SignaturGruppen

Signaturgruppens NSIS program

Hvad er en NSIS to-faktor løsning?

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 betydelig og høj (også benævnt Assurance level 3 og 4 i refererende dokumenter fra f.eks. AULA og fælleskommunal rammearkitektur), skal organisationerne årligt indlevere en revisionserklæring fra en uafhængig statsautoriseret revisor om overholdelsen af NSIS standardens krav. Revisionserklæringen skal suppleres af en ledelseserklæring.
For NSIS sikringsniveau betydelig og høj er der endvidere krav om, at brugerne identificerer sig ved hjælp af en to-faktor løsning med faktorer fra to forskellige af de tre kategorier: "noget kun brugeren ved", "noget kun brugeren har" og "noget kun brugeren er".

Der har endnu ikke etableret sig en best practise i markedet for hvorledes disse to-faktor løsninger kan realiseres teknisk, og der er derfor forskellige tolkninger af, hvilke løsninger der kan opfylde NSIS kravene.

Dette dokument giver Signaturgruppens bud på hvilke typer løsninger, der sandsynligvis kan opfylde to-faktor kravene og hvilke der sandsynligvis ikke vil kunne.

NSIS kravene til to-faktor løsning

Herunder vises de centrale krav fra NSIS version 2.0.

NSIS 2.0 afsnit 3.2.1 ser for niveau betydelig således ud:

Betydelig	3) Det Elektroniske Identifikationsmiddel skal gøre brug af mindst to Autentifikationsfaktorer fra forskellige kategorier. 4) Det Elektroniske Identifikationsmiddel er udformet således, at det kan antages, at det kun kan bruges, når det er den person, som det tilhører, der har kontrol over og er i besiddelse af det.

NSIS 2.0 afsnit 3.2.1 betydelig – anvendelse af to faktorer fra forskellige kategorier

I NSIS vejledningen til dette punkt, gives der yderligere instruktioner, som vist herunder:

Kravet om forskellige kategorier af Autentifikationsfaktorer henviser til kategorierne:

a) »indehaverbaseret Autentifikationsfaktor«: en Autentifikationsfaktor i form af en unik fysisk enhed, som Entiteten skal bevise at være i besiddelse af
b) »vidensbaseret Autentifikationsfaktor«: en Autentifikationsfaktor, som Entiteten skal bevise at have kendskab til (fx et kodeord), og som er hemmelig
c) »iboende Autentifikationsfaktor«: en Autentifikationsfaktor, der er baseret på et unikt fysisk træk hos en fysisk person, og som Entiteten skal bevise at have (fx biometri)

Dette betyder med andre ord, at to forskellige passwords ikke vil leve op til kravene, da de regnes for tilhørende samme kategori. Derimod vil et kodeord (kategori b) kombineret med et OTP nøglekort (kategori c) kunne regnes som to faktorer fra forskellige kategorier. En hardwareenhed beskyttet med password vil i de fleste tilfælde kunne regnes som to faktorer, idet enheden regnes som en indehaverbaseret faktor og kodeordet som en vidensbaseret faktor.

NSIS 2.0 vejledning til afsnit 3.2.1 betydelig – om de to faktorer

Ambitionen med sikringsniveau betydeligt er altså, at et identitetstyveri skal forudsætte, at angriberen skal kunne stjæle to af brugerens faktorer af forskellige kategorier.
Ambitionen er også, at der er samme høje beskyttelse imod kollegaer, administratorer og superbrugere, hvilket stiller store krav til processer omkring registrering, udlevering og supportsituationer som reset af glemt password.

På sikringsniveau betydelig må en kollega altså ikke kunne "låne" en anden kollegas identitet blot ved at låne eller gætte et eller flere af brugerens passwords.

Hvad er en to-faktor løsning, og hvad er ikke en to-faktor løsning?

Herunder oplistes en række eksempler på tekniske identifikationsløsninger. Rækkefølgen er valgt efter Signaturgruppens vurdering af den tekniske sikkerhedsstyrke af løsningen, således at de mest usikre nævnes først og de mest sikre sidst. I højre kolonne angives hvilket NSIS sikringsniveau Signaturgruppen vurderer løsningen kan understøtte, såfremt alle øvrige NSIS krav til det relevante sikringsniveau også er opfyldte i organisationen.

