Frequently Asked Questions

iShield Key 2 Series

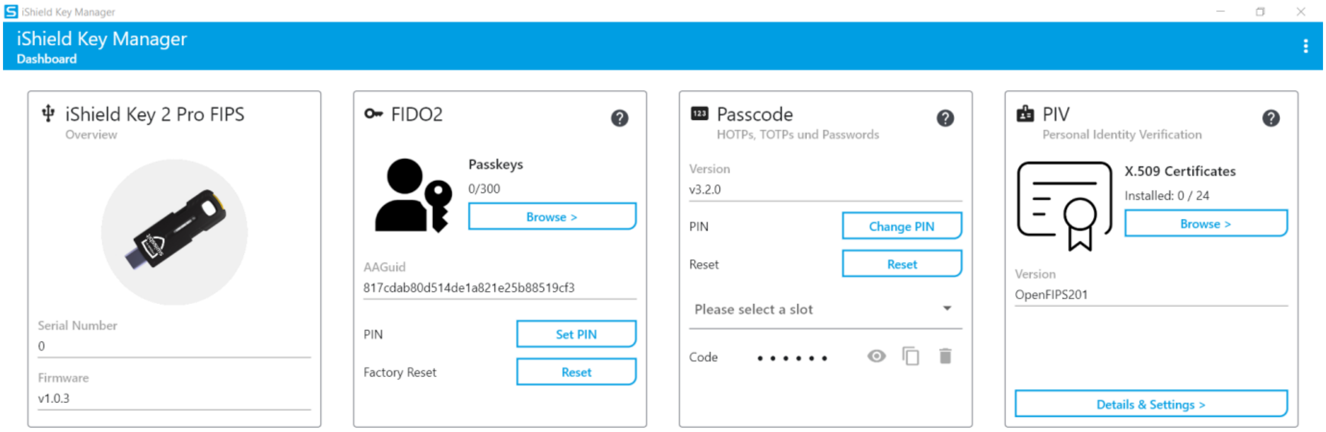
Date: January 17, 2025
Revision: 1.0
File:
FAQ_iShield-Key2-Series_V1.0_EN.pdf

1 Introduction

An iShield Key is a hardware security device designed for strong two-factor authentication (2FA) or multi-factor authentication (MFA). It strengthens account security by requiring both something you know (password & PIN) and something you own (the iShield Key).

1.1 How does an iShield Key work?

Once connected to a computer or NFC-enabled mobile device, the iShield Key can be configured using the iShield Key Manager (hereafter referred to as iKM). iShield Keys support multiple authentication protocols (FIDO2, HOTP, TOTP, Static Password, Smartcard/PIV).



iShield Key Manager
Dashboard

iShield Key 2 Pro FIPS
Overview
Serial Number: 0
Firmware: v1.0.3

FIDO2
Passkeys: 0/300
AAGuid: 817cdab80d514de1a821e25b88519cf3

Passcode
HOTPs, TOTPs und Passwords
Version: v3.2.0
Please select a slot
Code: • • • • • •

PIV
Personal Identity Verification
X.509 Certificates
Installed: 0 / 24
Version: OpenFIPS201

The iShield Key Manager is compatible with Windows, Mac, Linux and Android (TOTP only) devices.

1.2 What types of iShield Key 2 series are available?

iShield Key 2 FIDO2:

- USB-A & NFC
- USB-C & NFC

iShield Key 2 Pro:

- USB-A & NFC
- USB-C & NFC

iShield Key 2 Pro MIFARE:

- USB-A & NFC
- USB-C & NFC

iShield Key 2 Pro FIPS:

- USB-A & NFC
- USB-C & NFC

2 Differences iShield Key

The iShield Key 2 FIDO2 is a simple security key that is mainly used to protect online accounts and for passwordless login. It uses the FIDO2 standard for strong two-factor authentication.

The iShield Key 2 Pro, on the other hand, offers extended functions. In addition to FIDO2, it also supports OTP for offline scenarios and PIV for the secure storage of digital certificates. This makes it more flexible to use, especially in corporate environments.

The iShield Key 2 Pro MIFARE supports MIFARE technology, making it ideal for use in access control.

The iShield Key 2 Pro FIPS is equipped with a FIPS certified applet that has been certified by NIST in accordance with FIPS 140-3.

2.1 Summary

Feature	iShield Key 2 FIDO2	iShield Key 2 Pro	iShield Key 2 Pro MIFARE	iShield Key 2 Pro FIPS
FIDO2	✓	✓	✓	✓
HOTP	✗	✓	✓	✓
TOTP	✗	✓	✓	✓
PIV	✗	✓	✓	✓
MIFARE	✗	✗	✓	✗
FIPS	✗	✗	✗	✓

iShield Key 2 FIDO2: Ideal for private users or home office users who want to secure their online accounts with strong two-factor authentication. For example, for access to social media, email accounts and online banking.

iShield Key 2 Pro: In addition to the compatibility of the FIDO2 key, the Pro key offers support for other applications and services that use HOTP, TOTP and PIV, which facilitates integration into complex IT environments.

iShield Key 2 Pro MIFARE: Benefits from the new housing and MIFARE technology.

iShield Key 2 Pro FIPS: Ideal for users who require FIPS 140-3 certification.

3 Possible questions

3.1 How many slots offer applets

FIDO/Passkey: max 300, it depends on the Passkey properties. (relying party name, relying party id, username, user display name, user id, credential blob)

Passcode (TOTP + HOTP + Password): 42 slots. (2 slots support neither PIN-protected feature nor TOTP, they are intended for static password)

PIV: 24 Slots

3.2 Specific rules for each applet

3.2.1 FIDO2

iShield Key 2 Series (Gen. 2) supports CTAP 2.1, while iShield Key Series (Gen. 1) only supports CTAP 2.0. This means that the iShield Key 2 Series offers more benefits, such as the ability to list created credentials and passkeys and manage individual credentials.

3.2.2 Passcode (TOTP + HOTP + Password)

Foreword: iShield Key 2 series does not have a separate applet for HOTP. Instead, the modules for HOTP, TOTP and passwords are combined in a single applet.

PIN protection option: Users can protect TOTP, HOTP, and Password slots with a PIN.

Please note that if HOTP or Password slot is PIN protected, it cannot be assigned to touch gesture.

Locking rule: The PIN is irrevocably locked after 10 incorrect entries. A PIN reset is required, which deletes all login information in PIN-protected slots.

Reset: Successful authentication of the PIN resets the counter for failed attempts. A complete factory reset resets the TOTP function to the factory settings and deletes all TOTP data and login information.

3.2.3 Password

In the new iShield Key 2 series, we introduce the new "Touch" function, which allows you to easily call up new OTP tokens when you touch the contact. For the touch-controlled OTP functions, the iShield Key 2 series can store up to two different configurations. These OTP configurations are stored in so-called "OTP slots" and the user chooses which slot to use by determining how long to touch the gold contact. Both slots are intended for the touch function, so they cannot be configured for TOTP or with PIN protection.

