RC2

ActivID® BlueTrust Token User Guide

DOCUMENT REFERENCE: BLE_1.0_UG_04.2017

PRODUCT VERSION: 1.0

APRIL 2017

Copyright

Trademarks

Revision History

Date	Description	Document Version
April 2017	Initial release of the document.	1.0

Contacts

Americas	Europe
+1 800-872-5359 (toll-free) +1 949-732-2380	United Kingdom: +44 (0) 1440 714 850 France: +33 (0) 1.42.04.84.00
Asia Pacific	**Corporate**
+852-3160 9800	+1 800.237.7769

Technical Support

If you purchased your product from a third party, then please contact that third party for Technical Support.

For products purchased directly from HID Global, please go to http://www.hidglobal.com/support

Regulatory

CAUTION: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.
ATTENTION: Tout changement ou modification de cet appareil sans approbation explicite du manufacturer vous enlève les droits d'usage de cet équipement.

FCC

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.

FCC RF Exposure Information

This equipment complies with FCC radiation exposure limits set forth in an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

Canada Radio Certification

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

CE Marking

HID Global hereby declares that these Token readers are in compliance with the essential requirements and other relevant provisions of Directive 2006/95/EC.
Por el presente, HID Global declara que estos lectores de proximidad cumplen con los requisitos esenciales y otras disposiciones relevantes de la Directiva 2006/95/EC.
HID Global déclare par la présente que ces lecteurs à proximité sont conformes aux exigences essentielles et aux autres stipulations pertinentes de la Directive 2006/95/EC.
A HID Global, por meio deste, declara que estes leitores de proximidade estão em conformidade com as exigências essenciais e outras condições da diretiva 2006/95/EC.
HID Global bestätigt hiermit, dass die Leser die wesentlichen Anforderungen und anderen relevanten Bestimmungen der Richtlinie 2006/95/EC erfüllen.
HID Global dichiara che i lettori di prossimità sono conformi ai requisiti essenziali e ad altre misure rilevanti come previsto dalla Direttiva europea 2006/95/EC.
Download the R&TTE Declaration of Conformity (DoC) at: http://www.hidglobal.com/certifications

Typographic and Document Conventions

Typography	Description
blue	Cross-references within the document.
blue, underline	References to external web addresses.
bold	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
italic	File names, document titles, and file extensions.
`Code snippets`	Highlights `code snippets` within regular content.
`Code samples`	`Highlights code samples`
	**WARNING**: This symbol indicates a critical warning. It applies to actions that if taken or not taken will break the system. Read the warning carefully and follow it.
	**Important**: This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
	**Note**: This symbol indicates a note that should be of interest to the reader. It is not critical. Nevertheless, the reader should pay attention.

Table of Contents

1.0 Introduction

HID Global ActivID BlueTrust token is a multi-purpose contactless platform for IT and physical access that can be used for a 'One Click' authentication for a secure fast and easy usability.

1.1 Product Overview

HID Global ActivID BlueTrust token is ideally suited for the Enterprise, Banking and Healthcare organizations that need a quick end-user adoption where strong authentication is a priority.

Forgetting passwords is no longer a problem. End-users can easily get access to numerous online applications by leveraging the frictionless Bluetooth Low Energy (BLE) interface.

The device complies with OATH-based authentication and the FIDO Universal Second Factor (U2F) standard based on public cryptography. Technology giants such as Google®, Microsoft®, Visa®, or PayPal® support this standard.

1.2 Document Scope and Audience

This guide describes how to use and manage for ActivID BlueTrust token and is intended for end users.

Token deployment and customization is out the scope of this guide.

2.0 Getting Started

This section provides an overview of the token and explains the Bluetooth pairing process.

2.1 Token Overview

2.1.1 Available Functions

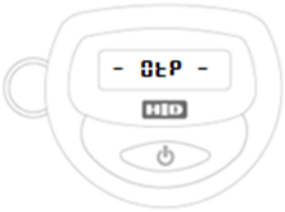
To access the token's menus and functions, press the button for 1, 2 or 3 seconds that correspond to:

- Short press (1 second) during which the status bar fills the screen once.
- Long press (2 seconds) during which the status bar fills the screen twice.
- Extended press (3 seconds) during which the status bar fills the screen 3 times.

Tip! Release the button as soon as the last dash appears.

Table 1: ActivID BlueTrust Token Menu and Functions

Action	Menu displayed	Functions available via a short press
Short press (1 second)	Bluetooth menu 	Short press to access the Bluetooth menu to either: • Pair the token to a computer • Register for FIDO U2F • Authenticate with FIDO U2F • Authenticate with a web-based OTP using the HID BlueTrust Token OTP plug-in

Long press (2 seconds)	OTP menu 	• Short press – generates an OTP.
		• Long press while a OTP is displayed to view the token's:
		  • Serial number
		  • Clock value
		  • Counter value
		  • Soft (firmware) version

Action	Menu displayed	Functions available via a short press
Extended press (3 seconds)	System menu 	Short press to view the system menu options: • RST K – reset the token's pairing keys • BATT – view the battery level **Note:** The menu also includes the advanced DFU and NFC options. For further details, contact your administrator.

Note: The token turns off automatically after a period of inactivity (by default, the timeout is 30 seconds).

2.1.2 Prerequisites

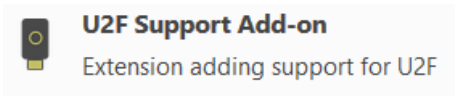
Platforms supported for Bluetooth 4.0 (or later):

Microsoft Windows® 10 (32 and 64-bit) with:

- Google Chrome® 41 or later
- Mozilla® Firefox® 51 or later

Notes:

- For compatibility reasons, Google Chrome is recommended when using the ActivID BlueTrust Token as a security key during the 2-step verification for a Google account.
- To support U2F devices, Mozilla Firefox requires a U2F Add-on available from https://addons.mozilla.org/fr/firefox/addon/u2f-support-add-on/?src=api.



Platforms supported for FIDO U2F:

- Microsoft Windows 10 (32 and 64-bit) via Bluetooth 4.0 (or later)
- Google Android® 6.0 via NFC

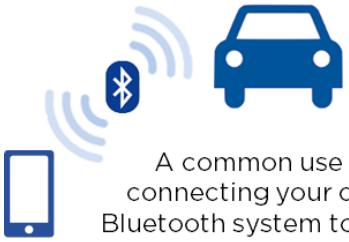
VPNs supported for Web-Based OTP via Bluetooth 4.0 (or later):

- Cisco® ASA software version 8.4
- Pulse Secure® PSA 300
- F5® 2000

2.1.3 About Bluetooth

Bluetooth is a wireless communication technology that provides a simple way to connect compatible devices so that they can work together.

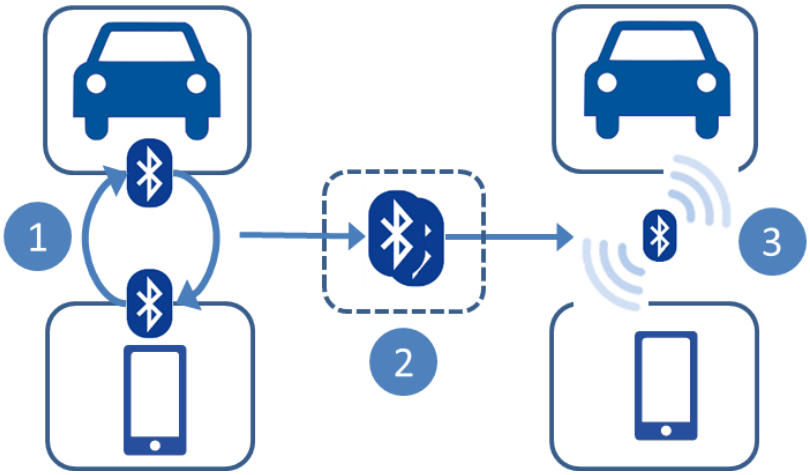
Bluetooth can be found everywhere, including most customer electronics.



