OS2faktor

Løsningsbeskrivelse

Version: 1.0.3
Date: 29.11.2018
Author: BSG

Indhold

1 Indledning

Dette dokument er en løsningsbeskrivelse for version 1.0 af OS2faktor, samt beskrivelsen for release 1.1, 1.2 og 1.3.

Formålet med dokumentet er at sætte scope for en fuld funktionelt version af OS2faktor, med fuld understøttelse af 2-faktor login til fagsystemer, herunder AULA.

Samtidig skal dokumentet belyse det fremtidige perspektiv i såvel videreudvikling som videre-implementering af OS2faktor, hvilket håndteres ved dokumentation af perspektiver, integrationsmuligheder og etablering af et initielt roadmap for fremtidige versioner af OS2faktor.

Endelig er dokumentet et beslutningsgrundlag for tilslutningen til OS2faktor projektet i OS2-regi, og har til mål at indeholde alle de relevante oplysninger som må indgå i denne beslutning.

Afsnit 2 indeholder en samlet, men overordnet, beskrivelse af OS2faktor, og suppleres af uddybende detaljer i de efterfølgende afsnit.

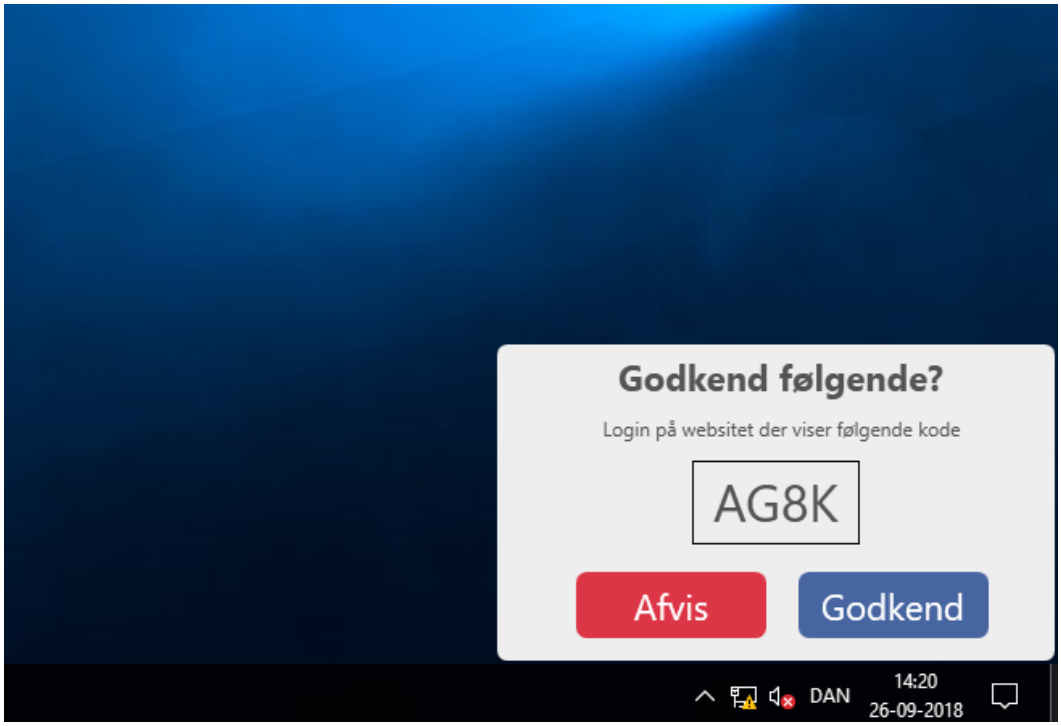
Afsnit 5 indeholder en beskrivelse af funktionaliteten i release 1.1, 1.2 og 1.3.

2 Overordnet beskrivelse af OS2faktor

OS2faktor er en 2-faktor autentifikationsløsning, der kan anvendes som 2. faktor i et login flow. Et typisk scenarie vil være at man anvender OS2faktor som supplement til ens normale brugernavn/kodeord login, hvormed man vil opnå 2-faktor sikkerhed i sit login.