If the customer does not require a static password, the slot can also be used as a HOTP slot.

3.2.4 PIV

Default PIN: 123456

Standard PUK: 12345678

Management PIN *01:02:03:04:05:06:07:08:01:02:03:04:05:06:07:08:01:02:03:04:05:06:07:08 (AES192)*

Locking rule: The PIN and PUK are locked after a certain number of incorrect entries when the maximum number of attempts (retries) is reached. If both PIN and PUK are locked, you must reset the PIV applet, which deletes all PIV data and restores the factory settings.

PIN and PUK retries: The default number of attempts for PIN and PUK is 5 and 3 respectively, but these values can be adjusted between 1 and 255.

Unlocking: The PUK can be used to unlock the PIN. If both are locked, a complete reset is required.

3.2.5 PIN Rules

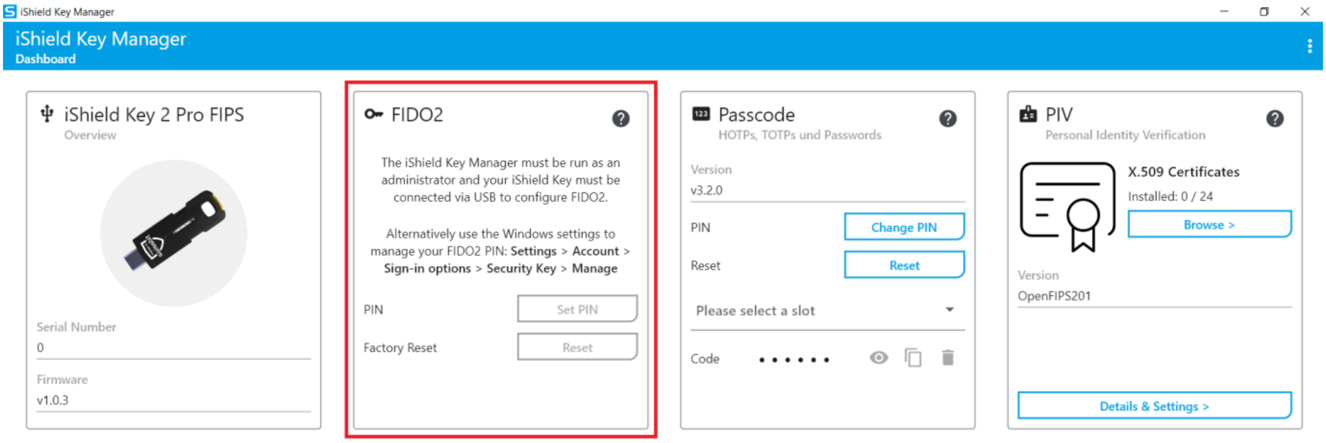
iShield Key 2 series could set the following new password rules for PIN and PUK:

1. The password must be at least 6 characters long.
2. A password with 4 identical characters is not permitted (e.g. 222248), but a password with 3 identical characters is permitted (e.g. 222485).
3. Sequences of numbers are not permitted (e.g. 123456).

3.3 iShield Key is not recognized:

- Ensure compatibility. (fully plugged in, the right way round)
- Try it with another device, e.g. smartphone via NFC

3.4 iKM shows FIDO2 grayed out



Serial Number 0

Firmware v1.0.3

The iShield Key Manager must be run as an administrator and your iShield Key must be connected via USB to configure FIDO2.

Alternatively use the Windows settings to manage your FIDO2 PIN: **Settings** > **Account** > **Sign-in options** > **Security Key** > **Manage**

PIN

Factory Reset

Version v3.2.0

PIN

Reset

Code ••••••

Installed: 0 / 24

Version OpenFIPS201

- Please start iShield Key Manager with administrator rights.

3.5 What to do if you lose your iShield Key?

- **Deactivate immediately:** Remove the lost iShield Key from authorized devices in online accounts.
- **Register backup:** Use a registered backup iShield key to restore access.
- **Account recovery:** Follow the service's account recovery procedure if no backup is available (other verification methods may be required).
- **Can someone steal my data?** No, the iShield Key does not give out any data. Without the PIN it is worthless and without the login data, e.g. e-mail address for Amazon account, and the PIN you set yourself.

3.6 iShield Key no longer works:

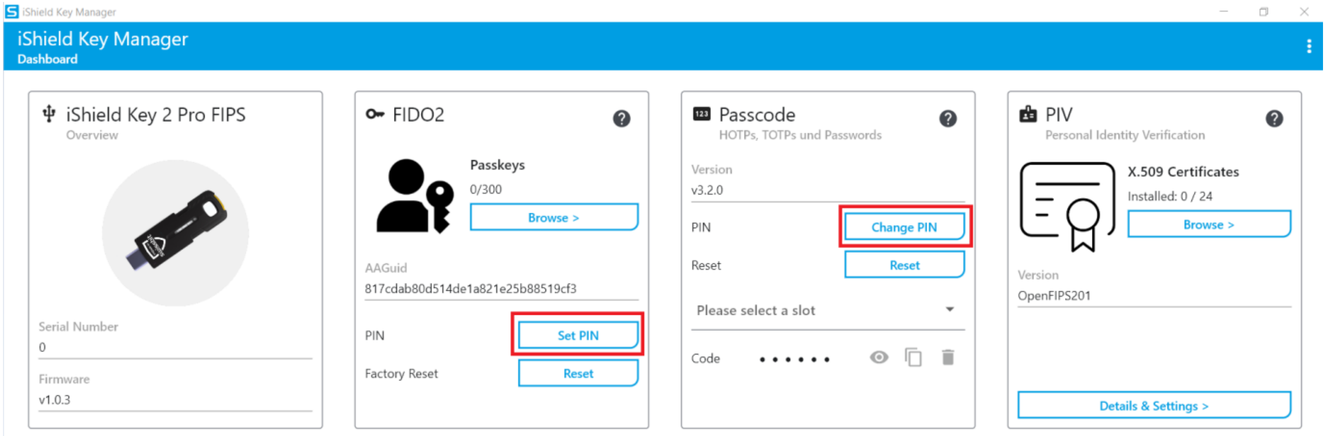
- Check for physical damage (cracks, bent connections).
- Check the configuration of the iShield key slots
- Reset applets in the iShield Key Manager (ATTENTION all data will be irrevocably deleted)

3.7 The service says that the iShield key code is invalid:

- **Time synchronization:** Some services require an exact time on the device. Check your time on the computer.
- **Slot configuration:** iShield keys have several "slots" that must be selected correctly.

