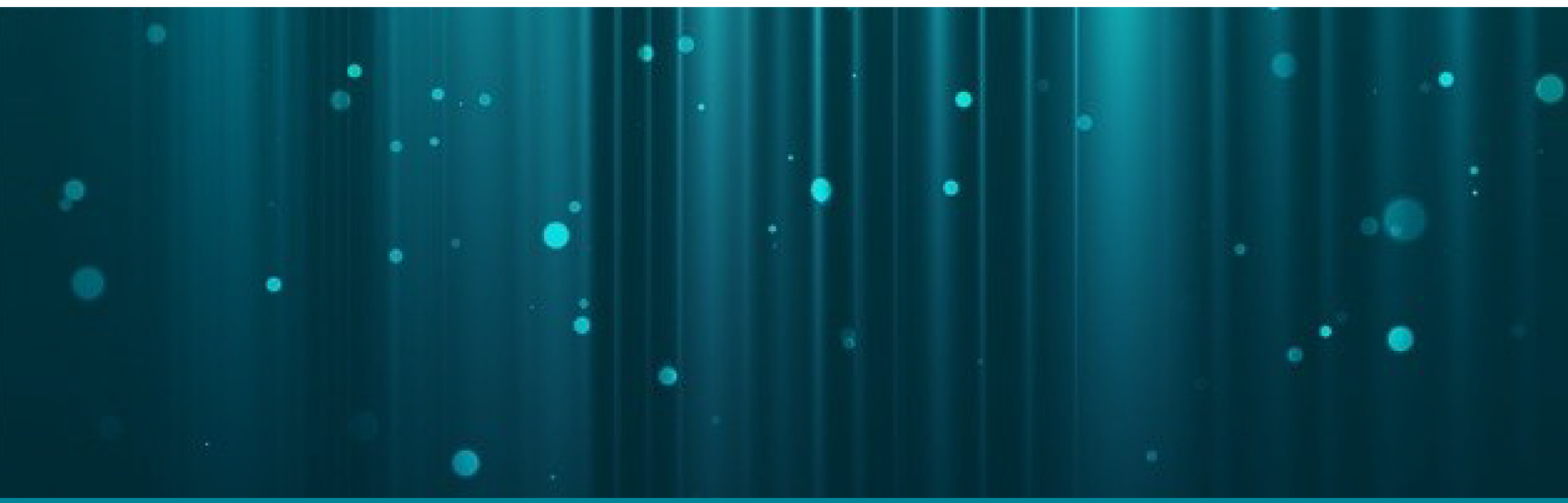
OneSpan



DIGIPASS FX7

User Manual

Version: 2024-08-01

Copyright Notice

Copyright © 2024 OneSpan North America, Inc. All rights reserved.

Trademarks

OneSpan™, DIGIPASS® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc., OneSpan NV and/or OneSpan International GmbH (collectively "OneSpan") in the U.S. and other countries.

OneSpan reserves all rights to the trademarks, service marks and logos of OneSpan and its subsidiaries.

All other trademarks or trade names are the property of their respective owners.

Intellectual Property

OneSpan Software, documents and related materials (“Materials”) contain proprietary and confidential information. All title, rights and interest in OneSpan Software and Materials, updates and upgrades thereof, including software rights, copyrights, patent rights, industrial design rights, trade secret rights, sui generis database rights, and all other intellectual and industrial property rights, vest exclusively in OneSpan or its licensors. No OneSpan Software or Materials may be downloaded, copied, transferred, disclosed, reproduced, redistributed, or transmitted in any form or by any means, electronic, mechanical or otherwise, for any commercial or production purpose, except as otherwise marked or when expressly permitted by OneSpan in writing.

Disclaimer

OneSpan accepts no liability for the accuracy, completeness, or timeliness of content, or for the reliability of links to and content of external or third party websites.

OneSpan shall have no liability under any circumstances for any loss, damage, or expense incurred by you, your company, or any third party arising from the use or inability to use OneSpan Software or Materials, or any third party material made available or downloadable. OneSpan will not be liable in relation to any loss/damage caused by modification of these Legal Notices or content.

Reservation

OneSpan reserves the right to modify these Notices and the content at any time. OneSpan likewise reserves the right to withdraw or revoke consent or otherwise prohibit use of the OneSpan Software or Materials if such use does not conform to the terms of any written agreement between OneSpan and you, or other applicable terms that OneSpan publishes from time to time.

Contact us

Visit our website: **https://www.onespan.com**
Resource center: **https://www.onespan.com/resource-center**
Technical support and knowledge base: **https://www.onespan.com/support**

If there is no solution in the knowledge base, contact the company that supplied you with the OneSpan product.