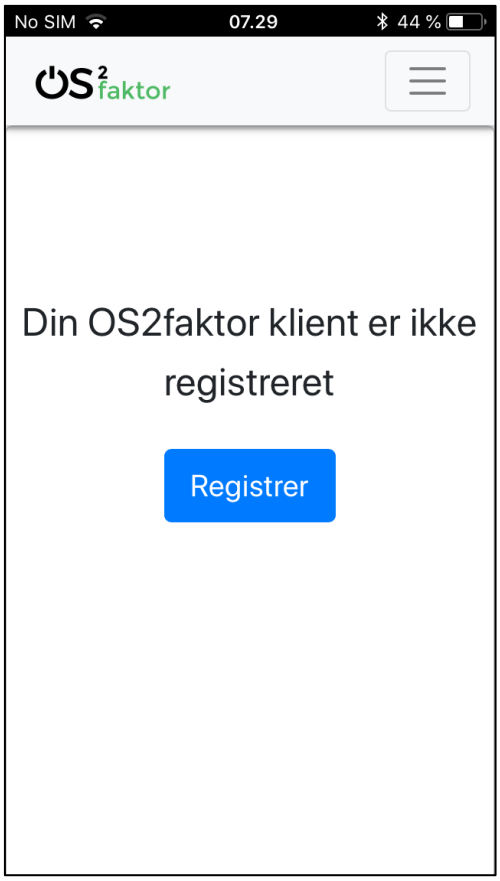
OS2faktor kan installeres både på PC/laptop og på smartphones/tables, med det formål at ramme brugerne på de enheder hvor de arbejder, så de ikke behøves at anvende flere enheder end nødvendigt i deres daglige arbejde.

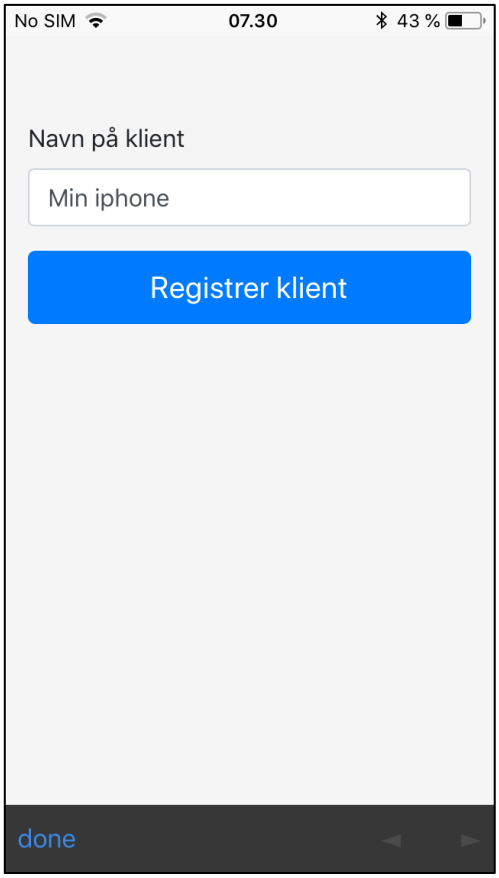
OS2faktor har fokus på at sikre et højt sikkerhedsniveau, uden at det går ud over brugervenligheden. For anvendere af PC/laptops betyder det f.eks. at de blot vil blive præsenteret for en ekstra godkendelsesdialog i forbindelse med login, placeret i højre/nederste hjørne af deres skrivebord.



Når en bruger logger på et fagsystem der kræver 2-faktor login, vil de blot skulle godkende denne dialog, hvorefter login er gennemført succesfuldt.

På samme måde har OS2faktor fokus på at reducere de administrative omkostninger ved at anvende en 2-faktor login løsning, ved bl.a. at understøtte 100% selvbetjening af OS2faktor klient-softwaren. Slutbrugerne kan gennemføre en fuld registrering af deres klient på egen hånd, både på PC/Laptop og smartphone/tablet klienterne. En skærmbillede af en ikke-registreret iPhone klienten er vist nedenfor.





OS2faktor løsningen kan anvendes til KOMBITs fagsystemer, herunder AULA og monopolbrudsystemerne, samt til alle fagsystemer som kommunen har koblet på deres AD FS.

OS2faktor kan også nemt integreres ind i andre fagløsninger og infrastrukturer som Office 365, Netscaler, VPN og lignende.

