swissbit®

Häufig Gestellte Fragen

iShield Key Serie

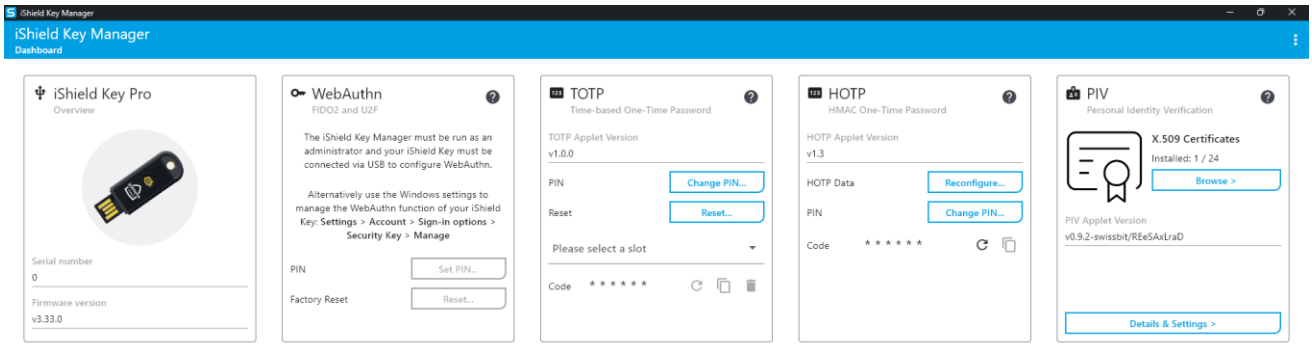
Date: 31 Oktober 2024
Revision: 1.0
File: FAQ_iShield-Key-Series_v1.0_DE.pdf

1 Einleitung

Ein iShield Key ist ein Hardware-Sicherheitsgerät, das für starke Zwei-Faktor-Authentifizierung (2FA) oder Multi-Faktor-Authentifizierung (MFA) entwickelt wurde. Es stärkt die Kontosicherheit, indem es sowohl etwas erfordert, das Sie kennen (Passwort & PIN), als auch etwas, das Sie besitzen (den iShield Key).

1.1 Wie funktioniert ein iShield Key?

Nach dem Anschließen an einen Computer oder ein NFC-fähiges Mobilgerät kann der iShield Key mithilfe des iShield Key Managers (im Folgenden iKM genannt) konfiguriert werden. iShield Keys unterstützen mehrere Authentifizierungsprotokolle (FIDO2, U2F, HOTP, TOTP, Smartcard/PIV).



Der iShield Key Manager ist mit Windows, Mac, Linux und Android (TOTP only) Geräten kompatibel.

1.2 Welche Arten von iShield Key gibt es?

iShield Key FIDO2:

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

Dieses Modell hat ein **BLAUES** Logo

iShield Key PRO:

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

Dieses Modell hat ein **WEIßES** Logo

2 Unterschiede iShield Key

Der iShield Key FIDO2 ist ein einfacher Sicherheitsschlüssel, der hauptsächlich zum Schutz von Online-Konten und zur passwortlosen Anmeldung dient. Er nutzt den FIDO2-Standard für eine starke Zwei-Faktor-Authentifizierung.

Der iShield Key Pro hingegen bietet erweiterte Funktionen. Neben FIDO2 unterstützt er auch OTP für Offline-Szenarien und PIV zur sicheren Speicherung von digitalen Zertifikaten. Damit ist er flexibler einsetzbar, besonders in Unternehmensumgebungen.

2.1 Zusammenfassung

Feature	iShield Key FIDO2	iShield Key Pro
FIDO2	✔	✔
HOTP	✘	✔
TOTP	✘	✔
PIV	✘	✔

iShield Key FIDO2: Ideal für Privatnutzer oder HomeOffice Nutzer, die ihre Online-Konten mit einer starken Zwei-Faktor-Authentifizierung sichern möchten. Beispielsweise für den Zugang zu sozialen Medien, E-Mail-Konten und Online-Banking.

iShield Key Pro: Zusätzlich zur Kompatibilität des FIDO2-Schlüssels bietet der Pro-Schlüssel Unterstützung für weitere Anwendungen und Dienste, die HOTP, TOTP und PIV verwenden, was die Integration in komplexe IT-Umgebungen erleichtert.

3 Hardware Defaults

3.1 Wie Viele Slots bieten Applets

FIDO/Passkey: 32 Slots

TOTP: 42 Slots

PIV: 24 Slots

3.2 Spezifische Regeln für jedes Applet

3.2.1 HOTP

Standard-PIN: 1234

Sperrregel: Nach 10 falschen Eingaben wird der PIN unwiderruflich gesperrt. Nach der Sperrung können Sie weiterhin Einmalpasswörter generieren, aber keinen geheimen Schlüssel oder Zähler ändern.

Reset: Eine erfolgreiche Authentifizierung des PINs setzt den Zähler für Fehlversuche zurück.

