Digdir

Oppfølging av avvik knytt til BankID

Informasjonsmøte for alle verksemder
2026-04-15

Agenda

- Kort status
- Teknisk behandling av sikkerheitsnivå i ID-porten
- Risikovurdering av tenester i ID-porten
- Trusler og sårbarheiter ved ulike sikkerheitsnivå etter *Identifikasjonsnivåforskriften*
- Kva gjer de som kundar i ID-porten no?

Digdir

Digdir

Kort status

Bakgrunn

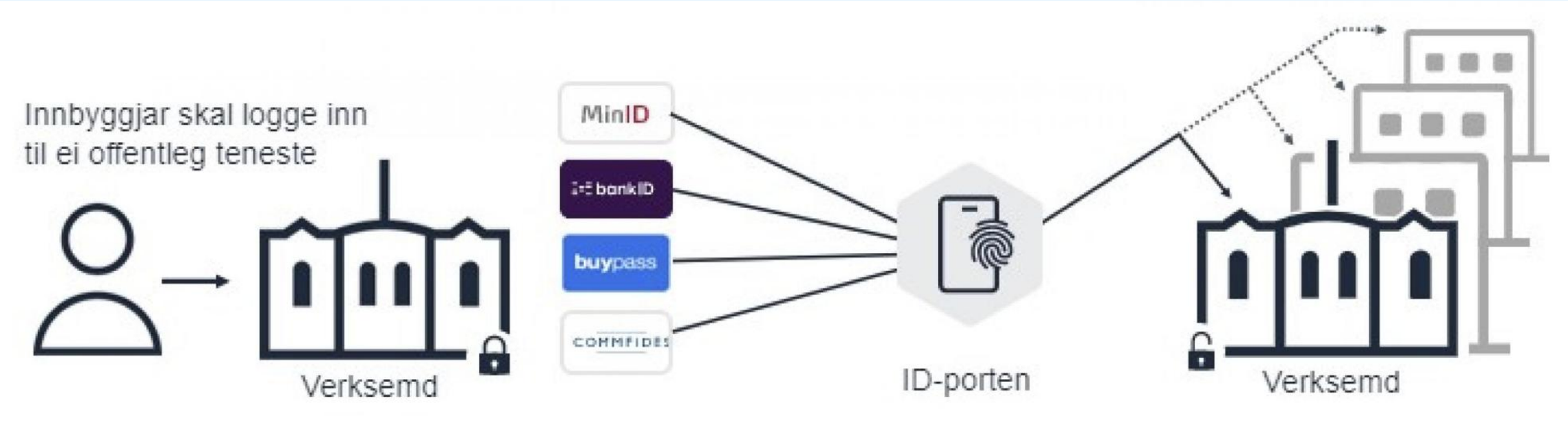
- NKOM har varsla at BankID kan miste godkjenninga si på sikkerheitsnivå “høgt”:

> *– BankID har hatt avvik knyttet til utsendelse av kodebrikken over flere år, og det er deres ansvar å passe på at de følger regelverket. Nkom har over lang tid informert og veiledet aktørene slik at de forstår hva de må utbedre for å være i tråd med lovverket.*
>
> *Bankene har nå fire uker på seg til å dokumentere at de tilfredsstiller kravet til sikkerhetsnivå “høyt”. Dersom det ikke skjer, vil BankID tas av listen over godkjente eID for det høyeste sikkerhetsnivået.*
>
> *Et eventuelt vedtak kan påklages til Digitaliserings- og forvaltningsdepartementet.*

Digdir

https://nkom.no/aktuelt/bankid-kan-miste-godkjenning-pa-hoyeste-sikkerhetsniva

Korleis er det i dag?



Digdir

Kva kan skje ?

- Digdir har avtale med BankID om bruk av eID på nivå høgt.

- A: BankID vert verande på nivå høgt
- B: BankID sjølvdeklarerer seg til nivå betydeleg
- C: BankID vert ikkje lenger tilgjengeleg i ID-porten

- (AB: BankID sine brukarar vert separert mellom betydeleg og høgt)

Digdir

Kva bør du gjere no ?

1. **Utføre risikovurdering.** Kan de kan endre sikkerheitsnivå på tenestene dykkar frå høgt til betydeleg?

2. **Analysere teknisk omfang** ved å endre tenestene. Kva må de førebu lokalt? Treng de støtte til dette?