4 First steps

The basic setup is very simple on the computer.



iShield Key Manager
Dashboard

iShield Key 2 Pro FIPS
Overview
Serial Number: 0
Firmware: v1.0.3

FIDO2
Passkeys: 0/300
AAGuid: 817cdab80d514de1a821e25b88519cf3

Passcode
HOTPs, TOTPs und Passwords
Version: v3.2.0
Please select a slot
Code: • • • • • •

PIV
Personal Identity Verification
X.509 Certificates
Installed: 0 / 24
Version: OpenFIPS201

There are different "applets" depending on the iShield Key model – FIDO2, Passcode and PIV. The FIDO2, Passcode and PIV applets must be set up before they are used for the first time. To do this, open the iKM (iShield Key Manager) on the computer and set the personal PINs for each applet. These PINs must be entered for each authentication, which is done by an automatic query from the computer.

4.1 Set-up steps:

Open iKM: Start the iShield Key Manager on your computer.

Select applet: Select the applet (FIDO2, Passcode or PIV) that you want to set up.

Set PIN: Enter a personal PIN for the selected applet and confirm it.

Repeat: Repeat the steps for each applet you want to use.

5 iShield Key functions

5.1 FIDO2

FIDO (Fast Identity Online) is an initiative that aims to revolutionize the way we authenticate ourselves online. At its core, it is about replacing passwords with more secure and user-friendly methods (e.g. passkeys)

5.1.1 FIDO2 and U2F: The building blocks

FIDO2: Enables passwordless login to websites and apps through the use of special security keys. (Passwordless login)

U2F (Universal Second Factor): A part of FIDO2 that focuses on the use of physical security keys as a second level of authentication in addition to the password. These keys are often connected to the device via USB or NFC and provide an additional layer of security.

5.1.2 How does it work?

Registration: You register your iShield Key with an online service.

Authentication: When you log in, the website requests confirmation of your key. This is done by simply inserting the iShield Key, after which you are asked to confirm the key by touching it.

Confirmation: Your device or key cryptographically confirms your identity without transmitting sensitive data over the Internet. The actual password never leaves the key!

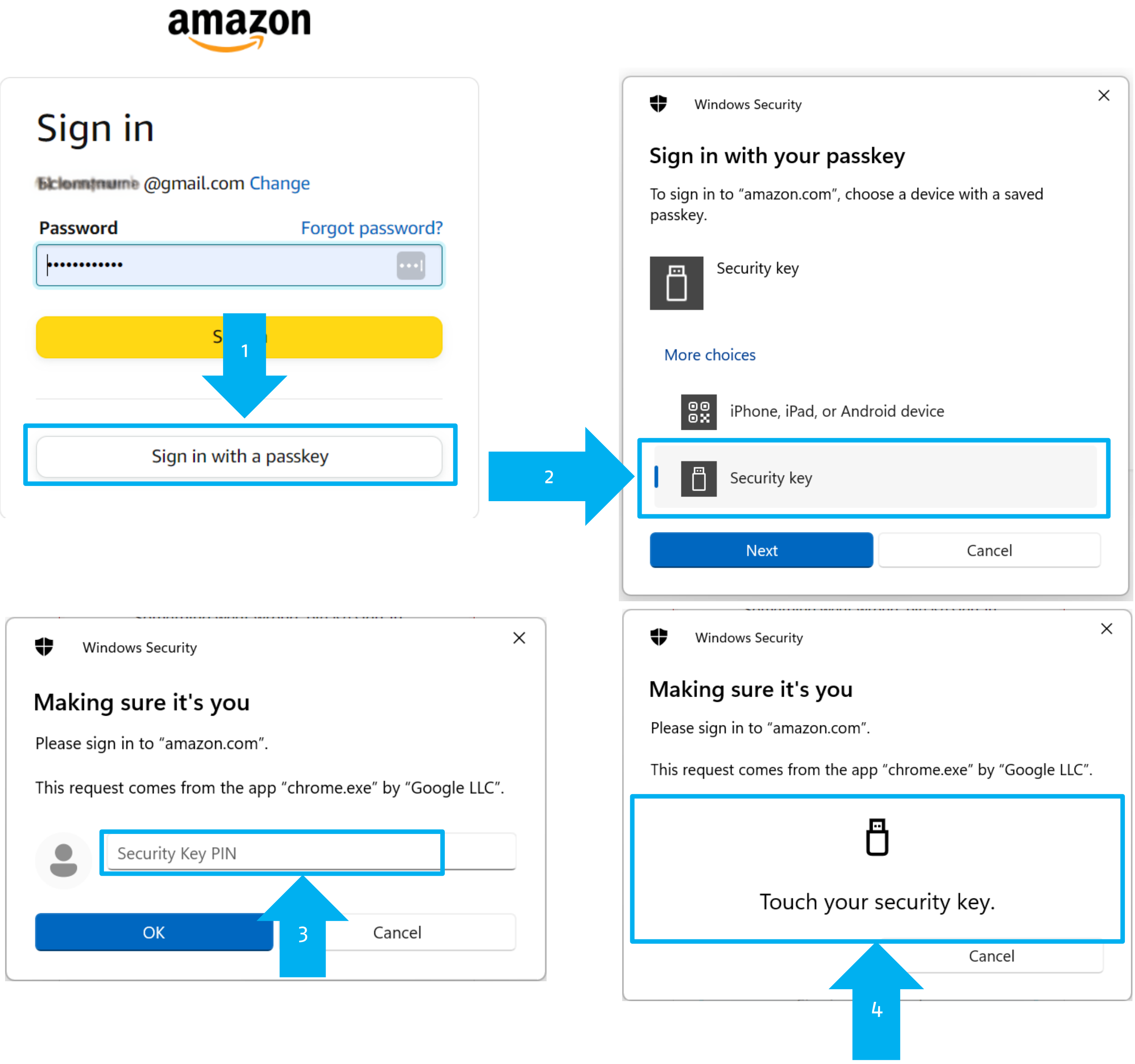
5.1.3 Broad acceptance

FIDO is supported by a large number of companies and organizations, including big names such as Google, Microsoft, Apple and many banks. The standards are supported in modern web browsers (Chrome, Firefox, Edge, etc.) and operating systems (Windows, macOS, Android, iOS). Confirmation is done by plugging in via USB or NFC (similar to contactless payment with a card).

5.1.4 Safety benefits of FIDO2

FIDO2 is considered more secure than conventional password-based systems as it uses public key cryptography and reduces the risk of phishing attacks. No sensitive data is transmitted during authentication, which further increases security.

5.1.5 Login with FIDO2 – "Passkey"



amazon

Sign in

[redacted] @gmail.com Change

Password

Forgot password?

Windows Security

Sign in with your passkey

To sign in to "amazon.com", choose a device with a saved passkey.

Security key

More choices

iPhone, iPad, or Android device

Security key

Windows Security

Making sure it's you

Please sign in to "amazon.com".

This request comes from the app "chrome.exe" by "Google LLC".

Security Key PIN

Windows Security

Making sure it's you

Please sign in to "amazon.com".