A common use is connecting your car's Bluetooth system to your smartphone to safely make and receive calls while driving.

Bluetooth also allows connecting peripherals such as keyboards, headsets and game controllers to computers, televisions and video game consoles.

1. For devices to work together, you have to perform a one-time pairing process during which devices share their Bluetooth data (such as the unique address) and a common secret key.



2. This data is stored in each device's memory and creates a 'bond' between them.

   You might need to validate the pairing by authenticating the connection using a passcode or PIN.

3. The paired devices will automatically detect and connect to one another as soon as they are within in range and with Bluetooth activated.

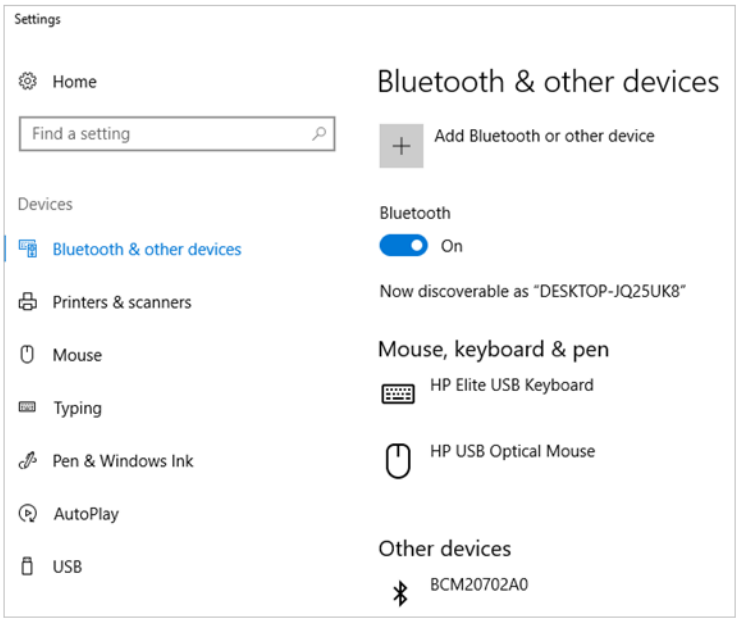
2.2 Pair Your Token on Microsoft Windows 10

This section explains how to pair your ActivID BlueTrust Token to a Microsoft Windows 10 computer.

Note: You only need to pair your token once with the computer. For subsequent connections, the token connects to your computer automatically.

1 Turn on Bluetooth on your Computer

1. Select **Start**, **Settings** and then **Devices**.
2. In the Devices menu, select **Bluetooth & other devices**.
3. Turn **On** Bluetooth.
4. Click + to **Add Bluetooth or other device**.



2 Prepare the BlueTrust Token for Pairing

Press the token button for 1 second until the status bar fills the display.

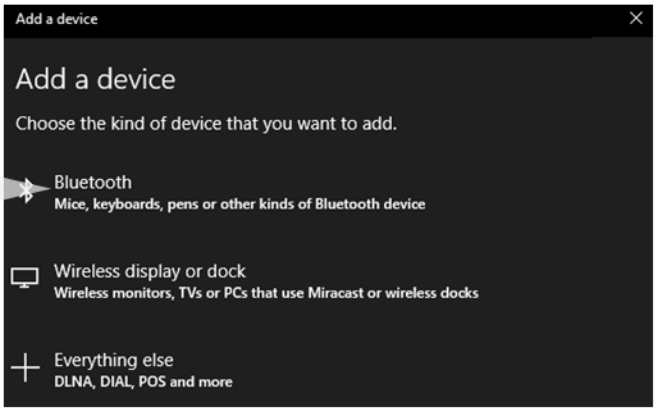
Tip! Release the button as soon as the last dash appears.

When **BLE** (Bluetooth menu) is displayed, press the button again to display **WAIT**.

The visibility period is 30 seconds.

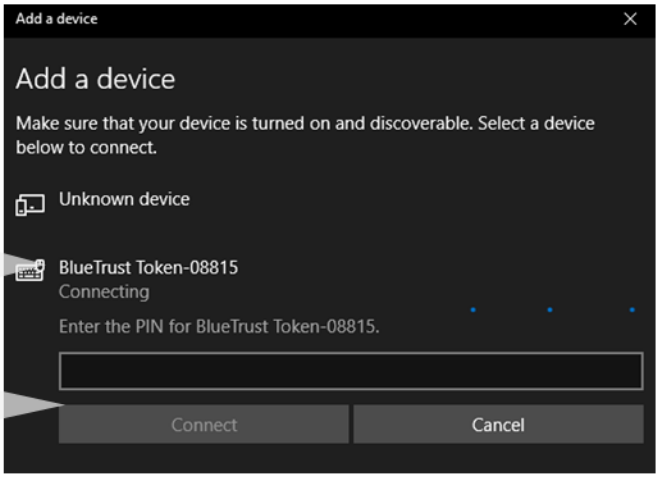
3 Start the Pairing Process

Click **Bluetooth**.

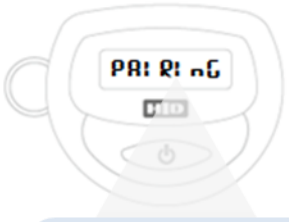


Click **BlueTrust Token** in list of available Bluetooth devices.

You are prompted to enter the pairing PIN for the token.



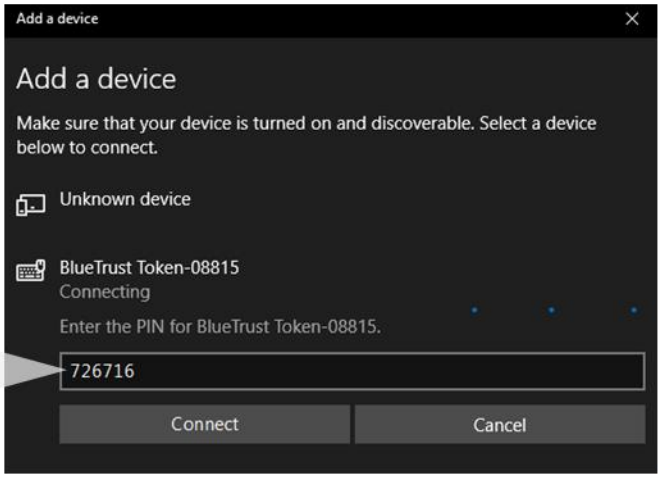
4 Get the Pairing PIN



Wait for the token to initiate the **PAIRING** process.

The token displays the pairing PIN of 6 numbers.

5 Enter the Pairing PIN

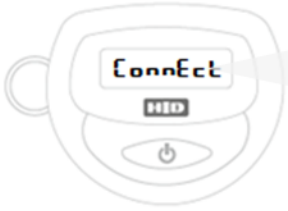


Enter the token's pairing **PIN**.

Click **Connect**.

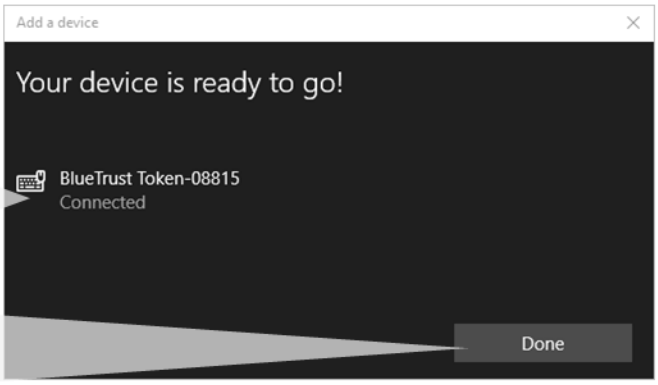
6 Pairing is Complete – BlueTrust Token is Ready to Use

Important! Do not turn off the token before **Connect** is displayed.



The token displays **Connect** for 45 seconds and then turns off.

