



Sikkerheds-USB-nøgle til MFA-login for studerende

Denne vejledning beskriver, hvordan du registrerer en sikkerheds-USB-nøgle, der bruger FIDO2 som autorisationspunkt. Du kan bruge sikkerheds-USB-nøglen som to-faktor-godkendelse, også kaldet **Multi Factor Authentication (MFA)**, når du vil logge på din KUMail.

Forudsætninger:

- Du skal have en sikkerheds-USB-nøgle. Denne kan købes i flere af de større online elektronikbutikker.
- Sikkerheds-USB-nøglen skal have teknologien FIDO2, ellers kan den ikke registreres.
- Du skal have et KU-brugernavn og password for at registrere din nøgle.
- Du skal allerede være registreret på to-faktor-løsningen (MFA-løsningen) for at kunne sætte sikkerheds-USB-nøglen op til brug.

Hvis du ikke allerede er registreret på to-faktor-løsningen (MFA), så kan du finde vejledning til dette på <https://it.ku.dk/hjaelp-til-login>.

Guide til at registrere sikkerheds-USB-nøglen:

Som studerende er du sikkert allerede registreret på to-faktor-løsningen i kraft af dit mobilnummer, og modtager sms med engangspassord, når du prøver at logge på en af de løsninger, hvor KU har implementeret to-faktor-løsningen – eksempelvis når du logger ind på KUMail.

Når du er registreret på to-faktor-løsningen kan du fortsætte med opsætningen af din sikkerheds-USB-nøgle:

1.

Tilgå på din computer hjemmesiden mfa.ku.dk. Indtast dit KU brugernavn og adgangskode for at logge ind.

KU Login

abc123

.....

LOG IND

[Glemt brugernavn](#)

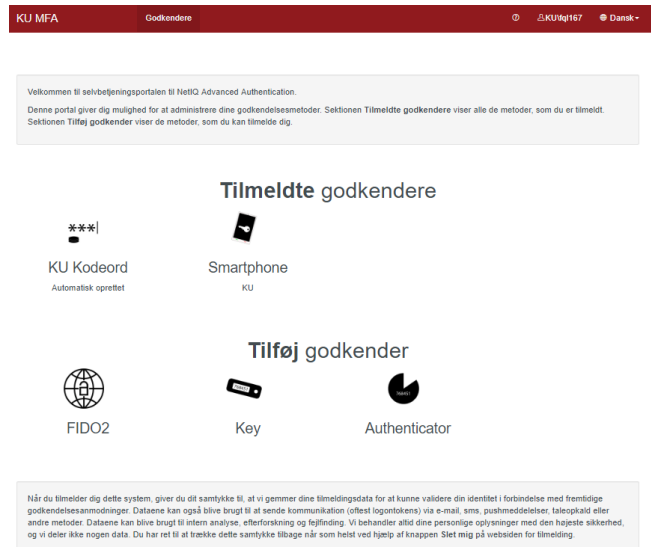
[Glemt kodeord](#)

[Glemt kodeord med NemID](#)



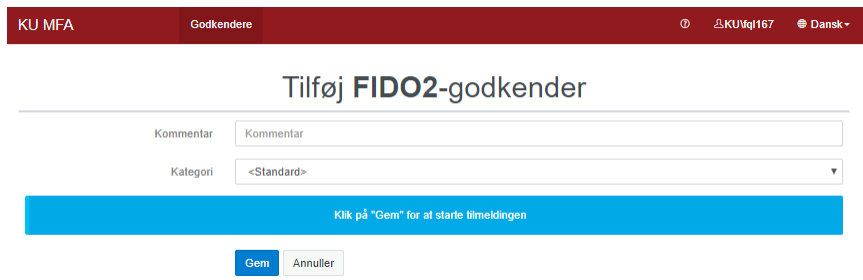
2.

Der vil nu blive vist et skærbillede som vist til højre. Tryk nu på **FIDO2** under **tilføj godkendere**.



3.

