DIGITALISERINGSSTYRELSEN

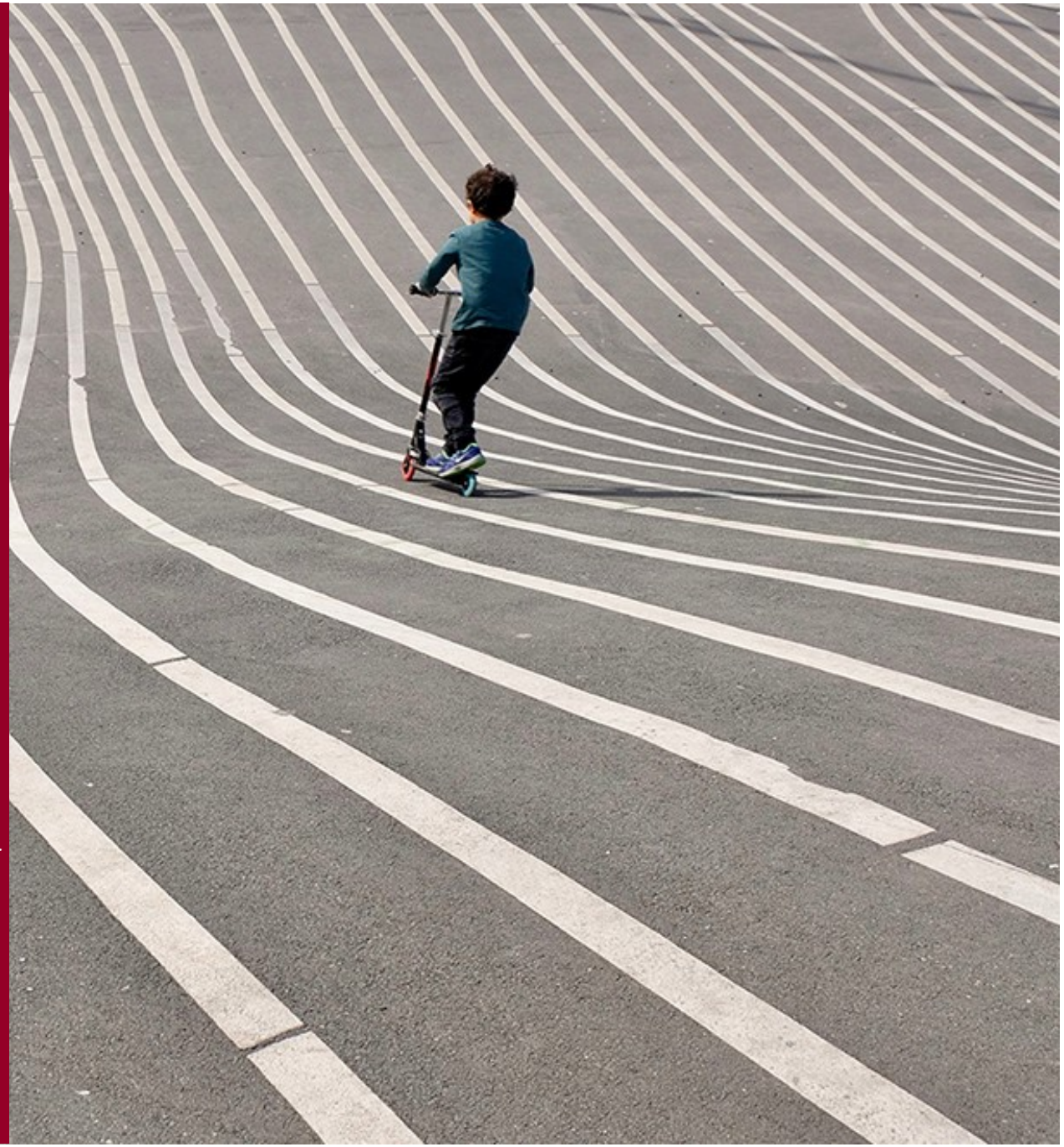
Velkommen til webinar om National Standard for Identiteters Sikringsniveauer (NSIS)

Hvis du ikke kan høre os, så prøv en af følgende:

- Genindlæs siden (tryk ctrl + r)
- Anvend Firefox eller Chrome som browser

Praktisk information:

- Vi starter selve webinaret kl.12.05 for at få alle med.
- Webinaret optages så du kan gense det senere eller dele det med kollegaer
- Du kan stille spørgsmål til os via funktionen ”questions”/”spørgsmål” i højre side. Det er kun dig selv og os fra Digitaliseringsstyrelsen, der kan se spørgsmålet



Christian Schmidt-Madsen

Digitaliseringsstyrelsen

Thomas Gundel

Ekstern konsulent

DIGITALISERINGSSTYRELSEN

Generelt om NSIS

Hvad er NSIS?

