OS2faktor Login

Windows Credential Provider

Version: 2.0.2
Date: 24.05.2023
Author: BSG

1 Formål

Der er udarbejdet en såkaldt Windows Credential Provider (WCP) til OS2faktor Login løsningen. Denne WCP understøtter følgende funktionalitet

- Mulighed for at etablere en NSIS login session helt fra windows login skærmen. Ved at anvende denne WCP vil brugerens initielle windows login blive brugt til at skabe single-signon sessionen, og brugeren slipper da for at anvende sit brugernavn/kodeord til at foretage det første web-baserede login
- Muligheden for at brugerne selv kan skifte kodeord via windows, uden at dette kræver at de skal gennem en re-aktiveringsproces i forhold til deres erhvervsidentitet.
- Muligheden for at brugerne kan genskabe et glemt kodeord direkte fra Windows Login siden

1.1 Forudsætning

WCP'en skal installeres på brugernes PC. Hvis der anvendes Citrix eller en anden form for fjernskrivebord, så skal WCP'en installeres på Citrix serverne.

Funktionaliteten til at etablere single-signon sessionen helt fra windows login skærmbilledet, fungerer ved at sessionen overdrages fra windows login skærmbilledet til browseren. Der er plugins til hhv Edge og Chrome som ikke er krævet, men forbedrer brugervenligheden.

Såvel WCP som browser plugins kan rulles ud på brugernes PC centralt, og kræver ikke at brugerne skal foretage nogen efterfølgende opsætning.

2 Installation af WCP

MSI pakken til at installere WCP'en kan hentes på OS2faktor websitet

https://www.os2faktor.dk/

Under Download findes et område til OS2faktor Login Agenter. Her ligger den seneste WCP samt tilhørende dokumentation (dette dokument).

WCP'en forudsætter at man har installeret den nyeste VC Redist pakke fra Microsoft. Der ligger en sådan på samme website, som kan downloades, så man er sikker på at denne også er installeret.

2.1 Lydløs installation af "VC Redistributable"

Microsoft leverer deres VC Redist pakker som EXE installere, der kan installeres uden interaktion via følgende kommando

```
VC_redist.x64.exe /q /norestart
```

2.2 Lydløs installation af WCP

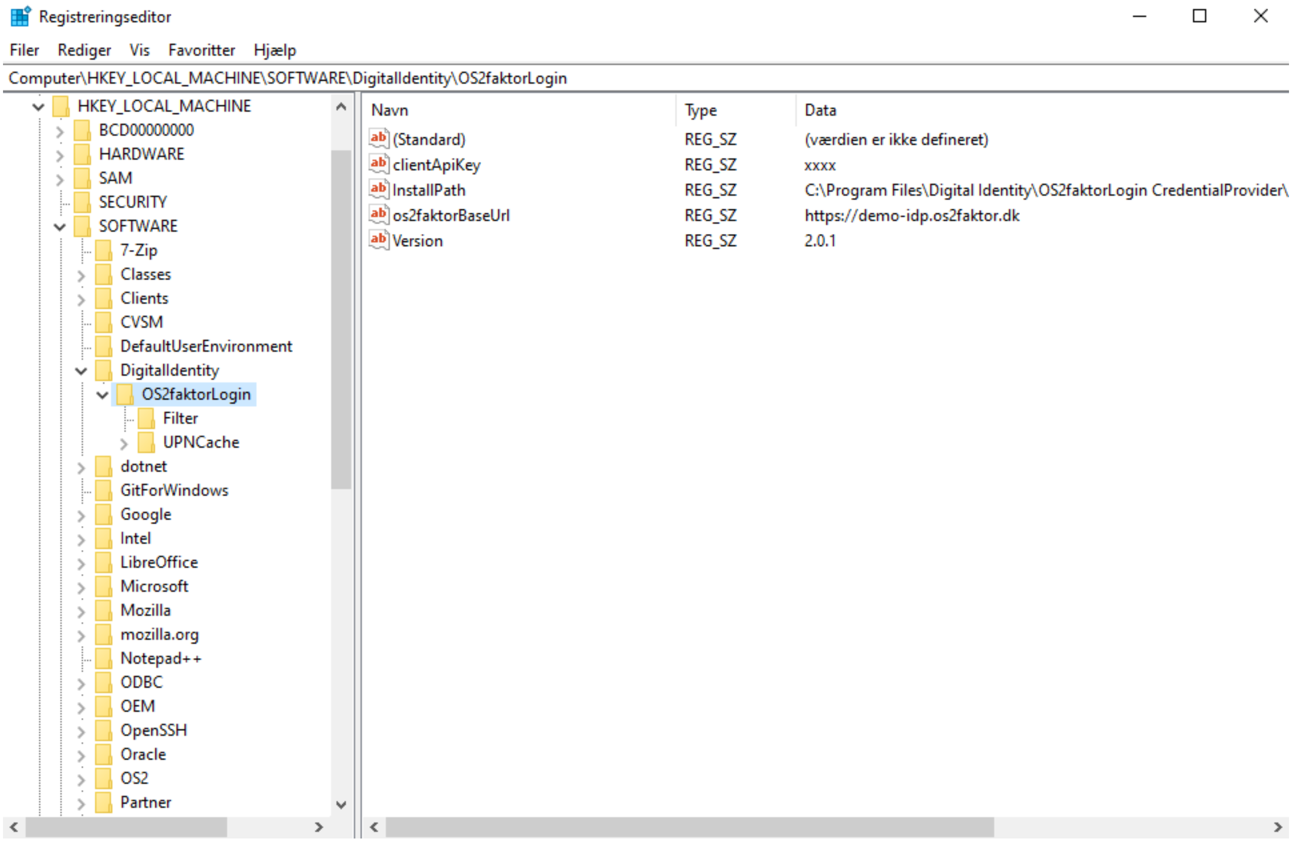
WCP'en leveres som en MSI pakke, der kan installeres lydløst via følgende kommando

```
msiexec /i os2faktor-CredentialProvider.msi /quiet
```