Identifikations faktorer	Beskrivelse	Sikkerheds-karakteristika	NSIS niveau
Brugernavn og password	Traditionel anvendelse af personligt brugernavn og password med almindelige IT sikkerhedspolitikker.	Kan udlånes, gættes, stjæles med keyloggere og resettes af superadministratorer.	Lav (2)

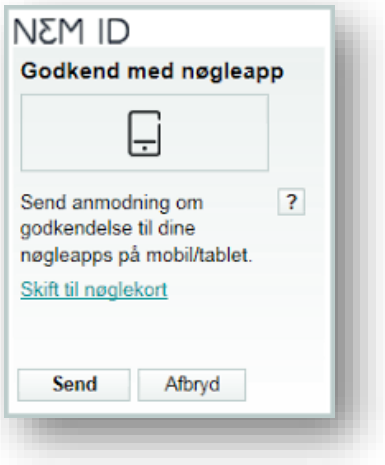
Brugernavn og password fra sikret netværk	Anvendelse af personligt brugernavn og password fra et sikkert virksomhedsnetværk med fysisk og logisk adgangskontrol	Alle brugere på netværket kan låne eller forsøge at gætte en brugers password. Superadministratorer kan resette password og overtage identitet.	Lav (2)
Brugernavn og password samt SMS	En meget udbredt sikkerhedsløsning i dag.	Kan angribes i telenetværk, hos eksterne tele-leverandører og hos brugeren. Standardiseringsorganisationerne er begyndt at udfase løsningen, da SMS er svære at beskytte og har angrebsflader i netværk, hos operatører og hos slutbrugerne. Særlig opmærksomhed kræves omkring sikker registrering og vedligehold af mobilnumre.	Lav/Betydelig (2-3)
Brugernavn og password til aktivering af medarbejdersignatur på central server på sikret netværket	Almindelig løsning anvendt i dag.	Alle brugere på netværket kan låne eller forsøge at gætte en brugers password. Superadministratorer kan resette password og overtage identitet. Der kan dog laves særlige logninger og begrænsninger af anvendelse.	Lav/Betydelig (2-3)
Brugernavn og password fra personligt device (Desktop, tablet etc.)	En løsning der findes fra flere leverandører, herunder Signaturgruppens SoloID	Hvis det personlige device er registreret sikkert til brugeren, skal en angriber både gætte password og skaffe sig adgang til device, altså to faktorer fra forskellige kategorier. Devices med TPM chip kan certificeres højere. Særlig opmærksomhed kræves overfor superadministratorer, registreringsprocesser og brugerens kontrol over device.	Betydelig (3)
Anvendelse af brugernavn og password samt bekræftelse fra personlig smartphone	En løsning der findes fra flere leverandører, herunder Signaturgruppens SoloID	Hvis den personlige smartphone er registreret sikkert til brugeren, skal en angriber både gætte password og stjæle smartphone, altså to faktorer fra forskellige kategorier. Smartphones med hardware nøglebeskyttelse kan certificeres højere.	Betydelig (3)

		Særlig opmærksomhed kræves overfor superadministratorer og registreringsprocesser. Det kan sikres at smartphone er beskyttet med login.	
Anvendelse af brugernavn og password samt bekræftelse med engangskode fra nøgleviser/nøglekort	En løsningsmodel som blandt andet anvendes til NemID privat.	Stærk kryptografisk sikring af selvstændig fysisk nøgle. Særlig opmærksomhed kræves overfor superadministratorerl, registreringsprocesser, brugerens kontrol over engangskode enhed og brugerens opmærksomhed omkring phishing risiko.	Betydelig (3)
Anvendelse af brugernavn og password med bekræftelse fra FIDO U2F nøgle	Anvendelse af U2F nøgler understøttes af flere cloud service leverandører herunder Google og fås også til Signaturgruppens SoloID.	Meget sikker løsning som også beskytter imod phishing. Stærk kryptografisk beskyttelse af selvstændig fysisk nøgle. Særlig opmærksomhed kræves overfor superadministratorer, registreringsprocesser og slutbrugeres bevaring af kontrol over U2F nøglen, så den ikke blot sidder i en desktop PC hele tiden, også når brugeren ikke er tilstede.	Høj (4)

Anvendelse af to faktorer fra samme enhed

Intuitivt er det naturligt at tænke, at de to identifikationsfaktorer "skal komme fra" to fysisk adskilte enheder. Den klassiske engangskode-viser, som har været anvendt i mange hjemme-arbejdsplads løsninger er for eksempel en selvstændig fysisk enhed, som brugeren bærer med sig. NemID Nøglekortet er et andet eksempel.

NemID understøtter også anvendelsen af NemID nøgleapp i stedet for nøglekort. Når man indtaster NemID bruger-id og password i sin mobilbrowser og derefter godkender med NemID nøgleapp på samme mobil, anvender man de to faktorer fra samme enhed.



NemID nøgleapp understøtter to faktorer fra samme enhed.

Tilslutning af chipkort til desktop PC er et andet klassisk eksempel som opfattes som en sikker to-faktor løsning. Men almindeligvis afgives brugerens password OG pinkoden til chipkortet fra desktoppen, og dette betyder, at en keylogger vil kunne fange begge koder, med fare for at en angriber kan afvikle valide transaktioner fra brugerens desktop, når brugeren har isat chipkort.

