

swissbit®

Product Data Sheet

FIDO2 Hardware Authenticator

iShield Key Series USB-A / NFC

Extended Temperature Grade

Date: July 26th, 2024
Revision: 1.05



Contents

1. PRODUCT SUMMARY	3
2. PRODUCT / SECURITY STANDARDS	4
3. ORDERING INFORMATION	5
4. PRODUCT DESCRIPTION	6
4.1 CURRENT CONSUMPTION	7
4.2 ENVIRONMENTAL SPECIFICATIONS	8
4.3 REGULATORY COMPLIANCE	9
4.4 MECHANICAL SPECIFICATIONS	9
4.5 RELIABILITY	9
5. ELECTRICAL INTERFACE	10
6. ELECTRICAL SPECIFICATION	10
7. PACKAGE MECHANICAL	11
8. FIDO FUNCTIONALITY	11
9. PART NUMBER DECODER	12
10. MARKING SPECIFICATION	14
11. REVISION HISTORY	15

iShield Key Series USB-A / NFC

1. Product Summary

Mechanical Details	Form Factor / Device Type
51.5 x 18.5 x 6mm Thermoplastic polyamide (PA) / matte finish Rear Touch sensor, keychain hole Water resistant, robust construction	CCID Smartcard, FIDO2 HID Device USB-A Device with NFC interface and multi-color LED
Operating Temperature Range	Certifications
Extended: -25 °C to 70 °C	FIDO2/CTAP2 Level 1 Certified Universal 2nd Factor (U2F) CTAP1 Certified Microsoft Certified
Platforms Supported	
Operating Systems: Browsers:	Windows 10/11, MacOS, iOS, iPadOS, Linux, Chrome, Android Firefox, MS Edge, Chrome, Apple Safari

2. Product / Security Standards



HOTP

Hash-based one time password (HOTP) is event-based and a combination of private key & counter-based one-time password.

Function:

- Secures two-factor authentication (2FA) for web services in legacy scenarios that do not support WebAuthn
- HOTP function can also be utilized for offline use case scenarios, where users don't have access to the internet to execute FIDO.

PIV

Personal Identity Verification (PIV) allows the iShield Key Pro to store personal credentials for a given individual.

PKI TOKEN for Authentication, encryption and digital signing

Function:

- Securing 2FA windows login (local, MS Active Directory & Azure Active Directory)
- Storing digital certificates and private keys securely. When you need to encrypt, decrypt or sign something, the token does this internally in a secure chip meaning the keys are never at risk of being stolen.
- Storing security keys for device identification, authentication and registration using pkcs#11 cryptographic standards

TOTP



Time-based one time password (TOTP) is time-based and a combination of private key & time-based one-time password.

Function:

- Secures two-factor authentication (2FA) for web services in legacy scenarios that do not support WebAuthn
- TOTP function can also be utilized for offline use case scenarios, where users don't have access to the internet to execute FIDO.

3. Ordering Information

Table 1: Standard Product List

Product Type		Product Series	Part Number	Supported Standards / Features
	USB-A NFC	iShield Key FIDO2	SNU20000D1PBAN0-E-01-110-SBT <i>(Delivery in tray)</i>	WebAuthn, FIDO2/CTAP2 Universal 2nd Factor (U2F) CTAP1,
			SNU20000D1PBAN0-E-01-110-SBB <i>(Delivery in single packaging)</i>	
	USB-A NFC	iShield Key Pro	SNU20000D1PBAN0-E-01-112-SBT <i>(Delivery in tray)</i>	WebAuthn, FIDO2/CTAP2 Universal 2nd Factor (U2F) CTAP1, HOTP (Event) TOTP (Time) Smartcard (PIV-compatible) OpenSC-compatible
			SNU20000D1PBAN0-E-01-112-SBB <i>(Delivery in single packaging)</i>	

4. Product Description



SECURED BY
swissbit

fido™
CERTIFIED FIDO2

swissbit

Made in Germany

iShield Key Pro: Key Facts

Swissbit iShield Key Pro (USB-A/ NFC) security key:

- Works with FIDO2 and U2F compatible websites and services, such as Google, Microsoft, Salesforce, Amazon Web Services, and many other services
- Supports FIDO2 and U2F standards
- Storage of maximum 32 passkeys
- Security: public and private key cryptography
- Additional security features: HOTP for simple login & PIV for storing security keys and simply accessing encrypted storage drives
- Management tool for configuration
- Durable security key with fully molded, robust and water resistant housing
- Tap-and-go authentication with NFC for mobile devices
- Touch authentication for USB-A interface
- OS: Windows 10 / 11, MacOS, iOS, Linux, Chrome OS, Android
- Browsers: Firefox, MS Edge, Google Chrome, Apple Safari

All-in-one iShield Security Key

Get in and login with ease

All-in-one security key:

- (1) Passwordless access to office
- (2) Log-in to Windows system (Active Directory) with 2FA
- (3) Accessing encrypted storage (BitLocker)
- (4) Access to enterprise relevant FIDO compliant web services



NFC

1 Access Control

PIV

2 Windows Login

PIV

3 Accessing Encrypted Storage

**fido™
CERTIFIED FIDO2**

4 Web Services Login

4.1 Current Consumption

The drive-level current consumption as a function of operating mode is shown in Table 2.

