OS2faktor Login

Windows Credential Provider

Version: 1.3.0
Date: 03.01.2022
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. Dette kræver at der er installeret et såkaldt browser plugin i brugerens browser. Der er plugins til hhv Edge og Chrome.

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
```

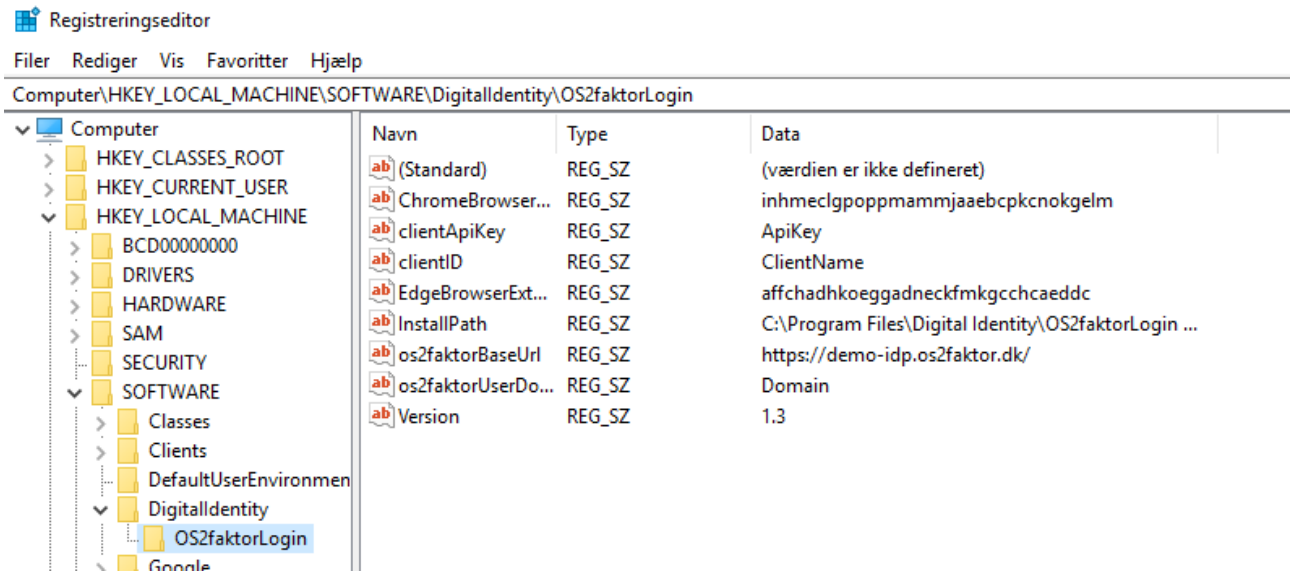
2.2 Lydløs installation af WCP

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. 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 4 af disse indeholder "dummy-værdier", der skal tilpasses den enkelte kommune der anvender løsningen.

- **clientApiKey**. Denne nøgle skal indeholde en klient nøgle, som udleveres af driftsoperatøren. Hverken nøglen eller nedenstående ID er specielt hemmelig, men bruges af driftsoperatøren til at spore hvilke WSP'er der laver hvilke kald, samt muligheden for at spærre for en given WSP hvis nødvendigt. Det er samme nøgle og ID der anvendes til alle installationer indenfor en kommune.
- **clientID**. Denne nøgle skal indeholde et klient ID, som udleveres af driftsoperatøren.
- **os2faktorBaseUrl**. Her skal der peges på kommunens OS2faktor Identity Provider.
- **os2faktorUserDomain**. Her skal ID'et på det domæne (AD domæne) som man anvender WSP'en på, angives. Driftsoperatøren kan evt oplyse denne.

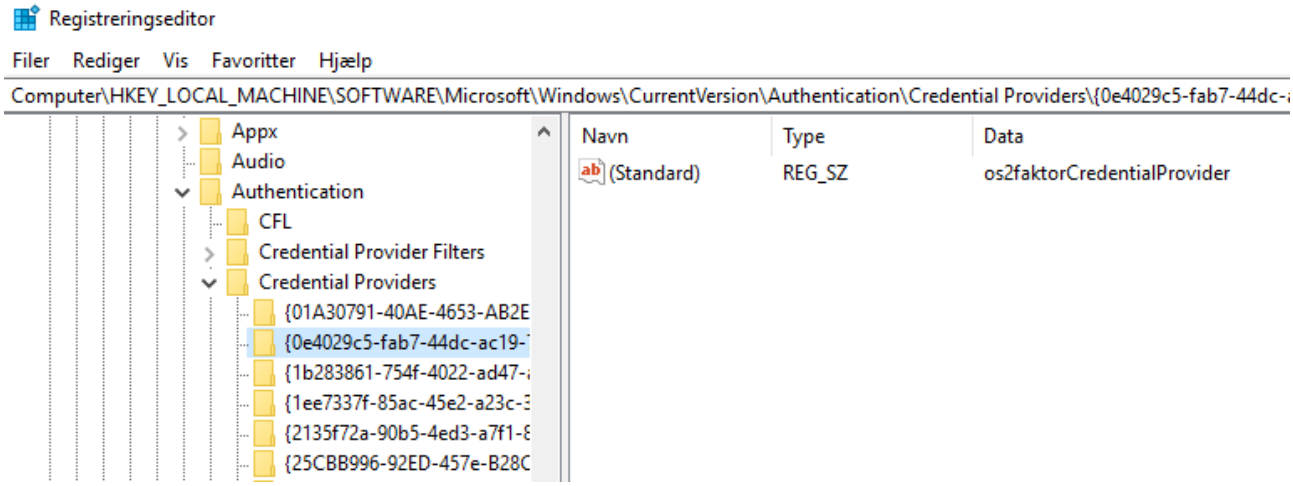
2.4 Fjerne/disable det almindelige login skærmbillede

Når man installerer en WCP, så tilføjer man blot en ekstra login mulighed i windows login skærmbilledet. Brugerne kan stadig anvende deres normale login skærmbillede, og dermed omgå/undgå den funktionalitet der ligger i WCP'en.

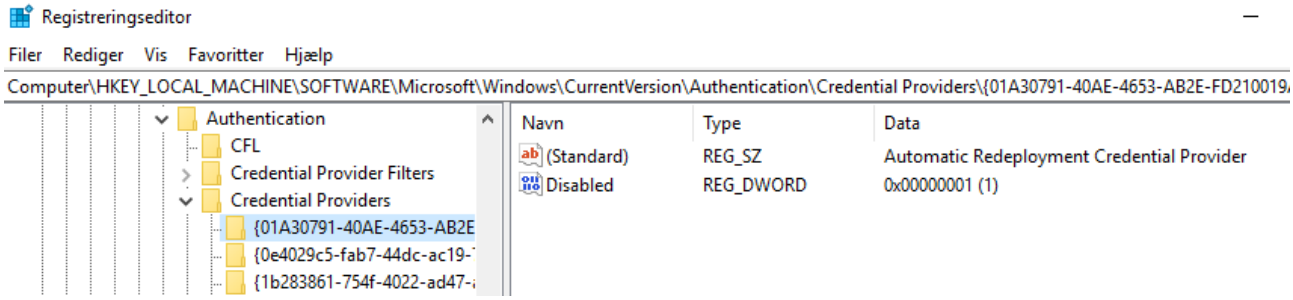
Hvis man ønsker helt at fjerne det gamle login skærmbillede, kan man gøre dette via Windows Regsitry. Alle login skærmbilleder (inkl dem som OS2faktor opsætter) er Windows Credentials Providers, og listen over disse findes i registry her

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
```