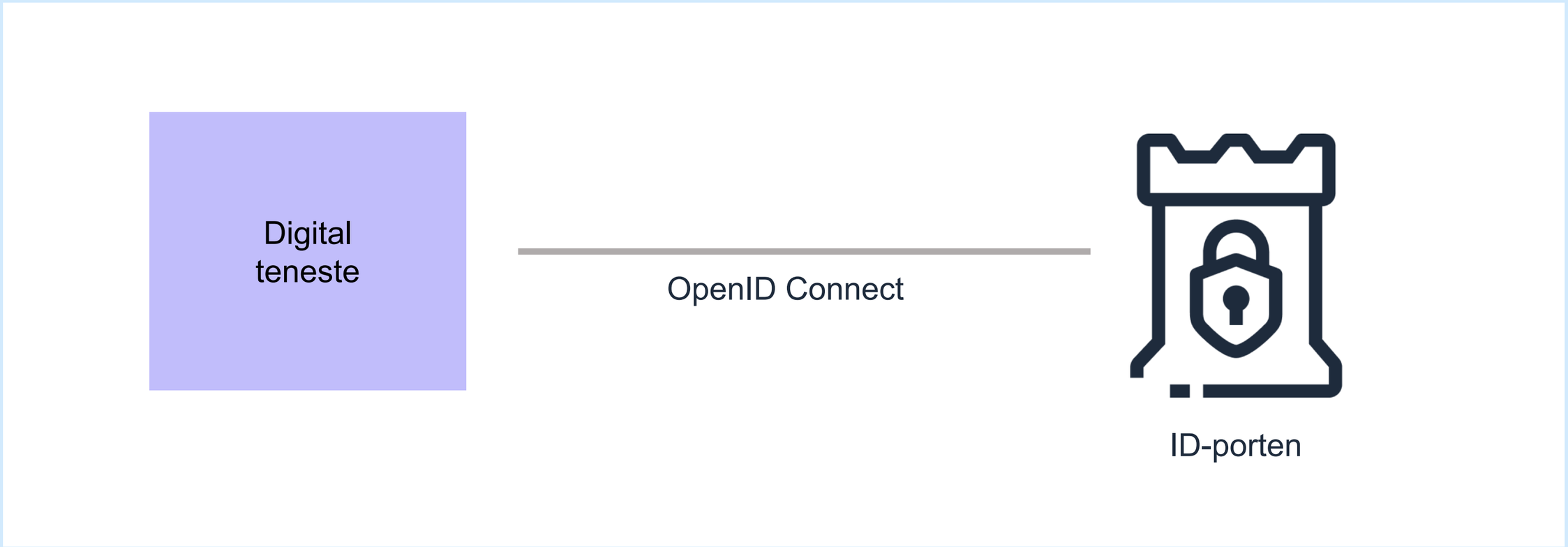
3. **Melde attende** til Digdir kva tenester som treng vere på nivå høgt, innan 20 april.

Digdir

Digdir

Teknisk behandling av sikkerhetsnivå

Integrasjon med ID-porten



Digdir

Teknisk flyt:

- Tenesta **førespør innlogging** på eit bestemt sikkerheitsnivå

- ID-porten viser potensielle eIDer som tilfredstiller førespurnad (selector)
- **Innbygger velger sin eID**
- **Innbygger autentiserer seg** hjå eID-leverandør

- Tenesta mottek innloggingspåstanden (id-token)
- **Teneste skal validere** at informasjonen i påstanden stemmer med det som vart førespurt.

Digdir

Teknisk flyt:

- Tenesta **førespør innlogging** på eit beste
- ID-porten viser potensielle eIDer som
- Tenesta mottek innloggingspåstanden

Sikkerheitsnivå er ein **dynamisk** parameter :

- ei teneste kan lett delast opp i “betydeleg” del og ein “høg” del
- ei teneste kan be om “step-up” etter eigen kontekst, td.
  - ved bestemte, viktige handlingar,
  - ved deteksjon av unormal aktivitet
- også mogeleg å be om tvungen re-autentisering

Kunde BER om sikkerheitsnivå.

Kunde MOTTEK både sikkerheitsnivå og metode.

Sikkerheitsnivå **acr** (Authentication Context Class Reference)	**Innloggingsmetode(r)** **amr** (Authentication Methods References)
idporten-loa-high	BankID
	Buypass
	Commfides
idporten-loa-substantial	Minid-APP
	Minid-OTC
	Minid-TOTP

Digdir

Digdir

Risikovurderinger

Ansvar

Virksomheten selv

Vurdere og gjennomføre analyser og tiltak

Digdir

Veilede og bidra med informasjon

Digdir

Hva krever sikkerhetsnivå høyt?

- Det finnes ingen faktiske regulatoriske krav som peker på noe sikkerhetsnivå.
- I praksis ligger derfor vurderingene til den enkelte virksomhet, og hvordan denne vurderer tjenestene og informasjonen som ligger bak autentiseringen.
- Digdir har i sin veileder likevel gitt noen eksempler på hvordan det ***kan*** brukes.
  - **Nivå lavt**: Innsyn i egne lekser mm, innsending av skjema (barnehagesøknad etc.), statistikkoppgaver.
  - **Nivå betydelig**:Taushetsbelagte opplysninger, blant annet innsyn og endring i egen skattemelding.
  - **Nivå høyt**: Taushetsbelagte opplysninger med særlig beskyttelsesbehov, herunder stigmatiserende opplysninger, forretningskritisk informasjon, sikkerhetskritisk informasjon og helseopplysninger.

