

Bedre digitale tjenester i kommunesektoren ved hjelp av nasjonal digital infrastruktur

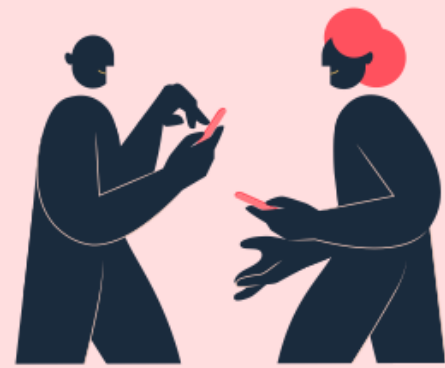
Digitaliseringsdirektoratet
Bodhild Therese Cirotzki

Digdir filmen

Våre målgrupper



Stat og kommune



Innbyggere



Næringsdrivende



Frivilig sektor

Virksomheter har ofte felles behov og utfordringer

- Samme funksjonalitet utvikles i hundrevis av versjoner, med ulik kvalitet, ulik sikkerhet og ulikt vedlikehold.
- Uten felles standard må hver virksomhet selv bygge og vedlikeholde egen sikkerhetsinfrastruktur.
- Innbyggere og næringsliv møter ulike innlogginger, skjema og kanaler fra tjeneste til tjeneste.

Når offentlige virksomheter løser de samme grunnleggende behovene hver for seg, får vi unødvendig dobbeltarbeid, ujevn sikkerhet og en fragmentert brukeropplevelse for innbyggere og næringsliv.

Tillit er essensielt

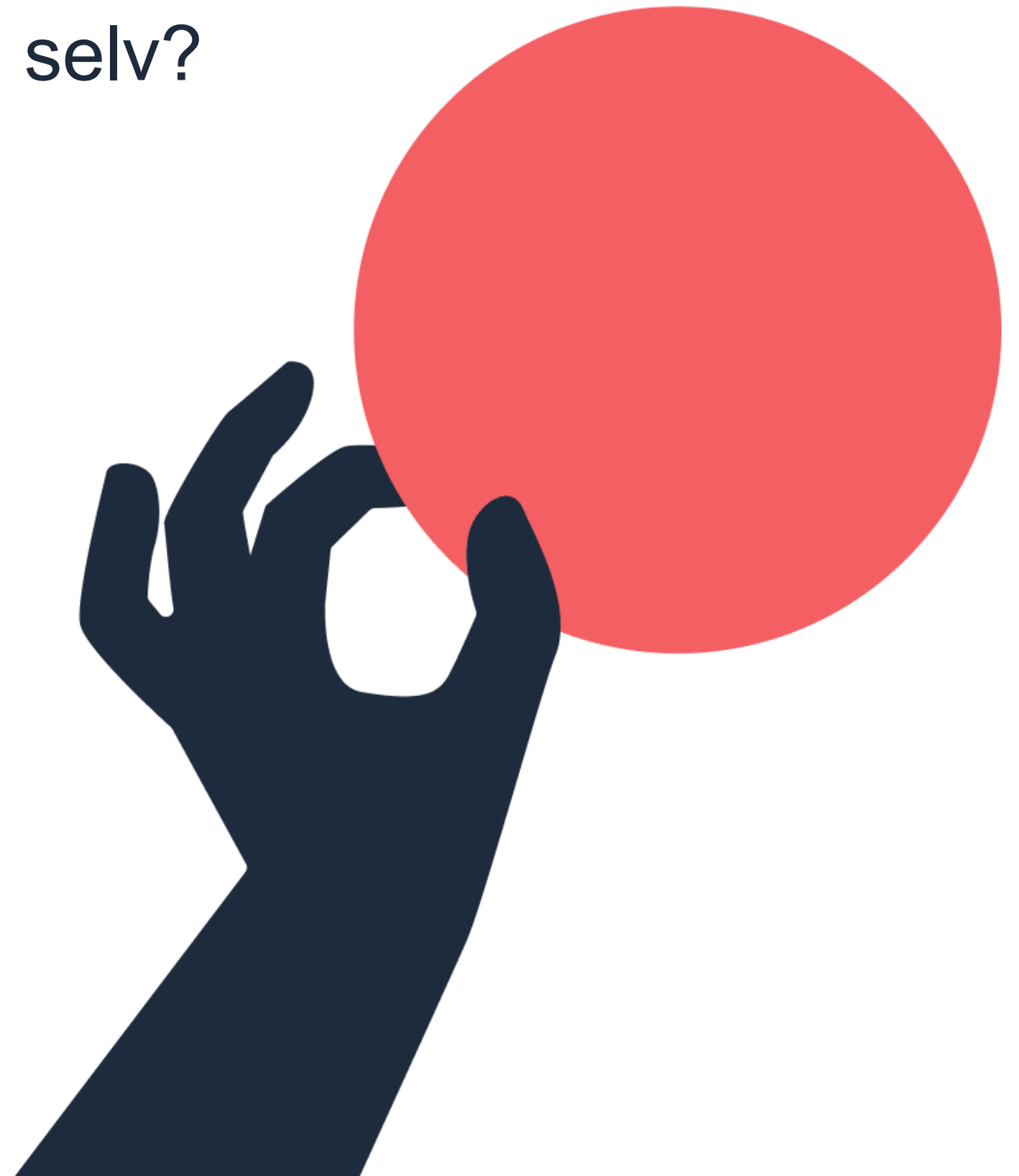
- Er du den du sier at du er?
- Har du rett til å handle på vegne av andre?
- Kommer meldingen faktisk fra den avsenderen den oppgir?
- Kan vi i ettertid dokumentere hva som skjedde og når?