Der er typisk en del af disse installeret, omend det er de færreste af dem der faktisk har sine egne login skærmbilleder (nogle bruges kun til remote desktop, nogle brugeres kun til skift kodeord, osv). Hver af disse har som udgangspunkt bare et navn, som vist nedenfor



Hvis man ønsker at disable en af disse, skal der blot tilføjes en DWORD indgang ved navn Disabled, med værdien 1, som vist nedenfor



Det normale windows login hedder ”PasswordProvider” ({60b78e88-ead8-445c-9cfd-0b87f74ea6cd}). Hvis man bruger andre loginmuligheder som Windows Hello, kan man ligeledes overveje at disable disse.

Da Windows husker de sidste par logins, kan det kræve et par login/logud forsøg før alle muligheder for at bruge en disabled WCP forsvinder fra login skærmbilledet.

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, via et plugin som skal være installeret i browseren.

På nuværende tidspunkt er der lavet plugins til hhv Chrome og Edge browserne. Her kan man anvende de standard plugins der også indeholder OS2faktor MFA funktionaliteten. Brugeren behøves ikke anvende disse plugins som MFA klient, og de behøves ej heller være registreret. Eksistensen af plugin’et i browseren er nok til at sessionen kan overdrages.

Disse plugins kan hentes hhv her og her

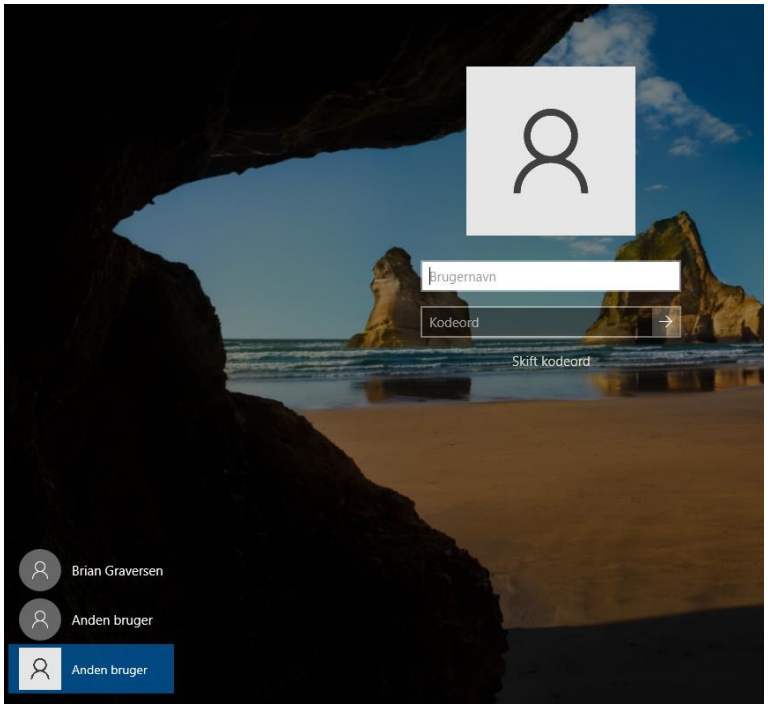
https://chrome.google.com/webstore/detail/inhmeclgpoppmammjaaebcpkcnokgelm