Danmark har alt på betydelig

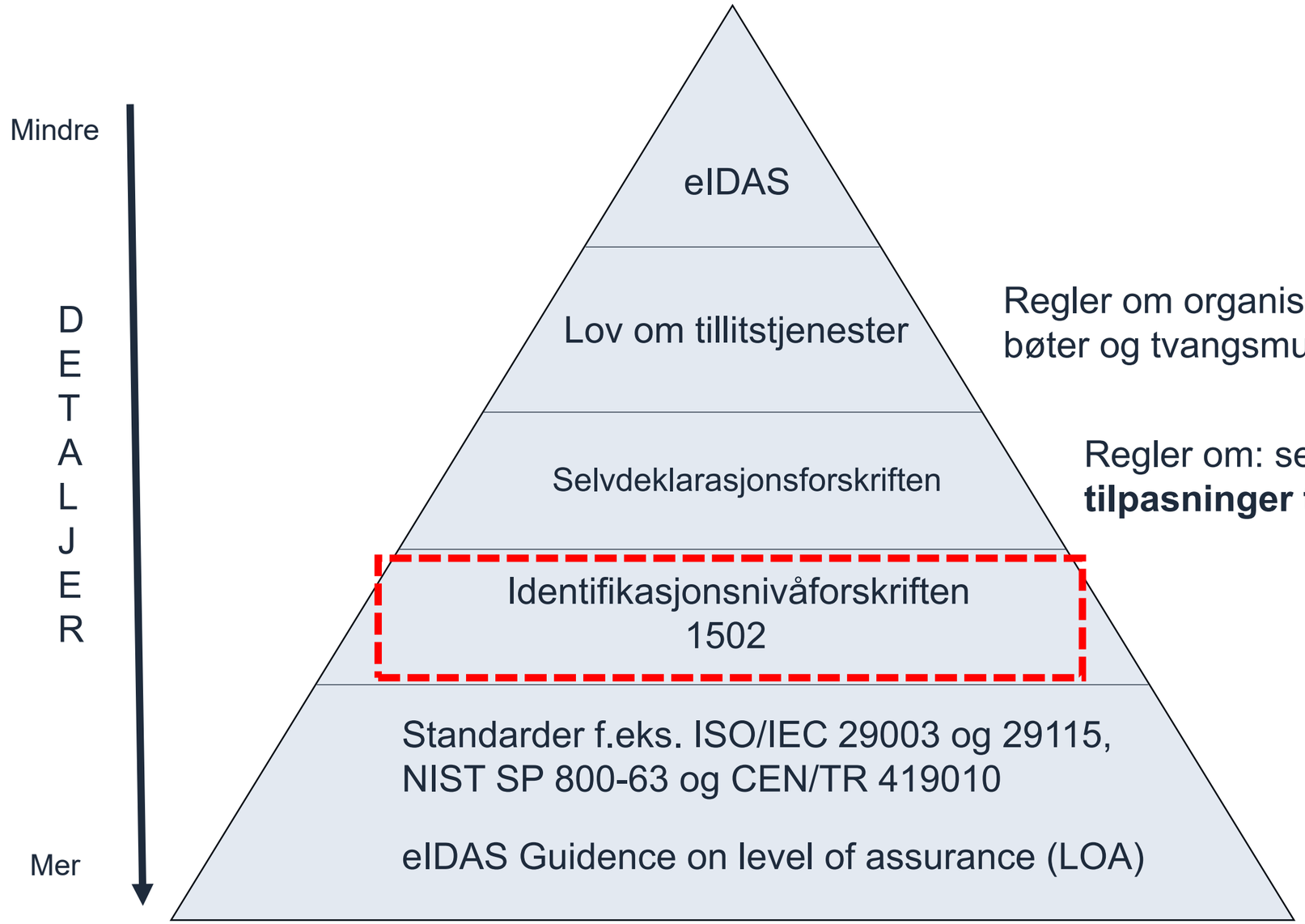
- I Danmark er tjenestene vurdert til å kreve nivå betydelig.
  - Det inkluderer danske digitale helsetjenester
- MitID utstedes stort sett på nivå betydelig
  - Høyt er mulig i enkelte kommuner

Digdir

Digdir

Om sikkerheitsnivåer
LoA

Regelverket for sikkerheitsnivå



Regler om organiseringa i Norge, t.d:
bøter og tvangsmulkt, klage, etc..

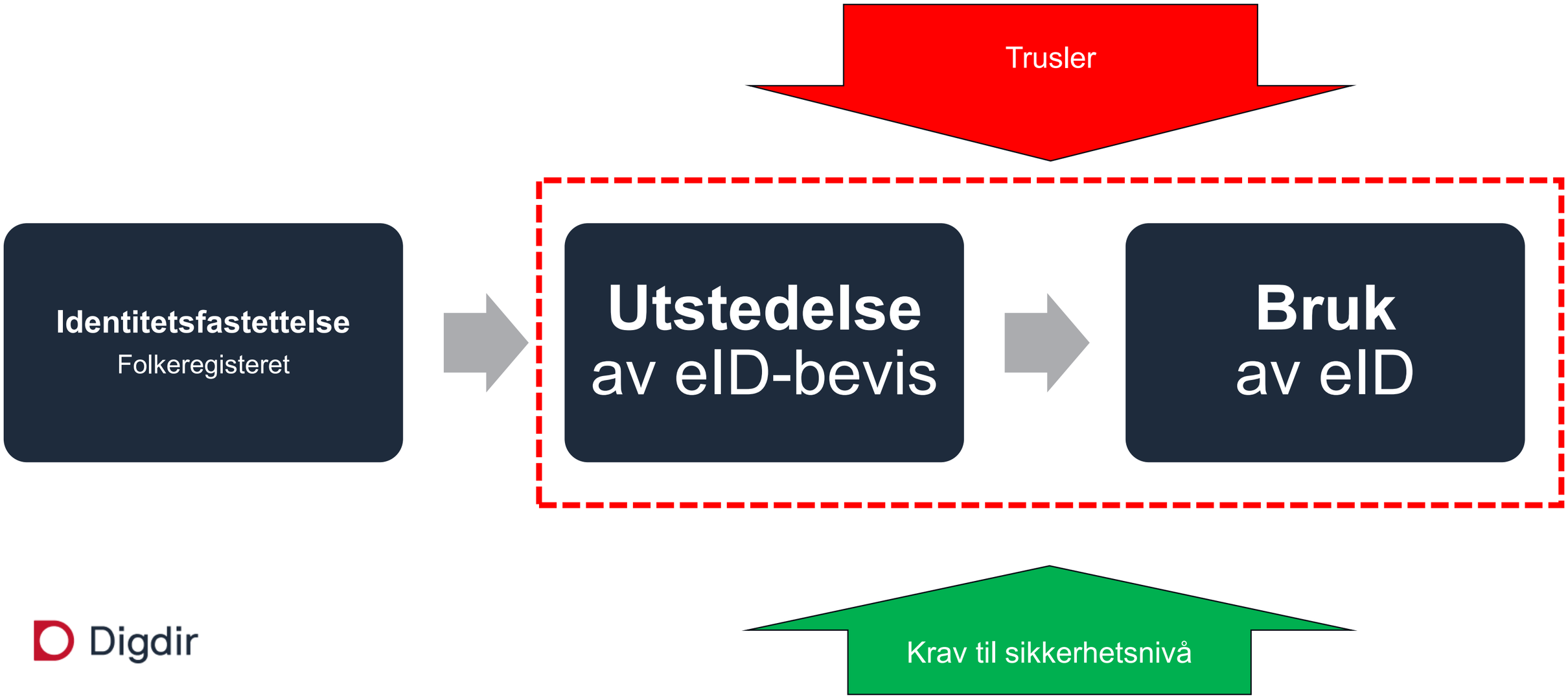
Regler om: selvdeklarasjon, tilsyn, **nasjonale tilpasninger til sikkerhetsnivåene**