Det centrale i NSIS er brugerens mulighed for at bevare ene-kontrollen over identifikationsfaktorerne, og ovenstående eksempel med chipkortet illustrerer at dette afhænger af flere forskellige omstændigheder ved løsningerne.

Så hvordan kan man lave en to faktor løsning fra ét device?

I vejledningen til høringsversionen til NSIS 2.0 beskrives det i afsnit 3.2.1, hvorledes smartphones med hardwarenøglebeskyttelse vil kunne certificeres til niveau høj.

Et særligt område, hvor det endnu ikke er almindeligt med certificering af kryptografiske processorer, er mobile enheder som smart phones etc. Her kan man på niveau Høj skele til nedenstående krav som alternativ til certificeringer:

1. Kryptografiske nøgler skal kun kunne anvendes, når enheden er låst op af brugeren, og kun fra den applikation, som har genereret nøglen.
2. Andre brugere (selv avancerede) med fysisk adgang til enheden skal ikke kunne tilgå eller bruge kryptografiske nøgler eller kunne overføre nøglemateriale til andre

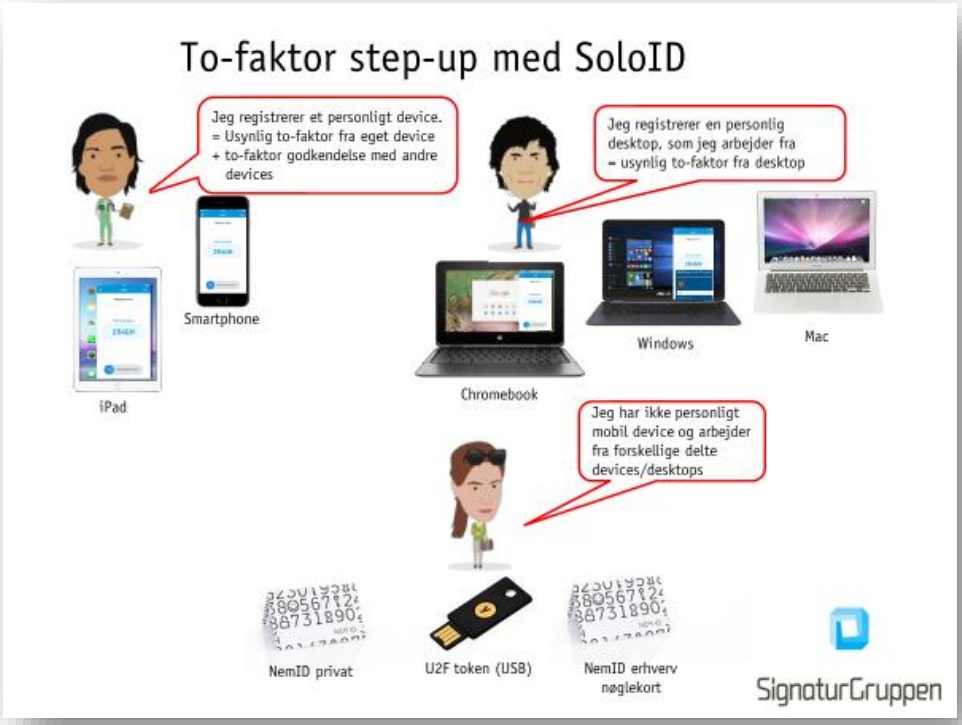
Udklip af afsnit 3.2.1 i vejledning til NSIS 2.0 høring – Smartphone med SE på niveau høj

I sammenligning med chipkortløsning kan man tænke på en smartphone med hardware nøglebeskyttelse som en enhed, hvor "chipkortet er fast monteret". I stedet for at brugeren beskytter chipkortet, bevarer brugeren kontrollen over hele smartphonen inkl. hardware nøgle-beskyttelsesenhed.

I ovenstående tabel over Signaturgruppens vurdering af styrke af identifikationsløsninger, har vi derfor også scoret anvendelse af brugernavn og password fra personligt device eller smartphone op på niveau betydeligt. Dette forudsætter, at device registreres sikkert til brugeren, samt at brugeren har mulighed for at beskytte dette device imod at andre kan tilgå det. Bemærk at det altså vil være muligt at opnå niveau betydelig ved at tilgå en løsning fra brugerens personlige device.

Hvad anbefaler Signaturgruppen?

Figuren herunder viser de vigtigste løsningsvarianter med Signaturgruppens SoloID.



Figur: Vigtigste løsningsvarianter for SoloID

SoloID – Sikker som NemID, let som SMS