The computer displays the BlueTrust Token as **Connected**.



Click **Done**.

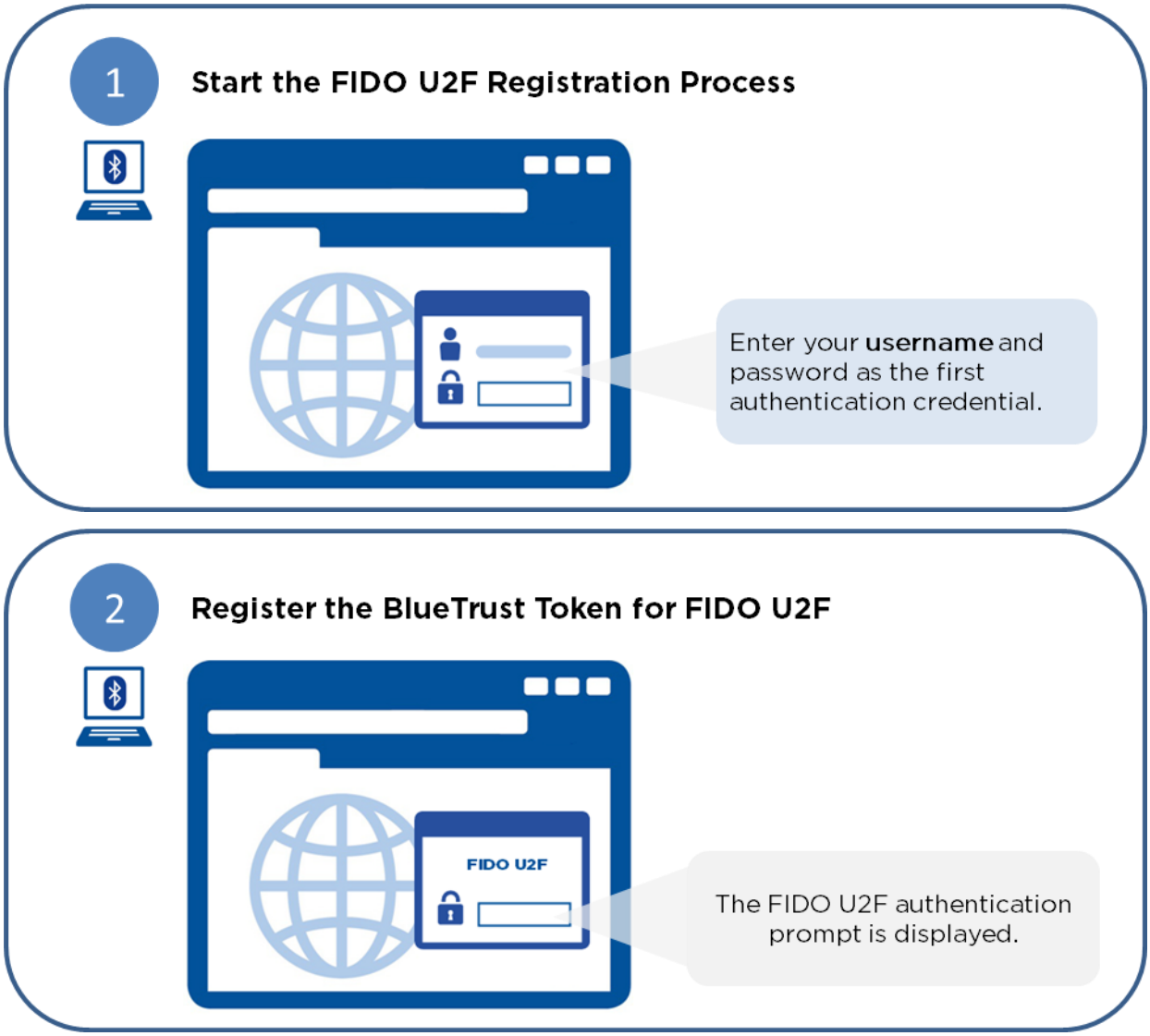
3.0 Authenticating with FIDO U2F

3.1 Register for FIDO U2F Authentication

The registration process varies according to the website or service you want to access.

For example, refer to the Google 2-Step Verification page at https://support.google.com/accounts/topic/7189195?hl=en&ref_topic=3382253

The following procedure provides an overview of the common steps.



3 Activate the Bluetooth Connection

Press the token button for 1 second until the status bar fills the display.

Tip! Release the button as soon as the last dash appears.

When **BLE** (Bluetooth menu) is displayed, press the button again to display **WAIT**.

The connection period is 30 seconds.

4 Validate the Registration

The BlueTrust Token is registered as the second authentication credential.

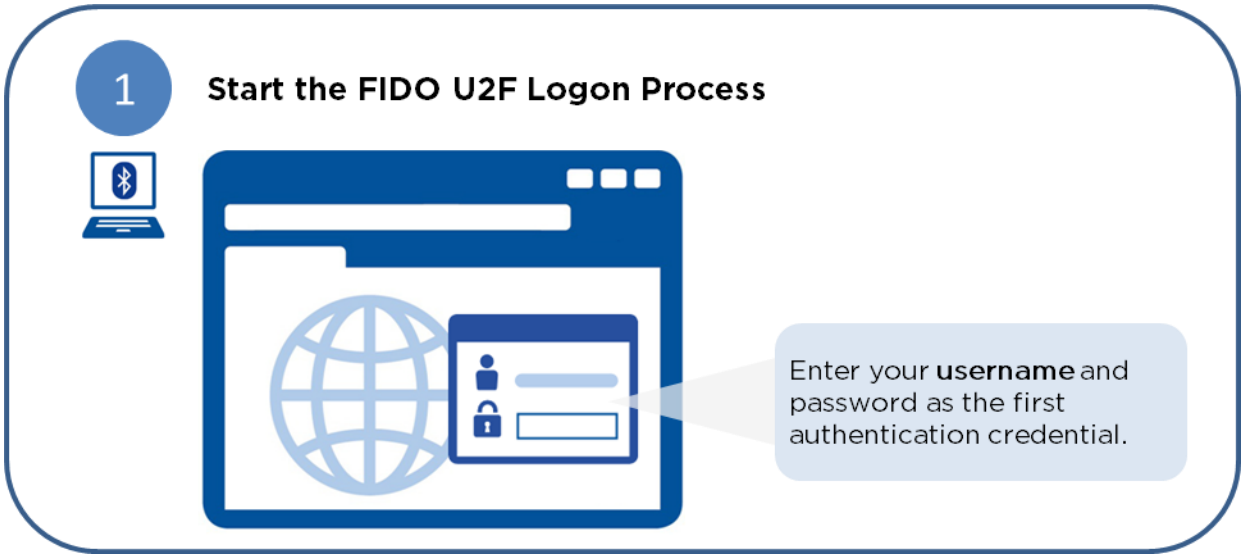
When **VALID?** is displayed, press the button to validate the registration.