- Overensstemmelse med eIDAS (EU-forordning).
- Sikringsniveau aka. “Level of Assurance” (LoA).
  - Lav, Betydelig, Høj.
  - NemID svarer til Betydelig – standard for privat MitID.

- Frivillig ordning – men “NSIS mærkning” kræver compliance.
- MitID og NemLog-in vil leve op til – og kræve – NSIS.

- Version 2.0.1 med vejledning 2.0.1a publiceret i december 2019.

Hvem er NSIS relevant for?

ID-tjenester

- Udstedere og videreformidlere af digitale identiteter; fx MitID, NemLog-in, Lokal IdP
- I NSIS termer: *elektronisk identifikationsordning* og *identitetsbroker*

Tjenesteudbydere

- Udbydere af forretningstjenester (selvbetjeningsløsninger); fx borger.dk
- Skal risikovurdere, men ikke anmeldes

Brugerorganisationer

- Organisationer der ønsker at udstede erhvervsidentiteter til deres medarbejdere
- Skal forholde sig, men ikke anmeldes

Typer af identiteter i NSIS

- Fysiske personer

  - Privatidentitet
- Juridiske enheder

  - Virksomhedsidentitet
- Fysiske personer associeret med juridiske enheder

  - Erhvervsidentitet (erstatter medarbejdersignatur)

Erhvervsidentiteter og privatidentiteter kan benytte samme private *identifikationsmidler*, men *identiteterne* er altid adskilte.

Nedbrydning af sikringsniveau

- Samlet sikringsniveau i NSIS betegnes ofte **LoA** (Level of Assurance)

- LoA kan nedbrydes i en række bestanddele:
  - **IAL** (Identity Assurance Level) – styrke af identitetssikring.
  - **AAL** (Authentication Assurance Level) – styrke af autentifikation.
  - **FAL** (Federation Assurance Level) – styrke af identitetsbroker.
- NSIS LoA er minimum af IAL, AAL og FAL.

- Eksempel:
  - En broker på niveau Betydelig, som formidler en autentifikation på niveau Høj og med Høj IAL, skal fx sætte det samlede LoA til Betydelig.

NSIS krav

- ID-tjenester skal leve op til en række forskellige krav.
- Kravene går på tekniske-, organisatoriske- og juridiske aspekter og dækker bredt risici ved identitetshåndtering.
- Vigtigste processer, som reguleres i NSIS:
  - Identitetssikring (fysiske personer, juridiske personer og forbindelser mellem disse)
  - Udstedelse og levering af Elektroniske Identifikationsmidler
  - Autentifikation
  - Videreformidling af autentifikation (broker)
  - Generel it-sikkerhed: baggrundstjek af medarbejdere, logning, drift, ISMS mv.
- Anmeldelsesproces på niveau Betydelig og Høj er baseret på revisions- og ledelseserklæringer, som indestår for, at krav er opfyldt.
- Krav om forsikring for private virksomheder.

Øget sikkerhed i registrering af erhvervsidentiteter

Ensartede og skærpede krav til identitetssikring af erhvervsidentiteter.

Vished for, hvilken fysisk person der er bag en erhvervsidentitet.

- Iht. NSIS sikringsniveau.
- Ikke en del af erhvervsidentitet, men kendt af NemLog-in som identitetsgarant.

Virksomhed står kun på mål for kobling mellem fysisk person og virksomhed.

Styrket kontrol med tilslutning af virksomheder som brugerorganisationer.

Initiel identitetssikring med privat NemID / MitID.

Krav om 2-faktor autentifikation i NSIS

- Autentifikationsfaktorer:
  - Indehaverbaseret (fx besiddelse af fysisk enhed)
  - Vidensbaseret (fx kendskab til kodeord)
  - Iboende (fx fysisk træk / biometri)
- Lav: mindst én
- Betydelig og Høj: mindst to fra forsk. kategorier

- Én enhed kan godt levere flere faktorer
- Ikke krav om biometri
- Ikke krav til de enkelte faktorers styrke
- Netværk tæller ikke som en indehaverbaseret faktor, da det ikke er en unik fysisk enhed, men en delt ressource.