Date: 2024-08-01

Contents

1 Product overview 1

1.1 Device overview 2

1.2 PIN protection 3

1.3 LED indicator 4

2 Getting started 5

2.1 First steps 5

2.2 Initial authenticator setup 6

2.3 Use the authenticator 8

3 FIDO authentication 9

3.1 Get started with FIDO authentication 10

4 Manage the authenticator 12

4.1 Change the PIN 13

4.2 Remove FIDO credentials 15

4.3 Reset authenticator 16

5 Technical specifications and system requirements 18

5.1 Technical specifications 18

5.2 System requirements 19

6 Safety notice and regulatory information 20

6.1 Safety notice 20

6.2 Regulatory and compliance information 21

Figures

Figure 1: Authenticator front 2

Figure 2: Authenticator back 2

Tables

Table 1: Description of LED 4

Table 2: Technical specifications for DIGIPASS FX7 18

Table 3: Certification and compliance 21

Procedures

To set the PIN (Windows Settings app) 6

To set the PIN (Google Chrome) 7

To register the authenticator 10

To sign in using FIDO authentication 10

To change the PIN (Windows Settings app) 13

To change the PIN (Google Chrome) 13

To remove FIDO credentials (Google Chrome) 15

To reset the authenticator (Windows Settings app) 16

To reset the authenticator (Google Chrome) 17

Product overview

1

Welcome to the *DIGIPASS FX7 User Manual*! DIGIPASS FX7 is a phishing-resistant authenticator that works out-of-the-box with nearly 1,000 of FIDO2–enabled services.

The **FIDO Alliance** develops standards for passwordless authentication. With FIDO (Fast IDentity Online), user authentication does not rely on static passwords or one-time passwords. Instead, users are authenticated via biometrics and FIDO–compliant authenticators.

The DIGIPASS FX7 authenticator works in connected mode via USB-C.

1.1 Device overview 2

1.2 PIN protection 3

1.3 LED indicator 4

1.1 Device overview

1.1.1 Authenticator front

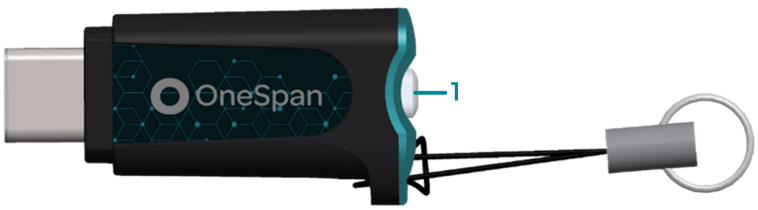


Figure 1: Authenticator front

1 Button with integrated LED

1.1.2 Authenticator back

Regulatory identifiers are printed on the back of the authenticator. The label contains a unique 10-digit serial number, both in text format and 2D barcode.

Figure 2: Authenticator back

1.2 PIN protection

The DIGIPASS FX7 authenticator performs user verification by PIN.

Since the DIGIPASS FX7 authenticator has no keypad, the PIN is entered on the device to which the authenticator is connected (typically a computer or a mobile device).

The PIN is composed of alphanumeric characters and must comply with the following rules:

- **Minimum length**: 4 decimal digits or 4 characters
- **Maximum length**: 63 bytes in UTF-8 representation. This corresponds to 63 characters if only standard ASCII characters are used, but corresponds to fewer characters if special characters are used (e.g. accented, Chinese,...).

NOTE: After 3 consecutive incorrect PIN attempts, the authenticator must be removed from the USB port and re-inserted.

CAUTION: After a total of 8 consecutive incorrect PIN attempts, the authenticator is locked. The authenticator must be reset, which effectively removes all data (credentials, accounts, PIN) and reverts the authenticator to factory settings.

1.3 LED indicator

The device has one LED integrated in the button.

Table 1: Description of LED

LED	Description
○ ○ ○ Blinking WHITE	User presence requested; waiting until button is pressed.
○ WHITE	Upon inserting the authenticator, the LED will shortly turn on to indicate that DIGIPASS FX7 is ready for operation.

Getting started

2

2.1 First steps

2.1.1 Turn the authenticator on/off

- To turn on the authenticator, connect your authenticator to a computer or a mobile device.
- To turn off the authenticator, unplug your authenticator.

2.1.2 Connect your authenticator

You can connect your authenticator via USB-C, or via aUSB-A to USB-C adapter.

2.2 Initial authenticator setup

The following applications provide facilities to set up and manage your authenticator:

- On *Windows*, you can manage your authenticator in the Windows Settings app.
- On *macOS* and *Linux*, you can manage your authenticator via the Google Chrome security settings.