Table 2: Current Consumption

Interface	Initialization	Idle	Unit
USB 2.0	30	19.5	mA

4.2 Environmental Specifications

4.2.1 Recommended Operating Conditions

The recommended operating conditions for the iShield Key Series are provided in Table 3.

Table 3: Recommended Operating Conditions¹

Parameter	Value
Extended Operating Temperature	-25 °C to 70 °C
Power Supply V _{CC} Voltage	5,0 V ± 10%

4.2.2 Recommended Storage Conditions

The recommended storage conditions are listed in Table 4.

Table 4: Recommended Storage Conditions

Parameter	Value
Extended Storage Temperature	-25 °C to 85 °C

4.2.3 Shock, Vibration and Humidity

The maximum shock, vibration and humidity conditions are listed in Table 5.

Table 5: Shock, Vibration and Humidity

Parameter	Value
Non-Operating Shock	1,500 g, 0,5 ms pulse duration, half-sine wave (IEC 60068-2-27, JESD22-B110)
Non-Operating Vibration	50 g, 10Hz – 2000Hz, 3 axes (IEC 60068-2-6,
Humidity (Non-Condensing)	85% RH 85 °C, 330 hrs, max. supply voltage (JESD22-A101)

¹ Adequate airflow is required to ensure the temperature.

4.3 Regulatory Compliance

The iShield Key Series USB-A / NFC comply with the regulations / standards listed in Table 6.

Table 6: Regulatory Compliance

Abbreviation	Regulation/ Standard
EMC	CE - 2014/30/EU FCC - 47 CFR Part 15 UKCA - S.I. 2016 No. 1091 and S.I. 2012 No. 3032
RoHS	2011/65/EU with 2015/863/EU and 2017/2102/EU
REACH	1907/2006/EU and 207/2011/EU
WEEE	2012/19/EU

4.4 Mechanical Specifications

Physical dimensions are detailed in Table 7. Figure 2 illustrates the iShield FID02 dimensions.

Table 7: Physical Dimensions

Physical Dimensions		Unit
Length	51,50±0,3	mm
Width	18,50±0,3	
Thickness (Max)	6,0±0,3	
Weight (Max Capacity)	8	g

4.5 Reliability

FIT and MTBF calculation

The Mean Time Between Failures (MTBF) for the Swissbit® iShield Key Hardware Authenticator is specified to exceed the value listed in the following Table 8.

Table 8: MTBF

Parameter	Value
MTBF (at 25 °C)	> 4,000,000 hours

5. Electrical Interface

The signal/pin assignments and descriptions are listed in Table 9.

Figure 1: USB2 Type-A connector pinout

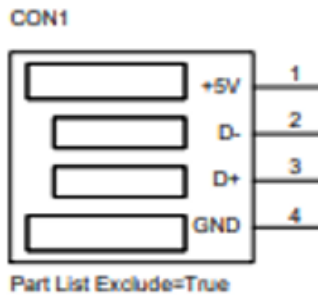


Table 9: Pin Assignment, Name and Description

Pin	Signal Name	Description
1	V_Bus	Operating voltage
2	D-	Data signal pair
3	D+	Data signal pair
4	GND	Power Ground

