

TILMELD DIG SOM BRUGER AF SIF


Som KU-ansat/studerende (se side 1-4) eller ekstern samarbejdspartner (se side 5-9) skal du tilmelde dig som bruger af SIF med en såkaldt 2-faktor-godkendelse, før du kan få adgang til et projekt med sensitive data.

TILMELDING MED EN KU-KONTO

TILMELDING

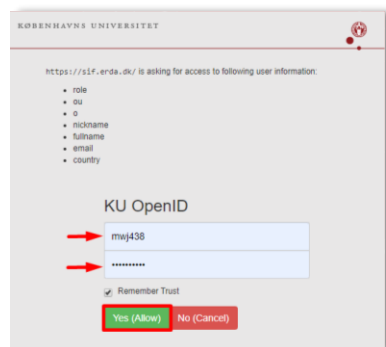
Gå på <https://sif.ku.dk/>

Klik på 'tilmelding'



I pop-op-vinduet under 'KU OpenID' skriver du:

1. Dit KU-brugernavn (Består af tre bogstaver og tre tal).
2. Dit personlige KU-kodeord, som du også bruger til fx KUNet.
3. Klik derefter på 'Yes (Allow)'




Nu er du oprettet som bruger på SIF.

2-FAKTOR GOD- KENDELSE

For at øge sikkerheden er det *obligatorisk* at benytte 2-faktor-godkendelse til al SIF-adgang.

Med 2-faktor-godkendelse tilføjer du et ekstra kontroltrin til den login-proces, som autentificerer dig. Udover at anmode om noget man kender (i dette tilfælde dit brugernavn og kodeord), så vil en 2-faktor-beskyttet konto også anmode om information fra noget, man har (tal-nøgle fra app på mobil/tablet).

Ved tilmelding til SIF skal du *én* gang igennem en guide, hvor du opsætter den obligatoriske 2-faktor-godkendelse.

	<p>Klik på 'Okay, let's go!'</p> <div data-bbox="432 268 1386 593"> <p>Two-Factor Auth</p> <p>2-Factor Authentication</p> <p>We demand 2-factor authentication on UCPH SIF for greater password login security. In short it means that you enter a generated single-use <i>token</i> from e.g. your phone or tablet along with your usual login. This combination makes account abuse much harder, because even if your password gets stolen, it can't be used without your device.</p> <p>Preparing and enabling 2-factor authentication for your login is done in four steps.</p> <p>Okay, let's go!</p> </div> <p>Nu kommer der en guide frem i SIF, du skal følge nøje.</p>
<p>TRIN 1. DOWNLOAD APP</p>	<p>På din mobil eller tablet* skal du downloade en af følgende apps: <i>Google Authenticator</i>, <i>FreeOTP</i>, <i>NetIQ Advanced</i>, <i>Authentication</i> eller <i>Authy</i>. Find appen dér, hvor du normalt downloader apps.</p> <p>Klik derefter på "I've got it installed!"</p> <div data-bbox="432 884 1386 1095"> <p>1. Install an Authenticator App</p> <p>You first need to install a TOTP authenticator client like Google Authenticator, FreeOTP, NetIQ Advanced Authentication or Authy on your phone or tablet. You can find and install either of them on your device through your usual app store.</p> <p>I've got it installed!</p> </div> <p>*Hvis du kun har en privat mobil/tablet og ikke ønsker at bruge den, har du mulighed for at få udleveret et lille apparat, som du kan bruge i stedet for. Kontakt support@sif.erd.dk for yderligere information.</p>
<p>TRIN 2. IMPORTÉR PERSONLIG 2-FAKTOR- KODE</p>	<p>Importér din personlige 2-faktor-kode med 'Scan your personal QR code' eller 'Enter your personal key'. Nedenfor følger eksempel med 'Scan your personal QR code'.</p> <p>Klik i SIF på 'QR code'</p> <div data-bbox="432 1417 1386 1709"> <p>2. Import Secret in Authenticator App</p> <p>Open the chosen authenticator app and import your personal 2-factor secret in one of two ways:</p> <ul style="list-style-type: none"> • Scan your personal QR code • Type your personal key code <p>The latter is usually more cumbersome but may be needed if your app or smart device doesn't support scanning QR codes. Most apps automatically add service and account info on QR code scanning, but otherwise you can manually enter it.</p> </div> <p>En QR-kode popper op i SIF</p>  <p>Åbn din downloadede app. Appsene er lidt forskellige. I nedenstående er det skærmbillede fra appen</p>