NemID nøgleapp understøtter to faktorer fra samme enhed.

DIGITALISERINGSSTYRELSEN

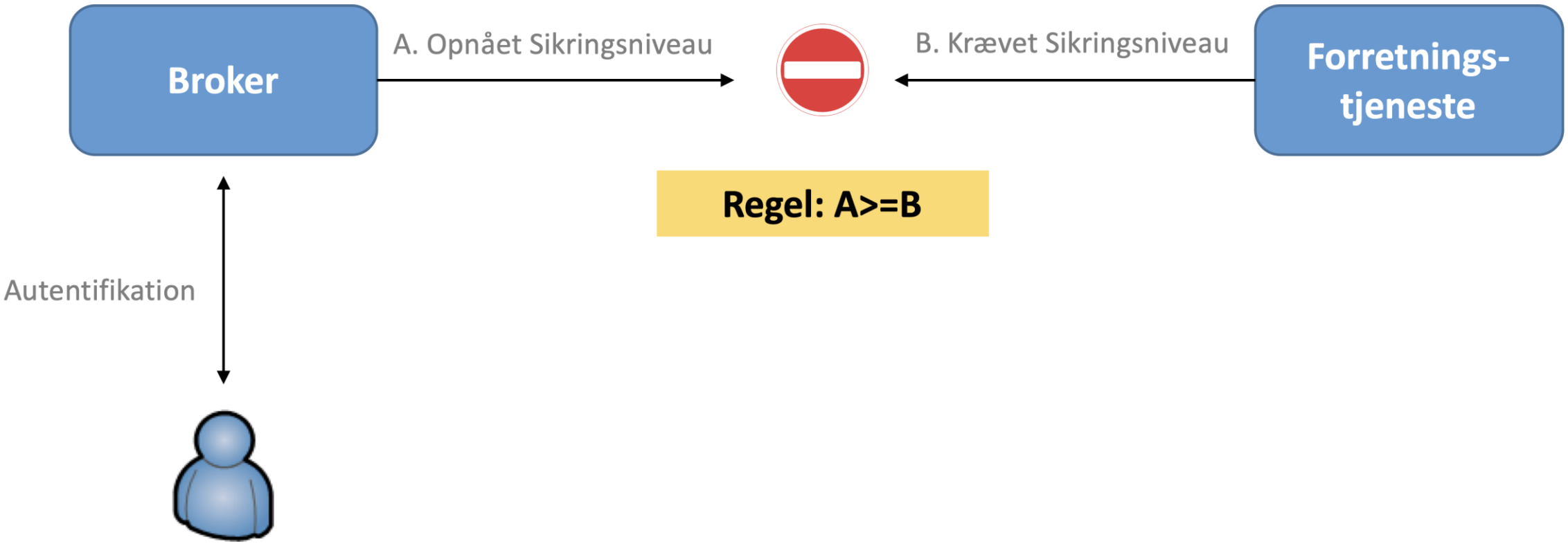
Sikringsniveau iht. risikovurdering

- Den enkelte tjeneste-udbyder er data-ansvarlig for egne data.
- Fastsættelse af krævet sikringsniveau for tjenesteudbyder ud fra risikovurdering.

- NSIS stiller ikke specifikke krav til sikringsniveau.
- Opmærksomhed på krav til brugergruppes sikringsniveau.

- Inspiration i “Vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere”.
- Støtteværktøj til fastsættelse af sikringsniveau.

