DIGITALISERINGSSTYRELSEN

NSIS

Februar 2020

Hvad er NSIS?

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

- 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

Tjenesteudbydere

- Udbydere af forretningstjenester (selvbetjeningsløsninger); fx borger.dk

Brugerorganisationer

- Organisationer der ønsker at udstede erhvervsidentiteter til deres medarbejdere

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

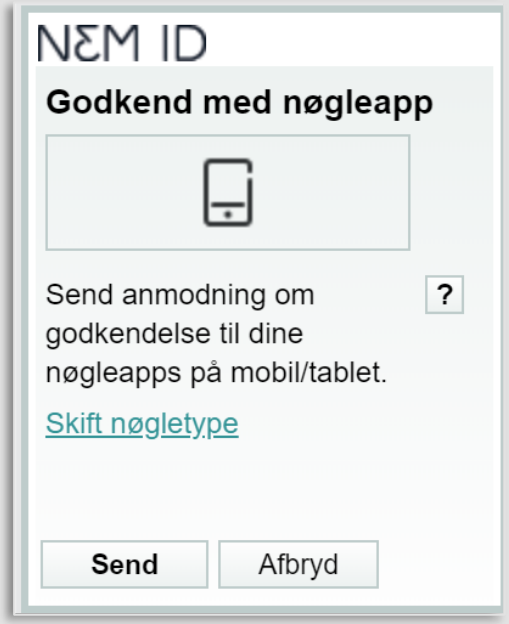
- ID-tjenester skal leve op til en række forskellige krav.
- Kravene går på tekniske-, organisatoriske- og juridiske aspekter og dækker bredt risici ved identitetshåndtering.
- Vigtigste processer, som reguleres i NSIS:
  - Identitetssikring (fysiske personer, juridiske personer og forbindelser mellem 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.

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

NSIS-dokumenter på Digst.dk og Digitaliser.dk

- 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

Til *aftagere* af identiteter

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.
- Gennemsnitlig på krav til brugergruppes sikringsniveau.

- Inspiration i "Vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere".
- Digitaliseringsstyrelsen arbejder på et støtte-værktøj til fastsættelse af sikringsniveau.

Tjenesteudbydere

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”.
- Digitaliseringsstyrelsen arbejder på et støtte-værktøj til fastsættelse af sikringsniveau.

DIGITALISERINGSSTYRELSEN

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 [illegible] som identitetsgarant.

Virksomhed står kun på mål for kobl[illegible]mellem fysisk person og virksomhed.

Styrket kontrol med [illegible] virksomheder som brugerorganisationer.

[illegible]el identitetssikring med privat eID.

Brugerorganisationer

DIGITALISERINGSSTYRELSEN

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 eID.

Implementerings- og kommunikationsaktiviteter

- **NemLog-in portalen:** www.nemlog-in.dk
  - Målgruppeopdelt information for brugerorganisationer, offentlige og private tjenesteudbydere.
  - Vejledninger, teknisk dokumentation, testmiljø mv.

- **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