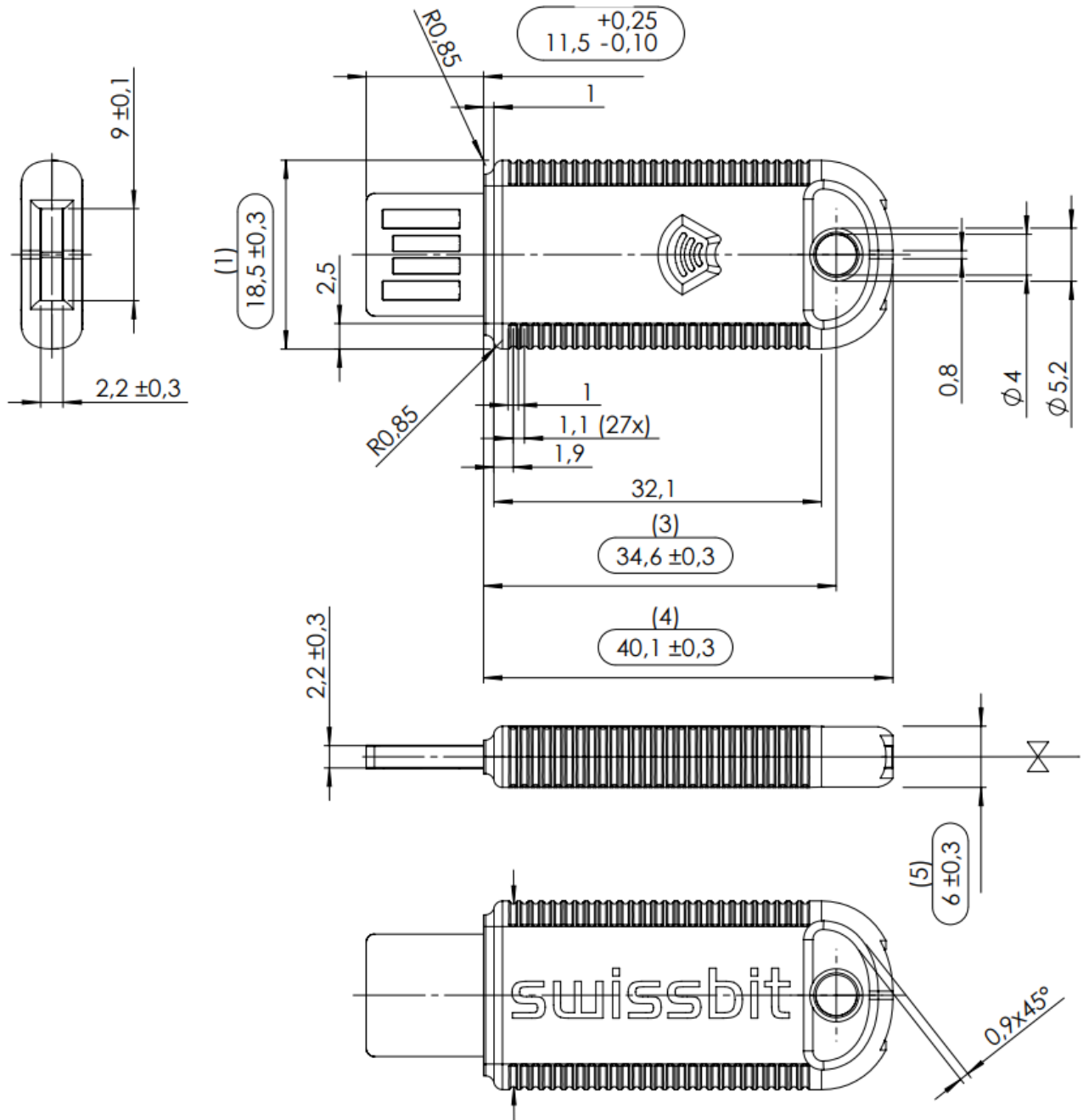
6. Electrical Specification

Table 10: Absolute Maximum Ratings

Parameter	Symbol	Min	Max	Unit
Power Supply Voltage	V_Bus	-0.5	6.0	V
Voltage at D+ and D-	V_Data	-0.5	5.0	

7. Package Mechanical

Figure 2: iShield Key USB-A / NFC



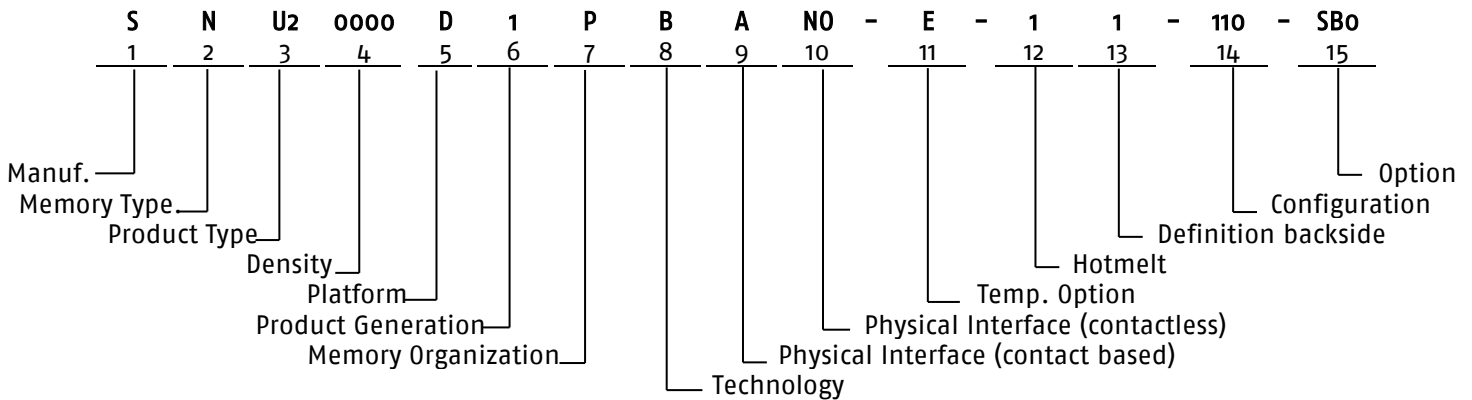
8. FIDO Functionality

See the following Table 11 for a list of FIDO Functionality.