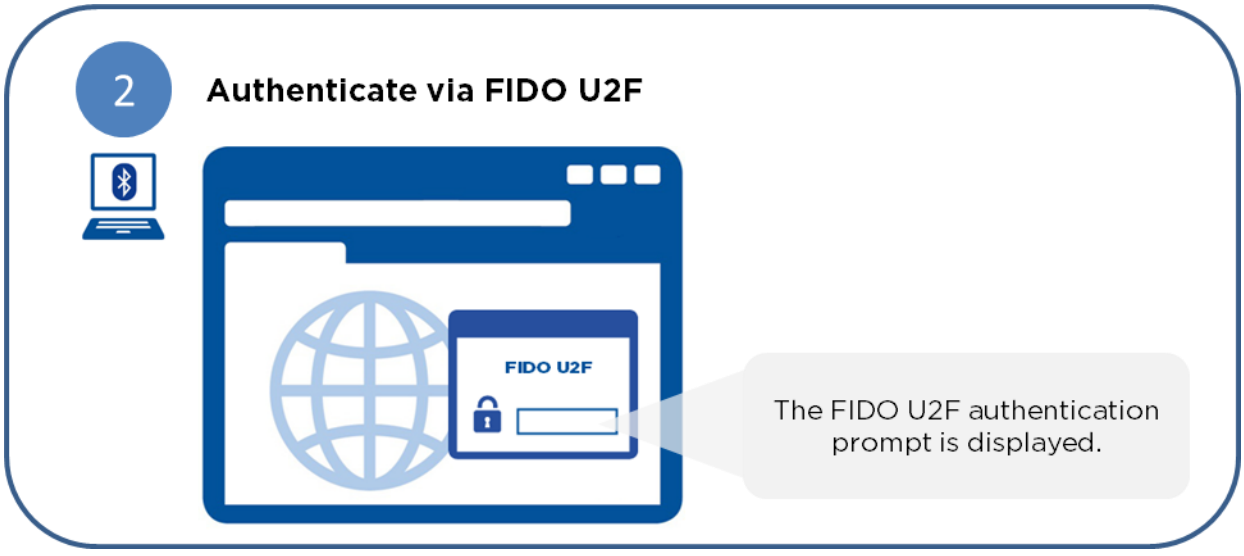
The BlueTrust Token displays **REGISTER** and then turns off.

3.2 Authenticate with FIDO U2F via Bluetooth

Prerequisites:

- You have paired the token with your computer (see section 2.2 Pair Your Token on Microsoft Windows 10 on page 9).
- You have registered for FIDO U2F authentication with the website or service you want to access.





3 Activate the Bluetooth Connection

Press the token button for 1 second until the status bar fills the display.

Tip! Release the button as soon as the last dash appears.

When **BLE** (Bluetooth menu) is displayed, press the button again to display **WAIT**.

The connection period is 30 seconds.

4 Validate the Authentication

The BlueTrust Token is validated as the second authentication credential.

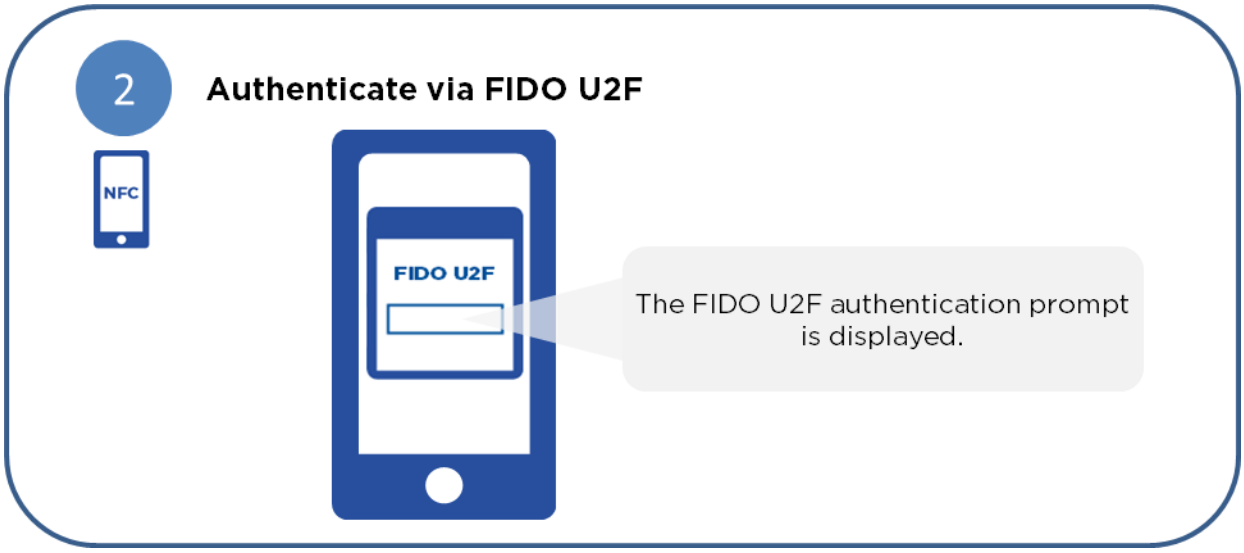
When **VALID?** is displayed, press the button to validate the authentication.

The BlueTrust Token displays **AUTHENT** and then turns off.

3.3 Authenticate with FIDO U2F in Contactless Mode (Android Only)

Prerequisites:

- You have registered for FIDO U2F authentication with the website or service you want to access.
- Your Android device is NFC-compatible.
- The latest version of Google Authenticator is installed (for further information, go to https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=fr).



3 Activate the Bluetooth Connection

Press the token button for 1 second until the status bar fills the display.

Tip! Release the button as soon as the last dash appears.

When **BLE** (Bluetooth menu) is displayed, press the button again to display **WAIT**.

The connection period is 30 seconds.

4 Validate the Authentication

Tap the screen of your device to validate the authentication.

The BlueTrust Token is validated as the second authentication credential.

4.0 Authenticating with a Web-Based OTP

This section explains how to authenticate using a web-based OTP generated by the ActivID BlueTrust Token and communicated to your browser via Bluetooth.

4.1 Install the Plug-In for Web OTP Authentication

The HID BlueTrust Token OTP extension/plug-in is available as setup file (*.msi*) that you must run to install the plug-in correctly.

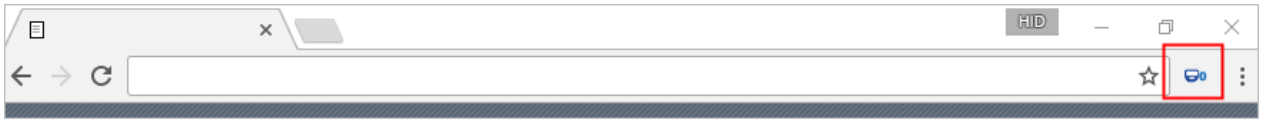
You can download the setup from the HID Global website at https://www.hidglobal.com/drivers.

For further information, contact your administrator.

Important: You must launch the browser and authorize the add-on before you can use it with the ActivID BlueTrust Token.

If the authorization prompt does not appear, use the browser's Extension management tool to manually authorize the plug-in.

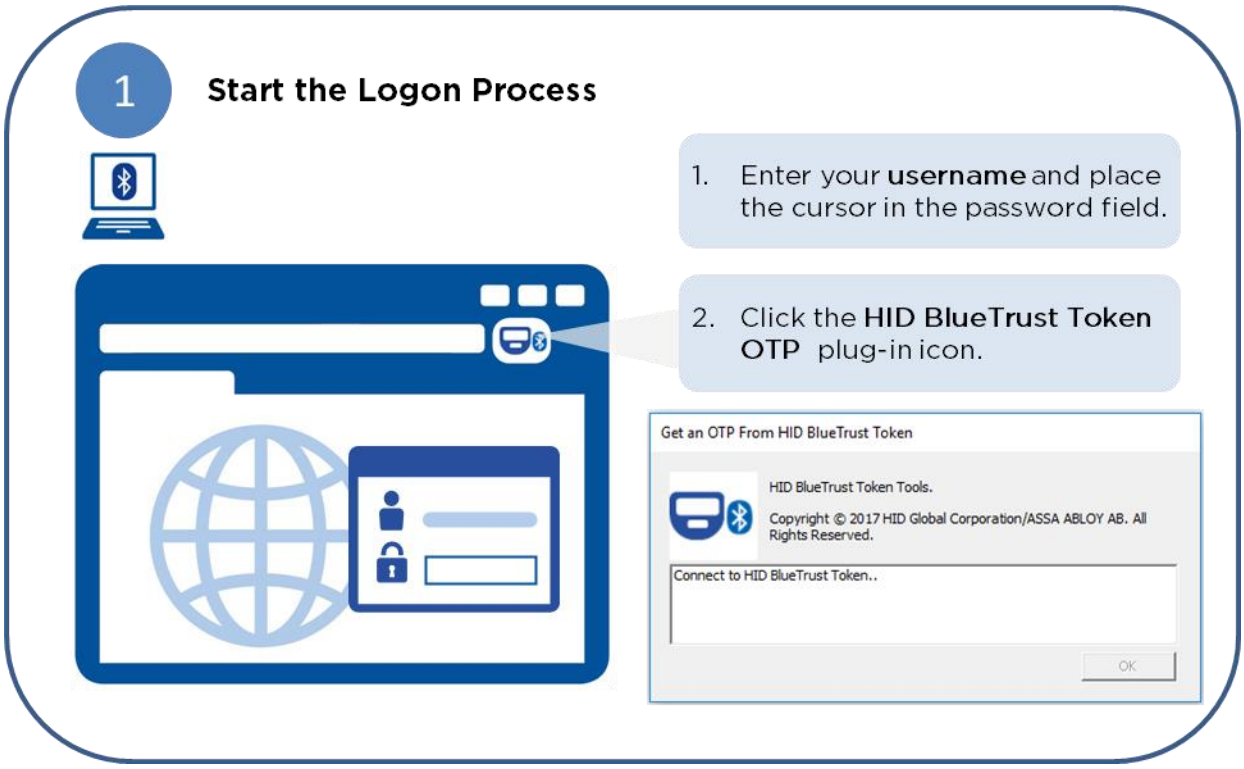
After installation, the HID BlueTrust Token OTP icon is added to the browser window:



4.2 Authenticate with a Web-Based OTP via Bluetooth

Prerequisites:

- You have paired the token with your computer (see section 2.2 Pair Your Token on Microsoft Windows 1 on page 9).
- You have installed and enabled the HID BlueTrust Token OTP plug-in in your browser (see section 4.1 Install the Plug-In for Web OTP Authentication on page 18).
- Your computer's Bluetooth service is turned on.



2 Activate the Bluetooth Connection

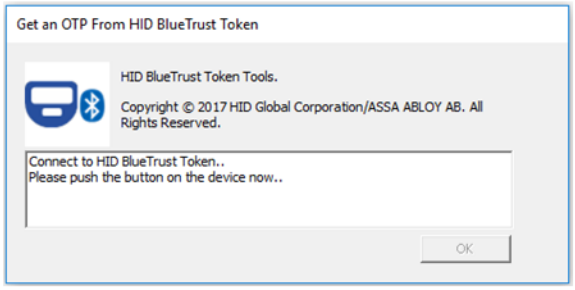
Press the token button for 1 second until the status bar fills the display.

Tip! Release the button as soon as the last dash appears.

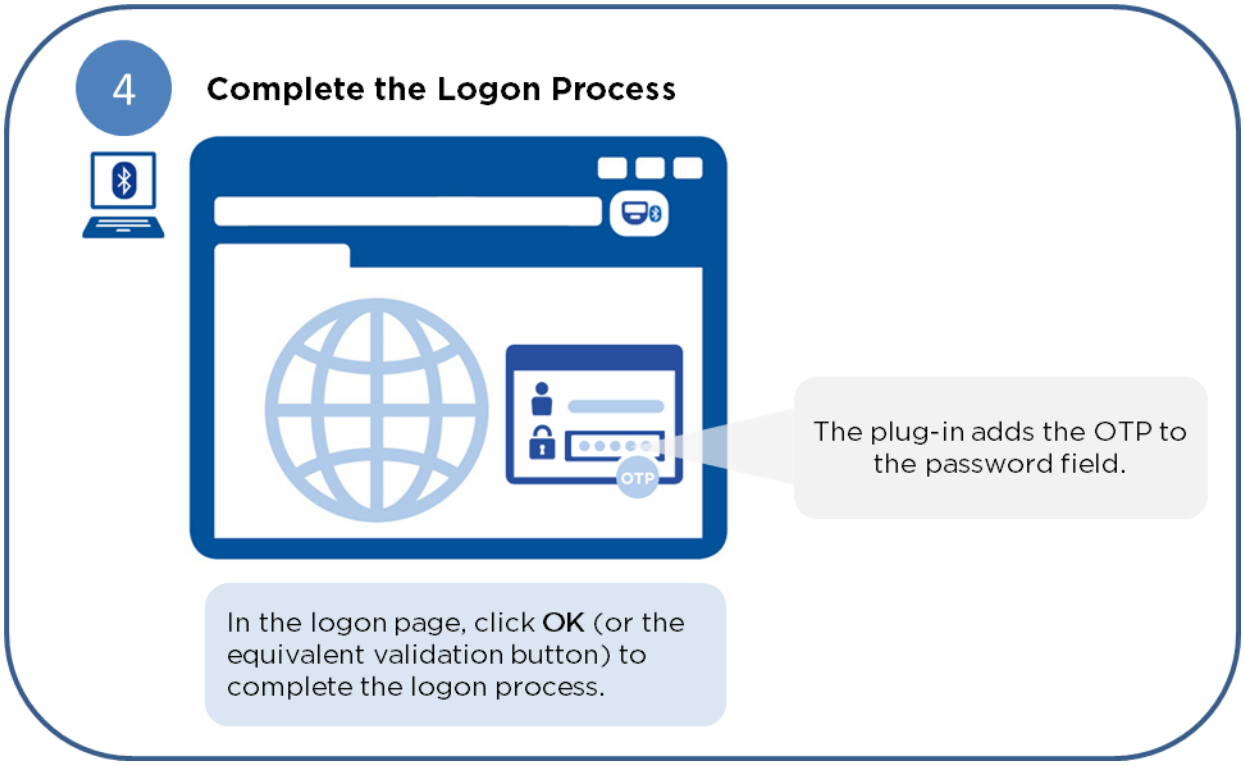
When **BLE** (Bluetooth menu) is displayed, press the button again to display **WAIT**.

The connection period is 30 seconds.