This request comes from the app "chrome.exe" by "Google LLC".

Touch your security key.

5.2 OTP

An OTP (One-Time Password) is like a secret code that is only valid once. Imagine you want to use your online banking. In addition to your normal password, you also receive an OTP, for example by text message on your cell phone. This code is only valid for a short time (often 30 seconds or one minute). When you enter it, you prove that you are really you and not someone who only knows your password.

5.2.1 Why is it safer?

Protects against password theft: Even if someone finds out your password, they cannot log in because they do not have the additional OTP code.

Always different: The OTP changes every time you log in, so it cannot simply be guessed or reused.

Additional security: The OTP provides a second layer of protection in addition to your password.

5.2.2 Different OTP methods

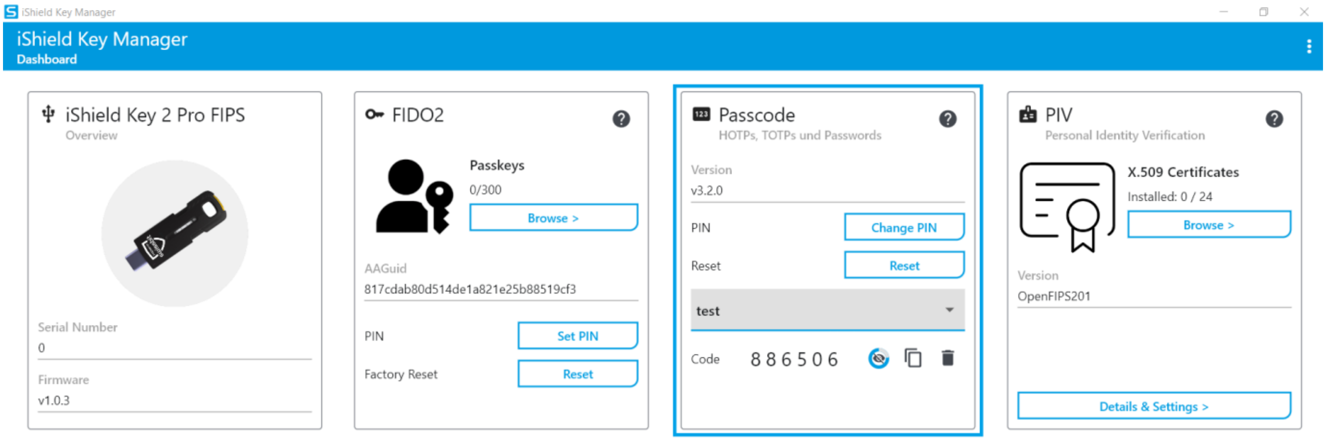
HOTP (HMAC-based One-Time Password): Generates OTPs based on a counter value. The code changes each time a new OTP is requested.

TOTP (Time-based One-Time Password): Generates OTPs based on the current time. These codes are only valid for a short time (often 30 or 60 seconds).

5.2.3 How do I get an OTP?

Via NFC: The code is displayed on your cell phone. (iShield Key Manager app required)

Via USB: The code is displayed on the computer. (iShield Key Manager app required)



iShield Key Manager
Dashboard

iShield Key 2 Pro FIPS
Overview
Serial Number: 0
Firmware: v1.0.3

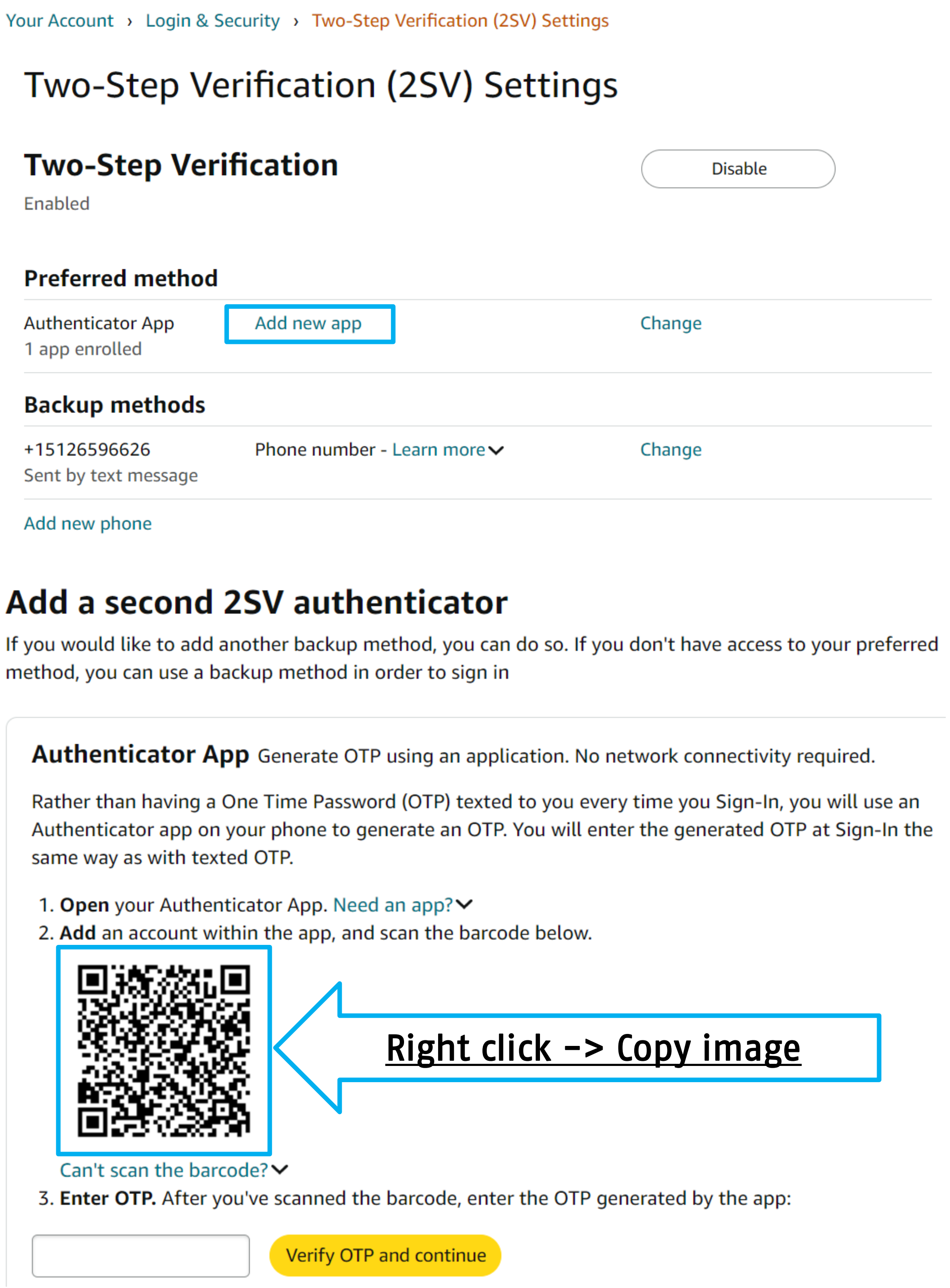
FIDO2
Passkeys: 0/300
AAGuid: 817cdab80d514de1a821e25b88519cf3
PIN
Factory Reset

