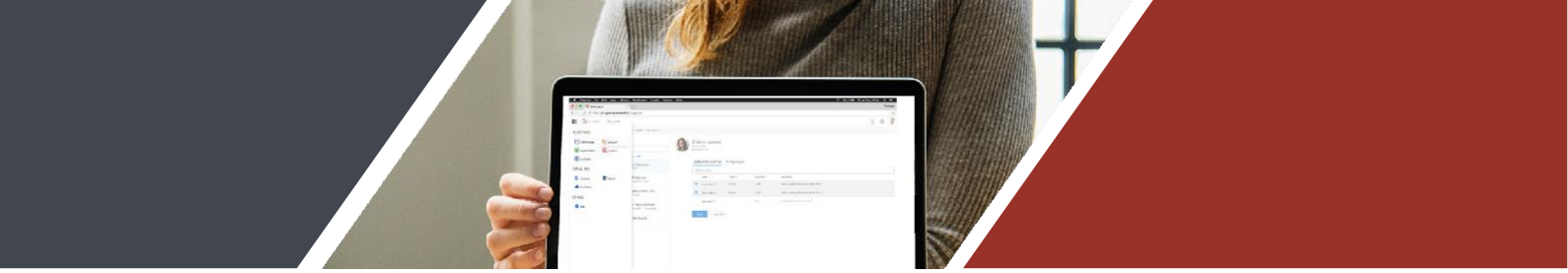

ID Connect: NemLogin og MitID

Med indførelsen af NemLogin 3.0 og MitID bliver NSIS 2.0 nu introduceret for kommunerne

Vi vil her give en kort og praktisk introduktion til nogle af de væsentlige ændringer, der vil komme i løbet af de kommende år. Vi vil ikke være alt for tekniske - i stedet beskriver vi de ændringer, det bringer med sig, og hvilke muligheder, det åbner op for i årene, der kommer.

ID Connect er pt. den eneste udbyder af en Hosted IdP-løsning til kommunerne, og derfor har vi selvfølgelig vores opmærksomhed rettet mod de kommende initiativer, der følger med det nye NemLogin 3.0 og MitID.

En del af de nye løsninger, og dermed den infrastruktur der følger med, er baseret på nyere og mere moderne teknologier, og dermed følger også andre nye sikringskrav herunder NSIS 2.0. Det bliver en stor ændring.

Væsentlig ændring nr. 1: Årligt tilbagevendende revisionskontroller
Hvert år skal f.eks. revisorerklæringer og dokumentation for at processerne er på plads udarbejdes. Vi er på vej mod en mere åben arkitektur, der helt naturligt kræver sikre og kontinuerligt kontrollerede processer.

For den enkelte kommune betyder det på den korte bane:

- LSS (Lokal Signatur Server) udgår – slut med medarbejder certifikater
- Den lokale IdP (MS-ADFS) skal fremover overholde NSIS 2.0-standarden
- OIOSAML 3.0 skal understøttes af den lokale Microsoft ADFS-løsning
- Er der brug for NSIS-niveau HØJ, kræves mere, end hvad NemID understøtter i dag.

Væsentlig ændring nr. 2: Hvem er du - oprettelse
Selvom det er fristende og nemt at benytte en Hosted IdP løsning som f.eks. ID Connect, er det stadig nødvendigt at fokusere mere på sikring af identiteten på brugeren i forbindelse med oprettelse og ansættelse af nye medarbejdere.

Højeste Niveau i NSIS vil fremover kræve, at brugeren er valideret, allerede når de oprettes i kommunens IT-system. Godkendt billeddokumentation på medarbejderen via f.eks. pas eller kørekort skal dokumenteres, og der skal generelt være en meget sikker og struktureret proces for ansættelse af medarbejdere. Det samme gør sig også gældende for eksisterende medarbejdere, hvis de også har brug for at komme på NSIS-niveau HØJ. De skal igennem samme proces, til trods for mange års ansættelse og tidligere adgang til de samme informationer.

Væsentlig ændring nr. 3: Hvem er du - login
Når brugeren skal tilgå en service, skal der i forbindelse med det reelle login være en yderligere validering af brugeren, så kommunen entydigt ved, at det reelt er den pågældende bruger fra kommunen.

I de nuværende interne løsninger har det typisk været nok med et sikkerhedsniveau, baseret på brugernavn og password, primært styret af at brugeren, som er valideret over for netværket via en netværksloginproces i forbindelse med opstart af sin arbejdsstation. Netværket vil ikke længere være at betragte som en faktor, og det vil derfor fremover oftere være nødvendigt for brugerne at foretage yderligere validering i forbindelse med login med for eksempel NemID, MitID eller anden ekstra faktor under login.