3 Validate the Authentication

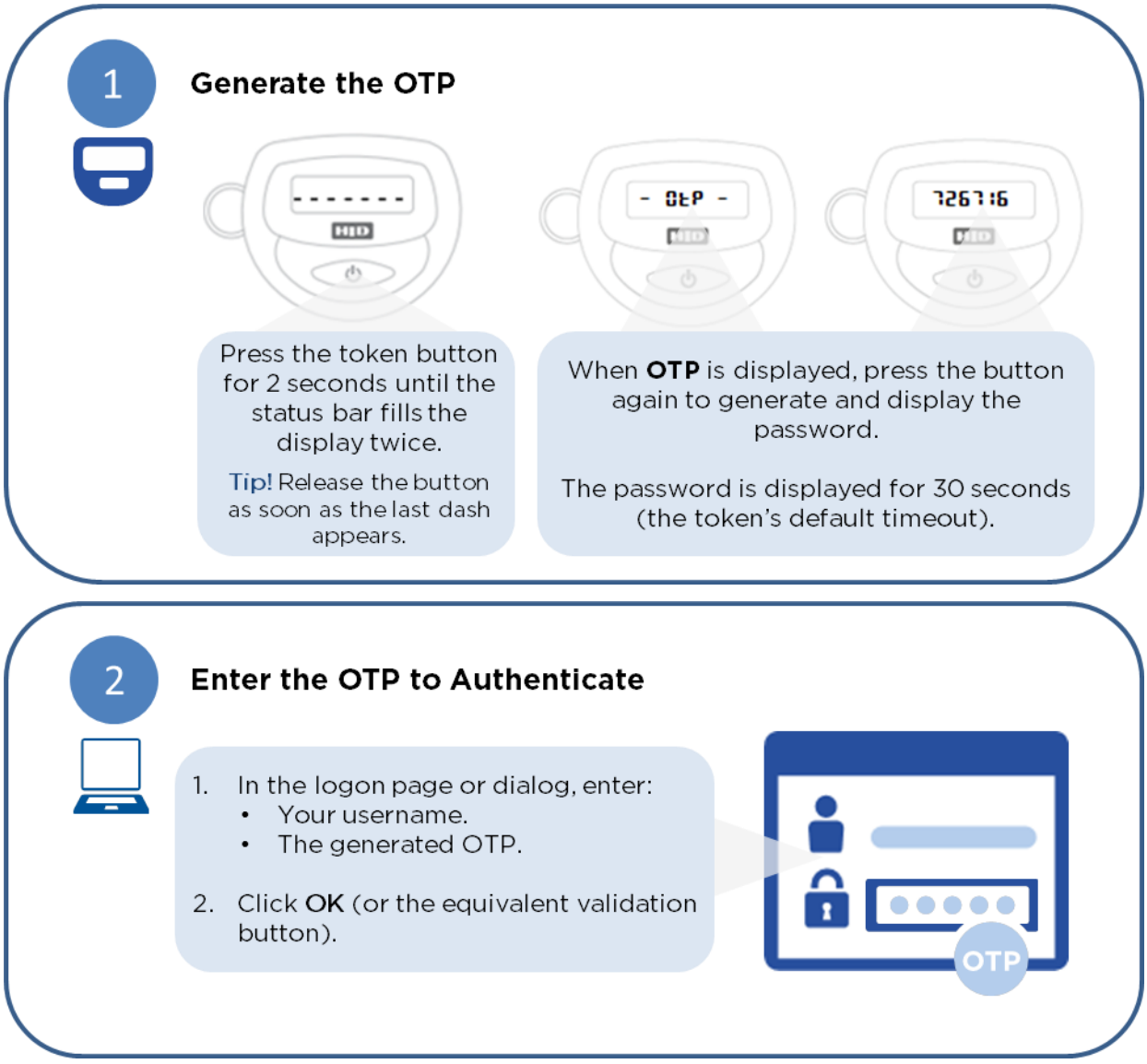


When **VALID?** is displayed, press the button to validate the authentication.


4
Complete the Logon Process
OTP
The plug-in adds the OTP to the password field.
In the logon page, click OK (or the equivalent validation button) to complete the logon process.

5.0 Authenticating with a Manual OTP

This section explains how to manually generate an OTP using the ActivID BlueTrust Token if your computer does not have Bluetooth interface.



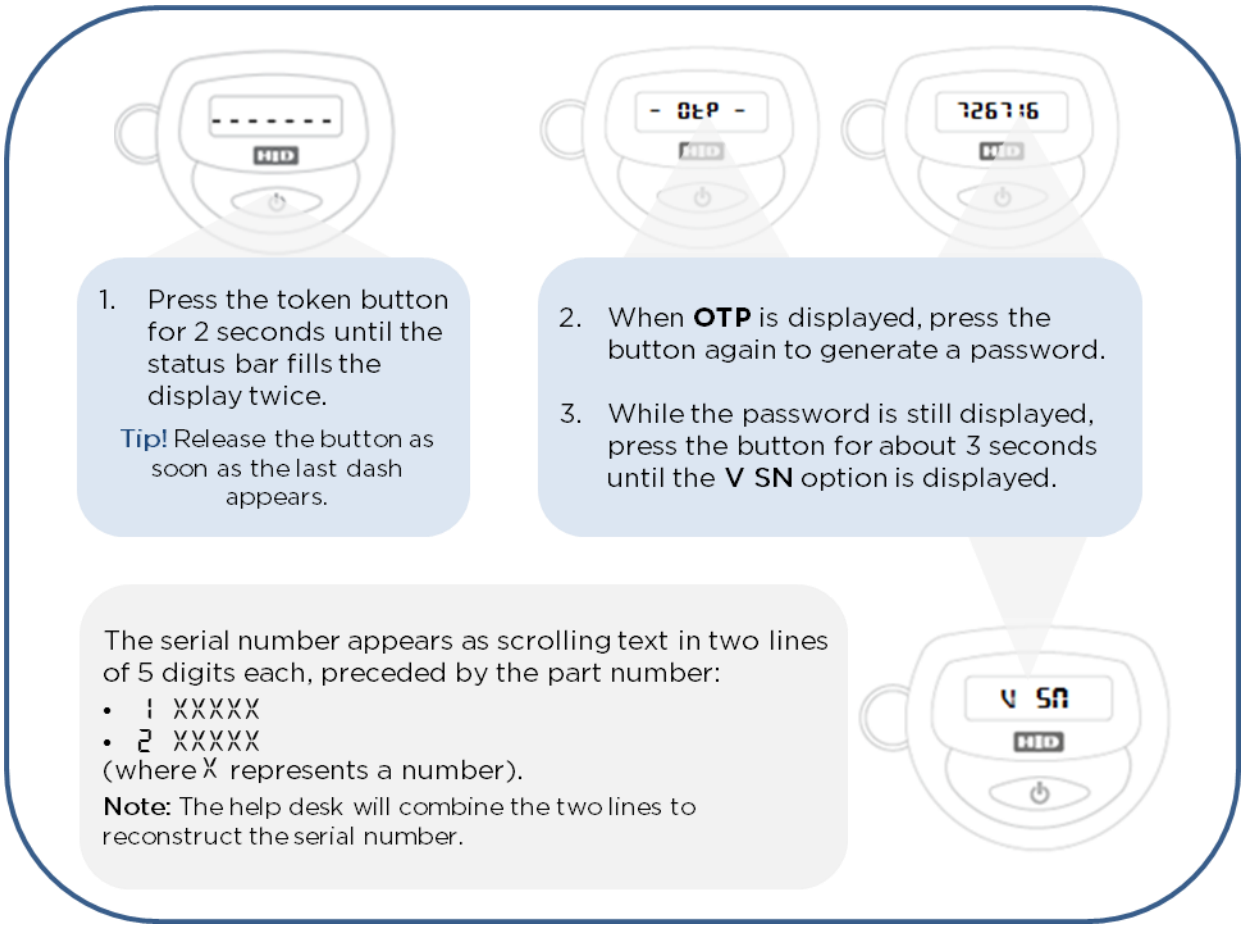
6.0 Managing the ActivID BlueTrust Token

This section explains how to manage the ActivID BlueTrust Token using the internal functions and menus.

6.1 View the Serial Number

The serial number is useful for identifying the ActivID BlueTrust Token in case the token's back sticker should come off.