3.2.2 TOTP

Option für PIN-Schutz: Benutzer können TOTP-Slots mit einem PIN schützen.

Sperrregel: Nach 10 falschen Eingaben wird der PIN unwiderruflich gesperrt. Ein PIN-Reset ist erforderlich, der alle Anmeldeinformationen in PIN-geschützten Slots löscht.

Reset: Eine erfolgreiche Authentifizierung des PINs setzt den Zähler für Fehlversuche zurück. Ein vollständiger Werksreset stellt die TOTP-Funktion auf die Werkseinstellungen zurück und löscht alle TOTP-Daten und Anmeldeinformationen.

3.2.3 PIV

Standard-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*

Sperrregel: Der PIN und PUK wird nach einer bestimmten Anzahl falscher Eingaben gesperrt, wenn die maximale Anzahl an Versuchen (Reties) erreicht ist. Wenn sowohl PIN als auch PUK gesperrt sind, müssen Sie das PIV-Applet zurücksetzen, wodurch alle PIV-Daten gelöscht und die Werkseinstellungen wiederhergestellt werden.

PIN und PUK Retries: Die Standardanzahl der Versuche für PIN und PUK beträgt 5 bzw. 3. Diese Werte können jedoch zwischen 1 und 255 angepasst werden.

Entsperrung: Der PUK kann verwendet werden, um den PIN zu entsperren. Wenn beide gesperrt sind, ist ein vollständiger Reset erforderlich.

4 Fehlerbehebung

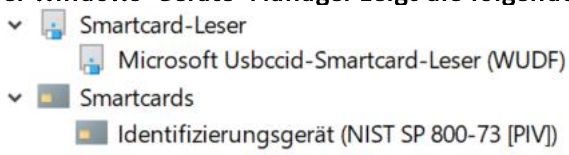
4.1 iShield Key wird nicht erkannt

- Stellen Sie die Kompatibilität sicher. (vollständig eingesteckt, richtig herum)
- Stecken Sie noch mal neu, die LED blinkt zunächst kurz rot, und dann etwa 1 Sekunde lang grün.
- Versuchen Sie es mit einem anderen Gerät z.B. Smartphone per NFC

4.2 iShield Key wird nicht von Windows erkannt

- Die FIDO2-Schnittstelle erfordert keine Software oder Treiber von Drittanbietern und sollte automatisch mit dem Betriebssystem sowie kompatiblen Anwendungen und Browsern funktionieren.
- Die PIV-Schnittstelle benötigt: 1) einen generischen Microsoft-Minitreiber und 2) einen USB-CCID-Smartcard-Lesetreiber, die beide automatisch über Windows Update installiert werden.

  Der Windows-Geräte-Manager zeigt die folgenden 2 Einträge an:



4.3 Die Smartcard ist schreibgeschützt / kann den angeforderten Vorgang nicht ausführen

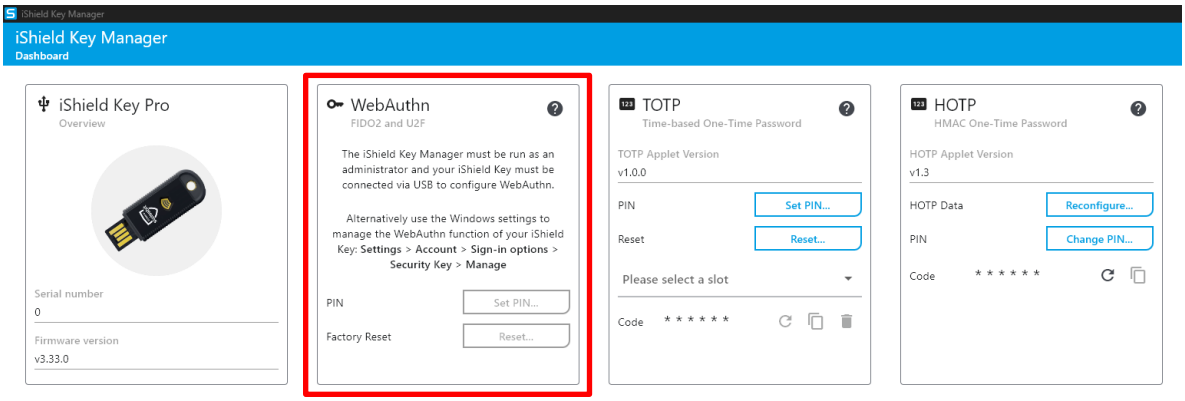
Wenn Ihr iShield Key Pro als schreibgeschützt angezeigt wird oder den gewünschten Vorgang nicht unterstützt, ist der OpenSC-Minitreiber möglicherweise nicht korrekt installiert. Um Ihren Schlüssel bereitzustellen, müssen Sie den OpenSC-Minitreiber verwenden (siehe User Manual Abschnitt 7.2.1).

Stellen Sie sicher, dass eine kompatible OpenSC-Version inkl. des OpenSC-Minitreibers korrekt installiert ist.