Eksempler på krav i 1502:

Nivå	Krav utstedelse, levering, aktivering (2.2.2)
Lav	Identifikasjonsmiddelet utleveres via en mekanisme som gjør at det kan **antas at det bare leveres til den tiltenkte personen**
Betydelig	Identifikasjonsmiddelet utleveres via en mekanisme som gjør at det kan **antas at det bare leveres til dets eier**
Høyt	**Aktiveringsprosessen kontrollerer** at identifikasjonsmiddelet **ikke er levert til andre enn dets eier**

Digdir

eID i ulike faser - livssyklus



Digdir

Identifikasjonsnivåforskriften 1502, struktur

2.1 Registrering

2.2 Håndtering av elektroniske identifiksasjonsmidler

2.3 Autentisering

2.4 Organisering

Digdir

Identifikasjonsnivåforskriften 1502 – 2.1

2.1 Registrering

Søknad
2.1.1

ID-kontroll
2.1.2

2.2 Håndtering av elektroniske identifikasjonsmidler

2.3 Autentisering

2.4 Organisering

Digdir

Identifikasjonsnivåforskriften 1502 – 2.2

2.1 Registrering

Søknad
2.1.1

ID-kontroll
2.1.2

2.2 Håndtering av elektroniske identifikasjonsmidler

2.2.2 Utstedelse, levering og aktivering

2.2.3 Tilbakekalling

2.2.3 reaktivering

2.2.3 Midlertidig oppheving

2.2.1 Egenskaper og utforming Autentiseringsmidler

2.3 Autentisering

2.4 Organisering

Digdir

Identifikasjonsnivåforskriften 1502 – 2.3

2.1 Registrering

- Søknad 2.1.1
- ID-kontroll 2.1.2

2.2 Håndtering av elektroniske identifikasjonsmidler

- 2.2.2 Utstedelse, levering og aktivering
- 2.2.3 Tilbakekalling
- 2.2.3 reaktivering
- 2.2.3 Midlertidig oppheving
- 2.2.1 Egenskaper og utforming Autentiseringsmidler