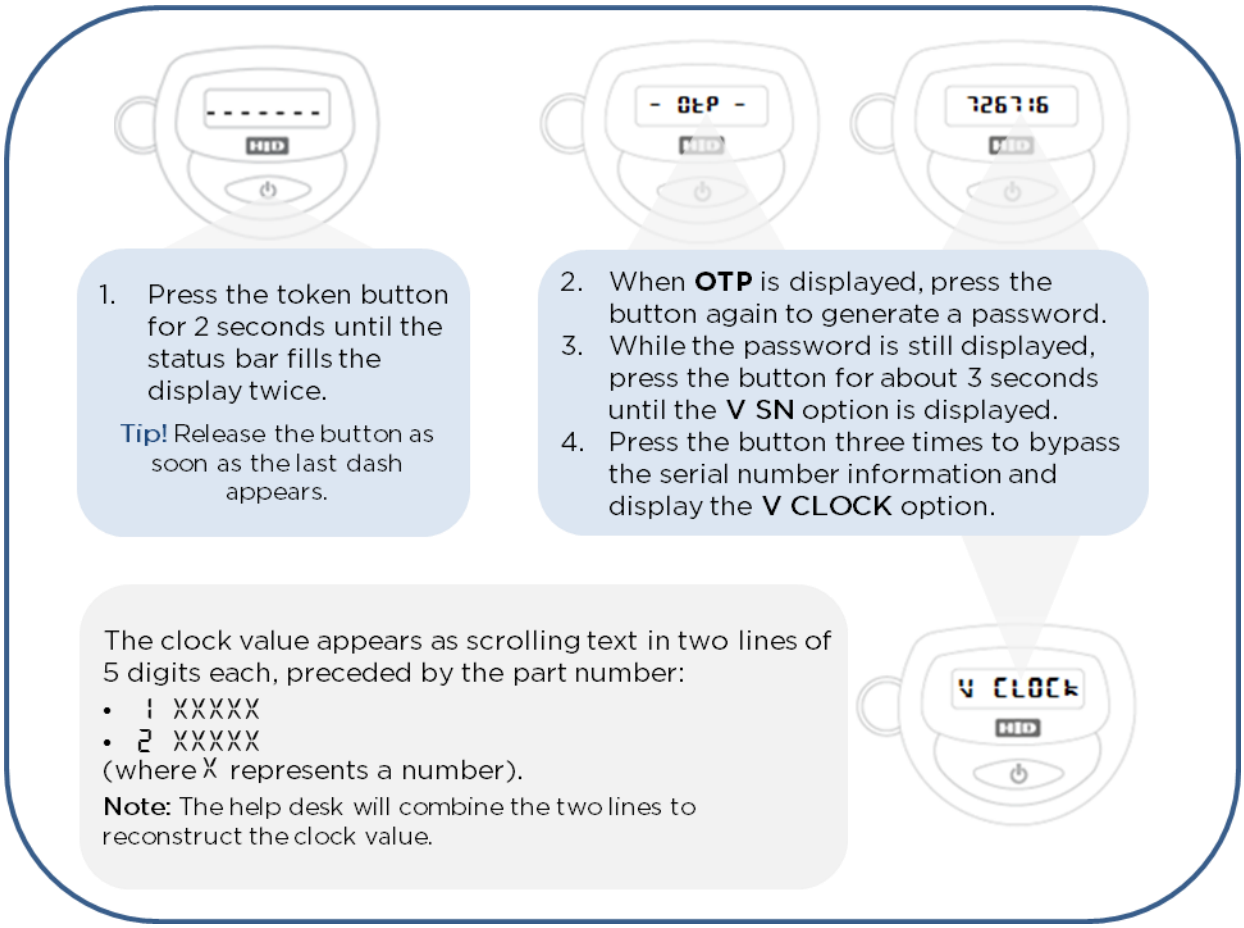
You can give the serial number to a Help Desk operator to resolve any synchronization issues with the token.



6.2 View the Clock Value

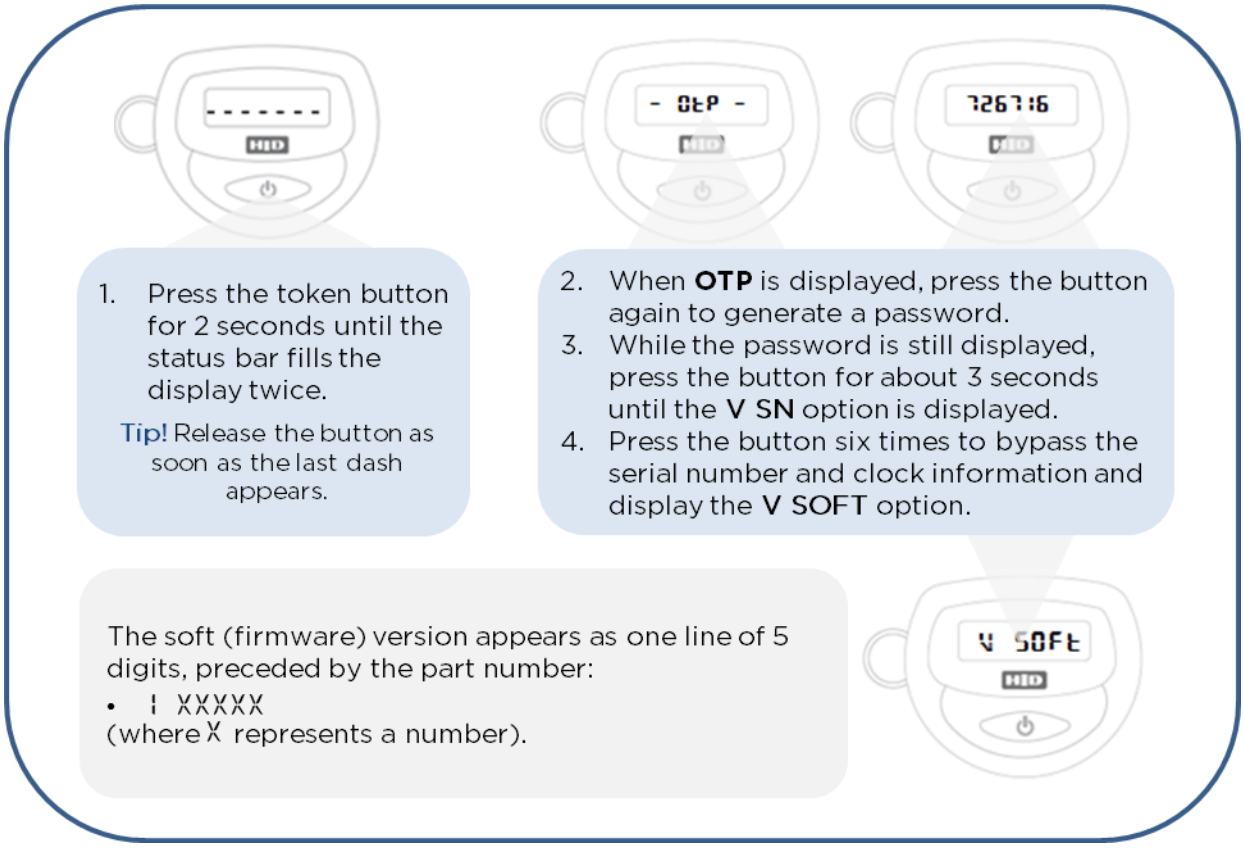
You can give the clock value to a Help Desk operator to resolve any synchronization issues with the ActivID BlueTrust Token.

Note: This procedure only applies to the ActivID BlueTrust Token when the clock information is available.



6.3 View the Soft Version

The soft version function displays the version of the firmware used by the ActivID BlueTrust Token.

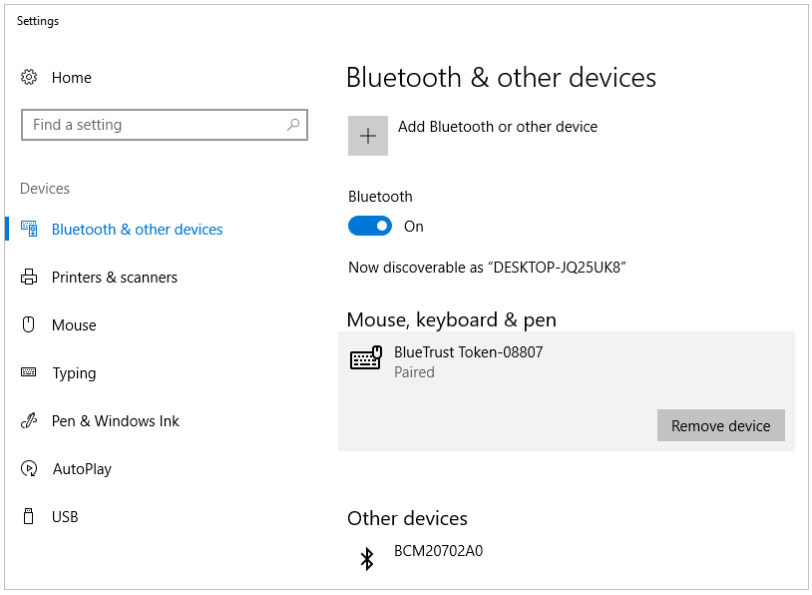


6.4 Remove a Pairing

This section explains how to remove the pairing between the ActivID BlueTrust Token and all the computers that are currently paired with the device.