4.4 „Eine interne Konsistenzüberprüfung ist fehlgeschlagen“

Der Fehler „Eine interne Konsistenzüberprüfung ist fehlgeschlagen“ wird oft durch eine Fehlkonfiguration von OpenSC verursacht. Bitte folgen Sie allen Schritten in User Manual Abschnitt 7.4: Überprüfen Sie Ihr OpenSC-Profilverzeichnis, management key file, die Umgebungsvariablen sowie die OpenSC-Konfigurationsdatei. Achten Sie dabei besonders auf den iShield PIV Modulpfad und das Vorhandensein der erforderlichen System runtime Bibliotheken.

4.5 iKM zeigt WebAuthn (FIDO2 und U2F) grau



Bitte iShield Key Manager mit Administrator Rechten starten. Falls Sie keine lokalen Administratorrechte haben, wenden Sie sich bitte an Ihren IT-Administrator für Unterstützung.

4.6 Was tun, wenn Sie Ihren iShield Key verlieren?

- **Sofort deaktivieren:** Entfernen Sie den verlorenen iShield Key von autorisierten Geräten in Online-Konten.
- **Backup registrieren:** Verwenden Sie einen registrierten Backup-iShield Key, um den Zugriff wiederherzustellen.
- **Kontowiederherstellung:** Befolgen Sie die Kontowiederherstellungsprozedur des Dienstes, wenn kein Backup vorhanden ist (möglicherweise sind andere Überprüfungsmethoden erforderlich).
- **Jemand kann meine Daten klauen?** Nein, der iShield Key gibt keine Daten heraus. Ohne dem PIN ist der reine Besitz und ohne die Login-Daten, z.B. E-Mail-Adresse für Amazon Konto, und dem selbst festgelegten PIN wertlos.

4.7 Der Dienst sagt, dass der iShield Key-Code ungültig ist:

- **Zeitsynchronisation:** Einige Dienste erfordern eine genaue Uhrzeit auf dem Gerät. Prüfen Sie Ihre Uhrzeit am Computer.
- **Slot-Konfiguration:** iShield Key's haben mehrere "Slots", die korrekt ausgewählt sein müssen.

4.8 iShield Key funktioniert nicht mehr:

- Auf physische Beschädigungen prüfen (Risse, verbogene Anschlüsse).
- Überprüfen Sie die Konfiguration der iShield Key-Slots
- Applets im iShield Key Manager zurücksetzen (ACHTUNG alle Daten werden unwiderruflich gelöscht)

5 Erste Schritte

5.1 iShield Key Manager Installation

Herunterladen des iShield Key Management Kits:

- Windows
  https://www.swissbit.com/files/public/ikm/iShield_Key_Management_Kit_Windows.zip
- Linux x86_64: Ubuntu, Debian
  https://www.swissbit.com/files/public/ikm/iShield_Key_Management_Kit_Linux.zip
- MacOS
  https://www.swissbit.com/files/public/ikm/iShield_Key_Management_Kit_macOS.zip

Jede ZIP-Datei enthält User Manual für iShield Key Manager (iKM), das Installationspaket für alle unterstützten Betriebssysteme, sowie das CLI (Command Line Interface) Tool für jedes dieser Betriebssysteme.

5.2 Einrichtungsschritte:

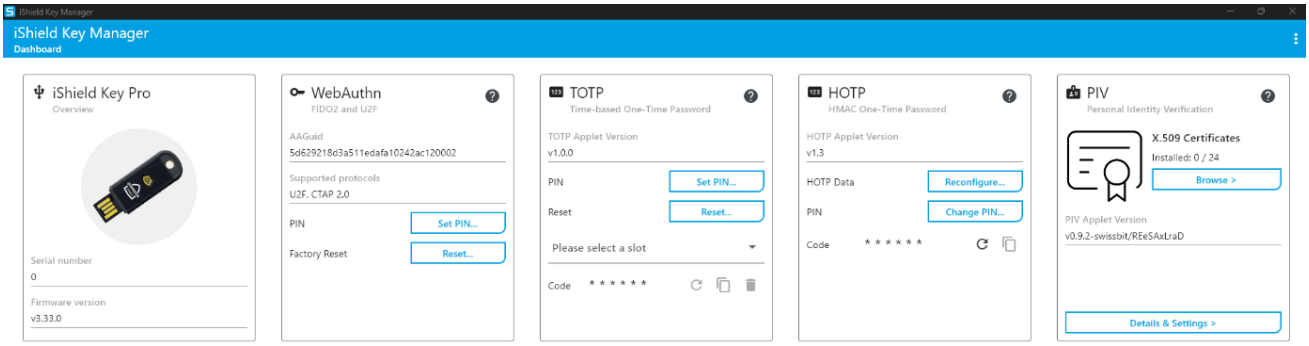
Die Grundeinrichtung erfolgt sehr einfach am Computer.

iKM öffnen: Starten Sie den iShield Key Manager auf Ihrem Computer.

Applet auswählen: Suchen Sie das Applet (WebAuthn, TOTP, HOTP oder PIV) aus, das Sie einrichten möchten.