Dette er spørsmål vi må kunne svare på for at digitale tjenester skal være trygge og til å stole på.



Hvorfor kan ikke alle bare løse dette selv?

- Vi må beskytte informasjonen
- Folk må kjenne seg igjen
- Vi bør ikke løse det samme problemet igjen og igjen
- Vi må kunne finne ut hva som har skjedd
- Vi må være klare til å følge med når verden endrer seg



Det vi tar for gitt

- At vi kan logge inn
- At informasjon når riktig mottaker
- At vi kan handle på vegne av en virksomhet
- At vi vet hvem som har gjort hva

Men det er ingen selvfølge

- Det fungerer fordi noen har tatt ansvar for de grunnleggende behovene på vegne av fellesskapet
- Fordi vi har valgt å løse dem sammen og ikke hver for oss

Gevinstene fellesløsningene gir oss

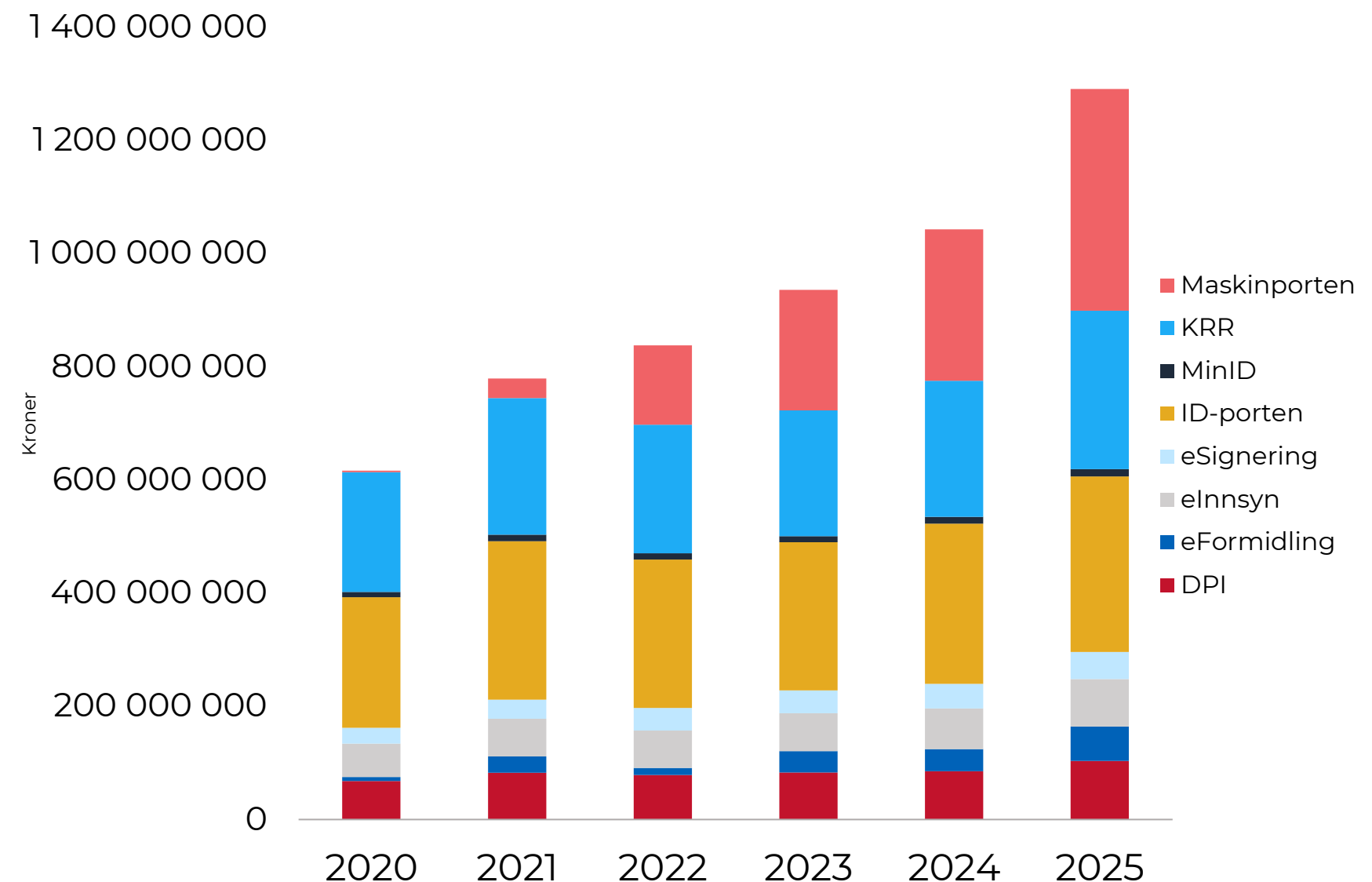
- Tryggere tjenester
- Enklere å utvikle nye tjenester
- Mindre dobbeltarbeid i offentlig sektor
- Enklere og mer forutsigbart møte med det offentlige

Fellesløsningene er mer enn tekniske komponenter i bakgrunnen, de er en del av grunnmuren for en offentlig sektor som skal være trygg, effektiv og til å stole på.