Passcode
HOTPs, TOTPs und Passwords
Version: v3.2.0
PIN
Reset
test
Code: 886506

PIV
Personal Identity Verification
X.509 Certificates
Installed: 0 / 24
Version: OpenFIPS201

5.2.4 Example Amazon on the computer:

Amazon: My Account -> Login and Security -> 2SV 2 Step Verification (2FA, 2 Factor Authentication)



Your Account › Login & Security › Two-Step Verification (2SV) Settings

Two-Step Verification (2SV) Settings

Two-Step Verification

Enabled

Preferred method

Authenticator App
1 app enrolled

Backup methods

+15126596626
Sent by text message

Phone number - Learn more

Add a second 2SV authenticator

If you would like to add another backup method, you can do so. If you don't have access to your preferred method, you can use a backup method in order to sign in

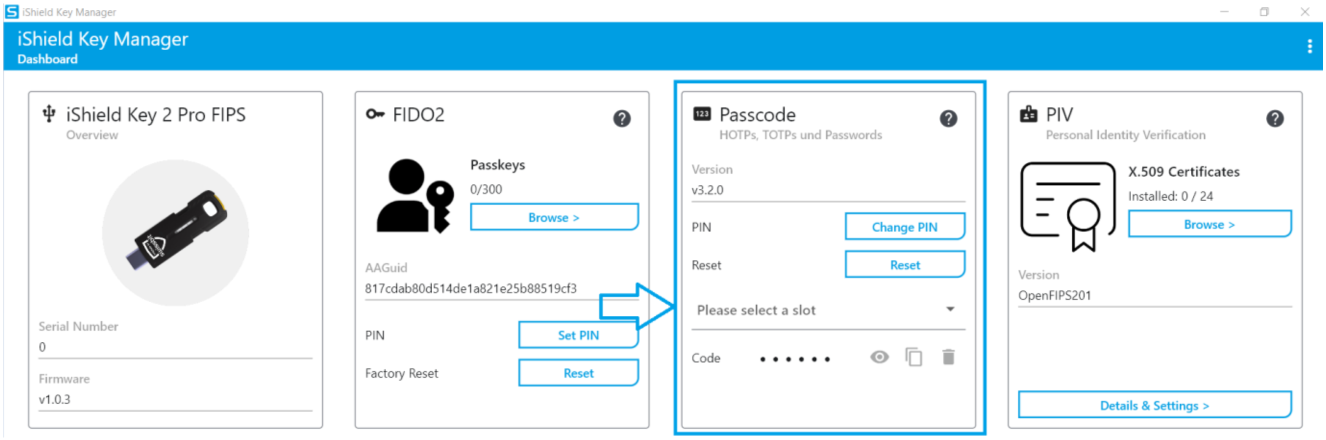
Authenticator App Generate OTP using an application. No network connectivity required.

Rather than having a One Time Password (OTP) texted to you every time you Sign-In, you will use an Authenticator app on your phone to generate an OTP. You will enter the generated OTP at Sign-In the same way as with texted OTP.

1. **Open** your Authenticator App. Need an app?
2. **Add** an account within the app, and scan the barcode below.

Right click -> Copy image

3. **Enter OTP.** After you've scanned the barcode, enter the OTP generated by the app:



Serial Number: 0

Firmware: v1.0.3

Passkeys: 0/300

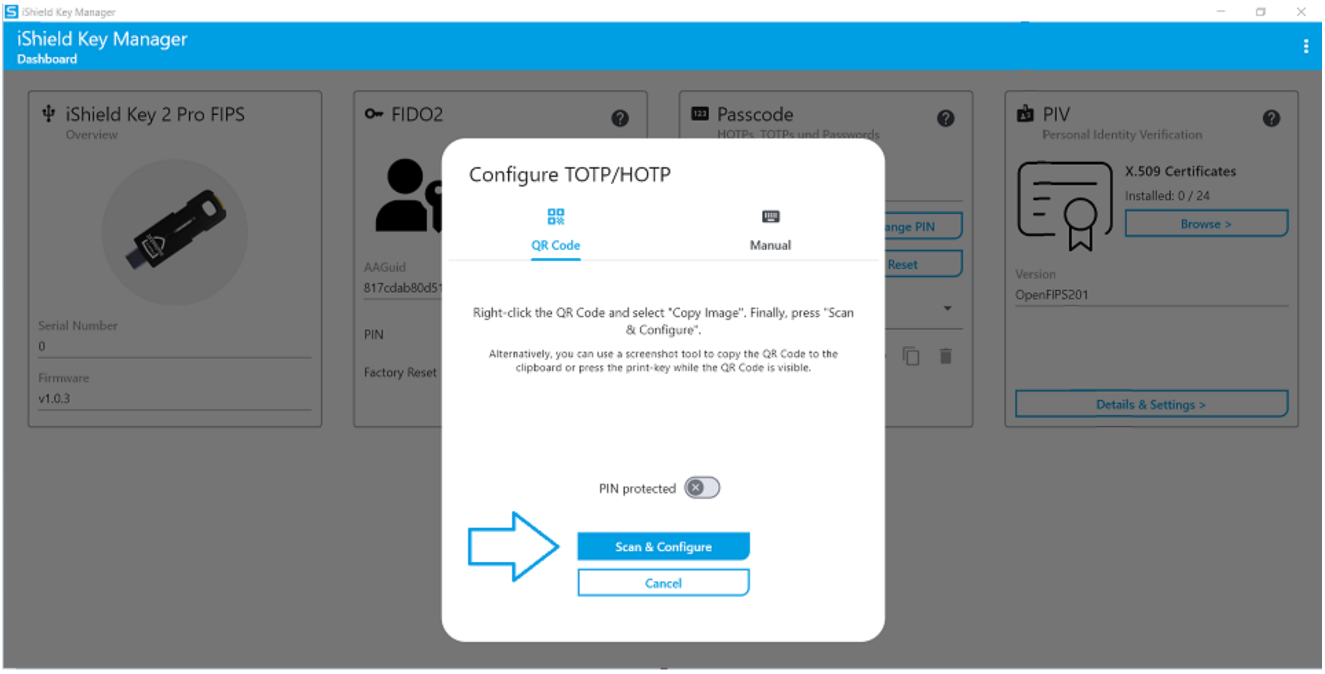
AAGuid: 817cdab80d514de1a821e25b88519cf3