2.3 Konfiguration af WCP

Konfigurationen af WCP'en forefindes i Windows Registry under nøglen HKEY_LOCAL_MACHINE\SOFTWARE\DigitalIdentity\OS2faktorLogin

Registry konfigurationen skal rulles ud på alle maskiner hvor WCP'en installeres, og følgende nøgler er nødvendige for at WCP'en fungerer efter hensigten



WSP'en sætter selv ovenstående nøgler op, men 2 af disse indeholder "dummy-værdier", der skal tilpasses den enkelte kommune der anvender løsningen.

- **clientApiKey**. Denne nøgle skal indeholde en klient nøgle, som kan findes i administratorportalen i OS2faktor Login. Nøglen er specielt hemmelig, men bruges af driftsoperatøren til at spore hvilke WCP'er der laver hvilke kald, samt muligheden for at spærre for en given WCP hvis nødvendigt. Det er samme nøgle der anvendes til alle installationer indenfor et givent domæne i en kommune.
- **os2faktorBaseUrl**. Her skal der peges på kommunens OS2faktor Identity Provider.

2.3.1 Tilpasse tekster på login skærmbilledet

Man kan ændre teksten til kodeordsskifte via en registreringsnøgle (hvis de udelades bruges default teksten)

- **ResetPasswordLinkText**. Teksten der vises for "skift kode" – default er "Jeg har glemt mit kodeord" hvis man ikke sætter denne nøgle.