NSIS ved login til tjeneste



DIGITALISERINGSSTYRELSEN

Støtte til TU's risikovurdering

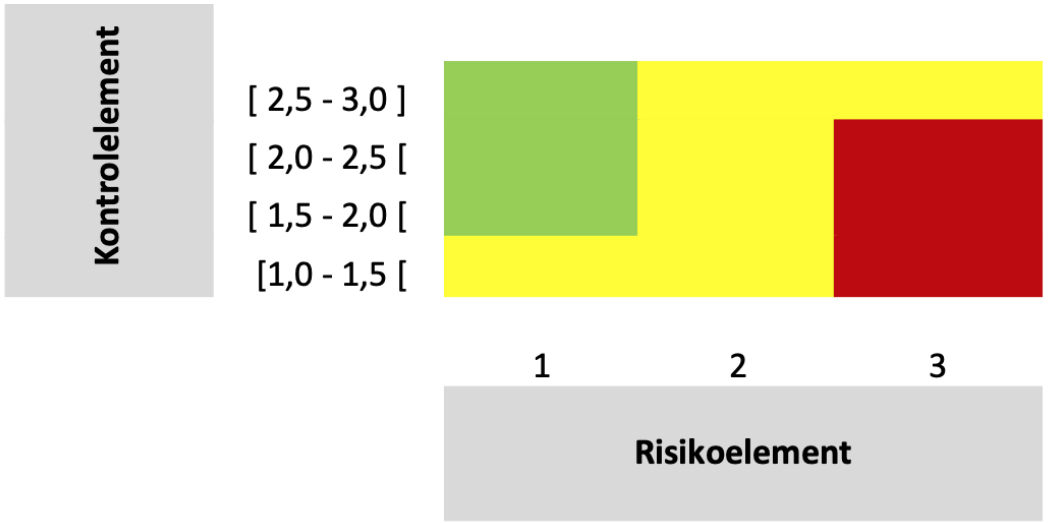
Excel-værktøj og vejledning til tjenesteudbydere

- Tjenesteudbydere vælger, hvilket sikringsniveau de stiller som krav til brugere. Dette sker på baggrund af risikovurdering.
- Til at støtte vurderingen har Digitaliseringsstyrelsen i samarbejde med KOMBIT udarbejdet et Excel-værktøj.
- Værktøjet er bevidst holdt simpelt og skal alene betragtes som en støtte til vurderingen, som guider gennem relevante overvejelser.

- Der vil som oftest være særlige forhold i en konkret tjeneste, som ikke kan dækkes af et generelt værktøj. Værktøjet skal derfor anvendes forsigtigt.
- Valg af sikringsniveau er i sidste ende en forretningsmæssig og sikkerhedsmæssig samlet vurdering, som ikke kan dikteres af et regneark!

Regnearkets opbygning

- Værktøjet består af en række spørgsmål inden for to dimensioner, som udfyldes med score og begrundelse:
  - Risikoelementer
  - Kontrolelementer
- På baggrund af scoren inden for disse dimensioner gives et bud på et samlet sikringsniveau.
- Risikoelementer afdækker fx mængden og følsomheden af personoplysninger, konsekvenser ved at uvedkommende får adgang, muligheden for at påvirke integritet og tilgængelighed af data.
- Kontrolelementer afdækker styrken af implementerede foranstaltninger, som fx finkornet adgangskontrol, logning, funktionsadskillelse, robusthed og test mv.



DIGITALISERINGSSTYRELSEN

Revision

Revision

- Revisionen er det vigtigste instrument i at sikre tilliden i NSIS.
- Visse aktører underlægges revision i NSIS (ved niveau Betydelig og Høj):
  - Dem der udsteder identifikationsmidler med NSIS niveau (**elektroniske identifikationsordninger**),
  - Dem som formidler en autentificeret identitet med NSIS niveau (**identitetsbroker**)
  - Tjenesteudbydere er **ikke** underlagt revisionskrav.
- Digitaliseringstyrelsen foretager ikke revision. Styrelsen vil primært sikre, at formalia er opfyldt, svare på principielle spørgsmål, samt agere på evt. henvendelser om sikkerhedsbrud.
- Revisionen baseres på en ISAE 3000 erklæring og skal udfyldes af en ekstern, statsautoriseret revisor:
  - Første erklæring kan være en type 1 erklæring som går på designet
  - Anden erklæring er en type 2 erklæring som går på den kørende løsning

DIGITALISERINGSSTYRELSEN

Revision – ved underleverandører

- Underleverandører skal levere tilsvarende erklæringer for relevante NSIS-krav.
- Det er vigtigt, at 'scope' erklæringer hensigtsmæssigt.
- Eksempel: En organisation køber en Lokal IdP 'as-a-service', men står selv for visse administrative processer:
  - Leverandøren af systemet kan komme med en standarderklæring for systemets design, driftmiljø osv., som kan genbruges på tværs af kunder.
  - Den enkelte kunde kan komme med en samlet erklæring, hvor revisor bygger 'oven på' leverandørens erklæring og kontrollerer de kundespecifikke forhold, som ikke er omfattet af leverandørens erklæring.
  - Samlet set skal revisionen dække alle relevante krav i NSIS.