The initial authenticator setup involves the following steps:

1. Set the PIN

2.2.1 Windows

▸ To set the PIN (Windows Settings app)

1. Connect your authenticator.
2. Click the Start button on your computer and select **Settings** to open the Windows Settings app.
3. Select **Accounts > Sign-in options**.
4. Click **Security Key**, then click **Manage**.
5. When prompted, press the button on the authenticator.

   The **Windows Hello setup** dialog is displayed.
6. Under **Security Key PIN**, click **Add**.
7. Specify and confirm the authenticator PIN, and click **OK**. See **1.2 PIN protection** for PIN requirements.

2.2.2 macOS and Linux

▸ To set the PIN (Google Chrome)

1. Connect your authenticator.
2. In Google Chrome, navigate to the **Manage security keys** page:
   - Click ⋮ **Customize and control Google Chrome** and select **Settings > Privacy and security > Security > Manage security keys**.

   -OR-

   - Type the following address in the address bar:

     chrome://settings/securityKeys
3. Click **Create a PIN**.
4. When prompted, press the button on the authenticator.
5. Specify and confirm the PIN, and click **Save**. See **1.2 PIN protection** for PIN requirements.
6. Click **OK** to complete the PIN creation.

2.3 Use the authenticator

The steps for using the DIGIPASS FX7 authenticator vary depending on your application provider's setup. See **3 FIDO authentication** for an overview of the FIDO registration and sign-in process.

FIDO authentication

3

For FIDO authentication, you first need to register your DIGIPASS FX7 authenticator with the relevant service. After successful registration, you can sign in to the service.

> **NOTE:** FIDO operations are accessible via compatible browsers.

3.1 Get started with FIDO authentication 10

3.1 Get started with FIDO authentication

Registration and authentication workflows vary depending on the options that are used by the browser and the platform.

3.1.1 Before you begin

Before you can get started with FIDO authentication, ensure that you have completed the initial authenticator setup. For more information, see **2.2 Initial authenticator setup**.

> **NOTE:** The system might, at the start of the registration process, automatically initiate the PIN setup procedure if no PIN has been set in the authenticator.

3.1.2 Register the authenticator and sign in

▸ To register the authenticator

1. Connect your authenticator via USB-C.
2. Follow the instructions for the relevant service to register the authenticator for FIDO authentication.

   During the registration process, you usually need to name the authenticator, press the button, and provide your PIN.

> **NOTE:** The DIGIPASS FX7 authenticator can save up to 100 discoverable credentials.

▸ To sign in using FIDO authentication

1. Connect your authenticator via USB-C.
2. Follow the instructions for the service to which you want to sign in.

   When prompted, press the button and provide your PIN for authentication.

NOTE: Whether a PIN is needed for authentication is decided by the service (Relying Party).

Manage the authenticator

4

Depending on your operating system, you can use the following applications for authenticator management:

- On *Windows*, you can manage your authenticator in the Windows Settings app.
- On *macOS* and *Linux*, you can manage your authenticator via the Google Chrome security settings.

4.1 Change the PIN 13

4.2 Remove FIDO credentials 15

4.3 Reset authenticator 16

4.1 Change the PIN

4.1.1 Windows

▸ To change the PIN (Windows Settings app)

1. Connect your authenticator and open the **Windows Hello setup** dialog in the Windows Settings app. See **2.2 Initial authenticator setup** for instructions to open the dialog.
2. Under **Security Key PIN**, click **Change**.
3. Do the following:
   a. Enter the old PIN.
   b. Enter and confirm the new PIN.

   See **1.2 PIN protection** for PIN requirements.
4. Click **OK**.

4.1.2 macOS and Linux

▸ To change the PIN (Google Chrome)

1. Connect your authenticator.
2. On the **Manage security keys** page of the Google Chrome security settings, click **Create a PIN**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. When prompted, press the button on the authenticator.

4. Do the following:
    a. Enter the old PIN.
    b. Enter and confirm the new PIN.

    See **1.2 PIN protection** for PIN requirements.
5. Click **Save**.

4.2 Remove FIDO credentials

4.2.1 Windows

The Windows Settings app does not support the removal of FIDO credentials.

4.2.2 macOS and Linux

In Google Chrome, you can view the list of discoverable credentials, and delete credentials as needed.

▸ To remove FIDO credentials (Google Chrome)

1. Connect your authenticator.
2. In the **Manage security keys** page of the Google Chrome security settings, click **Sign-in data**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. Locate the relevant credentials in the list and click the **Delete** icon.
4. Click **Done**.

4.3 Reset authenticator

In some situations it is necessary to restore the factory settings of the DIGIPASS FX7 authenticator, for example, if the PIN is locked.

