TWO-FACTOR AUTHENTICATION

In this manual we will explain how to configure our additional authentication mechanisms to be able to access protected PCB telematic resources requiring two-factor authentication.

1 TERMS AND DEFINITIONS

- **Two-factor authentication**: These are methods for electronically authenticating users using various factors. It is common for factors of different natures to be combined, such as something that the user knows (a password) and something that the user owns (a physical object).
- **Weak token** or **second weak factor**: This is an eight-digit figure that we will receive from the Barcelona Science Park's Information and Telecommunications Systems Department by letter. This second factor is not considered as being strong as it is static, it will be used to register our second strong authentication factor or to access services from the Animal Facility where we cannot enter with a device which we use as a second strong factor. The system will never ask us for the complete weak token figure, but rather we will be asked to provide three random digits.
- **Strong token** or **second strong factor**: This will be a dynamic authentication mechanism which will be considered more secure. We will have to configure this second factor ourselves through the self-service portal.
- **TOTP** (Time-based one-time password): This is the second strong factor method that we will use. Once the application has been configured, this will generate customised numbers for our user with a limited validity. The application will generate a new number every 30 seconds. The mobile applications Google Authenticator and Microsoft Authenticator are the most commonly used.

2 TWO-FACTOR VALIDATION

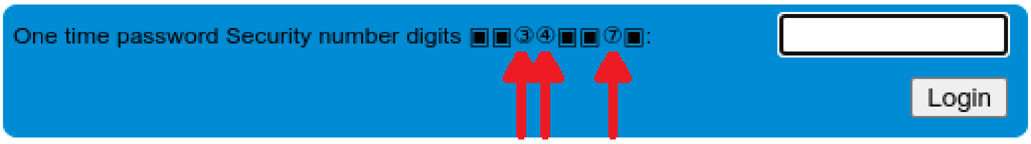
In order for you to be validated in services protected by a two-factor validation you need to have your username and password for the PCB services and have received the weak token (an eight-digit pin number) to start the first session. If this is not the case, contact the Barcelona Science Park's Information and Telecommunications Systems Department (sic@pcb.ub.es).

To work with the new two-factor authentication method, the first thing you will have to do is set up our second strong factor. As you haven't yet set it up, you will be able to validate it using your weak token.

2.1 Starting the session with the weak token

You should enter the https://identitat.pcb.ub self-service portal by validating yourself with your username, PCB services password and the weak token.

To log in using this weak token you must first enter the username and password. The system will then ask you for three of the eight digits of the weak token as indicated when you start the session.



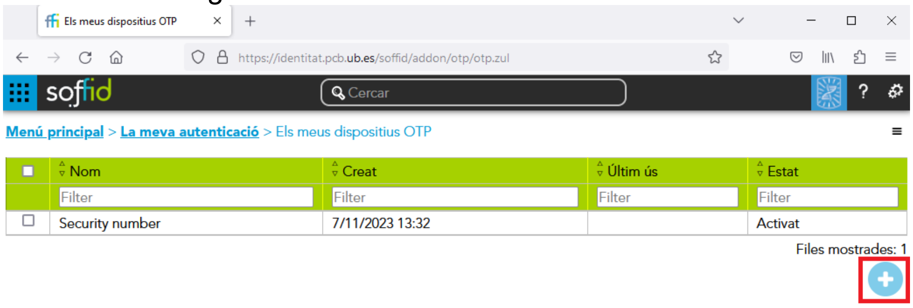
One time password Security number digits ▣▣③④▣▣⑦▣:

In this case, you should enter the digits in positions 3, 4 and 7.

You can see the process of entering the self-service portal in the video: https://youtu.be/CzbbbVH4fGg

2.2 Generating the strong token

Once you have accessed the self-service portal you can set up your second strong authentication factor. To do this you just have to register a new OTP for a "Time-based HMAC OTP" type of device. You have to go to the "*Els meus dispositius OTP*" (My OTP devices) option where you can see a list of all the factors that you have linked to your username. Initially you will only have the weak token. You have to click on the "plus" icon located at the bottom right of the list.

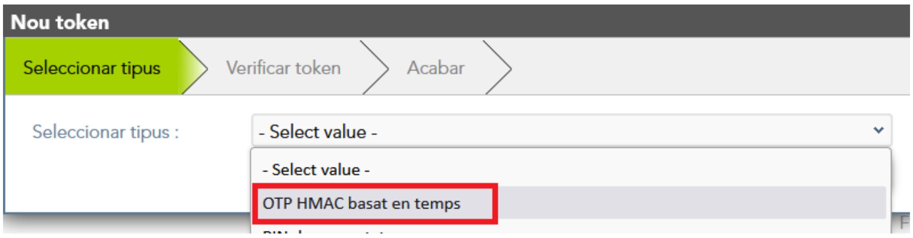


Menú principal > La meva autenticació > Els meus dispositius OTP

□	Nom	Creat	Últim ús	Estat
	Filter	Filter	Filter	Filter
□	Security number	7/11/2023 13:32		Activat

Files mostrades: 1

And tell it that you want to generate a new "*OTP HMAC basat en temps*" (Time-based HMAC OTP) token.