Table 11: Function

Function	Value
FIDO	U2F / FIDO2 (CTAP 2.0)
Interface	USB-A / NFC
Supported Standards (available in iShield Key Pro)	HOTP / PIV / OpenSC

9. Part Number Decoder



9.1 Manufacturer

Swissbit code	S
---------------	---

9.2 Memory Type

Non-Flash	N
-----------	---

9.3 Product Type

USB 2.0 Drive	U2
---------------	----

9.4 Density

No user space	0000
---------------	------

9.5 Platform

Compact USB SMT	D
-----------------	---

9.6 Product Generation

Generation	1
------------	---

9.7 Memory Organization

Security Product	P
------------------	---

9.8 Technology

Infineon SLE78	B
----------------	---

9.9 Physical Interface (contact based)

USB-A	A
-------	---

9.10 Physical Interface (contactless)

NFC	No
-----	----

9.11 Temperature Option

Extended Temperature Range: -25 °C to 70 °C	E
---	---

9.12 Definition of Technology for Non-Flash Products: Hotmelt

Black	o
-------	---

9.13 Definition of Technology for Non-Flash Products: Hotmelt Imprint (backside)

No imprint (flat backside)		0
Swissbit imprint		1

9.14 Configuration XYZ

X = Technology

FIDO2 / U2F		1
-------------	--	---

Y = Firmware Revision

FW Revision		1
-------------	--	---

Z = Feature list FIDO

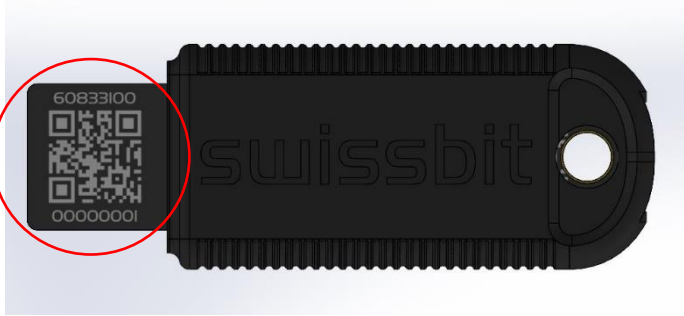

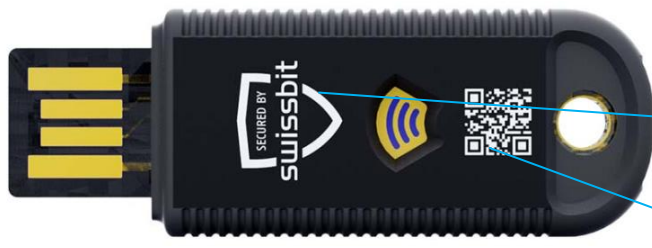
FIDO2, U2F		0
FIDO2, U2F, HOTP, PIV		1
FIDO2, U2F, HOTP, TOTP, PIV		2

9.15 Definition for Security Products

Swissbit iShield Key / Delivery in single packaging		SBB
Swissbit iShield Key / Delivery in tray		SBT

10. Marking Specification

Figure 3: iShield Key Series

Lasermarking / PCB (back side)	Swissbit iShield Key Series
	<p>iShield Key Pro iShield Key FIDO2</p> <p>QR Code with Lot number/counter Serialization number</p>
Digital printing (front side)	Swissbit iShield Key Series with secured by SB logo + QR-Code
	<p>iShield Key FIDO2</p> <p>Secured by Swissbit Logo color "blue"</p> <p>QR code color "white" (with link to landing page)</p>
	<p>iShield Key Pro</p> <p>Secured by Swissbit Logo color "white"</p> <p>QR code color "white" (with link to landing page)</p>

11. Revision History

Table 12: Document Revision History

Date	Revision	Description	Revision Details
20.01.2022	1.00	Initial release	Doc req. no. 5162
31.01.2022	1.01	Added iOS	Doc req. no. 5185
09.01.2023	1.02	Added new Product version with new Features	Doc req. no. 5969
31.03.2023	1.03	Added new Product name	Doc req. no. 6148
31.10.2023	1.04	Added new Product Partnumbers	Doc req. no. 6659

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. Moreover, 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.

© 2024 SWISSBIT AG All rights reserved.