

AUTENTICACIÓ DE DOBLE FACTOR

En aquest manual explicarem com configurar els nostres mecanismes d'autenticació addicionals per poder accedir als recursos telemàtics del PCB protegits amb autenticació de doble factor.

1 TERMES I DEFINICIONS

- **Autenticació de doble factor:** Son mètodes per autenticar electrònicament als usuaris utilitzant diversos factors. Habitualment es combinen factors de diferents naturaleses, com pot ser alguna cosa que l'usuari coneix (una contrasenya) i alguna cosa que l'usuari té (un objecte físic).
- **Token dèbil o segon factor dèbil:** Es un numero de 8 xifres que rebrem des de Sistemes d'Informació i Telecomunicacions per carta. Aquest segon factor no es considera fort ja que es estàtic, ens servirà per poder registrar el nostre segon factor d'autenticació fort o per accedir als serveis des del estabulari on no podem entrar amb un dispositiu que ens faci de segon factor fort. El sistema mai ens demanarà tot el token dèbil sinó que cada cop ens en demanarà 3 dígits aleatoris.
- **Token fort o segon factor fort:** Serà un mecanisme d'autenticació dinàmic que es considerarà mes segur. Aquest segon factor l'haurèm de configurar nosaltres mateixos des del portal d'autoservei.
- **TOPT (Time-based one-time password):** Es el mètode de segon factor fort que utilitzarem. Un cop configurada l'aplicació, aquesta ens generarà números personalitzats per el nostre usuari amb una vigència limitada. Cada 30 segons l'aplicació ens generarà un nou numero. Les aplicacions mòbils Google Authenticator i Microsoft Authenticator son les mes utilitzades.

2 VALIDACIÓ DE DOBLE FACTOR

Per poder-te validar en els serveis protegits per una validació de doble factor necessites tenir el teu usuari i contrasenya per els serveis PCB i haver rebut el token dèbil (un pin de 8 dígits) per fer el primer inici de sessió. Si no es així, posa't en contacte amb el departament de sistemes d'informació i telecomunicacions del Parc Científic de Barcelona (sic@pcb.ub.es).

Per treballar amb el nou mètode d'autenticació en dos factors el primer que haurèm de fer es configurar el que serà el nostre segon factor fort. Com que encara no el tens configurat et podràs validar utilitzant el teu token dèbil

2.1 Inici de sessió amb el token dèbil

Hauràs d'entrar al portal d'autoservei <https://identitat.pcb.ub.es> validant-te amb el teu usuari, contrasenya per els serveis PCB i el token dèbil.

Per iniciar sessió usant aquest token dèbil hauràs d'introduir primer l'usuari i la contrasenya i després el sistema et demanarà tres dels vuit dígits del token dèbil segons s'indiqui durant l'inici de sessió.



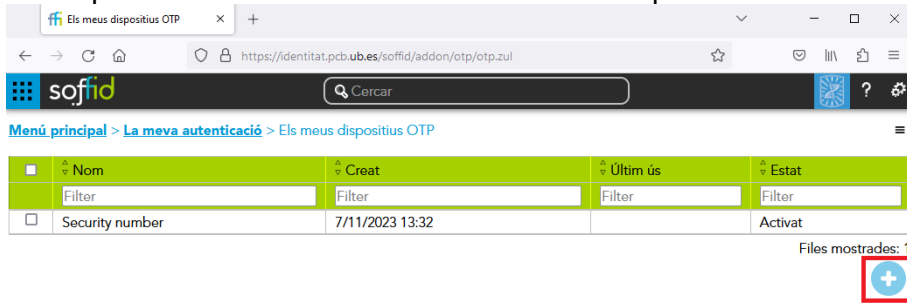
The image shows a blue login form. At the top, it says "One time password Security number digits" followed by eight small squares representing digits. The third, fourth, and seventh squares are highlighted with red arrows. To the right of these squares is a text input field. Below the input field is a "Login" button.

En aquest cas, hauries d'introduir els dígits en posicions 3, 4 i 7.