Nou token

Seleccionar tipus : - Select value -

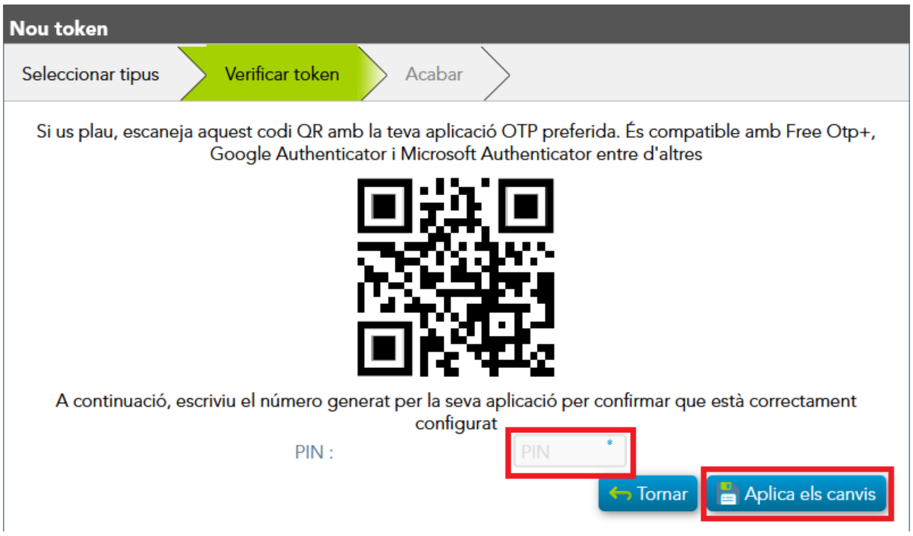
- Select value -
OTP HMAC basat en temps

The system will display a QR code you can use to configure the TOTP application you wish to use. You can choose any application compatible with the standard TOTP, we recommend that you use any of the usual mobile applications such as Google Authenticator or Microsoft Authenticator that are available for both Android and iOS.

You have to open the application and tell it that you want to add an account by scanning a QR code, the application will access the mobile phone's camera and you have to focus the image on the QR code generated by the self-service portal.

Once the application recognises the QR code, it will add it to its list of accounts and will generate a different numerical code every 30 seconds.

To finish the configuration, you have to enter the number generated by the application in the box under the QR code and press the "*Aplica els canvis*" (Apply the changes) button, making the authentication system for validating the configuration will be the strong token.



Nou token

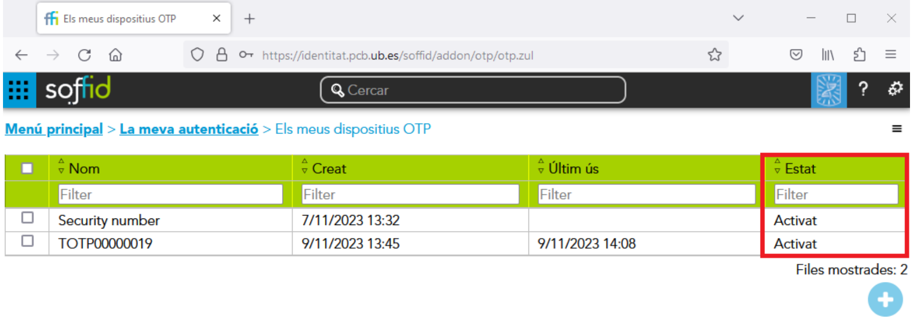
Seleccionar tipus > Verificar token > Acabar

Si us plau, escaneja aquest codi QR amb la teva aplicació OTP preferida. És compatible amb Free Otp+, Google Authenticator i Microsoft Authenticator entre d'altres

A continuació, escriviu el número generat per la seva aplicació per confirmar que està correctament configurat

PIN : PIN *

Once validated you will have completed the process to set up your strong token. In the list of your OTP devices you will have two entries, the one you already had for the weak token and the one you have added. If everything has worked properly, both of them must be in the "*Activat*" (Enabled) state.



Menú principal > La meva autenticació > Els meus dispositius OTP

☐	Nom	Creat	Últim ús	Estat
	Filter	Filter	Filter	Filter
☐	Security number	7/11/2023 13:32		Activat
☐	TOTP00000019	9/11/2023 13:45	9/11/2023 14:08	Activat

Files mostrades: 2

You can see the process of setting the strong token in the video: https://youtu.be/I6K65sR9N2Q

This process of setting the strong token only has to be done the first time. Once it has been set up you will have to use the numbers that it generates at all times to be able to access protected PCB services with two-factor authentication.

2.3 Starting a normal session (self-service portal and the VPN portal)

Once you have configured the second factor, whenever you want to log into the portal, the VPN or any other services protected by two-factor authentication you will have to enter the username, password and the OTP generated at that time by the authentication application (Google Authenticator, Microsoft Authenticator or the one you have set up).

You can see an example of the validation process of the VPN using the second strong factor in the video: https://youtu.be/A1ZW1x62RJ4.