1,3 mrd. kr i årlige gevinster i 2025

- +23 % vekst fra 2024
- Veksten drives av økt bruk

Historiske gevinster av Digdir sine fellesløsninger

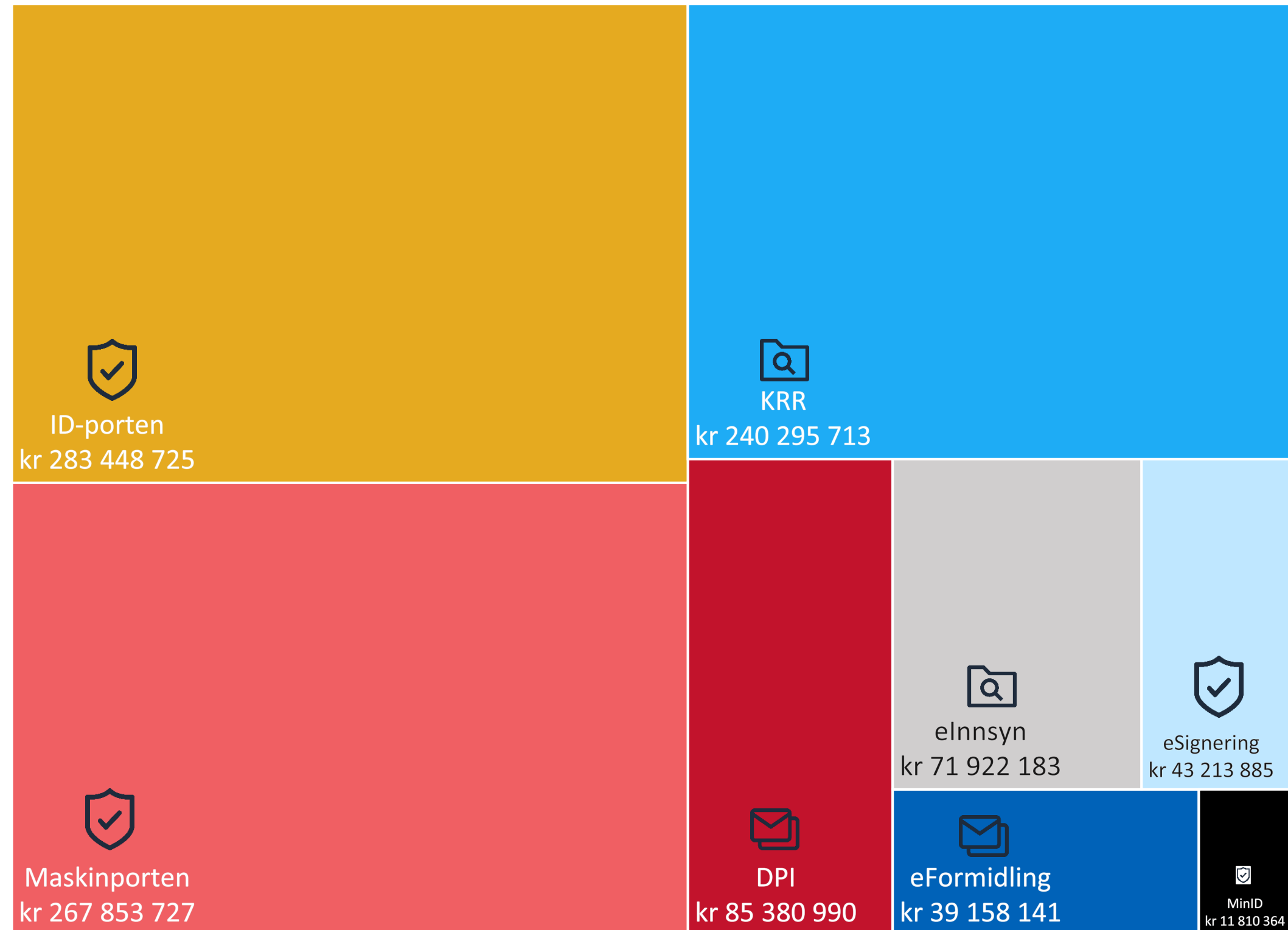


Hvor kommer verdien fra?

- 3 løsninger står for over 75 % av gevinstene
- Infrastruktur skaper stordriftsfordeler

Prissatte virkninger for fellesløsningene i 2025 (Totalt: 1 291 000 000 kr)

■ DPI ■ eFormidling ■ elnnsyn ■ eSignering ■ ID-porten ■ MinID ■ KRR ■ Maskinporten



Hva betyr det i praksis?