Google Authenticator, der vises. Klik på 'Scan stregkoden'



Scan nu QR-koden som du netop åbnede i guiden på SIF. Dvs. ret mobilens kamera op på QR-koden (Appen skal muligvis have tilladelse til at bruge dit kamera). Nu scanner appen QR-koden. Klik derefter på 'Done importing'



Din app kan nu generere 6-cifrede engangsnøgler (såkaldte tokens). I nedenstående eksempel er engangsnøglen '990 204'.



TRIN 3. VERIFICÉR, AT DET VIRKER

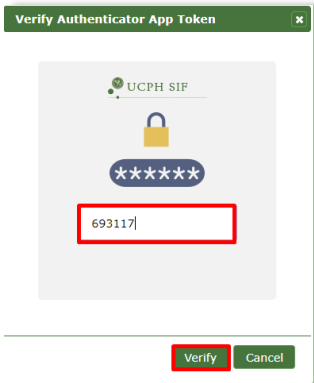
Du skal nu teste, at din 2-faktor-godkendelse er sat korrekt op, og at appen leverer de rigtige engangsnøgler.

3. Verify the Authenticator App Setup

Please **verify** that your authenticator app displays correct new tokens every 30 seconds before you actually enable 2-factor authentication. Otherwise you could end up locking yourself out once you enable 2-factor authentication!

It works!

Der kommer automatisk et pop-op-vindue frem, hvor du skal du skrive den engangsnøgle, appen viser (hvis det ikke kommer frem, skal du klikke på 'verify' i ovenstående). Vær opmærksom på, at engangs tal-nøglen skifter efter 30 sekunder.

	<p>Skriv den 6-cifrede engangsnøgle og klik på knappen 'Verify' i pop-op-vinduet</p>  <p>Hvis din 2-faktor-godkendelse lykkes, føres du direkte til næste trin.</p>
TRIN 4. AKTIVÉR 2-FAKTOR GODKEN-DELSEN	<p>Klik på 'Start Using UCPH SIF'</p> <div> <p>4. Enable 2-Factor Authentication</p> <p>Now that you've followed the required steps to prepare and verify your authenticator app, you just need to enable it below. This ensures that your future UCPH SIF logins are security-enhanced with a request for your current token from your authenticator app.</p> <p>SECURITY NOTE: please immediately contact the UCPH SIF admins to reset your secret 2-factor authentication key if you ever loose a device with it installed or otherwise suspect someone may have gained access to it.</p> <p>Enable 2-factor authentication and</p> <p>Start Using UCPH SIF</p> </div>
DU ER NU TILMELDT	<p>Tillykke! Nu er du tilmeldt SIF med 2-faktor-godkendelse.</p> <p>Nu kan du fremover gå på https://sif.ku.dk/, logge på med dit KU-brugernavn og personlige KU-kodeord efterfulgt af 2-faktor-godkendelse.</p> <p>Når du er færdig med at arbejde i SIF, så klik altid på 'Log ud'. Så er du sikker på, at ingen andre uretmæssigt får adgang til dine sensitive data.</p>
HJÆLP	<p>Se flere vejledninger på https://sif.ku.dk/ eller få personlig hjælp på support@sif.erda.dk</p>

TILMELDING FOR EKSTERN SAMARBEJDSPARTNER

TILMELDING

Gå på <https://sif.ku.dk/>

Klik på fanebladet 'Eksterne brugere'. Klik dernæst på 'tilmelding':