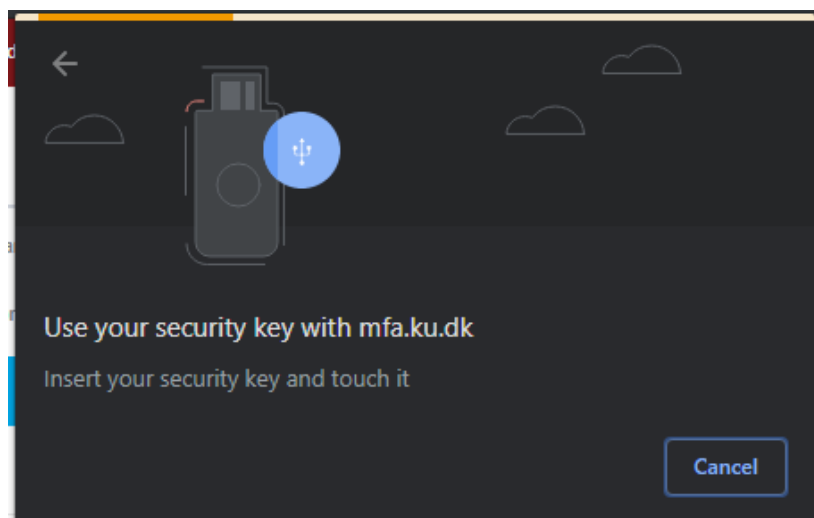
Udfyld **kommentar-feltet** med **KU** som en information til dig selv. Tryk på **Gem**.



4.

Et popup vindue som billedet til højre vil blive vist. Indsæt nu din nøgle i din computer.

NB! Trinene 4,5 og 6 kan variere ift. hvilken browser du bruger. Følg den vejledning, som står på din skærm.

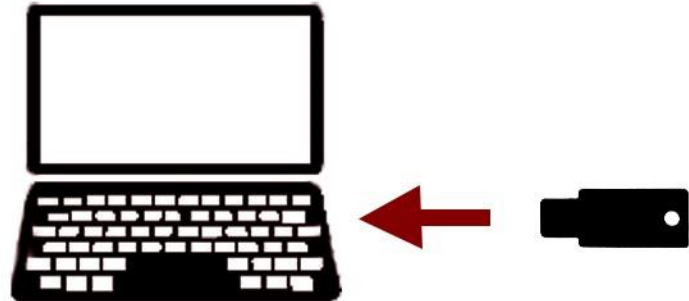


Contact KU-IT, if you have any questions



5.

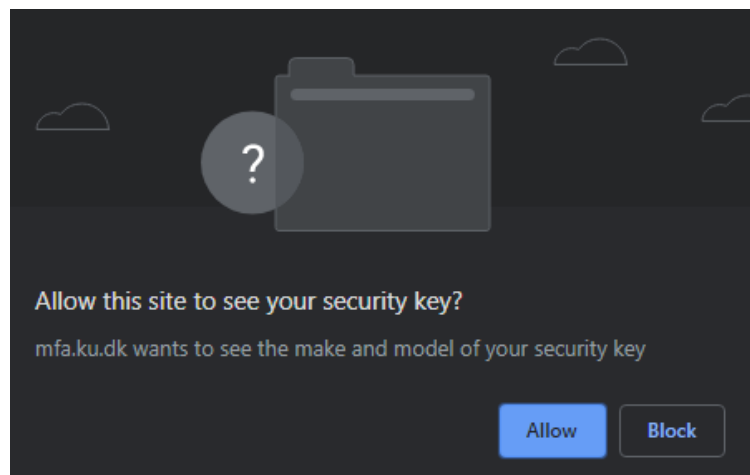
Når du indsætter din nøgle i din computer, vil nøglen lyse. Tryk på knappen på din nøgle, når du bliver bedt om det.



6.

Efter du har trykket på din nøgle vil popupvinduet ændre sig. Tryk her på **Allow** for at tillade at hjemmesiden må bruge din nøgle. Du kan også blive bedt om at oprette en pin kode. Hvis det er tilfældet opret en pinkode som du kan huske.

NB! Hvis du er for langsom kan denne session udløbe. Hvis det sker skal du opdatere hjemmesiden og prøve igen fra trin 2.