2.3.2 Understøtte offline UPN login

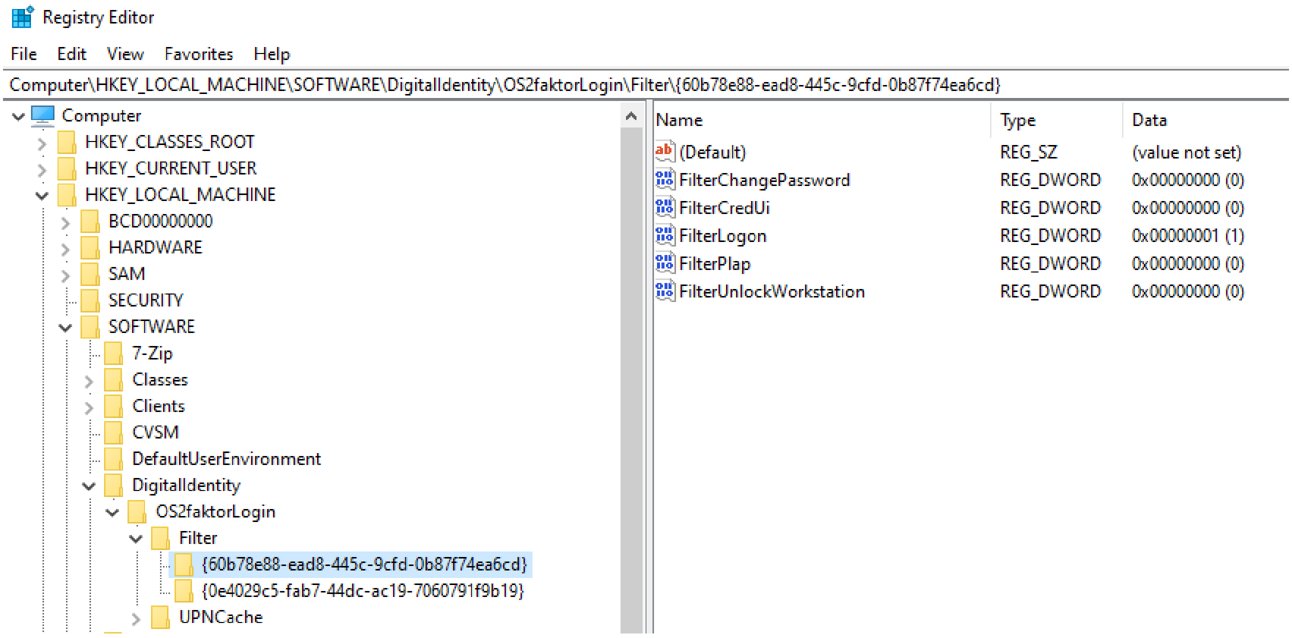
Hvis man foretager et login med sit UPN brugernavn, så foretager domain controlleren en veksling fra UPN til sAMAccountName. Dette virker kun når man er forbundet til domænet. Hvis man er offline (eller offsite), så fungerer UPN ikke som brugernavn til login med mindre man har fået OS2faktor WCP'en til at cache denne kobling.

I registry kan man tilføje denne setting som et DWORD og sætte værdien til "1" for at slå funktionaliteten til

upnCacheEnabled

2.3.3 Filtrer credential providers baseret på login scenarie

Hvis man har brug for at styre hvilke credentials providers der skal være tilgængelige, kan man i OS2faktor WCPs konfiguration opsætte dette.



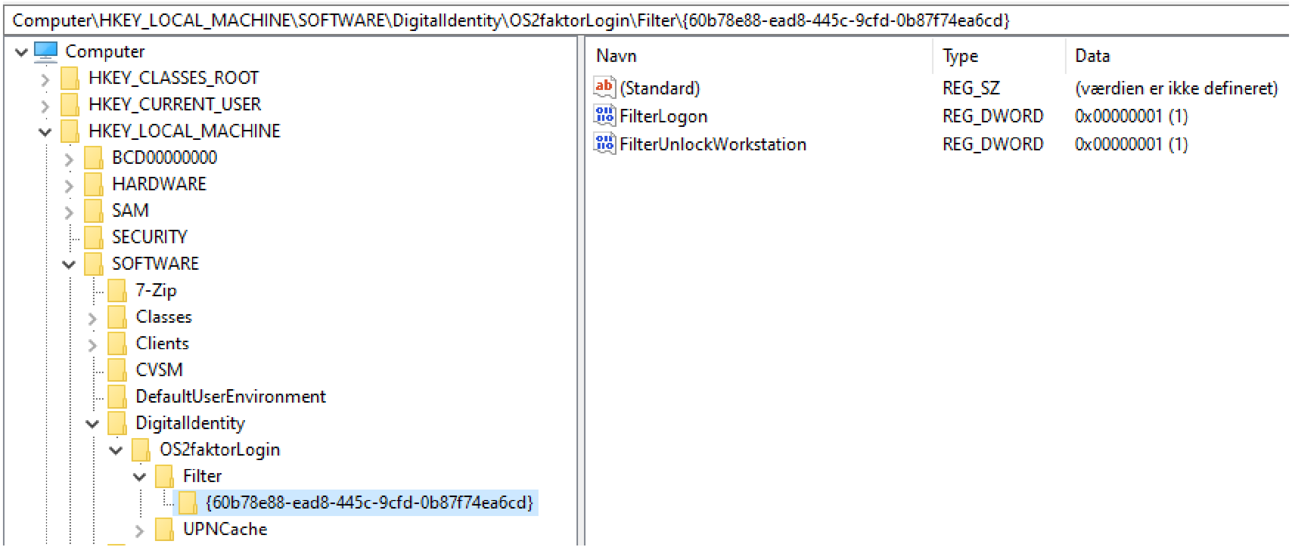
Under "HKEY_LOCAL_MACHINE\SOFTWARE\DigitalIdentity\OS2faktorLogin\Filter" Kan man oprette keys, som matcher CLSID (GUID) på de credential providers som man ønsker at lave et filter på. Derefter kan man som vist på det ovenstående billede tilføje REG_DWORD sat til enten 0(ingen filtrering) eller 1(filtrering) for 5 forskellige scenarier som en credential provider kan understøtte. Nedenfor er der en liste af beskrivelser af hvornår de forskellige scenarier bliver kaldt.