A factory reset deletes all personal information that is stored on the authenticator:

- PIN
- All credentials
- All accounts

4.3.1 Windows

▸ To reset the authenticator (Windows Settings app)

1. Connect your authenticator and open the **Windows Hello setup** dialog in the Windows Settings app. See **2.2 Initial authenticator setup** for instructions to open the dialog.
2. Under **Reset Security Key**, click **Reset**.
3. Click **Proceed** to confirm that you want to reset the authenticator.
4. When prompted, disconnect and reconnect the authenticator.
5. When prompted, press the button on the authenticator twice within 10 seconds after you have reconnected the authenticator.
6. When the reset is completed, click **Done**.

4.3.2 macOS and Linux

- To reset the authenticator (Google Chrome)

1. Connect your authenticator.
2. On the **Manage security keys** page of the Google Chrome security settings, click **Reset your security key**. See **2.2 Initial authenticator setup** for instructions to open the page.
3. When prompted, disconnect and reconnect the authenticator, then press the button on the authenticator.
4. When prompted, press the button on the authenticator to confirm the factory reset.
5. Click **OK** to complete the factory reset.

Technical specifications and system requirements

5

5.1 Technical specifications

Table 2: Technical specifications for DIGIPASS FX7

Size	35mm (49.5 w/cable) (L) x 35(W) x 10.8mm(H)
Weight	3g
Battery	No battery
Connector	USB-C
Power supply	Via USB-C, 4.40 to 5.50 volts
Dust & water resistance	Dust-safe and splashproof
Supported protocols	FIDO: • FIDO U2F • FIDO2.1: the device implements the CTAP2.1 specification

5.2 System requirements

Supported operating systems:

- Windows 10 version 1903 or later
- macOS 13 or later
- Ubuntu 22.04.2 or later
- Android 12 or later

Supported browsers:

- Google Chrome 111 or later
- All browsers that support the *FIDO2 WebAuthn API*

> **NOTE:** For a list of compatible operating systems and browsers, refer to **https://www.onespan.com/digipassfx7**.

Safety notice and regulatory information

6

6.1 Safety notice

> **CAUTION:** Failure to observe the safety instructions can result in fire, electric shock and other injuries or damage to the device or other property. The housing is made of plastic with sensitive electronic components inside.

Safety instructions

- Do not pierce, break, crush, or cut the device.
- Do not expose the device to an open flame or extremely high temperatures.
- Do not expose the device to liquids or extremely low air pressure.
- Do not drop the device.
- The device must be recycled or disposed of separately from household waste.

6.2 Regulatory and compliance information

Table 3: Certification and compliance

Short-term storage temperature	• -10° C to 50° C • 90% RH non-condensing	• IEC60068-2-78 (damp heat) • IEC60068-2-1 (cold)
Operating temperature	• 0° C to 45° C • 85% RH non-condensing	• IEC60068-2-78 (damp heat) • IEC60068-2-1 (cold)
Vibration	• 10 to 75 Hz • 10 m/s^2	• IEC60068-2-6
Drop	• 1 meter	• IEC60068-2-31
Emission		• EN55032
Immunity	• 4 kV contact discharges • 8 kV air discharges • 3 V/m from 80 to 1000 MHz	• EN55035
Compliant with European Directives		• CE: 89/336/EEC or 2004/108/EC • RoHS: 2002/95/EC • WEEE: 2002/96/EC
Compliant with Federal Communications Commission	• Yes	

Statement of Compliance with EU Directive

CE OneSpan NV declares that this DIGIPASS FX7 device is in compliance with the Essential requirements and other relevant provisions of Directive 2014/53/EU and 2015/863/EU.

The full Declaration of Conformity can be requested from:

Company: OneSpan NV

Address: De Kleetlaan 12A, 1831 Machelen

Belgium Email: legal@onespan.com

FCC Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications made to this equipment not expressly approved by OneSpan NV may void the FCC authorization to operate this equipment.

IC Notice for Canada

This Class B device complies with Canadian ICES-003 requirements for Information Technology Equipment (including Digital Apparatus). Cet appareil numerique de la classe B est conforme àa la norme NMB-003 du Canada.

This Device complies with Industry Canada License-exempt RSS standard(s). Operation is subject to the following two conditions: 1) this device may not cause interference, and 2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: 1) l'appareil ne doit pas produire de brouillage; 2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Correct disposal of this product (Waste Electrical and Electronic Equipment)

Applicable in the European Union and other European countries with separate collection systems

This marking shown on the product or its literature indicates that it should not be disposed of with other household waste at the end of its working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate this from other types of waste and recycle it responsibly to promote the sustainable reuse of material resources. Household users should contact either the provider of the product or their local government office, for details of where and how they can take this item for environmentally safe recycling. Business users should contact their supplier and check the terms and conditions of the purchase contract. This product should not be mixed with other commercial waste for disposal.