Version: v3.2.0

Code: ••••••

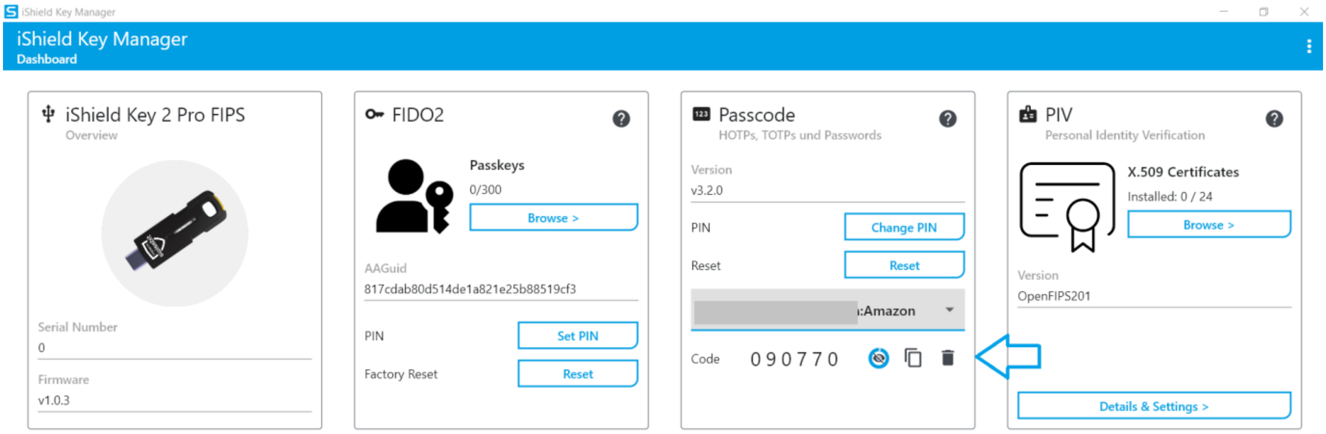
X.509 Certificates Installed: 0 / 24

Version: OpenFIPS201



Right-click the QR Code and select "Copy Image". Finally, press "Scan & Configure".

Alternatively, you can use a screenshot tool to copy the QR Code to the clipboard or press the print-key while the QR Code is visible.



Serial Number: 0

Firmware: v1.0.3

Passkeys: 0/300

AAGuid: 817cdab80d514de1a821e25b88519cf3

Version: v3.2.0

:Amazon

Code: 090770

X.509 Certificates Installed: 0 / 24

Version: OpenFIPS201

Copy the code and confirm it on Amazon. Finished

5.2.5 How can I see this code on my cell phone?

Download iShield Key Manager for the Android device (iOS not yet available)

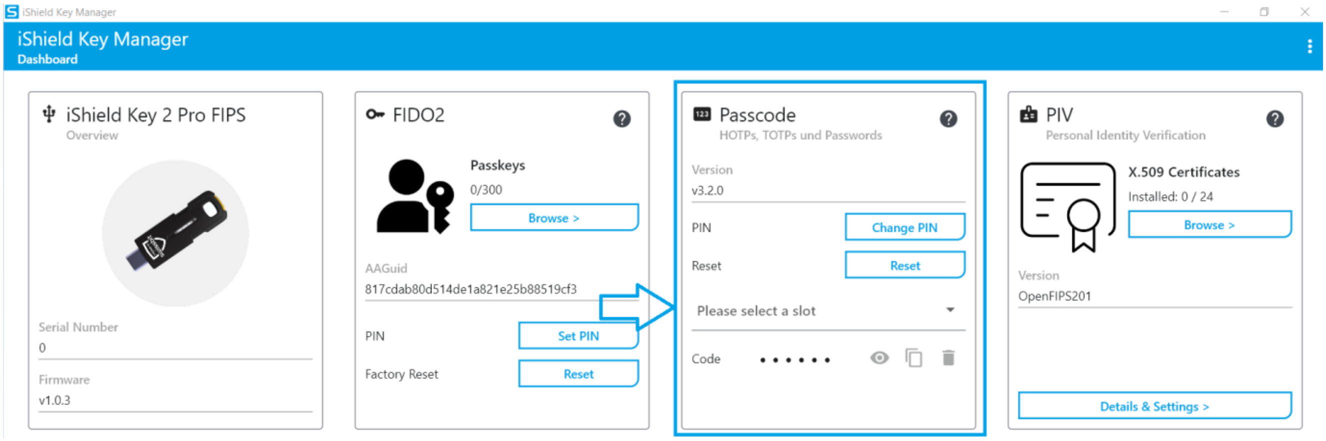
Hold the iShield Key to the **back of** the smartphone

After the first successful connection, you will receive an overview of all OTP accounts.

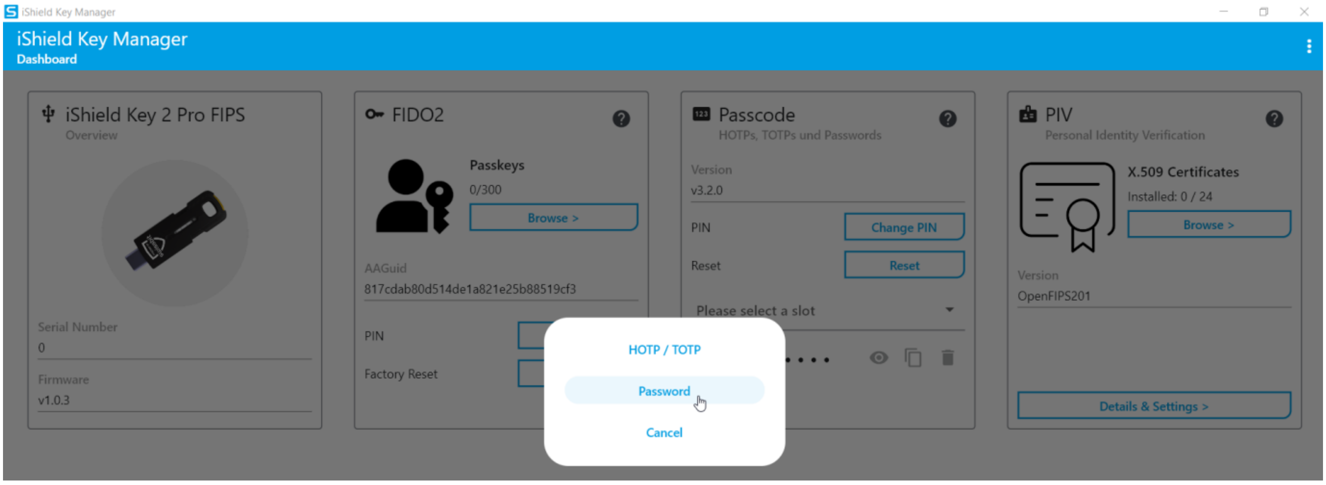
When the account is selected, a request appears to hold the key to the device again.