Setting	**Beskrivelse**
FilterChangePassword	Når en bruger efterspørger at skifte kodeord (Ctrl+Alt+Delete)
FilterCredUi	Bliver blandt andet brugt til Remote Desktop og hvis en bruger højreklikker på et program og vælger "kør som anden bruger"
FilterLogon	Når en bruger logger ind eller låser en computer op.
FilterPlap	Pre-Logon-Access Provider. Bliver brugt som SSO, så credentials kan overføres til en remote Computer
FilterUnlockWorkstation	I Windows 10 og nyere er dette slået sammen med Logon. Men af policy årsager kan man godt støde på UnlockWorkstation, begge disse skal håndteres ens.

Det er anbefalet at man kun filterer providers man ved hvad gør specifikt. Desuden er det anbefalet at man kun filterer i det/de scenarier som er nødvendigt og ikke bare filtrerer det hele fra.

2.3.4 Eksempel: Stop Windows egen credential provider fra at dukke op på log ind skærmbilledet

Hvis man gerne vil stoppe Windows normale credential provider (guid: 60b78e88-ead8-445c-9cfd-0b87f74ea6cd) fra at dukke op på login/unlock ser det således ud:



2.4 Sætte OS2faktor WCP som default login mekanisme

Det har tidligere været anbefalet at slå standard windows credentials provideren fra, men det er ikke længere nødvendigt, og anbefales ikke, da det kan give andre problemer.

I stedet anbefales det at man opsætter OS2faktor WCP'en som default WCP i windows, hvilket gøres på følgende måde

- Opret en ny Group Policy under "Computer Configuration -> Policies -> Administrative Templates -> System -> Logon"
- Slå politikken "Assign a default credential provider" til, og sæt værdien

```
{0e4029c5-fab7-44dc-ac19-7060791f9b19}
```

Herefter vælges OS2faktor WCP'en som standard WCP når en bruger foretager et login på en computer. Brugeren kan skifte til windows indbyggede WCP ved at klikke på "Sign-in options" under kodeordet – windows husker dette valg på PC'en.

2.4.1 Nulstil bruger præferencer for WCP

Når en bruger foretager et login husker Windows hvilken credentials provider, der blev brugt og gemmer den som den enkelte brugers præference. Det betyder at windows allerede har gemt den standard windows credentials provider som eksisterende brugeres præference. Derfor kan man nulstille denne præference så skiftet til OS2faktor WCP'en som default login mekanisme tager effekt.

Dette gør man ved at enten slette eller blanke alle key/value par under windows registry nøglen:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\UserTile

Bemærk at hvis man har slået Windows Password Credential Provideren fra i forbindelse med login som beskrevet i punkt 2.3.4 Behøver man ikke også at nulstille brugeres præferencer.

