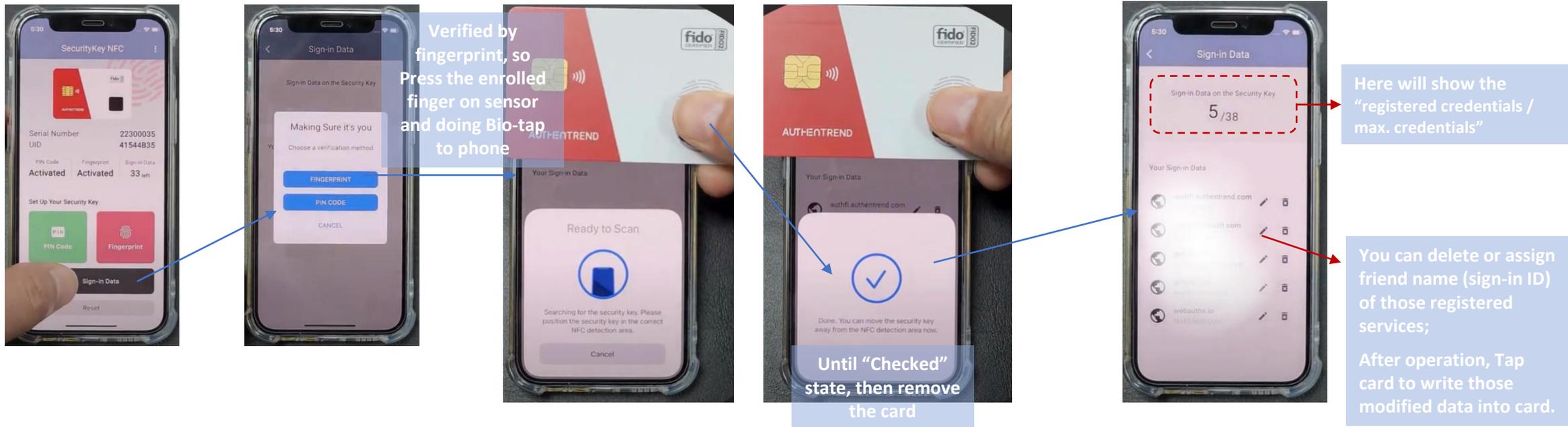




Step5: Manage Sign-in Data



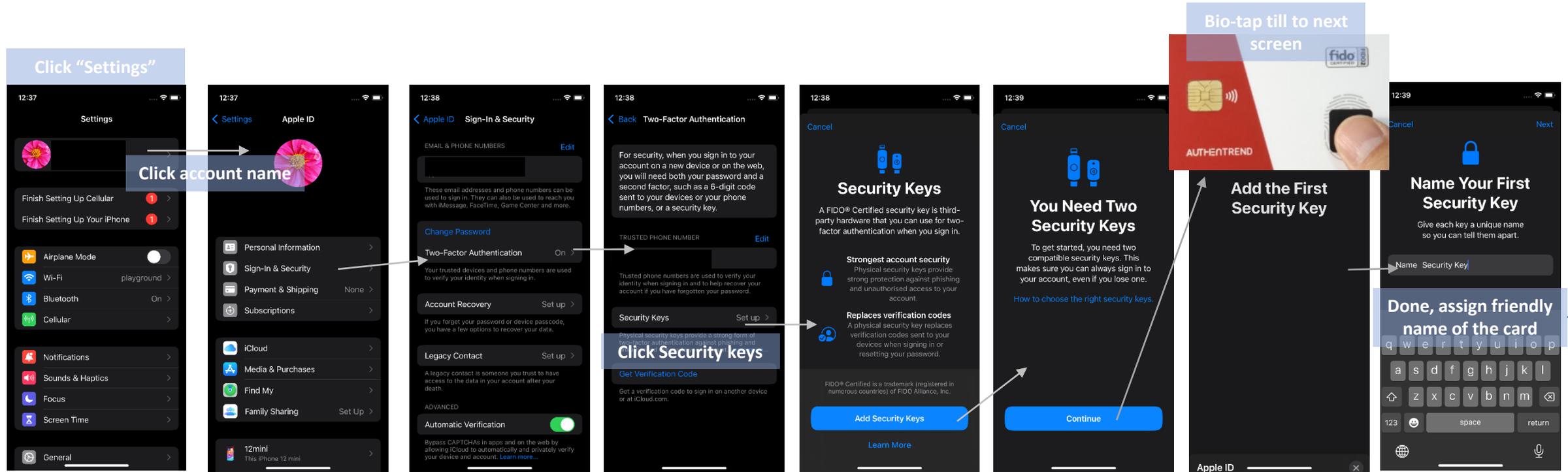
- Click “Sign-in Data”
 - Verify by fingerprint or PIN to continue
 - You can delete registered sign-in data from card, or assign friendly name (sign-in ID) for the registered services