Pots veure el procés d'entrar al portal d'autoservei en el vídeo https://youtu.be/Oh7g_fpsQp8

2.2 Generació del token fort

Un cop dins del portal d'autoservei podràs configurar el teu segon factor d'autenticació fort. Per fer-ho simplement has de registrar un nou dispositiu OTP de tipus "Time-based HMAC OTP". Has d'anar a la opció "Els meus dispositius OTP" on pots veure una llista de tots els segons factors que tens vinculats amb el teu usuari. Inicialment només tindràs el token dèbil. Has de prémer en la icona de la suma situada a la part inferior dreta de la llista



I dir-li que vols generar un nou token de tipus "OTP HMAC basat en temps"



El sistema mostrarà un codi QR que et servirà per configurar l'aplicació TOTP que vulguis utilitzar. Pots escollir qualsevol aplicació compatible amb el estàndard TOTP, et recomanem que utilitzis alguna de les aplicacions de mòbil habituals Google Authenticator o Microsoft Authenticator que estan disponibles per Android i iOS.

[En aquest enllaç trobaràs un exemple de configuració amb l'aplicació Google Authenticator de Android.](#)

Has d'obrir l'aplicació i dir-li que volem afegir un compte escanejant un codi QR, l'aplicació accedirà a la càmera del mòbil i has de centrar la imatge en el codi QR que t'ha generat el portal d'autoservei.


Un cop l'aplicació reconegui el QR l'afegirà en la seva llista de comptes i t'anirà generant un codi numèric diferent cada 30 segons.

Per finalitzar la configuració has d'introduir el número que et genera l'aplicació en la casella sota el codi QR i prémer el boto "Aplica els canvis", d'aquesta forma el sistema d'autenticació podrà validar la configuració del token fort.

Nou token

Seleccionar tipus → Verificar token → Acabar

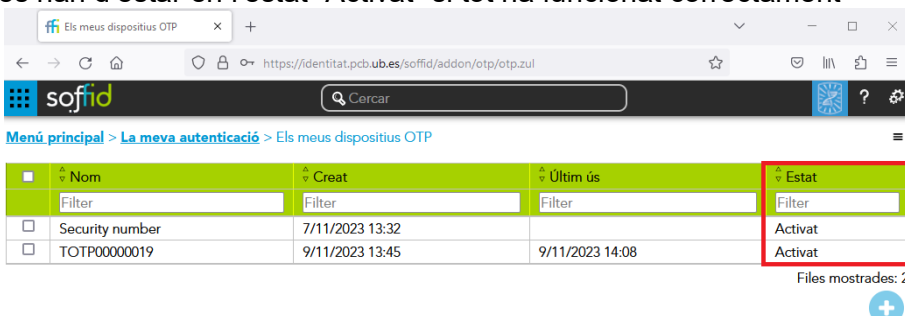
Si us plau, escaneja aquest codi QR amb la teva aplicació OTP preferida. És compatible amb Free Otp+, Google Authenticator i Microsoft Authenticator entre d'altres



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

PIN :

Un cop validat has completat el procés per configurar el teu token fort. En la llista dels teus dispositius OTP tindràs dues entrades, la que ja tenies per el token dèbil i la que has afegit. Les dues han d'estar en l'estat "Activat" si tot ha funcionat correctament



<input type="checkbox"/>	Nom	Creat	Últim ús	Estat
<input type="checkbox"/>	Security number	7/11/2023 13:32		Activat
<input type="checkbox"/>	TOTP00000019	9/11/2023 13:45	9/11/2023 14:08	Activat

Files mostrades: 2

Pots veure el procés de configurar el token fort en el vídeo <https://youtu.be/LiiWkiUyXgw>

Aquest procés de configuració del token fort només cal fer-lo la primera vegada. Un cop configurat hauràs d'utilitzar els números que ens generi en cada moment per accedir als serveis PCB protegits amb autenticació de doble factor.

2.3 Inici de Sessió habitual (portal d'autoservei i VPN)

Una vegada tens configurat el segon factor, sempre que vulguis iniciar sessió al portal d'autoservei, la VPN o altres serveis protegits per l'autenticació de doble factor hauràs d'introduir usuari, contrasenya i l'OTP que et generi en aquell moment l'aplicació d'autenticació (Google Authenticator, Microsoft Authenticator o la que hagueu configurat).

Pots veure un exemple del procés de validació a la VPN utilitzant el segon factor fort en el vídeo <https://youtu.be/eiVIRVKYSO4>