OS2faktor

Pseudonym API

Version: 1.0.0
Date: 95.02.2019
Author: BSG

Indhold

1 Indledning

Dette dokument beskriver formålet med, og anvendelsen af, pseudonym API'et.

Målgruppen er arkitekter og teknikere, der forestår den tekniske integration til OS2faktor.

1.1 Formål med pseudonym API'et

1.1.1 Hvordan ved man hvilke OS2faktor klienter en bruger har?

Når en medarbejder registrerer en OS2faktor klient, tildeles klienten et unikt OS2faktor ID, som er det der skal anvendes af en Connector (fx AD FS), når klienten skal aktiveres i forbindelse med login.

For at Connectorere ikke behøves at kende de OS2faktor ID'er som en given bruger har, anbefales alle brugere at knytte sit NemID til OS2faktor klienten. Dette håndteres af brugeren selv, via den enkelte OS2faktor klient, uden at kommunen aktivt skal gøre noget.

Det betyder at en Connector ikke behøves kende brugernes OS2faktor ID'er, men i stedet kan lave opslag på hhv personnummer eller NemID PID (det unikke ID som en brugers NemID er tildelt).

Den mest almindelige integration vil være opslag på personnummer, evt suppleret med enkelte brugere som skal have registreret deres OS2faktor ID direkte, da de ikke kan bruge NemID.

1.1.2 Hvad hvis en Connector ikke har adgang til personnumre på brugerene?

Hvad hvis en Connector ikke kender brugernes personnumre, fx hvis personnummeret ikke ligger i Active Directory, og AD FS Connectoren henter disse numre derfra?

I sådan et tilfælde anvendes pseudonymer. Man kan i OS2faktor infrastrukturen registrerer pseudonymer på sine ansatte, og så lade Connectoren bruge disse i stedet for personnumre.

Det fungerer ved at man indlæse en liste af personnummer-til-pseudonym lister i OS2faktor backenden, og så laver man opslag på pseudonymet i stedet for personnummeret.

Illustreret ved nedenstående tabel

Personnummer	**Pseudonym**
1111111118	pia.pedersen
1111111119	jens.hansen

Der er ingen krav til hvad man anvender som pseudonym, men et godt valg kunne være brugerens AD kontonavn. Det er en oplysning som er tilgængelige for de fleste Connectors, herunder AD FS Connectoren. Man kan også registrere flere pseudonymer på det samme personnummer hvis dette er nødvendigt i ens tekniske setup (fx hvis brugeren har flere AD konti).

2 Den tekniske integration

Udvekslingen af personnummer-til-pseudonym data skal ske via en integration fra kommunens datakilde til OS2faktor backenden. Der er på OS2faktor udstillet et sikret API, som den enkelte kommune kan indlæse pseudonymer til. API'et modtager data i et simpelt JSON format, og der sker altid en fuld overskrivning af de data når nye data indlæses.

Der er udarbejdet et powershell script, der viser hvordan man kan hente data fra en SQL database, og så sende dem til OS2faktor infrastrukturen.

Man kan enten tilpasse dette powershell script, eller man kan udvikle sin egen integration, afhængig af typen af datakilde man ønsker at trække fra.

Powershell scriptet kan hentes her

https://www.os2faktor.dk/download/pseudonym-loader.ps1

og man kan fx opsætte powershell scriptet som et skeduleret job på en windows server, der afvikles en gang om dagen, så man sikrer at data holdes ajour.

2.1 API beskrivelse

Hvis man ønsker at udvikle sin egen integration, eller blot vil vide mere om API'et, så man lettere kan tilpasse powershell scriptet, så er det beskrevet i dette afsnit.

2.1.1 Endpoint for API'et

API'et er tilgængelig på dette endpoint

https://backend.os2faktor.dk/api/municipality/pseudonyms

For at kalde API'et skal man bruge en API nøgle. Man har ved tilslutningen til OS2faktor infrastrukturen fået udleveret en kommune-nøgle. Denne nøgle er forskellige fra den AD FS nøgle man anvender til sin AD FS integration, og anvendes alene til integrationen til dette pseudonym API. Hvis man er I tvivl om hvad ens API nøgle er, så tager man kontakt til helpdesk@digital-identity.dk.

2.1.2 API'et kaldes på følgende måde

Der skal udføres en HTTP POST mod ovenstående endpoint, hvor man angiver følgende HTTP headers i sit kald

```
Content-Type: application/json

ApiKey: xxxxxxxx
```

ApiKey skal udfyldes med ens API nøgle.

2.1.3 Input til API'et har følgende format

De data der skal læses ind i API'et er en liste af personnummer/pseudonym mapninger, som leveres i et JSON format. Formatet er meget simpelt, og har nedenstående struktur

```
[
    {
        "pseudonym":  "pia.pedersen",
        "ssn":  "K3b9tAV9cSdvl4lwV5v38FGxfZgeIuCaxeTSs1xaa0w="
    },
    {
        "pseudonym":  "jens.hansen",
        "ssn":  "WUhTv/3XUdW4WVPKGg1JlaUmm70dNavzw0qtyycSX6Q="
    }
]
```

Ovenstående er et eksempel på indlæsning af data der matcher den tabel der blev vist i afsnit 1.1.2, hvor de to brugeres pseudonym/personnummer indlæses.

De to data-felter der indgår skal udfyldes med følgende oplysninger

- **pseudonym**. Udfyldes med brugerens pseudonym i klartekst (fx brugerens sAMAccountName)
- **ssn**. Udfyldes med en sha256 digest af brugerens personnummer, base64 enkodet. Bemærk at personnummeret skal være uden bindestreg, dvs 10 cifre uden andet.

Hvis man laver sin egen integration, kan man med fordel anvende de to fiktive personnumre vist i dette dokument som en kontrol af at ens sha256/base64 enkodning udføres korrekt. Værdierne vist i JSON eksemplet matcher de to personnumre når de er korrekt enkodet.

2.1.4 Fuldt eksempel

Et eksempel på et validt kald til endpointet (med en tilfældig ikke-fungerende API nøgle) er vist nedenfor

POST https://backend.os2faktor.dk/api/municipality/pseudonyms

```
Content-Type: application/json
ApiKey: 3f137564-e4fb-4e6e-bd51-356ac44e2ad9
```

```
[
    {
        "pseudonym":  "pia.pedersen",
        "ssn":  "K3b9tAV9cSdvl4lwV5v38FGxfZgeIuCaxeTSs1xaa0w="
    },
    {
        "pseudonym":  "jens.hansen",
        "ssn":  "WUhTv/3XUdW4WVPKGg1JlaUmm70dNavzw0qtyycSX6Q="
    }
]
```