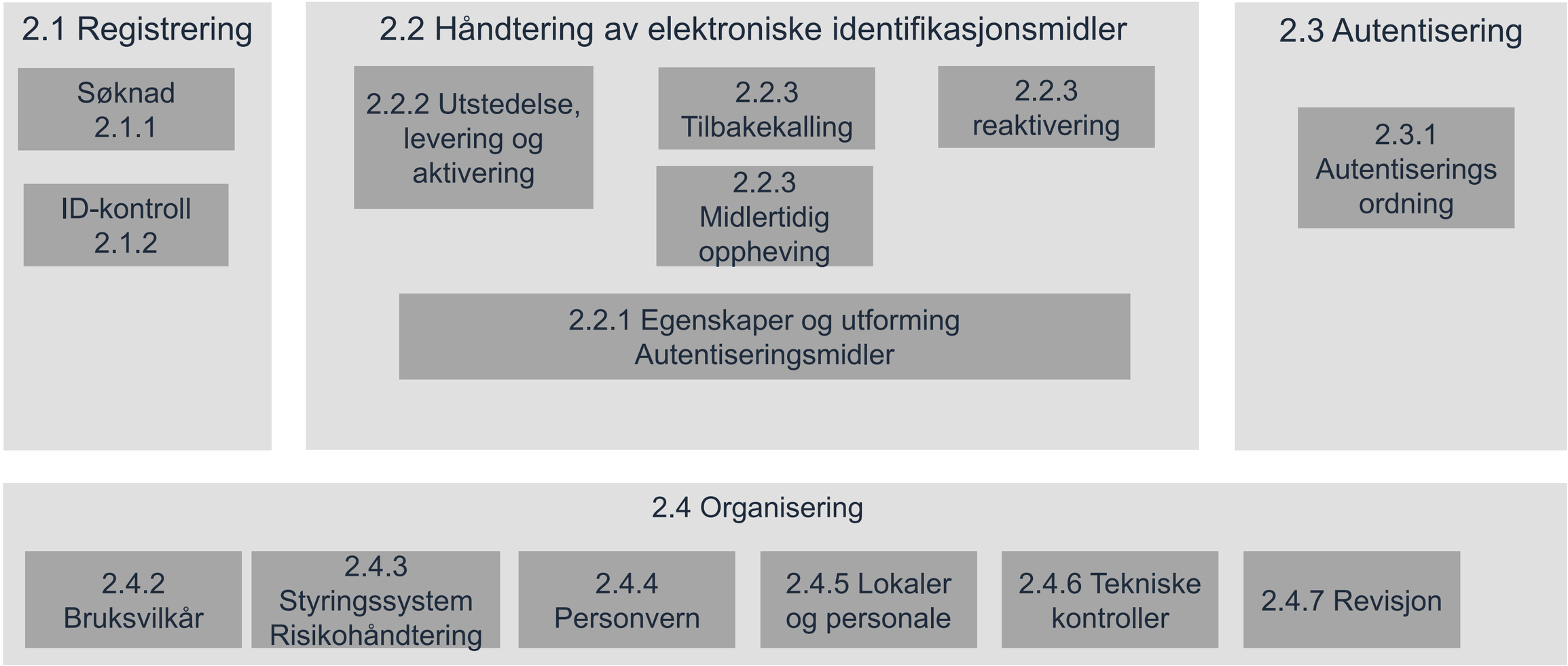
2.3 Autentisering

- 2.3.1 Autentiserings ordning

2.4 Organisering

Digdir

Identifikasjonsnivåforskriften 1502 – 2.4



Digdir

Kva skil nivåa ?

2.1 Registrering

Søknad
2.1.1

ID-kontroll
2.1.2

Fysisk oppmøte

Norsk tilpassing:
Post til folkeregistrert adresse

2.2 Håndtering av elektroniske identifiksasjonsmidler

2.2.2 Utstedelse, levering og aktivering

Aktiveringsprosessen kontrollerer at det elektroniske identifikasjonsmiddelet ikke er levert til andre enn dets eier.

via en mekanisme som gjør at det kan antas...

2.2.3 reaktivering

2.2.3 Tilbakekalling

2.2.3 Midlertidig oppheving

2.2.1 Egenskaper og utforming, Autentiseringsmidler

“...eieren [kan] på en sikker måte ... hindre at det blir brukt av andre”.

«...bare kan brukes dersom eieren har kontroll over eller er i besittelse av det»

2.3 Autentisering

2.3.1
Autentiseringsordning

høy angrepskapasitet

moderat angrepskapasitet

2.4 Organisering

2.4.2 Bruksvilkår

2.4.3 Styringssystem
Risikohåndtering

2.4.4 Personvern

2.4.5 Lokaler og personale

2.4.6 Tekniske kontroller

2.4.7 Revisjon

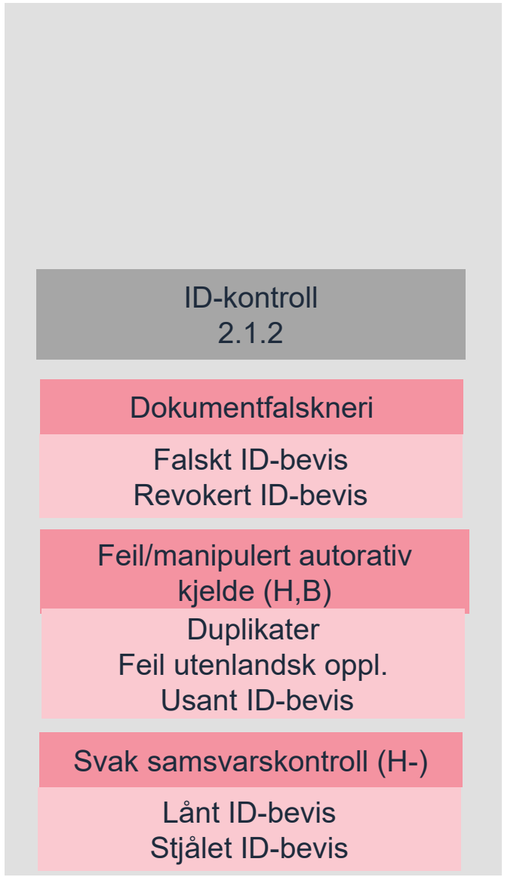
jevnlig ekstern revisjon

Digdir

høgt

betydelig

Høg vs. betydeleg : 2.1.2 ID-kontroll



Dokumentfalsk: vurdert som lav risiko (for norske dokumenter)

- Risikobildet er nok større for utanlandske id-dokument
- Men for “betydeleg”: i Norge blir det som hovedregel ikkje kontrollert noko i id-dokument (sender noko i posten istaden)

Manipulere Folkeregisteret: lav risiko, og lik for begge sikkerheitsnivå

Samsvarskontrollen:

- Betydeleg: norsk tilpassing betyr at det i praksis ikkje blir utført noko kontroll av person opp mot eit dokument. Trusselen blir om brukeren har kontroll på eigen postkasse ? (neste slide)
- Høgt: Varierande kvalitet på post-i-butikk-kontrollen

Digdir

Trussel | Døme

Høg vs. betydeleg : 2.2.2 utlevering og aktivering

På høgt: kravet (“..kontroller at...”) gjer at risikoen er knytt til kvaliteten på kontroll-mekanismen. Vanskeleg å seie noko generelt om, men id-kontroll er jo ein opplagd og mogeleg kontrollmekanisme, og då vil truslane dokumentfalsk og samsvarskontroll kome opp att her.

