Use USB-Security key (Yubikey/ FIDO 2/Token) for login to KU Systems

You can use USB-Security key (Yubikey/ FIDO 2/Token) for **M**ulti **F**actor **A**uthentication (MFA), on the systems, where KU-IT has applied MFA.

USB-A

Over time there will be more systems with MFA requirement, this being because based on the goal of KU being the worlds most secure university in the world.

At KU, you will have the option of using two kinds of USB security keys, as shown in the pictures on the right side of this page:

1. Yubikey for employees (Personalized).
2. FIDO2 for students.

USB-C

Theese two USB-Security keys are basicly alike, the only difference being that the Yubikey is configured specifically for employees, this being because the requirement of an extra security layer, because of employees typically have access to sensitive data.

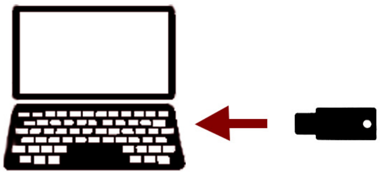
Employees: Must order the yubikey through IT Self Service Portalen and must in the payment process define alias and place-code. If in doubt about any details don't hesitate to contact your nearest manager to have these details in place beforehand.

Students: Must buy their yubikey or other security key through retails stores like: dustinhome.dk, proshop.dk or computersalg.dk. The price varies, but is usally around 350 kr.

For Employees with Yubikey:

For this example VPN is used, but in principle it works the same way for other systems

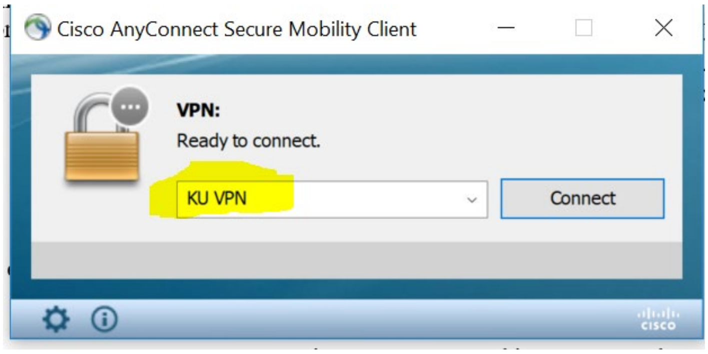
1.
Open the system you want to log in to (VPN is used for this example) and Put your YubiKey/Token/Key in one of USB slots on the computer



3.
Log in to the system

If it’s VPN then:

- Open Cisco AnyConnect VPN client.
- Make sure you are connecting to KU VPN (otherwise type vpn.ku.dk) as shown in the picture.
- Click on ”Connect”.
- Type your KU username and password.
- **NB:** UCPH password cannot contain the special character '**&**' because login will fail.

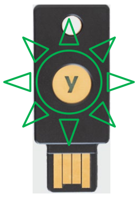


Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

KU VPN

4.
Swipe your finger over the lighting point of the key.

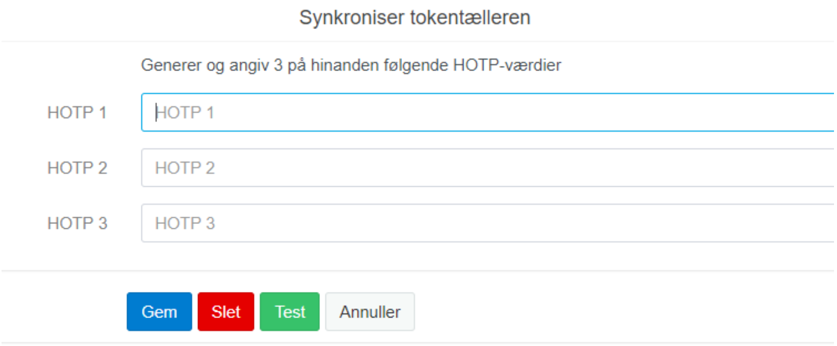


5.
A password is now registered in the system and you are at this point Multi Factor Authenticated.

6.
Go to the site mfa.ku.dk to check the **Token** (Key) is registered under Tilmeldte godkendere. Isn’t it registered go to clause 9.
Is the token registered, but there is still **no** connection it may be because the **Token** is no longer synchronized.
It is therefore necessary to synchronise the **Token** (Key).

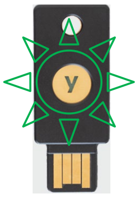
7.
Click the key icon (Token) to start the synchronization. Scroll to the heading **Synchronize Tokentæller/ Synchronize the token counter**)

1. Put the Token (Key) in one of the USB slots.
2. Choose **Token** (Key)
3. Place the cursor in **HOTP1**
4. Move the finger over the bright point on the Token. This is done three times, once per HOTP
5. Finish by clicking **Save**


Synkroniser tokentælleren

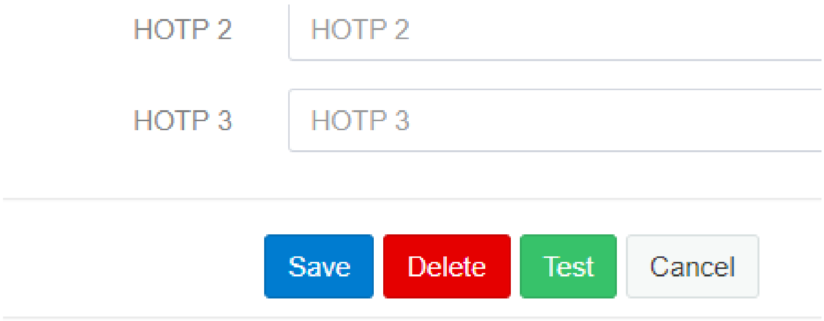
Generer og angiv 3 på hinanden følgende HOTP-værdier

HOTP 1 HOTP 1
HOTP 2 HOTP 2
HOTP 3 HOTP 3



***NB!** It does not matter which finger you use, as it is not a fingerprint.*

8.
Click **Test** to see if it works.


HOTP 2 HOTP 2
HOTP 3 HOTP 3

9.
If it is still not possible to register your Token. Contact Service desk or report the error at [IT Self-service]