PIN setzen: Geben Sie eine persönliche PIN für das ausgewählte Applet ein und bestätigen Sie diese.

Wiederholen: Wiederholen Sie die Schritte für jedes Applet, das Sie verwenden möchten.



Es gibt je nach iShield Key Modell unterschiedliche „Applets" – WebAuthn, TOTP, HOTP und PIV. Die Applets WebAuthn, TOTP und PIV müssen vor der ersten Verwendung eingerichtet werden. Hierfür öffnet man den iKM (iShield Key Manager) am Computer und setzt die persönlichen PINs für jedes Applet. Diese PINs müssen bei jeder Authentifizierung eingegeben werden, was durch eine automatische Abfrage vom Computer erfolgt.

Bitte beachten Sie, dass der iShield Key Manager als **Administrator** ausgeführt werden muss, um das WebAuthN Applet unter Windows zu verwalten.

6 iShield Key Funktionen

6.1 FIDO2

FIDO (Fast Identity Online) ist eine Initiative, die sich zum Ziel gesetzt hat, die Art und Weise, wie wir uns online authentifizieren, zu revolutionieren. Im Kern geht es darum, Passwörter durch sicherere und benutzerfreundlichere Methoden zu ersetzen (z.B. Passkeys)

6.1.1 FIDO2 und U2F: Die Bausteine

FIDO2: Ermöglicht die passwortlose Anmeldung auf Websites und Apps durch den Einsatz von speziellen Sicherheitsschlüsseln. (Passwortloses Anmelden)

U2F (Universal Second Factor): Ein Teil von FIDO2, der sich auf die Verwendung von physischen Sicherheitsschlüsseln als zweite Authentifizierungsstufe zusätzlich zum Passwort konzentriert. Diese Schlüssel werden oft über USB oder NFC mit dem Gerät verbunden und bieten eine zusätzliche Sicherheitsebene.

6.1.2 Wie funktioniert das?

Registrierung: Sie registrieren Ihren iShield Key bei einem Online-Dienst.

Authentifizierung: Bei der Anmeldung fordert die Webseite eine Bestätigung von ihrem Schlüssel an. Dies geschieht durch einfaches Einstecken des iShield Key, anschließend erfolgt die bitte den Schlüssel durch Berührung zu bestätigen.

Bestätigung: Ihr Gerät oder Schlüssel bestätigt Ihre Identität kryptografisch, ohne dass sensible Daten über das Internet übertragen werden. Das tatsächliche Passwort verlässt niemals den Schlüssel!