På “betydeleg” så har me 3 truslar knytt til postgang ved bruk av norske tillegget. Desse kan utnyttast typisk av nærståande.

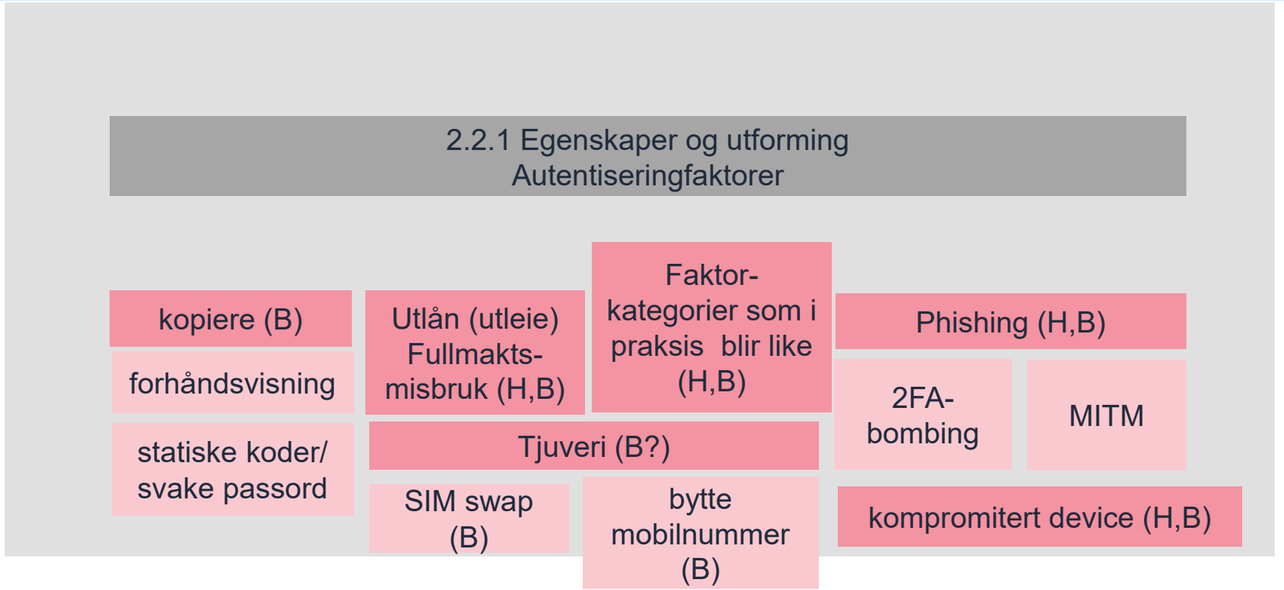
Digdir

Trussel | Døme

Høg vs. betydeleg : 2.2.1 eigenskapar

2.2 Håndtering av elektroniske identifiksasjonsmidler

Betydelig	• **Minst 2 autentiseringsfaktorer** fra ulike kategorier • Utformet slik at det **antas** at det bare kan brukes dersom eieren har kontroll
Høyt	Kravene til betydelig, samt: • Identifikasjonsmiddelet er **beskyttet mot kopiering og manipulering**, og **mot angripere med høy angrepskapasitet** • Identifikasjonsmiddelet er utformet slik at eieren på en **sikker måte kan hindre** at det blir brukt av andre



- Nokre faktorer (som SMS) klarar ikkje oppnå krava til høgt
- Phishing og utlån blir i liten grad hindra noko særleg av høgt-krava

Digdir

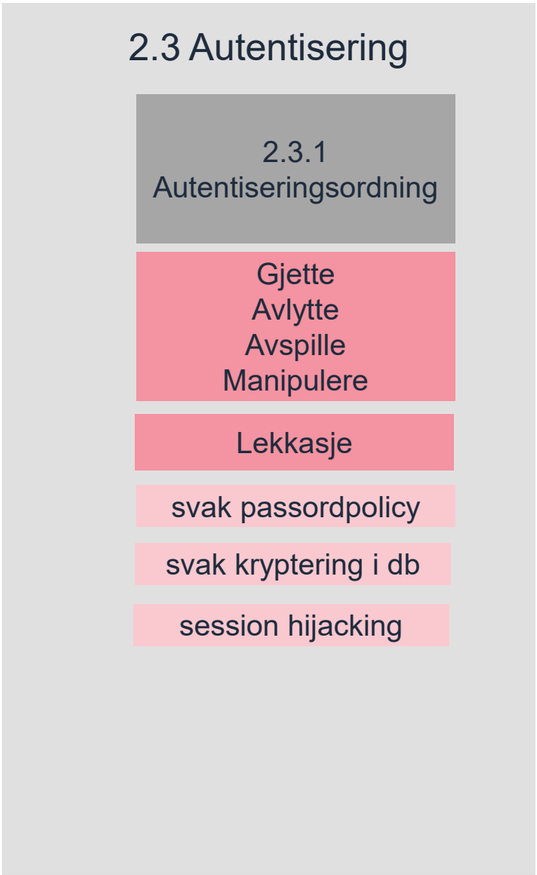
Trussel | Døme

Høgt vs betydeleg: 2.3.1

- Høg angrepskapasitet er typisk APT / fremmed makt-type aktørar

⇒ klar skilnad på sikkerheitsnivåa

  - etterlevelse vil då verte handtert gjennom ekstern revisjon på “høgt”
  - Ei betydeleg-løysing bør likevel demonstrere at dei føl beste praksis, og tiltaka mot slike truslar er typisk “no-brainere”. Men ingen krav til ekstern revisjon som kan bevise dette.