Også for de brugere, der blot skal benytte adgang baseret på NSIS-niveau MELLEM. NemID, som vi kender, kan stadig bruges til at hæve sikringsniveauet i NSIS 2.0 til MELLEM, hvilket vil være fint til de fleste transaktioner. Skal man på NSIS HØJ vil det typisk ske med en hardware-baseret validering som f.eks. via en Yubikey nøgle, der er baseret på samme standard som frigives med MitID (FIDO-standard).

Væsentlig ændring nr. 4: Fra Lokal Signatur Server (LSS) til Lokal Identity Provider (IdP)
Den forældede signaturløsning erstattes nu af en moderne teknologi, der ikke længere kræver personlige certifikater. Det er en god nyhed, da det er en styrkelse af sikkerheden og ultimativt også en styrkelse af brugervenligheden.

Kommunens lokale Microsoft-løsning skal nu til at være Lokal IdP og skal derfor nu til tale OIOsaml. Microsoft har ikke planer om at komme til at forstå, hvorledes man kommunikerer med det offentlige i Danmark, og derfor har jeres normale leverandør sikkert allerede mange gode tilbud på, hvordan man kan gå fra den nuværende løsning til den nye og mere moderne arkitektur. En arkitektur som vil være fundamentet for de næste 10-15 års datasikkerhed og kommunikation.

Ønsker man ikke at påtage sig opgaven med at opbygge og vedligeholde processerne omkring en Lokal IdP-løsning, kan ID Connect påtage sig opgaven, og levere en Hosted IdP-løsning, som en del af vores samlede service – det fortæller vi selvfølgelig gerne mere om.

Væsentlig ændring nr. 5: Fra Dansk standard til europæisk standard
Den nye standard er udtænkt til kunne fungere på tværs af både Danmark og Europa. Den kommende arkitektur er for måske første gang ikke kun udviklet ud fra danske behov, men baseret på standarder der blev vedtaget tilbage i 2015 på europæisk niveau.

Det betyder, at det nationale ID i Danmark (det kommende MitID) kommer til at kunne bruges i andre europæiske lande, men måske vigtigere er det, at andre Europa borgere også vil kunne komme til Danmark og validere sig med deres Nationale ID. Det bliver realiteten inden for ganske få år. Det åbner op for et nyt og anderledes integreret Europa, hvor en korrekt valideret medarbejder uanset nationalitet (inden for EU) vil kunne valideres og tildeles adgang til kommunale systemer. Det kan konkret gøre anvendelse af vikarer og løst tilkoblede medarbejdere langt mere sikker, og på trods af en stejl adgangskurve til den nye arkitektur, vil det blive spændende at se, hvad det også medfører af nye og spændende muligheder.

Væsentlig ændring nr. 6: Fra statisk til dynamisk arkitektur
Ultimativt vil der blive stillet højere krav til kommunerne i forbindelse med sikring af brugerne, lokal arkitektur, revisorerklæringer og så videre. Men vi er også på vej mod en ny arkitektur, der vil bevæge sig hurtigt og blive inspireret af nye og bedre løsninger i højere grad, end den nuværende arkitektur har båret præg af.

Det betyder konkret, at der vil opstå langt flere muligheder fremover. Nye teknologier og nye services vil opstå. Og kigger man bare på den nuværende lokale arkitektur fra KOMBIT og Digitaliseringsstyrelsen, er det helt givet, at de services, der fremover vil blive tilbudt igennem føderationsservices, vil stige massivt over de kommende år. Kravene til at kunne styre brugeradgang til specifikke services langt mere specifikt vil eksplodere, og man skal forvente at afsætte flere ressourcer til at styre adgang til services i fremtiden. Nye og brugervenlige services kan reducere opgaven, hvilket vi er fortalere for, men det fjerner ikke opgaven.

Tal med ID Connect
Ud over rollebaseret bruger- og adgangsstyring, fungerer ID Connect's løsninger/produkter også som en Hosted IdP-løsning. Det gør os i stand til at reducere en stor del af sikkerhedsarbejdet i forbindelse med NSIS 2.0. Vi kan ligeledes påtage os ansvaret for integration og governance på jeres eksisterende infrastruktur samt binde jeres eksisterende brugere sammen med offentlige services leveret via KOMBIT adgangsstyring (SKI 02.19), samt de offentlige services, der fremover bliver udbudt via den kommende NemLogin 3.0 arkitektur.