Register Card to Passkey enabled Service



- Example from iCloud **iOS** (but it needs 2 security key as a backup)

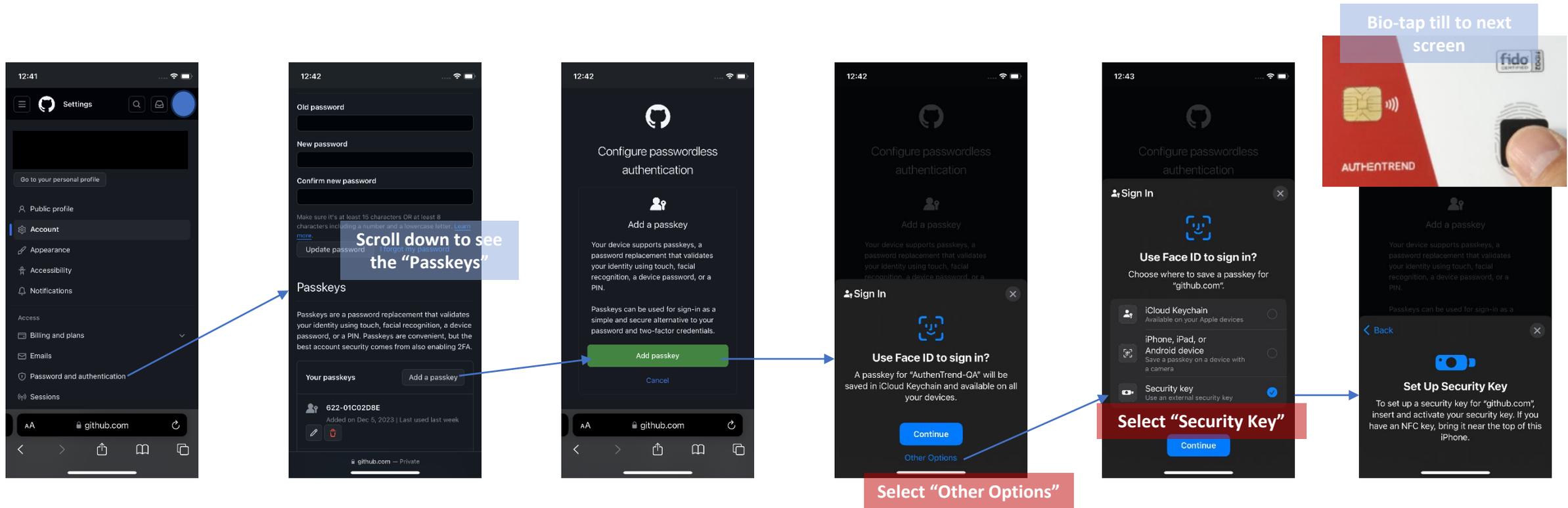


Then, register 2nd security key/card if you have.