https://microsoftedge.microsoft.com/addons/detail/os2faktor-edge-extension/affchadhkoeggadneckfmkgcchcaeddc

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

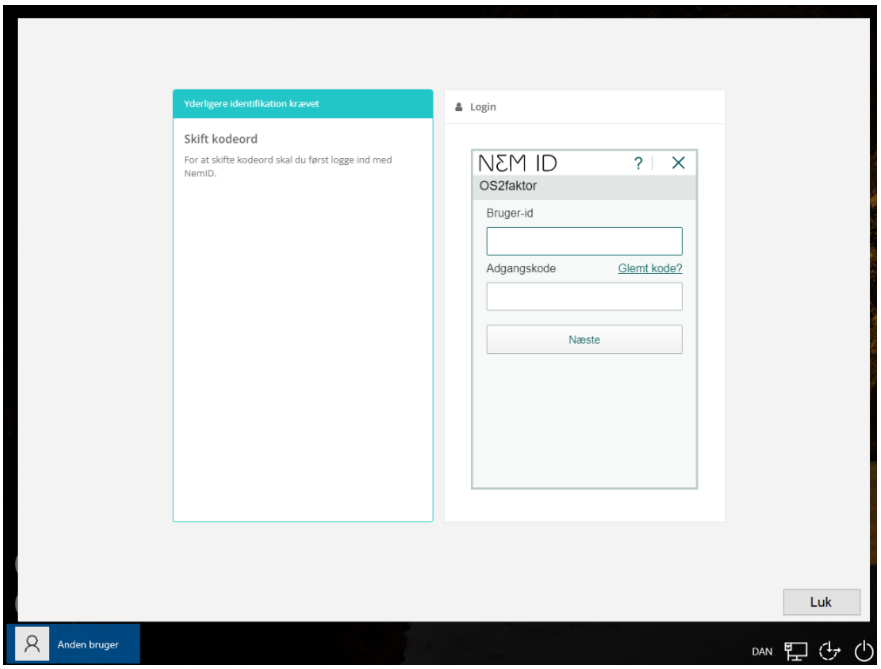
4 Afprøvning af funktionalitet

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

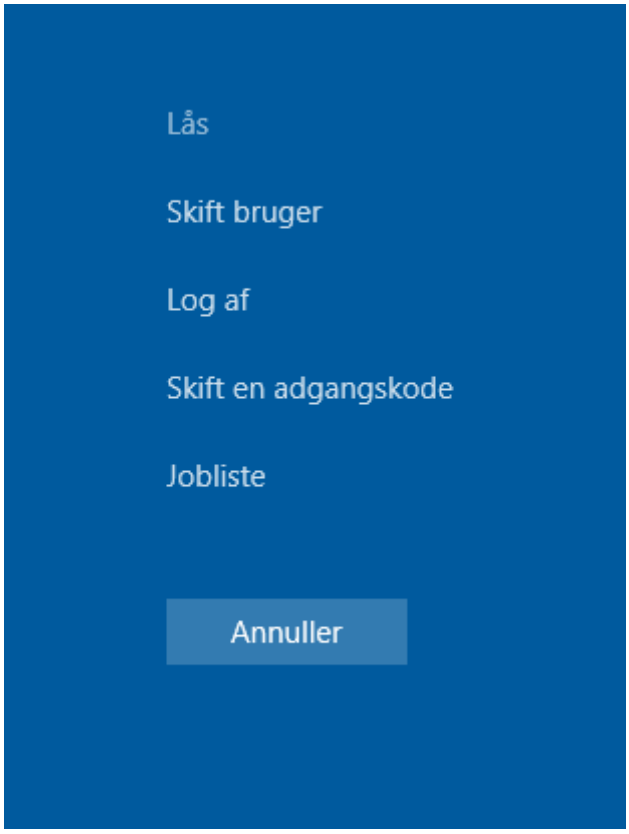


Hvis ikke den "hvide" udgave af login skærmbilledet kommer frem, så er det højest sandsynligt en fejl-konfiguration, eller at VC Redist pakken fra Microsoft ikke er installeret.

Her kan man enten foretage et normalt login (som vil etablere OS2faktor login sessionen som en side-effekt), eller man kan trykke på "Skift kodeord", og så får man nedenstående mulighed for at gendanne et glemt 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.