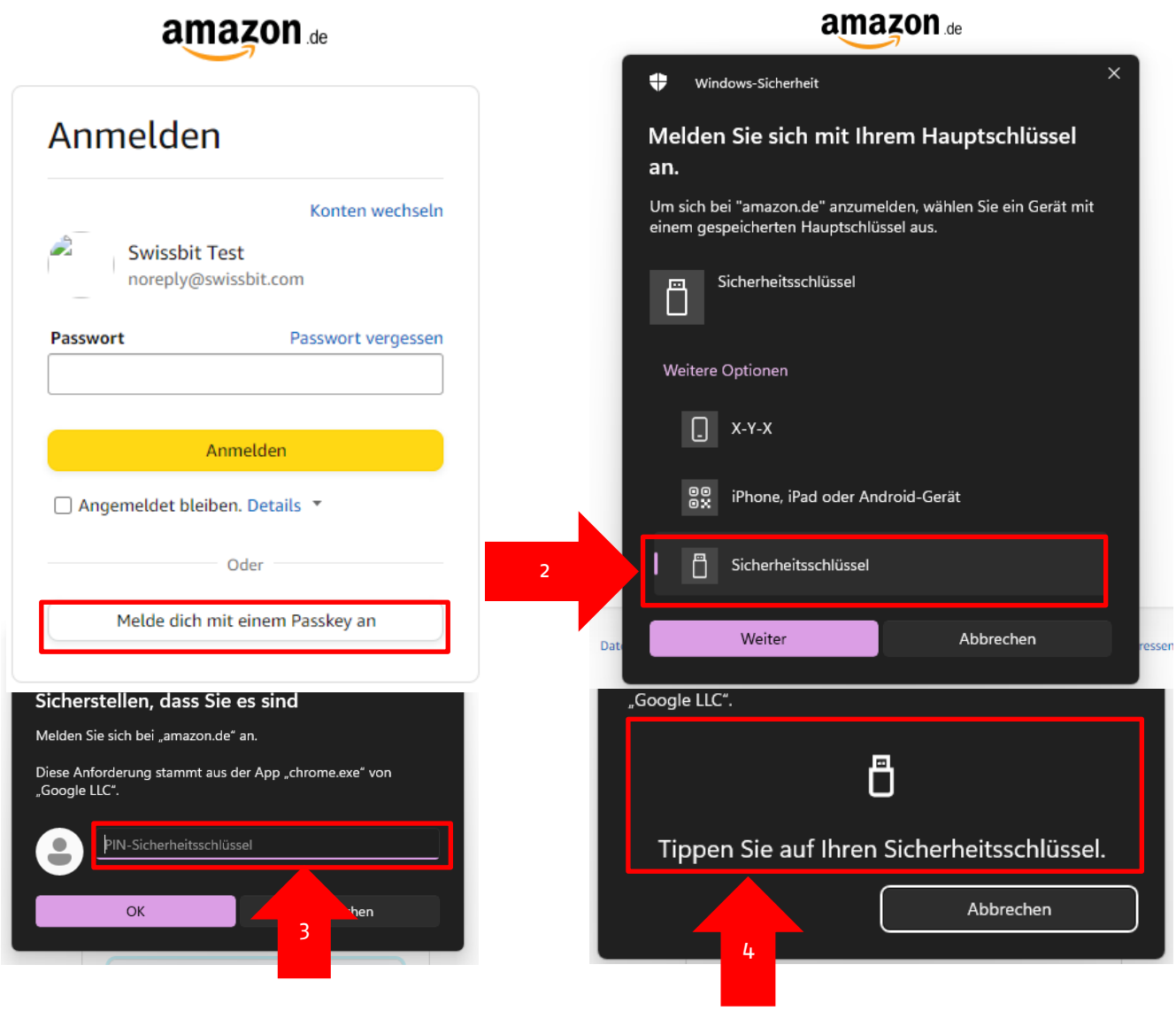
6.1.3 Breite Akzeptanz

FIDO wird von einer Vielzahl von Unternehmen und Organisationen unterstützt, darunter große Namen wie Google, Microsoft, Apple und viele Banken. Die Standards werden in modernen Webbrowsern (Chrome, Firefox, Edge usw.) und Betriebssystemen (Windows, macOS, Android, iOS) unterstützt. Die Bestätigung erfolgt durch Einstecken per USB oder per NFC (ähnlich wie kontaktloses Bezahlen mit der Karte).

6.1.4 Sicherheitsvorteile von FIDO2

FIDO2 gilt als sicherer als herkömmliche Passwort-basierte Systeme, da es Public-Key-Kryptographie verwendet und das Risiko von Phishing-Angriffen reduziert. Bei der Authentifizierung werden keine sensiblen Daten übertragen, was die Sicherheit weiter erhöht.

6.1.5 Anmeldung mit FIDO2 – „Passkey“



6.2 OTP

Ein OTP (One-Time Password) ist wie ein geheimer Code, der nur einmal gültig ist. Stell dir vor, du willst dein Online-Banking nutzen. Zusätzlich zu deinem normalen Passwort bekommst du noch einen OTP zugeschickt, zum Beispiel per SMS auf dein Handy. Dieser Code ist nur für kurze Zeit gültig (oft 30 Sekunden oder eine Minute). Wenn du ihn eingibst, beweist du, dass du wirklich du bist und nicht jemand, der nur dein Passwort kennt.

6.2.1 Warum ist das sicherer?

Schützt vor Passwortdiebstahl: Selbst, wenn jemand dein Passwort herausfindet, kann er sich nicht anmelden, weil er den zusätzlichen OTP-Code nicht hat.

Immer anders: Der OTP ändert sich jedes Mal, wenn du dich anmeldest, also kann er nicht einfach erraten oder wiederverwendet werden.

Zusätzliche Sicherheit: Der OTP bietet eine zweite Schutzschicht, zusätzlich zu deinem Passwort.

6.2.2 Unterschiedliche OTP-Methoden

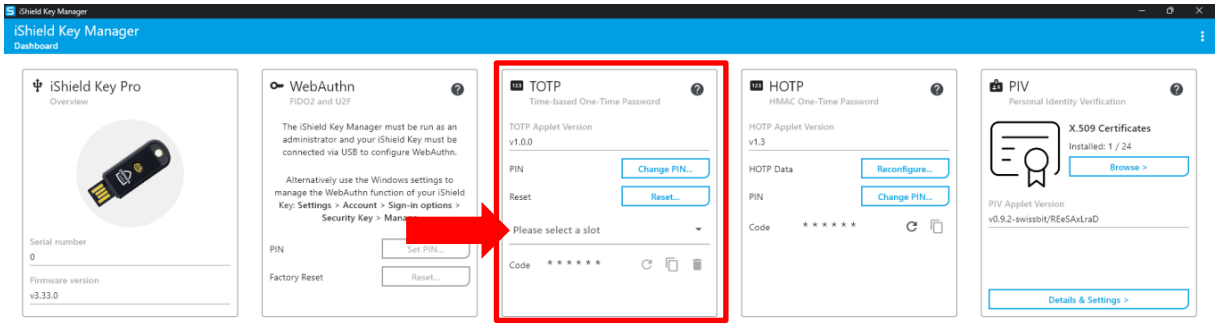
HOTP (HMAC-based One-Time Password): Generiert OTPs basierend auf einem Zählerwert. Der Code ändert sich jedes Mal, wenn ein neuer OTP angefordert wird.

