Signaturgruppens NSIS program

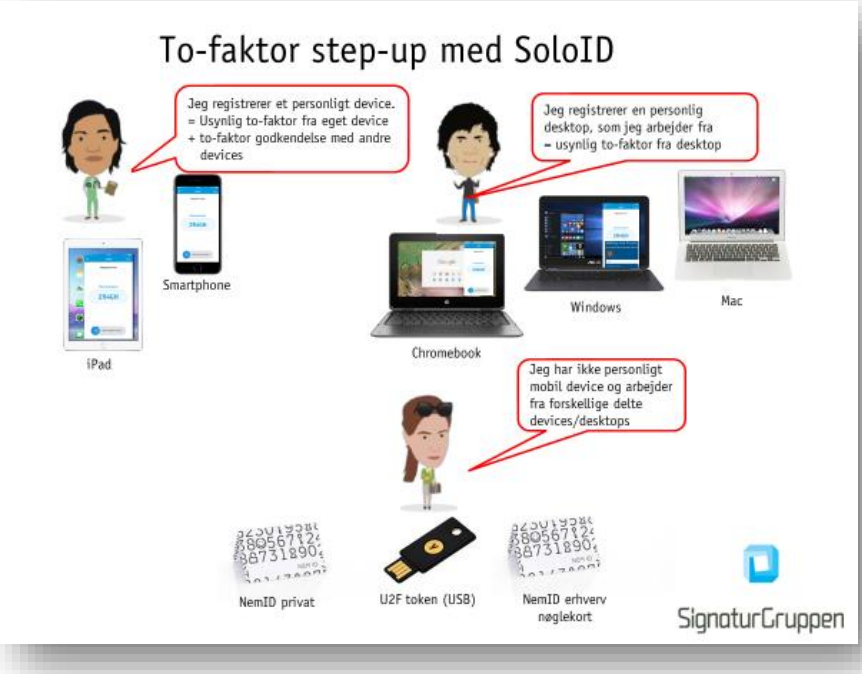
Anvendelse af Signaturgruppens SoloID til brugere med delte devices

Signaturgruppen har siden 2016 investeret målrettet i at etablere SoloID to-faktor sikkerhedsløsningerne, både til mobile devices og desktops. Målet med SoloID to-faktor løsningerne er at optimere sikkerheden således at virksomhederne kan opnå compliance med NSIS sikringsniveau 3 og 4, uden at gå på kompromis med brugervenligheden og produktiviteten hos medarbejderne.

NSIS er den nye standard der supplerer NemID medarbejdersignatur fremadrettet, når medarbejderne skal på nationale tjenester som behandler følsomme data. For at blive compliant med NSIS sikringsniveauerne skal organisationerne årligt indlevere en revisionserklæring fra en uafhængig statsautoriseret revisor om overholdelsen af NSIS standardens krav. Revisionserklæringen skal suppleres af en ledelseserklæring.

Dette dokument beskriver hvordan personale som anvender delte arbejdsgiver devices, såsom personale i daginstitutioner og ældrepleje, kan anvende SoloID til at tilgå data som kræver identifikations på NSIS sikringsniveau "betydelig" (3).

Figuren herunder viser de vigtigste løsningsvarianter med SoloID.



Figur: Vigtigste løsningsvarianter for SoloID

Daginstitutionsområdet skal fra 2020 anvende Aula. Dette betyder, at personalet her får brug for at kunne lave to-faktor identifikation for at kunne tilgå følsomme data.

I mange daginstitutioner har man i dag dog kun delte devices stillet til rådighed af arbejdsgiveren. Disse devices anvender typisk et bredt spektrum af operativsystemer med IoS, Android, Windows, Mac OS og Chrome OS. Desuden understøtter mange af disse devices ikke USB eller NFC.

Dette gør det vanskeligere at etablere brugervenlig og sikker identifikation til disse brugergrupper.

Signaturgruppen har undersøgt området og identificeret et antal forskellige løsningsstrategier som gives herunder til inspiration og videre sparring og produktudvikling.

Metode 1: Registrér device til personen en hel vagt
Hvis personalet typisk har et device udleveret en hel vagt, kan medarbejderen registrere sin SoloID app med privat NemID ved vagtens begyndelse og så anvende SoloID hele vagten.

Metode 2: Anvend en fælles Windows PC til de følsomme opgaver
Sikkerhedshensyn kan tale for, at adgang til følsomme oplysninger sker fra en administrativ computer i et kontor. Personalet vil kunne fortsætte med at tilgå almindelige oplysninger som nu, men når følsomme oplysninger tilgås, går personalet ind på et kontor til en desktop, som er underlagt Kommunens IT sikkerhedspolitik etc.

Metode 3: Lad personalet anvende SoloID fra personlige smartphones
Personale som gerne vil installere SoloID på en personlig smartphone kan anvende step-up fleksibelt og brugervenligt fra alle devices.

Metode 4: Lad personalet anvende NemID privat eller erhverv til step-up
Personale kan enten anvende NemID privat, f.eks. med NemID nøgleapp, eller få udleveret et NemID til erhverv nøglekort som kan anvendes som step-up fra alle devices.

Metode 5: Udlevér personlige U2F nøgler som fungerer med de relevante devices (Bluetooth, NFC, USB)
U2F sikkerhedsnøgler fås i flere varianter, hvoraf nogle også fungerer med IoS devices via Bluetooth tilknytning. Apple er desuden undervejs med at åbne for NFC anvendelse fra deres devices. Dette kan gøre denne type løsninger mere brugervenlige at anvende i takt med udviklingen.

SoloID – Sikker som NemID, let som SMS