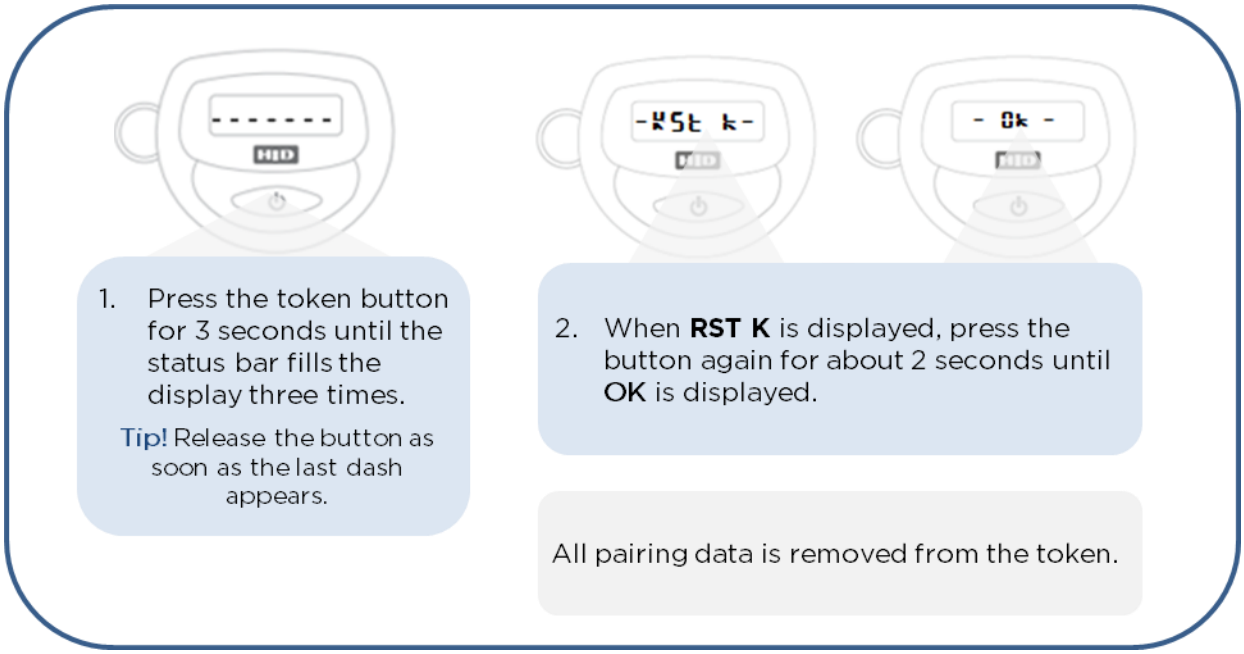
For security reasons, it is recommended that you perform the following steps to make sure that the pairing is removed completely.

1. On your computer or device, delete the pairing with the ActivID BlueTrust Token.



On Microsoft Windows 10, select the ActivID **BlueTrust Token** in the list of Bluetooth devices and click **Remove device**.

2. Remove the existing pairing keys stored in the ActivID BlueTrust Token using the **RST K** menu to reset them.

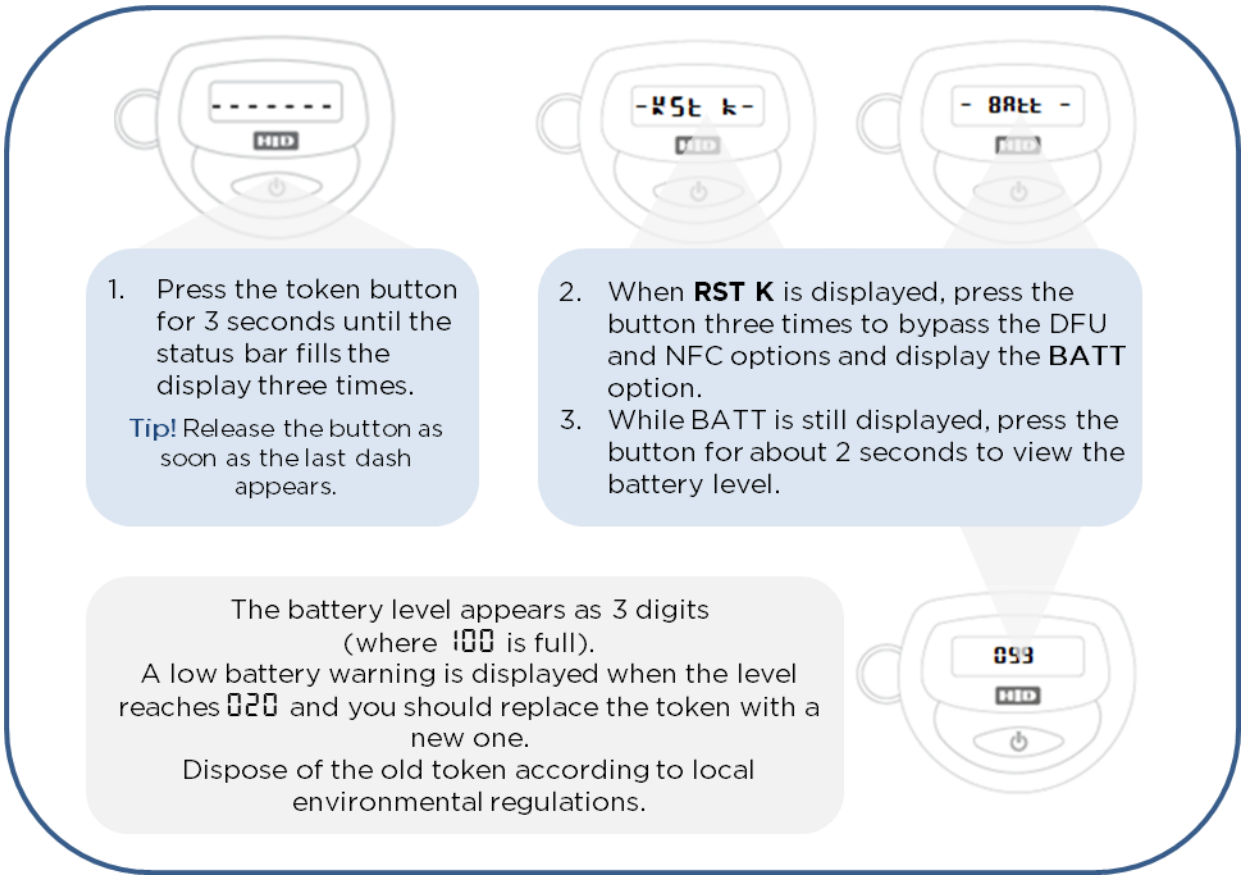


6.5 View the Battery Level

The battery function displays the current power level of the token's internal battery.

Note: The ActivID BlueTrust Token is a disposable device, to be replaced by a new one when the battery runs out. Low battery power is indicated by a fading display.

The token is delivered with a Lithium battery (CR2450) with an expected lifetime of 5-years based on 10 short Bluetooth transactions per day.



6.6 About the DFU and NFC Options

The following options are displayed by the system menu but are advanced features reserved for administrators:

- DFU (Device Firmware Upgrade) – to upgrade the token's firmware.
- NFC (Near Field Communication) – to configure the NFC parameters for connection to a reader.

For further information, contact your system administrator.

7.0 Troubleshooting the ActivID BlueTrust Token

This section explains how to troubleshoot any issues that might occur as you use the ActivID BlueTrust Token.

Issue	Solution
You are unable to pair the device on a computer when the token is already connected to another computer within Bluetooth range.	Turn off the Bluetooth service on the other computer and restart the pairing process. Alternatively, if this is not possible, remove the pairing between the ActivID BlueTrust Token and all the computers that are currently paired with the device using the Rst K menu.
You turned off the device during the pairing process (while Connect was displayed). As a result, the ActivID BlueTrust Token is registered on the computer with a driver error.	Remove the BlueTrust Token from the Bluetooth list and restart the pairing process.