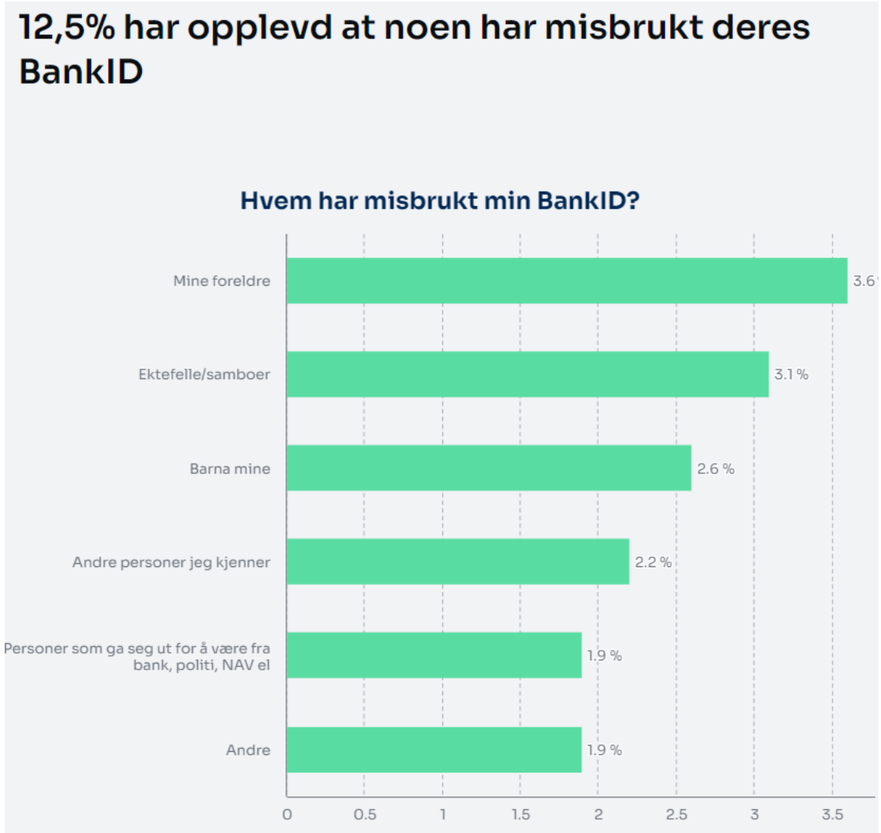
høy angrepskapasitet

moderat angrepskapasitet

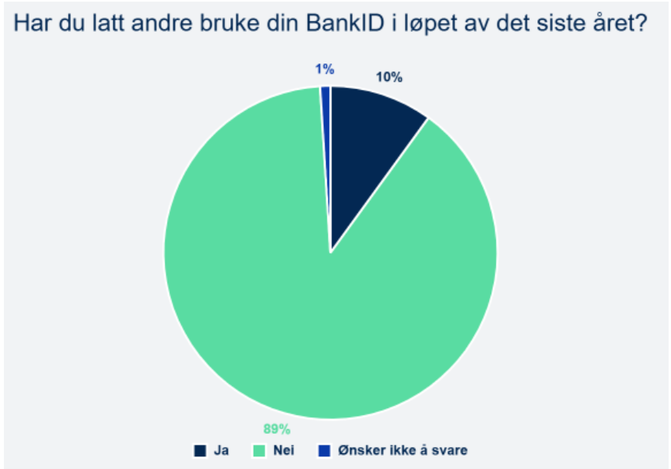
Digdir

Trussel | Døme

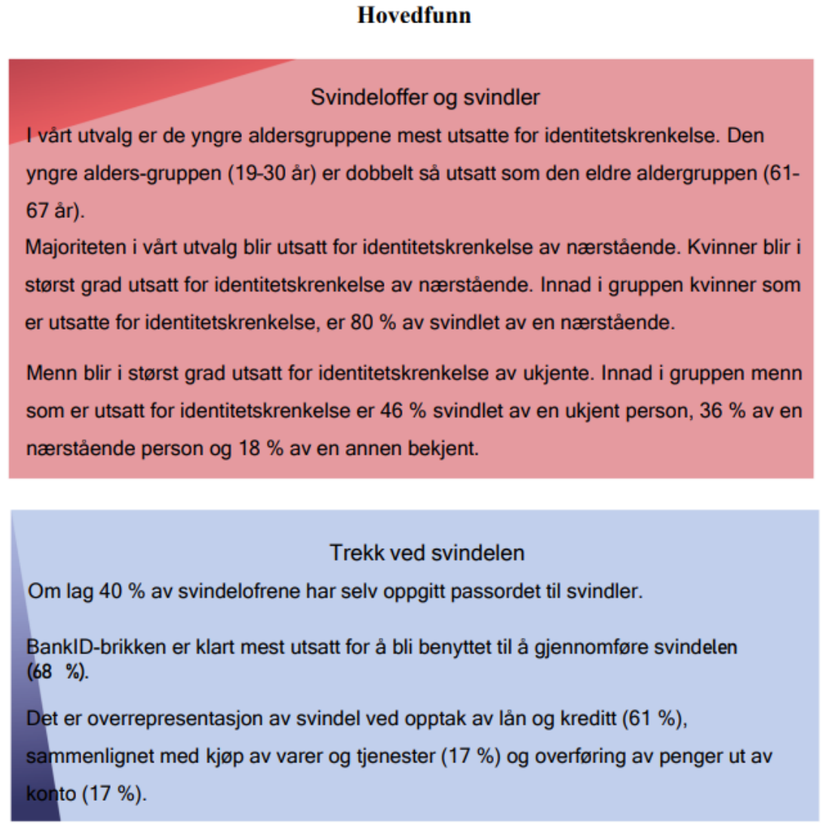
Størst risiko i bruksfasen: Mellommenneskelige forhold