2.1 Løsningskomponenter

OS2faktor leverancen består af følgende løsningskomponenter

- En Windows 7/10 desktop klient, der leveres som en Windows Installer, der kan distribueres ud på brugernes PC/laptops af kommunens it-afdeling
- En iPhone/iPad app, der kan installeres via Apple App Store
- En Android app, der kan installeres via Google Play
- En AD FS integrationskomponent
- Selve OS2faktor backend løsningen
- Dokumentation af OS2faktor API'et, der kan anvendes til egne integrationer

2.2 Leverancemodel

OS2 har nedsat en koordinationsgruppe, der er med det funktionelle indhold af OS2faktor løsningen, og udarbejder roadmap og tidsplaner for fremtidig udvikling. Dette dokument beskriver funktionaliteten i version 1.0 af OS2faktor, samt kommende releases som beskrevet i afsnit 5.

Kommunerne der tilslutter sig OS2faktor styrer så løbende, gennem koordinationsgruppen, videreudvklingen af OS2faktor, herunder nye klienter, nye integrationer m.m. som måtte ønskes.

Leverandøren af OS2faktor har ansvaret for distribution af nye releases, fejlrettelser m.m., via de respektive release-kanaler (Google Play, Apple App Store, osv).

Information om kommende releases informeres løbende til de tilsluttede kommuner, med fuld transparens i økonomi, prioritering af opgaver og beslutninger via OS2s governance model.

2.3 Status

Den beskrevne funktionalitet til version 1.0 er på nuværende tidspunkt (oktober 2018) udviklet, og er under afprøvning i en af pilotkommunerne. Version 1.0 er klar til fuld udrulning ultimo november 2018.

Der er i afsnit 5 angivet tidsplan for de kommende releases.

2.4 Drift af OS2faktor løsningen

Der etableres fælles drift af løsningen i OS2-regi, og det vil være muligt for den enkelte kommune at tilslutte sig den fælles driftmodel, eller at etablere egen drift af løsninge hvis dette ønskes.

Hvis man ønsker at drifte løsningen lokalt, skal man etablere de fornødne servere, overvågning m.m. i egen it-infrastruktur.

3 Løsningsbeskrivelse

OS2faktor løsningen består af nogle kernekomponenter, der udgår selve infrastrukturen, samt en række klienter og integrationer.

I dette afsnit beskrives hhv kernekomponenterne, klienterne og integrationer adskildt. For hver type beskrives hvad der er med i version 1.0, og hvad der er af integrationsmuligheder.

3.1 Kernekomponenter

OS2faktor er bygget op omkring nogle kernekomponenter der udgør selve infrastrukturen, som klienterne og integrationerne bygger oven på. Denne infrastruktur er ansvarlig for

- Registrering af OS2faktor klienter
- Integration til NemLog-in
- Integration til Apple og Googles notifikationsservere
- Backend for selve login-flowet når OS2faktor klienter anvendes til 2-faktor login

Infrastrukturen udstiller sikre API'er, rettet mod hhv OS2faktor klienterne, og de integrationer der ønsker at gøre brug af OS2faktor som en login mekanisme. Disse API'er, samt administrationen af adgangen til dem, sker via kernekomponenterne.

3.1.1 Integrationsmuligheder

De eksisterende klienter og integrationer er bygget oven på de API'er som kernekomponenterne udstiller, og via disse er det muligt at bygge nye OS2klienter, for på den måde at kunne understøtte flere klient-platforme end dem som OS2faktor version 1.0 kommer med.

Klient API

API'et der er udstillet til at bygge klienter, understøtter følgende funktionalitet

- Registrering af klient
  - herunder muligheden for CPR kobling via NemID/NemLog-in
- Mulighed for at registrere sig som modtager af push-beskeder fra hhv Google og Apples notifikationsservere
- Både REST og WebSocket API'er til at modtage login-beskeder
- Både REST og WebSocket API'er til at godkende/afvise login-beskeder

Server API

Infrastrukturen udstiller ligeledes API'er, der kan anvendes til at bygge integrationer direkte ind i fagsystemer, ind i ens VPN klienter, i Netscaler, OWA Webmail eller lignende systemer, hvor man ønsker at anvende OS2faktor.