TOTP (Time-based One-Time Password): Generiert OTPs basierend auf der aktuellen Zeit. Diese Codes sind nur für eine kurze Zeit gültig (oft 30 oder 60 Sekunden).

6.2.3 Wie bekomme ich einen OTP?

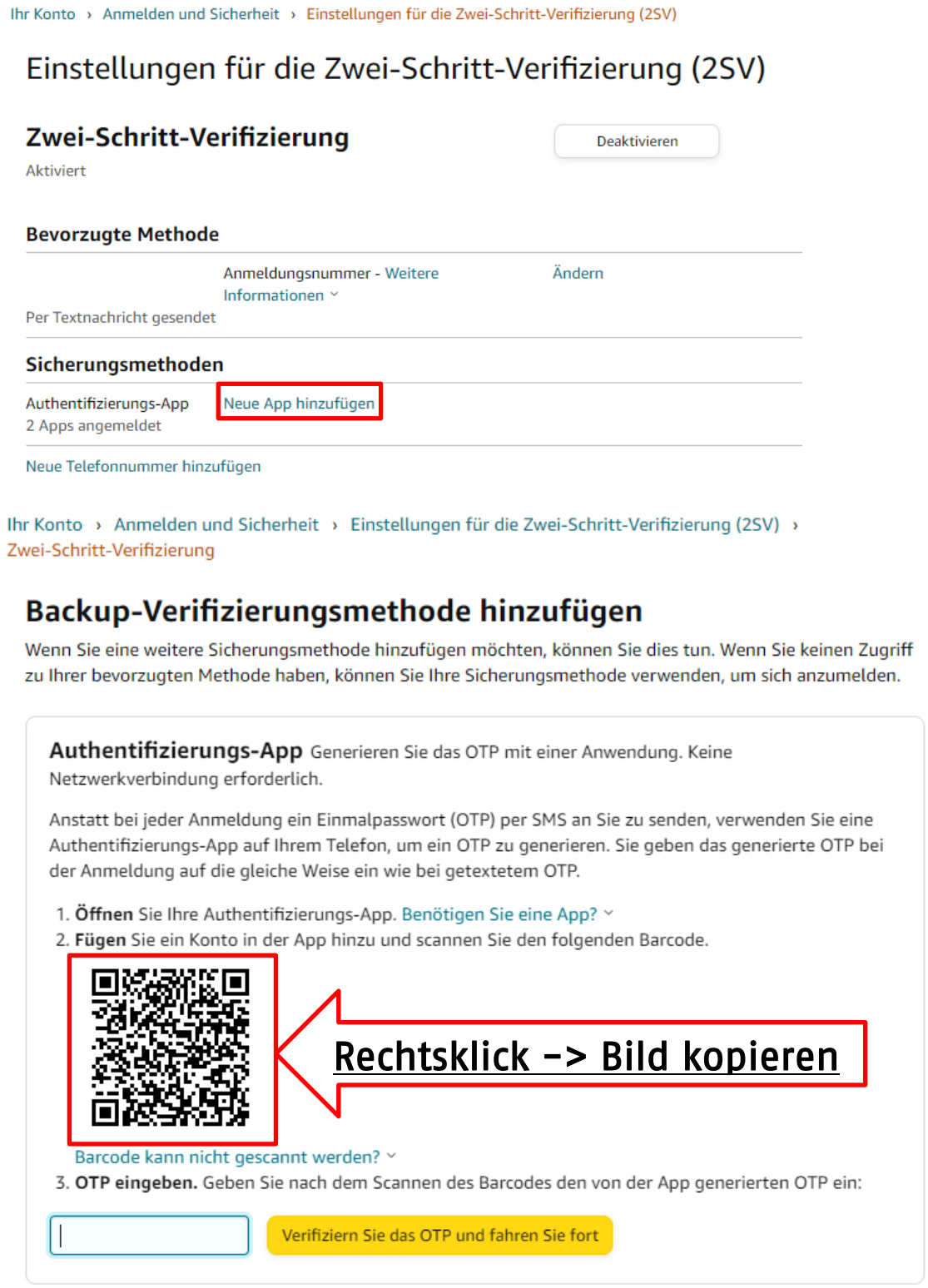
Per NFC: Sie bekommen den Code auf dem Handy angezeigt. (iShield Key Manager App benötigt)