NORSIS, "Nordmenn og digital sikkerhetskultur" (2023)



NORSIS, «Elektronisk ID og svindel" (2024)



UIO, "Rapport om misbruk av eID", SODI 1/22 (2022)

Digdir

Oppsummert

- Det er ingen regulatoriske krav til hvilket sikkerhetsnivå en gitt tjeneste må være på
- Den største forskjellen mellom "Høyt" og "Betydelig" er kravet om fysisk oppmøte for utstedelse.
  - I tillegg skal “Høyt” beskytte mot kapasitet tilsvarende “fremmed makt”
  - En eID på “Betydelig” – vil være mer utsatt for ID-tyveri i nære relasjoner, pga postgang (og litt pga. sms)
- Erfart misbruk er størst i bruksfasen og i nære relasjoner
  - Dette må adresseres med andre typer av tiltak – uavhengig av eID

Digdir

Digdir

Kva bør de som kundar i ID-porten gjere no?

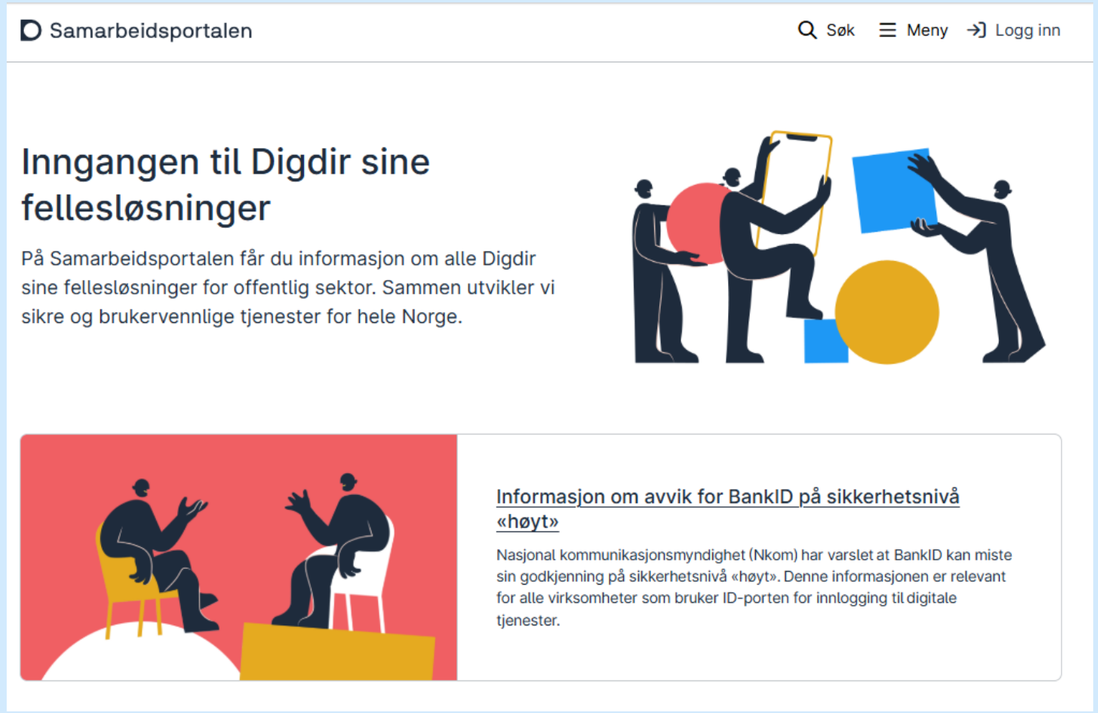
Kva bør de som kundar i ID-porten gjere no?

- **Gjennomfør ny risikovurdering** for dykkar tenester
  - Er det tilstrekkjeleg med sikkerheitsnivå betydeleg?
- **Sett ned sikkerheitsnivået** til betydeleg dersom risikovurderinga tilseier det
- Meld tilbake til oss dersom de **framleis har tenester på sikkerheitsnivå høgt**
  - Tilbakemeldingsskjema
  - Frist måndag 20. april

Digdir

Informasjon på Samarbeidsportalen

- Hald dykk oppdatert på saka på Samarbeidsportalen
- Spesielt viktig informasjon blir sendt til varslingspunkt for ID-porten
  - Alle kunder bør vere registrert med varslingspunkt



Digdir

Kontaktpunkt

Servicedesk

E-post: servicedesk@digdir.no

Digdir

Digdir

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Havnegata 48, 8900 Brønnøysund
Skrivarvegen 2, 6863 Leikanger
Lørenfaret 1C, 0580 Oslo