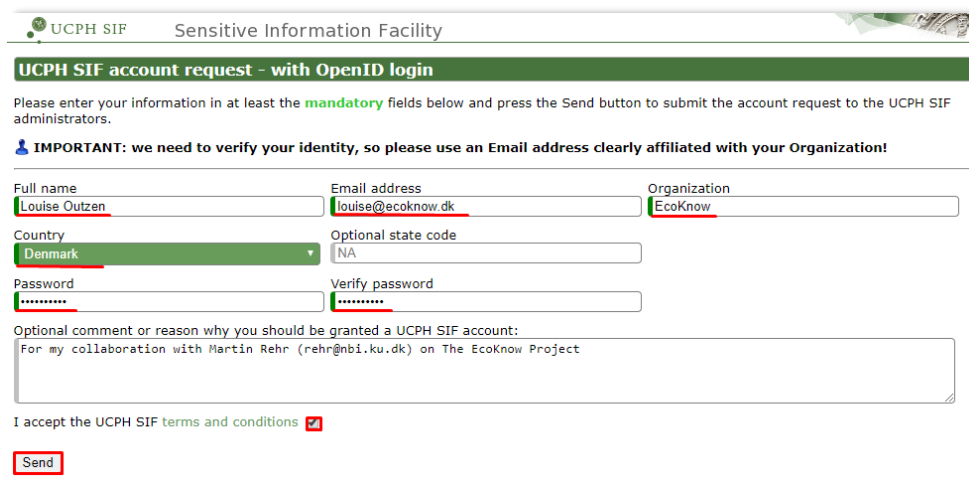


The screenshot shows the UCPH SIF website interface. At the top, there are two tabs: 'KU / UCPH brugere' and 'Eksterne brugere'. The 'Eksterne brugere' tab is selected and highlighted with a red box. Below the tabs, there is a green button labeled 'Tilmeld dig SIF uden en KU-konto?'. Under this button, there is a smaller green button labeled 'tilmelding', which is also highlighted with a red box.

Du skal nu udfylde formularen med dine oplysninger:

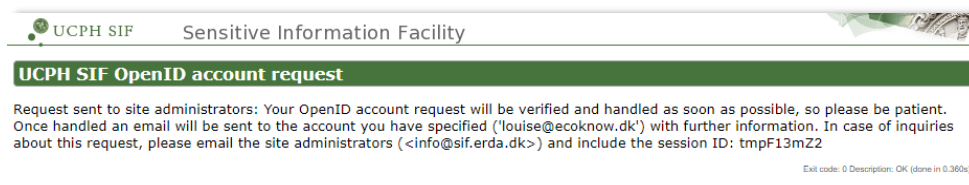
- Full name: *Skriv dit fulde navn*
- Email address: *Din arbejds e-mail (Ingen trejdeparts e-mail tjenester såsom hotmail, gmail eller yahoo)*
- Organization: *Navnet på din arbejdsplads/virksomhed*
- Country: *Vælg dit land i rullemenuen*
- Password: *Find på et tilpas svært kodeord til din SIF-adgang. Det skal bestå af minimum 10 tegn og indeholde både små og store bogstaver samt tal og specialtegn. I 'Verify password' gentager du kodeordet.*
- Optional comment ...: *Henvis til den ansatte på Københavns Universitet, du samarbejder med (navn + e-mail) og på hvilket projekt.*
- I accept ...: *Læs 'terms and conditions' og sæt flueben i feltet*

Klik på 'Send'



The screenshot shows the 'UCPH SIF account request - with OpenID login' form. The form includes fields for Full name (Louise Outzen), Email address (louise@ecoknow.dk), Organization (EcoKnow), Country (Denmark), Optional state code (NA), Password, and Verify password. There is also a text area for an optional comment or reason why you should be granted a UCPH SIF account. Below the form, there is a checkbox for 'I accept the UCPH SIF terms and conditions' which is checked. A 'Send' button is located at the bottom of the form.