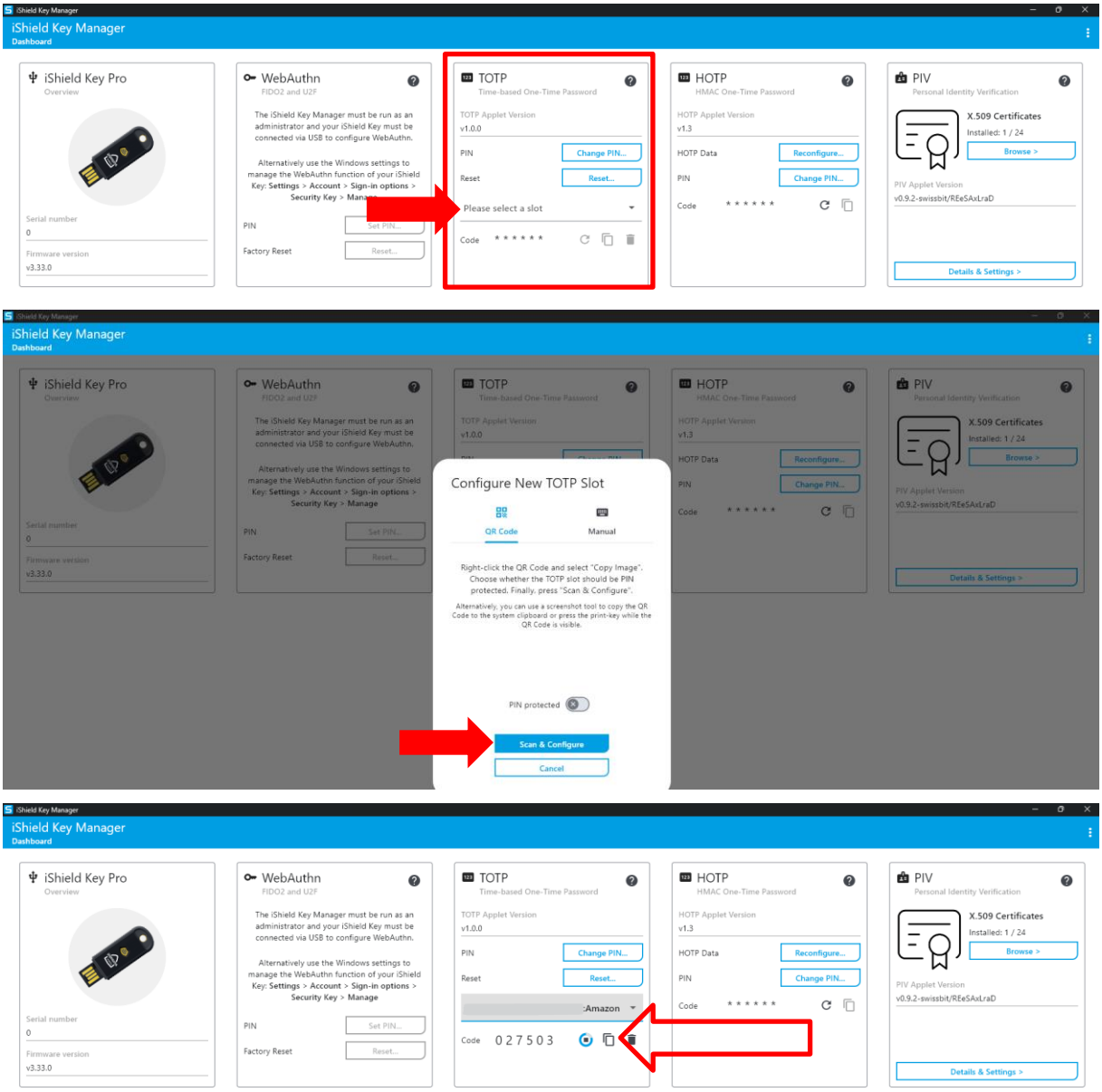
Per USB: Sie bekommen den Code auf dem Computer angezeigt. (iShield Key Manager App benötigt)



6.2.4 Beispiel Amazon am Computer:

Amazon: Mein Konto -> Anmelden und Sicherheit -> 2SV 2 Schritt Verifizierung (englisch. 2FA, 2 Factor Authentication)





Code kopieren, und bei Amazon bestätigen. Fertig

6.2.5 Wie kann ich diesen Code am Handy sehen?

iShield Key Manager für das Android Gerät herunterladen (iOS aktuell noch nicht verfügbar)

iShield Key **hinten** an das Smartphone halten

Nach der ersten erfolgreichen Verbindung erhält man eine Übersicht über alle OTP-Accounts.

Bei Auswahl des Accounts erscheint eine Anfrage den Key ein weiteres Mal an das Gerät zu halten.

7 So verbessert der iShield Key die Sicherheit:

7.1 Physische Sicherheit

Einzigartigkeit: Hardware-Sicherheitsgeräte sind physische Gegenstände, die nicht leicht kopiert oder gestohlen werden können.

Unabhängigkeit: Sie arbeiten unabhängig vom Betriebssystem des Computers oder Mobilgeräts, was sie weniger anfällig für Software-basierte Angriffe macht.

7.2 Starke Authentifizierung

Zwei-Faktor-Authentifizierung (2FA): Hardware-Sicherheitsgeräte wie der iShield Key bieten eine zusätzliche Sicherheitsschicht, indem sie als zweiter Faktor neben dem Passwort verwendet werden.

Passwortlose Authentifizierung: Der iShield Key unterstützt auch die passwortlose Anmeldung, was das Risiko von Passwort-Diebstahl eliminiert.