3 Installation af Browser Plugin

Når en bruger foretager et login via windows login skærmen, så etableres en session til OS2faktor Identity Provideren. Denne session overdrages til brugerens web-browser. For at gøre denne overdragelse mere brugervenlig er der blevet lavet en extension til browseren, som uden at brugeren skal gøre noget gør overdragelsen hurtigere og sørger for brugeren bliver forstyrret minimalt af den.

På nuværende tidspunkt er der lavet plugins til hhv Chrome og Edge browserne.

Disse plugins kan hentes hhv her og her

https://chrome.google.com/webstore/detail/os2faktor-wcp-single-sign/ogjjhkickifcfhgkaljkmpafencmngok

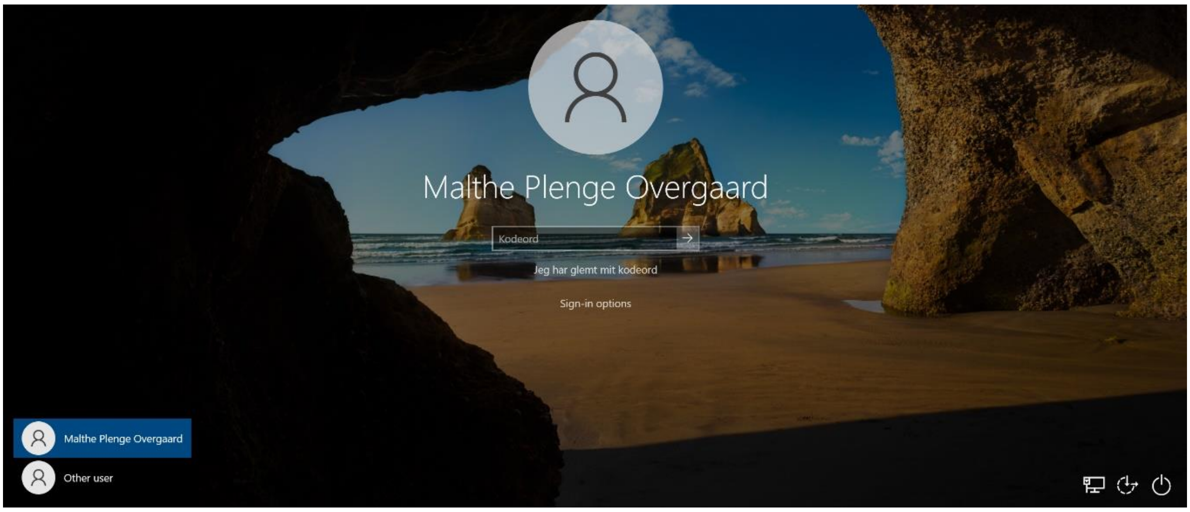
https://microsoftedge.microsoft.com/addons/detail/os2faktor-wcp-single-sign/ahlhgghfccpckibphgadoihmbmjidhjk

Disse kan rulles ud på brugerens PC på normal vis, uden at brugeren skal være involveret i processen.