Register Card to Passkey enabled Service



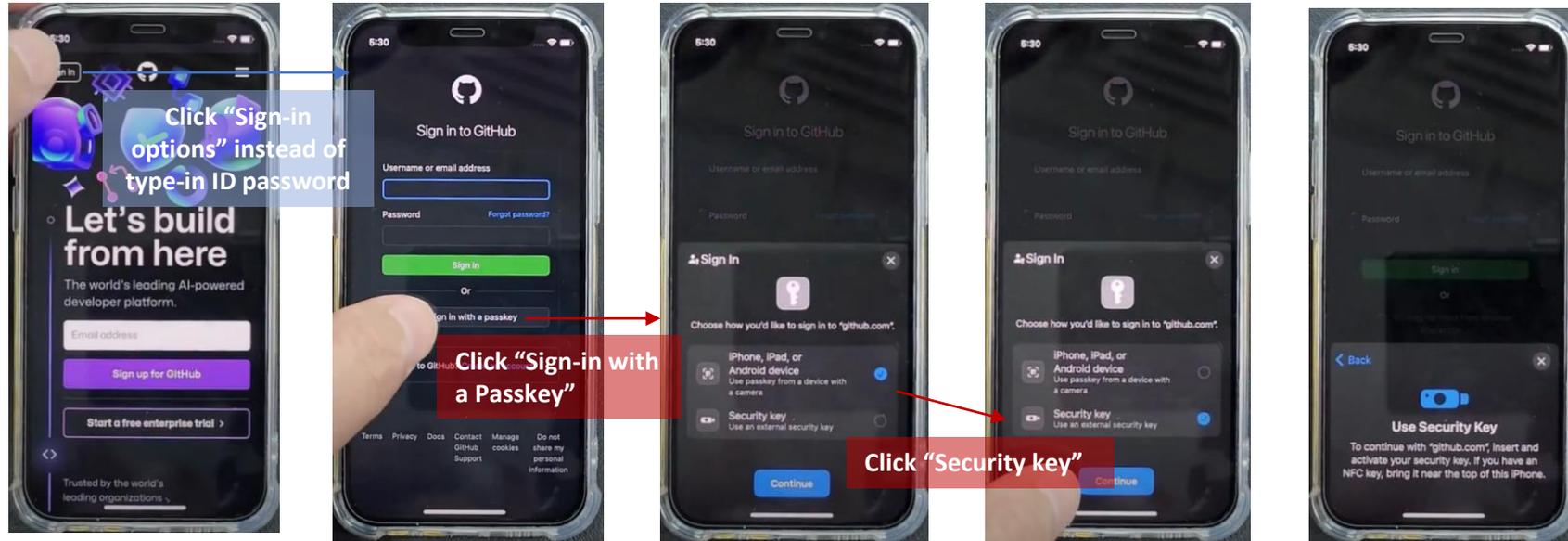
- Example from Github



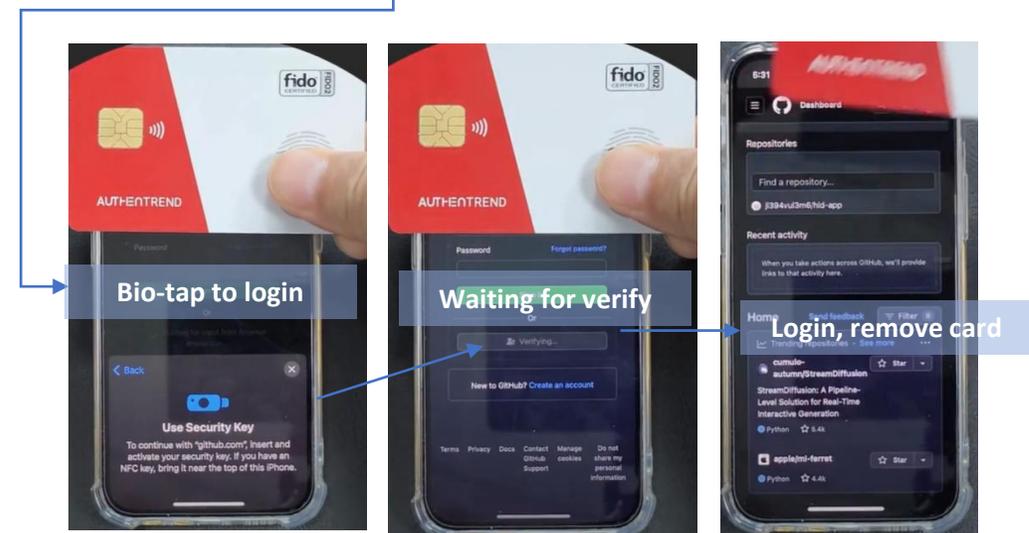
Authentication as a Passkey



- Example from Github



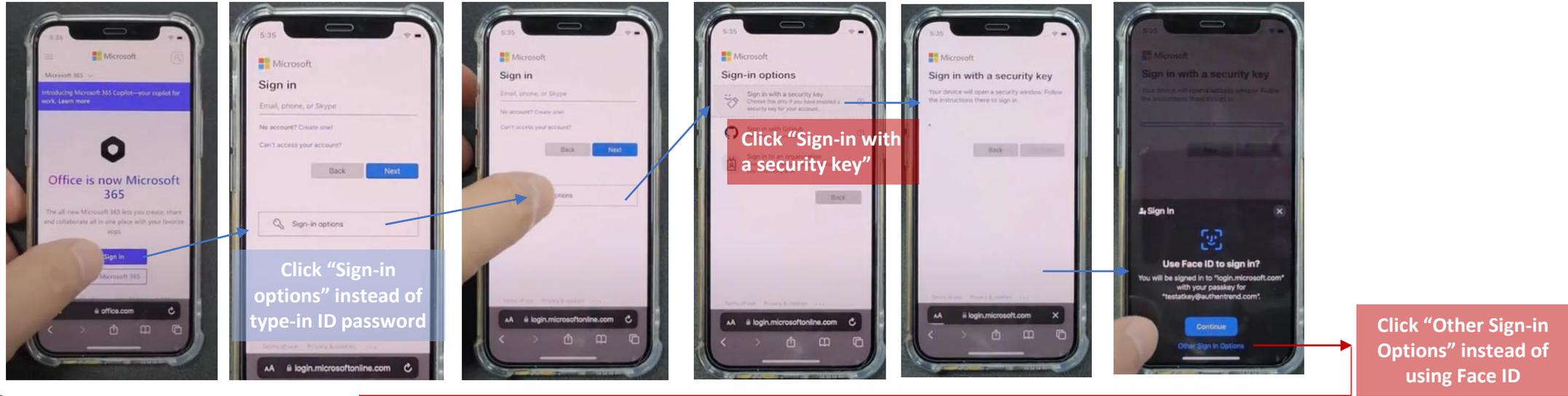
iOS By Safari browser for NFC Passkey



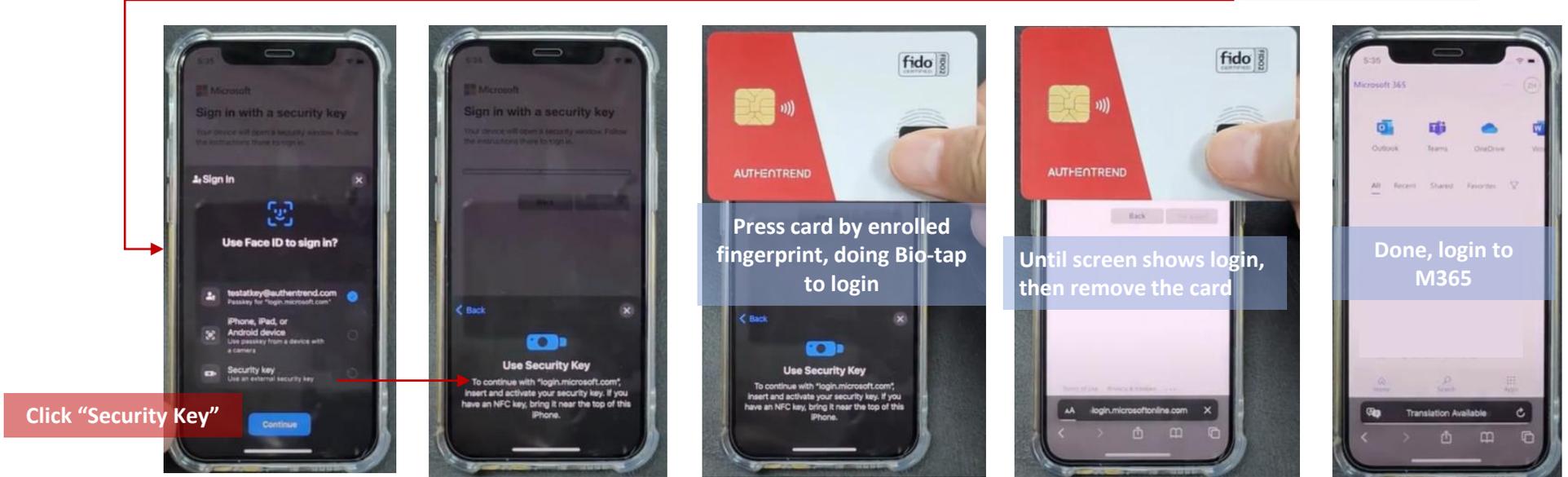
Authentication as a Passkey



- Example from Microsoft 365 Here assumes you already register Card as a security key to your Microsoft365 account



iOS *By Safari browser for NFC Passkey*





Visit <https://authentrend.com/atkey-card-nfc/> for more information
Or mail to customer.support@authentrend.com for advanced contact



Thank you!

No more phishing! Start your passwordless login from today.

AUTHENTREND