Dit ønske om at tilmelde dig som bruger af SIF bliver nu sendt til SIF-administratorerne



The screenshot shows the 'UCPH SIF OpenID account request' confirmation page. It states that the request has been sent to site administrators and will be verified and handled as soon as possible. It also mentions that an email will be sent to the account specified (louise@ecoknow.dk) with further information. In case of inquiries about this request, it asks to email the site administrators (<info@sif.erda.dk>) and include the session ID: tmpF13mZ2. At the bottom, there is a small text: 'Exit code: 0 Description: OK (done in 0.360s)'.

Når SIF-administratorerne har accepteret din anmodning, får du tilsendt en e-mail.

LOG IND	<p>Klik på linket til SIF i den tilsendte e-mail og login på SIF.</p> <p>Skriv din e-mail og dit SIF kodeord. Klik på 'yes'.</p> <div data-bbox="438 338 1337 528"> <p>Username (email): <input type="text" value="louise@ecoknow.dk"/></p> <p>Password: <input type="password" value="....."/></p> <p>Remember Trust: <input checked="" type="checkbox"/></p> <p>Proceed: <input checked="" type="button" value="yes"/> <input type="button" value="no"/></p> </div>
2-FAKTOR GOD-KENDELSE	<p>For at øge sikkerheden er det <i>obligatorisk</i> at benytte 2-faktor-godkendelse til al SIF-adgang.</p> <p>Med 2-faktor-godkendelse tilføjer du et ekstra kontroltrin til den login-proces, som autentificerer dig. Udover at anmode om noget man kender (i dette tilfælde dit brugernavn og kodeord), så vil en to-faktor-beskyttet konto også anmode om information fra noget, man har (tal-nøgle fra app på mobil/tablet).</p> <p>Ved tilmelding til SIF skal du <i>én</i> gang igennem en guide, hvor du opsætter den obligatoriske 2-faktor-godkendelse.</p> <p>Klik på 'Okay, let's go!'</p> <div data-bbox="429 976 1321 1312"> <p>Two-Factor Auth</p> <p>2-Factor Authentication</p> <p>We demand 2-factor authentication on UCPH SIF TEST for greater password login security. In short it means that you enter a generated single-use <i>token</i> from e.g. your phone or tablet along with your usual login. This combination makes account abuse much harder, because even if your password gets stolen, it can't be used without your device.</p> <p>Preparing and enabling 2-factor authentication for your login is done in four steps.</p> <p><input checked="" type="button" value="Okay, let's go!"/></p> </div> <p>Nu kommer der en guide frem i SIF, du skal følge nøje.</p>
TRIN 1. DOWNLOAD APP	<p>På din mobil eller tablet skal du downloade en af følgende apps: <i>Google Authenticator</i>, <i>FreeOTP</i>, <i>NetIQ Advanced</i>, <i>Authentication</i> eller <i>Authy</i>. Find appen dér, hvor du normalt downloader apps.</p> <p>Klik derefter på 'I've got it installed'</p> <div data-bbox="438 1585 1385 1787"> <p>1. Install an Authenticator App</p> <p>You first need to install a TOTP authenticator client like Google Authenticator, FreeOTP, NetIQ Advanced Authentication or Authy on your phone or tablet. You can find and install either of them on your device through your usual app store.</p> <p><input checked="" type="button" value="I've got it installed!"/></p> </div>
TRIN 2. IMPORTÉR PERSONLIG 2-FAKTOR KODE	<p>Importér din personlige 2-faktor-kode med 'Scan your personal QR code' eller 'Enter your personal key'. Nedenfor følger eksempel med 'Scan your personal QR code'.</p> <p>Klik i SIF på 'QR code'</p>

2. Import Secret in Authenticator App

Open the chosen authenticator app and import your personal 2-factor secret in one of two ways:

- Scan your personal **QR code**
- Type your personal **key code**

The latter is usually more cumbersome but may be needed if your app or smart device doesn't support scanning QR codes. Most apps automatically add service and account info on QR code scanning, but otherwise you can manually enter it.

En QR-kode popper op i SIF:



Åbn din downloadede app.