5.3 How to use the Password function

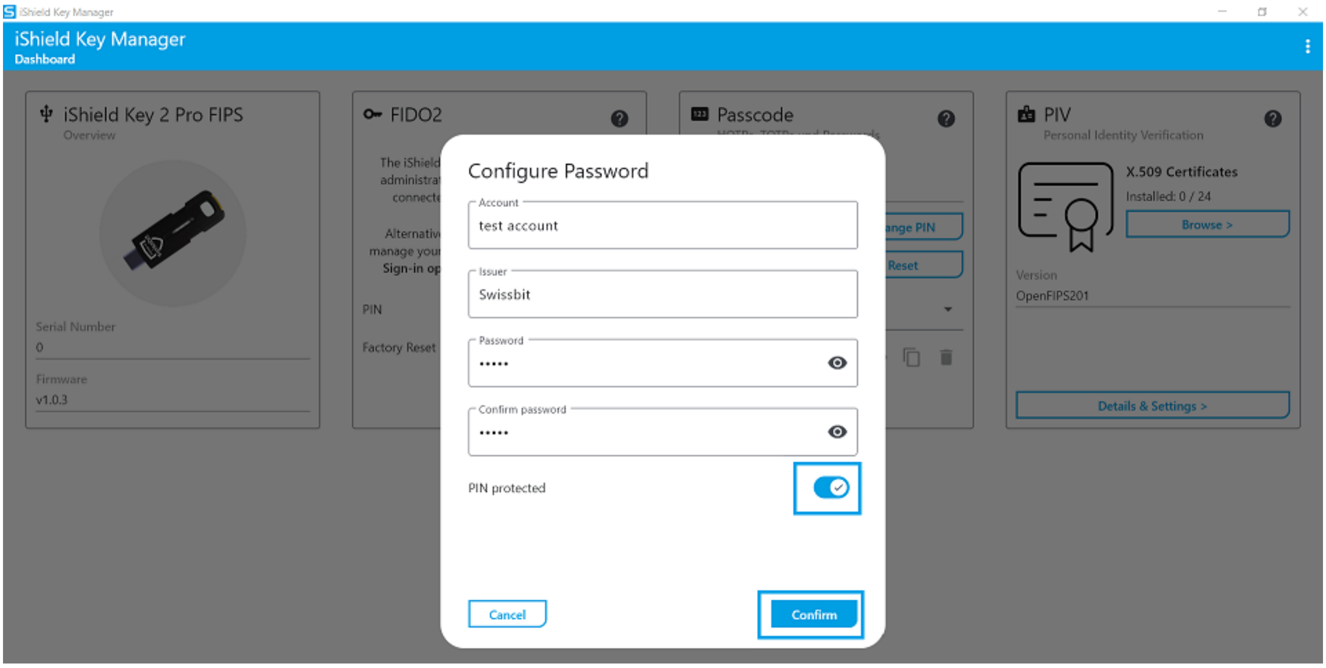
Password function is a new feature in iShield Key 2 series. You can configure it by selecting a slot in Passcode applet and create a password slot.



Select the password slot.



Fill in the account and password and confirm it.


Configure Password

Account: test account

Issuer: Swissbit

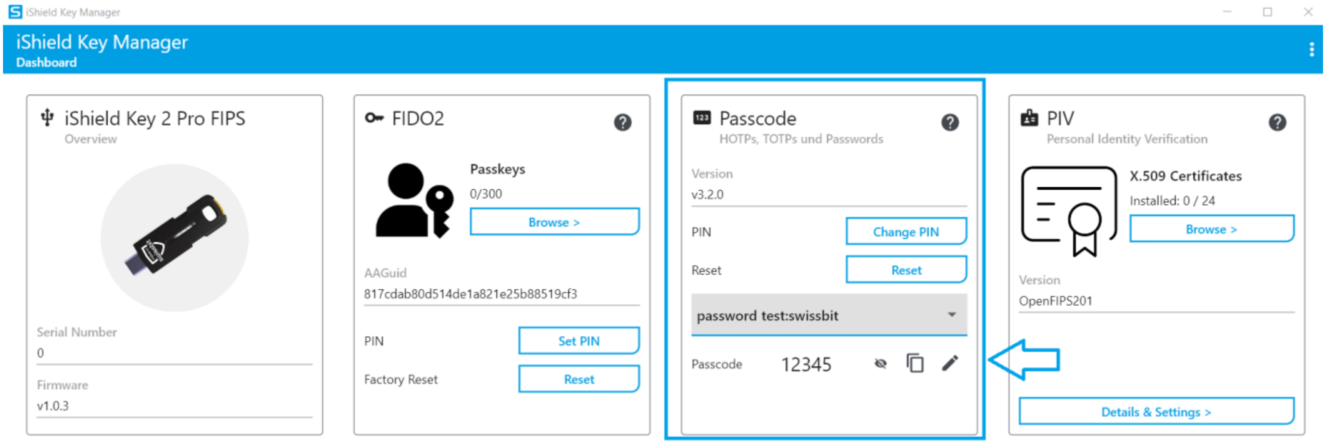
Password: •••••

Confirm password: •••••

PIN protected: ☑

If you choose PIN protected feature on, then you need to type in the PIN for passcode applet every time for the read of your password.

Please note that PIN protected slots cannot be used for the short or long touch function.



iShield Key Manager
Dashboard

iShield Key 2 Pro FIPS
Overview
Serial Number
0
Firmware
v1.0.3

FIDO2
Passkeys
0/300
Browse >
AAGuid
817cdab80d514de1a821e25b88519cf3
PIN Set PIN
Factory Reset Reset

Passcode
HOTPs, TOTPs und Passwords
Version
v3.2.0
PIN Change PIN
Reset Reset
password test:swissbit
Passcode 12345

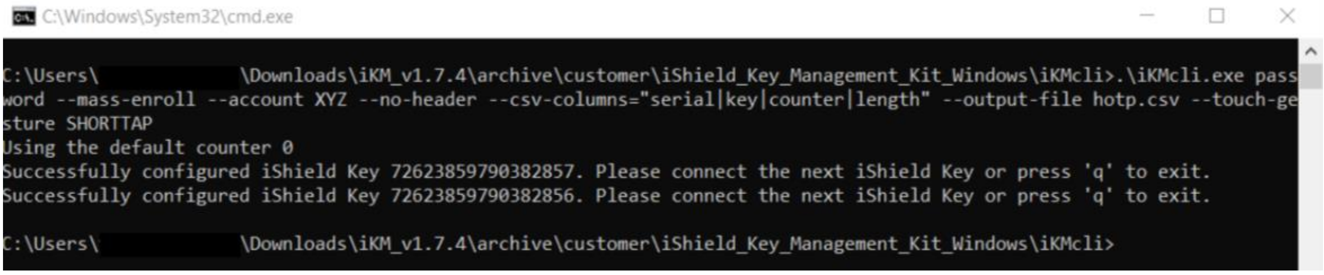
PIV
Personal Identity Verification
X.509 Certificates
Installed: 0 / 24
Browse >
Version
OpenFIPS201
Details & Settings >

5.4 How to deploy the iShield Key for Mass Enrollment

Mass Enrollment is a function now only available in our iKMcli. Mass Enrollment can seed an HOTP slot of multiple iShield Key's. The keys must be connected sequentially. The HOTP function of each iShield Key is seeded with a random secret/key, which is recorded in a CSV file alongside the iShield Key's serial number, the initial counter value and the length of the HOTP. The output format of the random secret/key can be set with --key-format. You can use --csv-columns and --no-header for optional configuration.