Disse API'er udstiller følgende funktionalitet, alle udstillet via et REST API

- Opslag på hvilke OS2faktor klienter en given bruger har
  - Som søgeparametre kan man anvende AD-kontonavn, CPR-nummer, PID og en liste af kendte devices som man mener brugeren anvender
- Afsendelse af en login-besked til en bestemt OS2faktor klient
- Modtage status på en login-besked (godkendt/afvist status)
  - API'et til status-notifikation er delt i to, så der er et offentligt statusopslag, der anvender en 1-gangs nøgle, samt det beskyttede API, som serverens backend kan anvende. Det offentlige opslag kan fx anvendes hvis man har en usikret komponent, der skal have adgang til status på et login forsøg.

Management API

Der er endvidere et simpelt management API, hvor det er muligt for en kommune at indlæse og vedligeholde en AD-konto/CPR-nummer mapningstabel. Dette er tiltænkt scenarier hvor kommunen ikke har mulighed for at anvende CPR-nummeret som opslagsnøgle på login-tidspunkt, men stadig ønsker at gøre brug af CPR-nummer tilknyttet på OS2faktor klienterne.

Via indlæsning af mapningstabellen, vil det være muligt at anvende AD kontonavn i stedet for CPR som opslagsnøgle på login tidspunktet.

3.2 Klienter

Der leveres 3 klienter i version 1.0 af OS2faktor. Disse klienter er

- En iOS klient, der kan afvikles på iPhone og iPad. Denne klient distribueres via Apple App Store, og kan enten installeres direkte af slutbrugeren, eller automatisk via kommunens MDM system
- En Android klient, der kan afvikles på Android smartphones og tablets, samt på Chromebooks der understøtter Android applikationer. Denne klient distribueres via Google Play, og kan enten installeres direkte af slutbrugeren, eller automatisk via kommunens MDM system
- En Windows desktop klient, der kan installeres på både Windows 7 og Windows 10 desktops. Disse klienter distribueres som MSI installer pakker, som kommunen kan installere via deres normale software-installations setup

Disse klienter dækker langt størstedelen af brugsscenariene, men det er som nævnt også muligt at udvikle yderligere klienter, fx gennem OS2faktor videreudviklingen.

3.3 Connectors

OS2faktor kommer med en connector til AD FS i version 1.0. Denne connector understøtter OS2faktor login flowet for brugere der logger på fagsystemer via kommunens AD FS.

AD FS connectoren er implementeret som et standard multi-factor-authentication modul til AD FS, og vil fungere med AD FS 3.0 og 4.0 (Windows Server 2012 R2 og Windows Server 2016). Ved kommende releases af AD FS vil integrationen opdateres til at understøtte disse som en del af den løbende videreudvikling og vedligehold af OS2faktor løsningen.

AD FS integrationen understøtter en række (konfigurable) funktioner, herunder

- Integration til OS2faktor infrastrukturens login-flow
- Muligheden for at foretage knytning af sin OS2faktor enhed til sin AD konto som en del af login flowet
- Mulighed for at indlejre links og hjælpetekster til slutbrugerne, så de kan få kommune-tilpasset hjælp under brugen af OS2faktor

4 Udruldning og implementering

OS2faktor er designet med fokus på selvbetjening og fleksibilitet i integrationerne, så man kan opnå et højt niveau af brugervenlighed og minimal arbejde i forbindelse med implementeringen af 2-faktor sikkerhed.

Alle klienter er designet til automatisk udruldning, men kan også nemt installeres af slutbrugerne selv, fx på BYOD og hjemme PC'ere.

Registreringsprocessen ligger op til stor fleksibilitet, hvor en slutbruger kan nøjes med blot at navngive sin klient som det eneste krævede trin under registreringen, og så senere lave en CPR nummer tilknytning via NemID hvis dette ønskes. Kommunen kan vælge at tillade selv-registrering af OS2faktor klienter via AD FS integrationen, for på den måde at understøtte brugere der ikke ønsker en CPR nummer tilknytning til deres OS2faktor klient.

Som en del af OS2faktor projektet udarbejdes (og vedligeholdes) en scenarie-manual, der beskriver hvordan man kan anvende OS2faktor i forskellige scenarier. Fx hvordan man i praksis håndterer dele-PC'ere, dele-tablets, bring-your-own-device scenarier m.m.