Revisionen i praksis

- Der er udarbejdet et Excel-regneark med alle krav i NSIS, som revisor og anmelder skal udfylde.
- Anmelder beskriver, hvordan krav opfyldes, herunder de implementerede tiltag.
- Anmelder beskriver endvidere kontrolmål - hvordan man konstaterer, om tiltag er implementeret.
- Revisor beskriver revisionshandlinger inkl. observationer samt konklusionen for hvert krav.

Anmelders beskrivelse af opfyldelse (Praksis)	Anmelders beskrivelse af kontrolmål (SMART)	Revisionshandlinger ved udført revision	Resultat af udført revision
Udfyldes af NSIS anmelder	*Udfyldes af NSIS anmelder*	*Udfyldes af revisor*	*Udfyldes af revisor*
Udfyldes af NSIS anmelder	*Udfyldes af NSIS anmelder*	*Udfyldes af revisor*	*Udfyldes af revisor*
Udfyldes af NSIS anmelder	*Udfyldes af NSIS anmelder*	*Udfyldes af revisor*	*Udfyldes af revisor*

Lokal IdP og NSIS krav

- En organisation med Lokal IdP vil som regel både agere som:
  - Udsteder af lokale identifikationsmidler (elektronisk identifikationsordning) [NSIS kap. 3, 4, 5]
  - Identitetsbroker (formidling af autentificerede brugere) [NSIS kap. 4, 6]
- Dvs. det er alle kravene i NSIS, der vil være relevante.

Lokal IdM og NSIS krav

- Brugerorganisationer kan vælge at tilslutte et lokalt IdM-system til NemLog-in.
- Med et lokalt IdM-system kan erhvervsidentiteter håndteres lokalt og synkroniseres til NemLog-in's erhvervsløsning.
- Der er to modeller for IdM-løsninger med hver sine NSIS krav:
  - "Lokal IdM light" er en model, hvor brugerorganisationen ikke udsteder egne identifikationsmidler. Denne model kræver ikke NSIS anmeldelse, men blot overholdelse af specifikke sikkerhedskrav.
  - "Fuld Lokal IdM", hvor brugerorganisationen også udsteder identifikationsmidler (dvs. kombination af Lokal IdM og IdP). Denne model kræver NSIS anmeldelse.

NSIS ikrafttræden

Ikrafttræden – hvor og hvornår

- I OIOSAML 3 mod Tjenesteudbydere ved Go-live (mulighed)
- Ved tilslutning af Brugerorganisation efter Go-live (krav)
- Niveau Høj for personer bliver først muligt efter MitID Go-live

NSIS dokumenter

- Standarden (2.0.1)
- Vejledning til standarden (2.0.1a)
- Revisionsvejledning
- Skema til revisionsvejledning (Excel)
- Skabelon til anmeldelse

Til *udbydere* af identiteter

- Vejledning til tjenesteudbydere
- Støtte til TU's risikovurdering

Til *aftagere* af identiteter

Live spørgsmål fra deltagerne

Live spørgsmål fra deltagerne

Emne 1

Risikovurdering af tjenester

Emne 2

Implementering af sikringsniveauer

Emne 3

Anmeldelse af Lokal IdP

Emne 4

Implementering af NSIS i praksis

Implementerings- og kommunikationsaktiviteter

- **NemLog-in portalen:** www.nemlog-in.dk
  - Målgruppeopdelt information for brugerorganisationer, offentlige og private tjenesteudbydere
  - Vejledninger, teknisk dokumentation, testmiljø mv.
  - Kommende webinar 14. maj om referenceimplementeringer, opslagstjenester, den nye signeringskomponent og erstatningen til PID/RID

- **Digitaliseringsstyrelsens** implementeringssite
  - Relevant information om overgangen til MitID og NemLog-in
  - Implementeringsværktøjer: Screeningsværktøj, ordbog, mv.

- **Nyhedsbreve**
  - Nyt om NemLog-in: Tilmeld dig her
  - Nyt om overgangen til NemLog-in3 og MitID: Tilmeld dig her

- **NSIS-standarden:** Læs mere her

DIGITALISERINGSSTYRELSEN

Tak for i dag

Christian Schmidt-Madsen

Digitaliseringsstyrelsen

Thomas Gundel

Ekstern konsulent