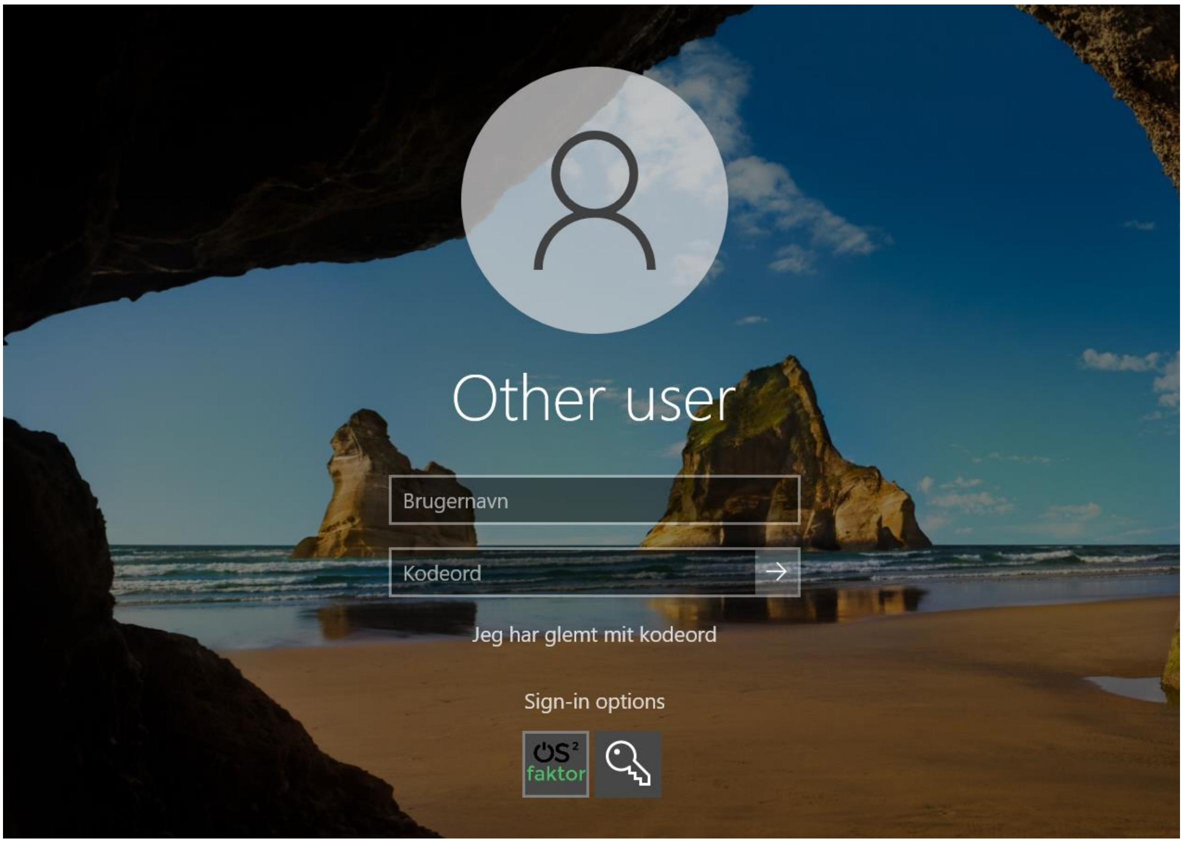
Dette kan for eksempel gøres ved at kræve at bestemte extensions bliver installeret via Group Policy.

4 Afprøvning af funktionalitet

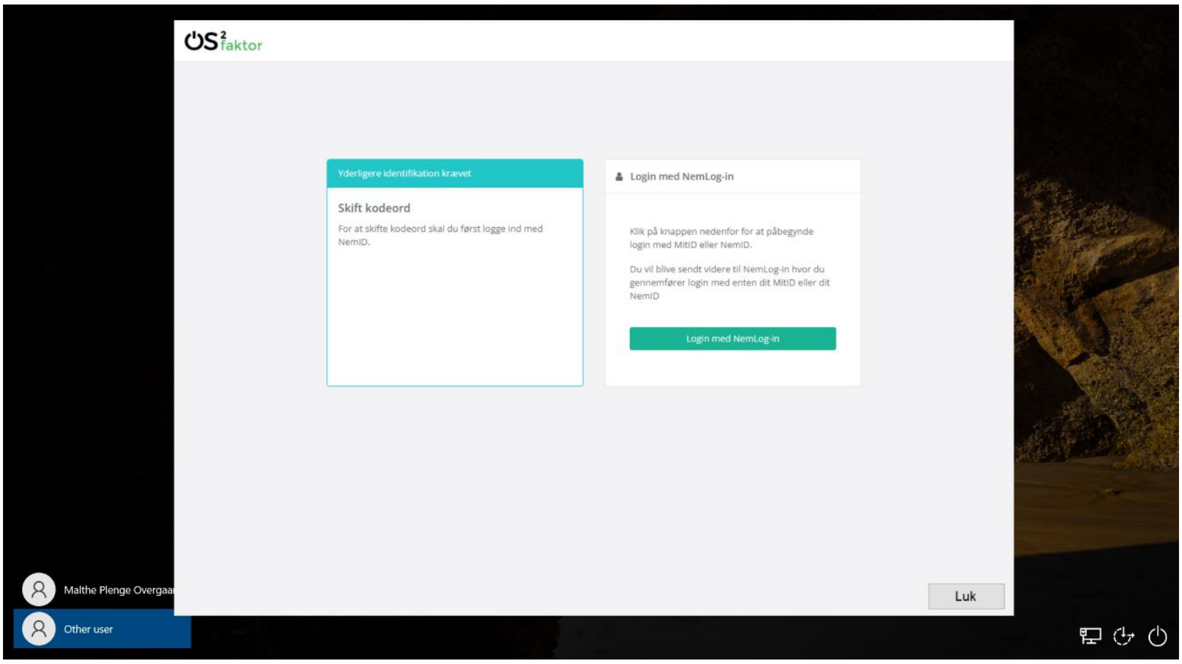
Når WCP'en er installeret (og korrekt konfigureret), kan man anvende den til login ude fra login skærmen. Det skal se cirka sådan her ud