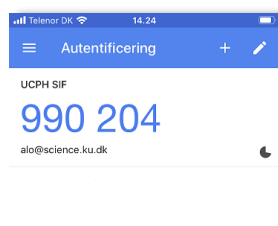
Appsene er lidt forskellige. I nedenstående er det skærmbillede fra app'en *Google Authenticator*, der vises. Klik på 'Scan strekkoden':



Scan nu QR-koden som du netop åbnede i guiden på SIF. Dvs. ret mobilens kamera op på QR-koden (Appen skal muligvis have tillade til at bruge dit kamera). Nu scanner appen QR-koden. Klik derefter på 'Done importing'



Din app kan nu generere 6-cifrede engangsnøgler (såkaldte tokens). I nedenstående eksempel er engangsnøglen '990 204'.



TRIN 3. VERIFICÉR, AT DET VIRKER

Du skal nu teste, at din 2-faktor-godkendelse er sat korrekt op, så appen leverer de rigtige engangsnøgler.

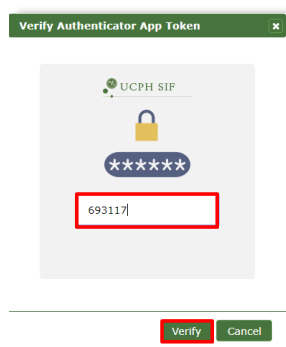
3. Verify the Authenticator App Setup

Please **verify** that your authenticator app displays correct new tokens every 30 seconds before you actually enable 2-factor authentication. Otherwise you could end up locking yourself out once you enable 2-factor authentication!

It works!

Der kommer automatisk et pop-op-vindue frem, hvor du skal du skrive den engangsnøgle, appen viser (hvis det ikke kommer frem, skal du klikke på 'verify' i ovenstående). Vær opmærksom på, at engangs tal-nøglen skifter efter 30 sekunder.

Skriv den 6-cifrede talnøgle og klik på knappen 'Verify' i pop-op-vinduet



Hvis din 2-faktor-godkendelse lykkes, føres du direkte til næste trin.

TRIN 4. AKTIVÉR 2- FAKTOR GODKEN- DELSEN

Klik på 'Start Using UCPH SIF'

4. Enable 2-Factor Authentication

Now that you've followed the required steps to prepare and verify your authenticator app, you just need to enable it below. This ensures that your future UCPH SIF logins are security-enhanced with a request for your current token from your authenticator app.

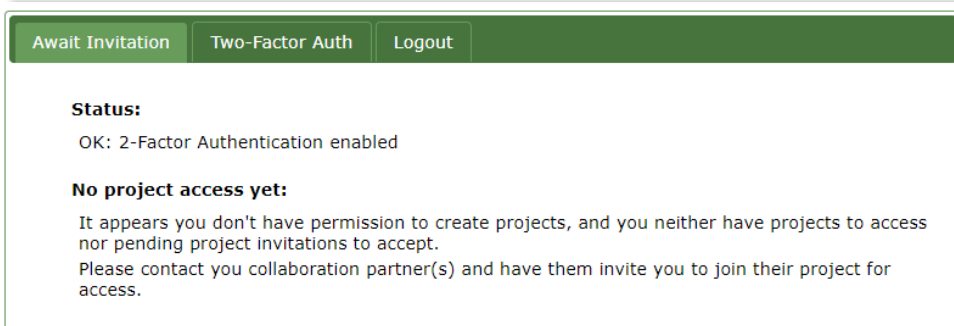
SECURITY NOTE: please immediately contact the UCPH SIF admins to reset your secret 2-factor authentication key if you ever loose a device with it installed or otherwise suspect someone may have gained access to it.

Enable 2-factor authentication and

Start Using UCPH SIF

DU ER NU TILMELDT

Tillykke! Du er nu tilmeldt SIF med 2-faktor-godkendelse.



	<p>Nu kan du vente på, at din samarbejdspartner på Københavns Universitet inviterer dig til at deltage i et projekt.</p> <p>Du vil modtage en e-mail, når det sker.</p>
HJÆLP	<p>Se mere på https://sif.ku.dk/ eller få personlig hjælp på support@sif.erda.dk</p>