7.3 Schutz vor Phishing

Herausforderungsbasierte Authentifizierung: Diese Geräte verwenden kryptografische Schlüsselpaare zur Authentifizierung, wodurch sie immun gegen Phishing-Angriffe sind. Selbst wenn ein Benutzer auf einen bösartigen Phishing-Link klickt, kann der Angreifer ohne den physischen Schlüssel keine Anmeldung durchführen.

7.4 Kryptografische Sicherheit

Privater Schlüssel bleibt sicher: Der private Schlüssel wird sicher auf dem Gerät gespeichert und verlässt das Gerät niemals, wodurch er vor Malware und anderen bösartigen Programmen geschützt ist.

Starke Verschlüsselung: Hardware-Sicherheitsgeräte nutzen fortschrittliche kryptografische Methoden, um die Sicherheit zu gewährleisten.

7.5 Kompatibilität und Unterstützung

Breite Unterstützung: Der iShield Key ist mit vielen gängigen Betriebssystemen, Browsern und Online-Diensten kompatibel. Dies erleichterten die Integration und Nutzung.

Standards: Sie unterstützen offene Standards wie FIDO2 und U2F

7.6 Einfache Handhabung

Benutzerfreundlichkeit: Diese Geräte sind oft einfach zu bedienen. Sie müssen lediglich in einen USB-Port gesteckt oder drahtlos an das Gerät gehalten werden (z.B. NFC), um zu funktionieren.

Keine Installation notwendig: In den meisten Fällen sind keine speziellen Treiber oder Software-Installationen erforderlich, was die Verwendung vereinfacht.

7.7 PIV

Der iShield Key Pro unterstützt Industriestandards für die PKI-Smartcard-Authentifizierung auf verschiedenen Betriebssystemen (Windows, macOS, Linux), um eine zertifikatsbasierte Anmeldung zu ermöglichen. Der iShield Key Pro wird sowohl als Smartcard-Lesegerät als auch als kompatible Smartcard erkannt, die die notwendigen Public/Private Schlüsselpaare und Zertifikate zur Authentifizierung, Codesignierung und Verschlüsselung enthält.

8 Warum iShield Key?

8.1 iShield Key vs SMS & E-Mail 2FA

Schwachstellen von SMS-basierter 2FA:

- **Phishing-Angriffe:** Betrüger können gefälschte Webseiten oder Nachrichten erstellen, die so aussehen, als kämen sie von deinem echten Anbieter. Sie verleiten dich dazu, deinen OTP (Einmalpasswort) einzugeben, und können so auf dein Konto zugreifen.
- **SIM-Swap-Angriffe:** Kriminelle können deinen Mobilfunkanbieter dazu bringen, deine Telefonnummer auf eine neue SIM-Karte zu übertragen. Dadurch erhalten sie deine SMS-Nachrichten, einschließlich der OTPs, und können deine Konten übernehmen.

Schwachstellen von E-Mail-basierter 2FA:

- **Phishing-Angriffe:** Ähnlich wie bei SMS können Betrüger gefälschte E-Mails versenden, um dich zur Preisgabe deines OTPs zu bringen.
- **E-Mail-Konto-Kompromittierung:** Wenn dein E-Mail-Konto gehackt wird, hat der Angreifer Zugriff auf alle deine E-Mails, einschließlich der OTPs.

Wie iShield Key eine sicherere Alternative bietet:

iShield Key ist ein physischer Sicherheitsschlüssel, der als zweite Authentifizierungsstufe dient. Er wird über USB oder NFC mit deinem Gerät verbunden und generiert OTPs ohne Internetverbindung. Das macht ihn resistent gegen Phishing- und SIM-Swap-Angriffe.

Vorteile von iShield Key:

- **Physischer Schutz:** Der Schlüssel muss physisch vorhanden sein, um OTPs zu generieren. Das macht es Angreifern schwer, ihn zu stehlen oder zu duplizieren.
- **Keine Internetverbindung erforderlich:** Da der Schlüssel offline funktioniert, ist er nicht anfällig für Phishing-Angriffe, die auf das Abfangen von Nachrichten angewiesen sind.
- **Einfach zu bedienen:** Der Schlüssel lässt sich einfach per Antippen aktivieren und generiert sofort einen OTP.

8.2 Sind iShield Key's unhackbar?

Der iShield Key ist sehr sicher und bietet einen starken Schutz für Ihre Daten und Online-Konten. Es ist jedoch wichtig, sich bewusst zu sein, dass kein Gerät vollkommen unangreifbar ist. Durch die Verwendung des Schlüssels in Kombination mit anderen Sicherheitsmaßnahmen können Sie Ihre Online-Sicherheit erheblich verbessern.

Der iShield Key FIDO2 and iShield Key Pro sind nicht anfällig für die Side-Channel-Angriffe, die Mitte 2024 als Schwachstelle gemeldet wurden. Swissbit hat das Secure Element ersetzt, das in Geräten anderer Hersteller weiterhin anfällig ist.

9 Änderungshistorie

Date	Revision	Details
31.10.2024	1	Initial release