Command line tool example:

```
.\iKMcli.exe password --mass-enroll --account XYZ --no-header --csv-columns="serial|key|counter|length" --output-file hotp.csv --touch-gesture SHORTTAP
```



```
C:\Windows\System32\cmd.exe
C:\Users\[redacted]\Downloads\iKM_v1.7.4\archive\customer\iShield_Key_Management_Kit_Windows\iKMcli>.\iKMcli.exe pass
word --mass-enroll --account XYZ --no-header --csv-columns="serial|key|counter|length" --output-file hotp.csv --touch-ge
sture SHORTTAP
Using the default counter 0
Successfully configured iShield Key 72623859790382857. Please connect the next iShield Key or press 'q' to exit.
Successfully configured iShield Key 72623859790382856. Please connect the next iShield Key or press 'q' to exit.

C:\Users\[redacted]\Downloads\iKM_v1.7.4\archive\customer\iShield_Key_Management_Kit_Windows\iKMcli>
```

Please take note, the above defined columns in the csv file are optional and the user can decide which columns he needs. Example only "serial|key|counter" or no columns.

6 This is how the iShield Key improves security:

6.1 Physical security

Uniqueness: Hardware security devices are physical objects that cannot be easily copied or stolen.

Independence: They work independently of the operating system of the computer or mobile device, which makes them less susceptible to software-based attacks.

6.2 Strong authentication

Two-factor authentication (2FA): Hardware security devices such as the iShield Key provide an additional layer of security by being used as a second factor alongside the password.

Passwordless authentication: The iShield Key also supports passwordless login, which eliminates the risk of password theft.

6.3 Protection against phishing

Challenge-based authentication: These devices use cryptographic key pairs for authentication, making them immune to phishing attacks. Even if a user clicks on a malicious phishing link, the attacker cannot log in without the physical key.

6.4 Cryptographic security

Private key remains secure: The private key is securely stored on the device and never leaves the device, protecting it from malware and other malicious programs.

Strong encryption: Hardware security devices use advanced cryptographic methods to ensure security.

6.5 Compatibility and support

Broad support: The iShield Key is compatible with many common operating systems, browsers and online services. This facilitates integration and use.

Standards: They support open standards such as FIDO2 and U2F

6.6 Easy handling

Ease of use: These devices are often easy to use. They only need to be plugged into a USB port or held wirelessly to the device (e.g. NFC) to work.

No installation necessary: In most cases, no special drivers or software installations are required, making it easy to use.

6.7 PIV

The iShield Key Pro supports industry standards developed for PKI smart card authentication to operating systems (Windows, MacOS, Linux) to enable certificate-based login to these systems. The iShield Key Pro is detected as both a smart card reader and a compliant smart card containing the public/private key-pairs and certificates required for authentication, code signing and encryption.

7 Why iShield Key?

7.1 iShield Key vs SMS & E-Mail 2FA

Vulnerabilities of SMS-based 2FA:

Phishing attacks: Scammers can create fake websites or messages that look like they come from your real provider. They trick you into entering your OTP (one-time password) and can then access your account.

SIM swap attacks: Criminals can trick your mobile provider into transferring your phone number to a new SIM card. This allows them to receive your SMS messages, including OTPs, and take over your accounts.

Vulnerabilities of email-based 2FA:

Phishing attacks: Similar to SMS, fraudsters can send fake emails to trick you into revealing your OTP.

Email account compromise: If your email account is hacked, the attacker will have access to all your emails, including OTPs.

How iShield Key offers a more secure alternative:

iShield Key is a physical security key that serves as a second level of authentication. It is connected to your device via USB or NFC and generates OTPs without an internet connection. This makes it resistant to phishing and SIM swap attacks.

Advantages of iShield Key:

Physical protection: The key must be physically present in order to generate OTPs. This makes it difficult for attackers to steal or duplicate it.

No internet connection required: Since the key works offline, it is not vulnerable to phishing attacks that rely on intercepting messages.

Easy to use: The key can be activated simply by tapping it and immediately generates an OTP.

7.2 Are iShield keys unhackable?

The iShield Key is very secure and offers strong protection for your data and online accounts. However, it is important to be aware that no device is completely invulnerable. By using the key in combination with other security measures, you can significantly improve your online security.

8 Change history

Date	Revision	Details
01.17.2025	1	Initial release

Disclaimer:

No part of this document may be copied or reproduced in any form or by any means, or transferred to any third party, without the prior written consent of an authorized representative of Swissbit AG ("SWISSBIT"). The information in this document is subject to change without notice. SWISSBIT assumes no responsibility for any errors or omissions that may appear in this document, and disclaims responsibility for any consequences resulting from the use of the information set forth herein. SWISSBIT makes no commitments to update or to keep current information contained in this document. The products listed in this document are not suitable for use in applications such as, but not limited to, aircraft control systems, aerospace equipment, submarine cables, nuclear reactor control systems and life support systems. Furthermore, SWISSBIT does not recommend or approve the use of any of its products in life support devices or systems or in any application where failure could result in injury or death. If a customer wishes to use SWISSBIT products in applications not intended by SWISSBIT, said customer must contact an authorized SWISSBIT representative to determine SWISSBIT willingness to support a given application. The information set forth in this document does not convey any license under the copyrights, patent rights, trademarks or other intellectual property rights claimed and owned by SWISSBIT. The information set forth in this document is considered to be "Proprietary" and "Confidential" property owned by SWISSBIT.

ALL PRODUCTS SOLD BY SWISSBIT ARE COVERED BY THE PROVISIONS APPEARING IN SWISSBIT'S TERMS AND CONDITIONS OF SALE ONLY, INCLUDING THE LIMITATIONS OF LIABILITY, WARRANTY AND INFRINGEMENT PROVISIONS. SWISSBIT MAKES NO WARRANTIES OF ANY KIND, EXPRESS, STATUTORY, IMPLIED OR OTHERWISE, REGARDING INFORMATION SET FORTH HEREIN OR REGARDING THE FREEDOM OF THE DESCRIBED PRODUCTS FROM INTELLECTUAL PROPERTY INFRINGEMENT, AND EXPRESSLY DISCLAIMS ANY SUCH WARRANTIES INCLUDING WITHOUT LIMITATION ANY EXPRESS, STATUTORY OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.