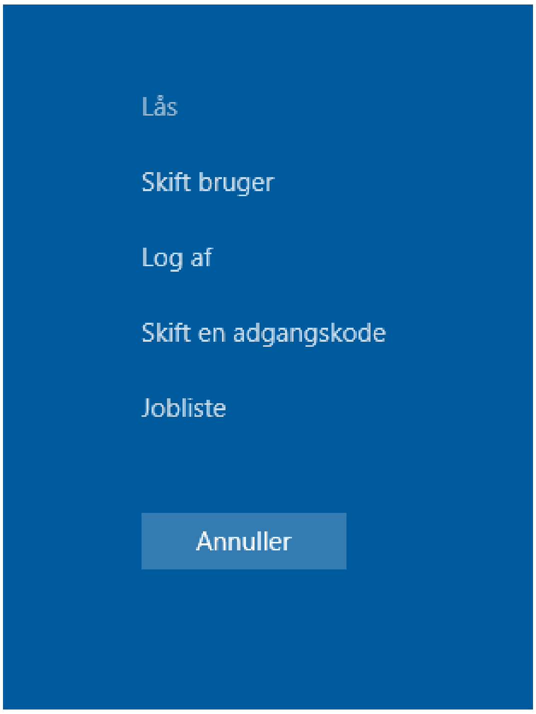
Hvis man kan se linket "Jeg har glemt mit kodeord" under kodeordsfeltet, så er WCP'en korrekt opsat. Hvis man ønsker at gøre brug af en anden WCP, fx den standard indbyggede i windows, så kan man skifte ved at klikke på "Sign-on options", hvor man så ser disse muligheder



Hvis man klikker på linket "Jeg har glemt mit kodeord", åbner følgende skærmbillede, hvor man kan foretage login med NemID eller MitID, og derefter vælge et nyt kodeord.



Endeligt kan man foretage et almindeligt password skifte som bruger, som vist nedenfor (forudsætter at man er logget ind med OS2faktor WCP'en)



Og dette kodeordsskifte vil så skifte brugerens kodeord både i OS2faktor og på Windows.

5 Fejlsøgning

Til fejlsøgningsformål kan man slå logning til på WCP'en. Dette gøres via windows registry (samme placering som de normale indstillinger). Her kan man tilføje en eller flere af nedenstående nøgler, for at tilføje logning på de enkelte funktioner.

Det anbefales ikke at have logning slået til under normal drift, da det kan påvirke både logintiden, samt introducerer udfordringer med store logfiler over tid.

- **CredentialProviderLogPath**. Her kan man angive den fulde sti til en logfil, hvor man ønsker at generelle WCP logs skal skrives til.
- **CreateSessionLogPath**. Her kan man angive den fulde sti til en logfil, hvor man ønsker at logs vedrørende sessions-overdragelse skal skrives til.
- **ChangePasswordLogPath**. Her kan man angive den fulde sti til en logfil, hvor man ønsker at logs vedrørende skift kodeord (brugerens normale kodeordsskifte) skal skrives til.
- **ResetPasswordLogPath**. Her kan man angive den fulde sti til en logfil, hvor man ønsker at logs vedrørende password reset skal skrives til.
- **SessionEstablisherLogPath.** Her kan man angive den fulde sti til en logfil, hvor man ønsker at logs vedrørende sessions-overdragelse skal skrives til.