Et typisk implementeringsforløb med OS2faktor kunne se ud som følger

1. Der indgås en driftaftale med OS2 omkring brugen af OS2faktor infrastrukturen
2. Der udarbejds kommune-specifikt vejledningsmateriale til installation og registrering af OS2faktor klienter til medarbejerne (med udgangspunkt i standard materialet). Vejledningen dækker hvordan medarbejderne får installeret en klient, og hvordan de skal registrere den
    a. Evt ruller man automatisk OS2faktor klienterne ud på slutbrugernes laptops og/eller smartdevices via MDM
3. AD FS integrationen opsættes for kommunen (1-2 timers arbejde for en system-administrator i kommunen)
    a. Her skal tages nogle valg om hvordan man ønsker at lave opslag mod OS2faktor infrastrukturen, og om man vil bruge CPR-nummer, PID eller fx AD-konto som opslagsnøgler, og om man vil tillade at brugerne foretager tilknytning af OS2faktor klienter til deres AD konto som en del af login forløbet.

4. I AD FS slår man 2-faktor sikkerhed til på de fagapplikationer hvor det kræves
    a. Dette kan gøres per applikation, og også per bruger/brugergruppe

5 Roadmap

Der er på nuværende tidspunkt planlagt tre yderligere releases, med følgende tidsplan

- **Release 1.1**. Ultimo januar '19
- **Release 1.2**. Medio marts '19
- **Release 1.3**. Medio april '19

Indholdet af de enkelte releases er beskrevet nedenfor

5.1 Release 1.1

Dette release indeholder 3 yderligere funktioner, ud over den beskrevet i release 1.0.

Lokal pinkode beskyttelse

Windows og Chrome klienterne understøtter lokal pinkode beskyttelse, som kan slås til på installationstidspunktet. Hvis pinkode beskyttelse er slået til, skal brugerne vælge en pinkode ved registrering af klienten, som skal indtaste hver gang de anvender deres OS2faktor klient.

Den enkelte kommune kan selv vælge om de ønsker at brugerne skal anvende pinkode, ved at konfigurere installationspakken inden den installeres hos slutbrugerne.

Understøttelse for Chrome / Chromebook klienter

En klient til installation i Chrome browseren, der kan anvendes bl.a. på Chromebooks, men også på andre desktop computere, bl.a. Mac, Linux og Windows PC'ere.

Klienten publiceres i Google Play storen, og kan på den måde distribueres via MDM værktøjer.

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-5

Understøttelse for YubiKeys til login via AD FS

En 2-faktor løsning for dele-computere, hvor man kan bruge en YubiKey (fysisk nøgle) som 2-faktor autentifikation i forbindelse med login via AD FS.

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-7

5.2 Release 1.2

Dette release indeholder 3 yderligere funktioner, ud over den beskrevet i release 1.0 og 1.1.

Dokumentation af Netscaler opsætning til OS2faktor

Muligheden for at kombinere OS2faktor og Netscaler adgangsstyring er allerede til stede i den første release, men i forbindelse med release 1.2 udarbejdes vejledninger og dokumentation til hvordan man sætter dette op i Netscaler.

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-6

Anvendelse af OS2faktor i forbindelse med VPN

Der udarbejdes en RADIUS komponent, der kan installeres lokalt i den enkelte kommune, og anvendes til 2-faktor login via OS2faktor, når der etableres en VPN forbindelse til kommunens VPN infrastruktur.

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-3

Mulighed for at etablere VPN forbindelse direkte fra Windows login skærmen

Der udarbejdes en såkaldt "Credential Provider" til Windows, der gør det muligt at etablere en VPN forbindelse direkte fra Windows Login skærmen, i forbindelse med at brugeren foretager login til Windows Desktop

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-4

5.3 Release 1.3

Dette release indeholder 3 yderligere funktioner, ud over den beskrevet i release 1.0, 1.1 og 1.2

Mulighed for at få tildelt et nyt kodeord (password reset)

Der udarbejdes funktionalitet til at slut-brugeren selv kan resette sit AD-kodeord, ved at gennemføre et NemID login

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-9

Mulighed for at kræve 2-faktor login til udvalgte Windows Servere

Der udarbejdes en såkaldt "Credential Provider" til Windows, der gør det muligt at kræve 2-faktor login på de servere hvor denne provider er installeret. På den måde kan man øge sikkerehdsniveauet på udvalgte Windows Servere.

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-10

Udvidet pinkode funktionalitet

Der udarbejdes en fleksibel pinkode-model, der gør det muligt at kræve pinkode-beskyttede klienter i bestemte login scenarier.

Læs evt mere her

https://os2web.atlassian.net/browse/OS2FAK-11