7.

På hjemmesiden skifter **FIDO2** nu placering fra at være under **Tilføj godkender** til at være placeret under **Tilmeldte godkendere**.

The screenshot shows the 'KU MFA' portal. At the top, there is a navigation bar with 'Godkendere', a user profile icon, 'KU fql167', and a language dropdown set to 'Dansk'. Below the navigation bar is a welcome message: 'Velkommen til selvbetjeningsportalen til NetIQ Advanced Authentication. Denne portal giver dig mulighed for at administrere dine godkendelsesmetoder. Sektionen Tilmeldte godkendere viser alle de metoder, som du er tilmeldt. Sektionen Tilføj godkender viser de metoder, som du kan tilmelde dig.' The main content area is divided into two sections: 'Tilmeldte godkendere' and 'Tilføj godkender'. The 'Tilmeldte godkendere' section contains three items: 'FIDO2' (with a globe icon and 'KU' below), 'KU Kodeord' (with a password field icon and 'Automatisk oprettet' below), and 'Smartphone' (with a smartphone icon and 'KU' below). The 'Tilføj godkender' section contains two items: 'Key' (with a USB key icon) and 'Authenticator' (with a circular icon). At the bottom of the screenshot is a disclaimer: 'Når du tilmelder dig dette system, giver du dit samtykke til, at vi gemmer dine tilmeldingsdata for at kunne validere din identitet i forbindelse med fremtidige godkendelsesansøgninger. Dataene kan også blive brugt til at sende kommunikation (ofte logontokens) via e-mail, sms, pushmeddelelser, taleopkald eller andre metoder. Dataene kan blive brugt til intern analyse, efterforskning og fejlfinding. Vi behandler altid dine personlige oplysninger med den højeste sikkerhed, og vi deler ikke nogen data. Du har ret til at trække dette samtykke tilbage når som helst ved hjælp af knappen 'Slet mig på websiden for tilmelding.'

8.

Du har nu adgang til din KUmail via MFA.

>> [Klik her for at læse vejledningen om hvordan du logger ind på KUmail med din sikkerheds-USB-nøgle.](#)

9.

Du kan teste på din computer om MFA virker. På siden **Tilmeldte godkendere** klikker du på **FIDO2**.

This screenshot shows the 'Tilmeldte godkendere' section of the MFA portal. It features three items: 'FIDO2' with a globe icon and 'KU' below it; 'KU Kodeord' with a password field icon and 'Automatisk oprettet' below it; and 'Smartphone' with a smartphone icon and 'KU' below it.

Contact KU-IT, if you have any questions



10.

På websiden
**Rediger
godkenderen
FIDO2** klikker
du på **Test**.

Rediger godkenderen **FIDO2**

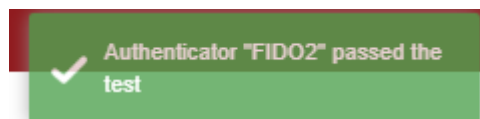
Kommentar	<input type="text" value="KU"/>	
Kategori	<input type="text" value="<Standard>"/>	
Klik på "Gem" for at starte tilmeldingen		
<input type="button" value="Gem"/> <input type="button" value="Slet"/> <input type="button" value="Test"/> <input type="button" value="Annuller"/>		

11.

Du skal nu gøre ligesom i trin 4 og 5.

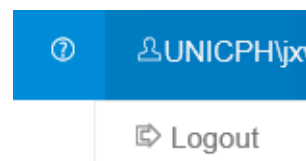
12.

Du får besked om, at din nøgle er godkendt i computerens højre hjørne.



13.

Logout gøres ved at trykke på dit brugernavn i øverste højre hjørne og så trykke på logout.



NB! Hvis du er logget på KU's netværk f.eks. eduroam på KU eller på det kablede netværk, skal du ikke lave en to-trins godkendelse for at komme på KUMail. Det samme gælder, hvis du har sat KUMail op via en app på din telefon, igennem det indbyggede mailprogram på MAC eller igennem outlook på din computer. FIDO2 virker ikke til VPN.

Contact KU-IT, if you have any questions