Offentlig sektor

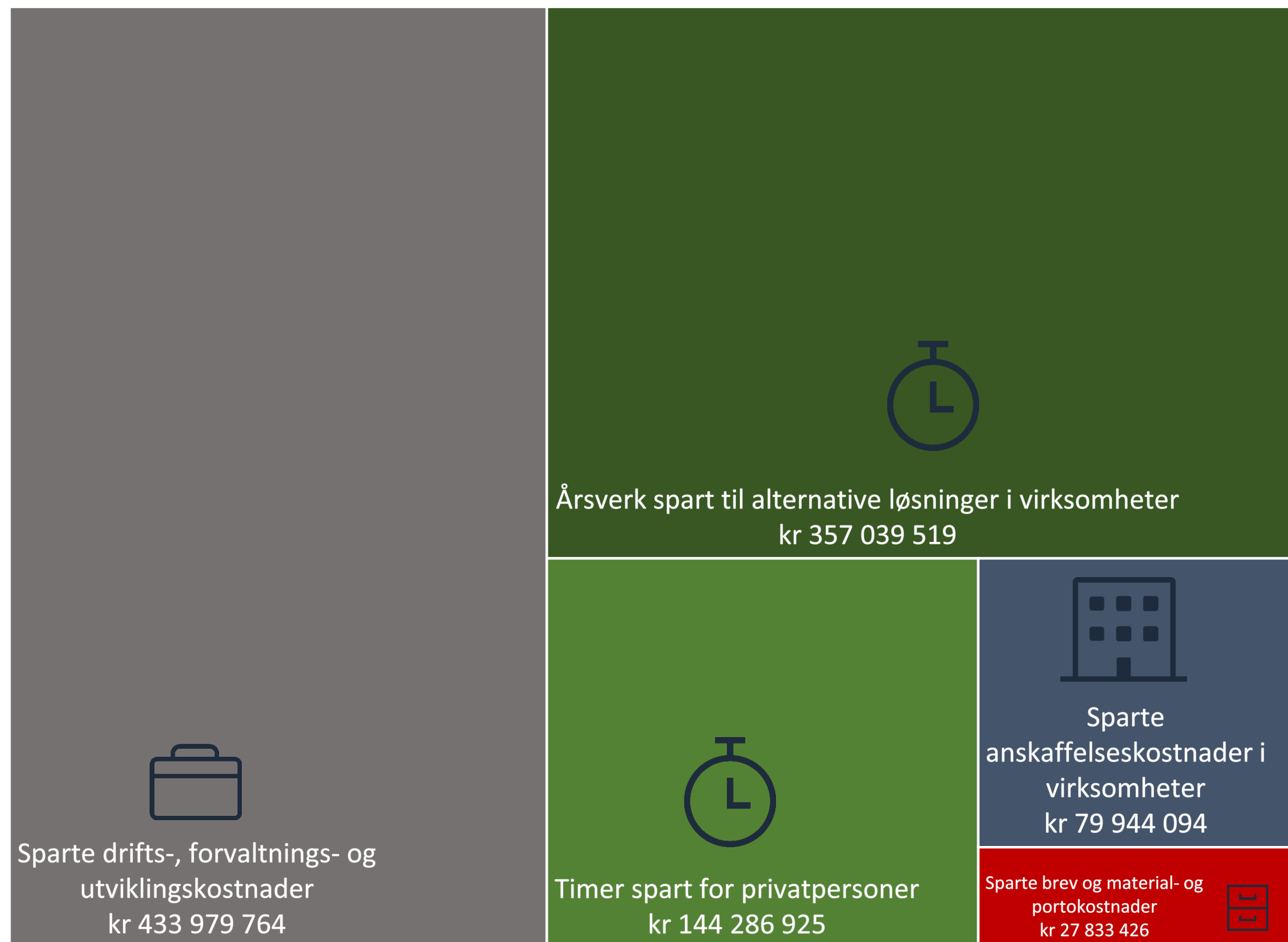
- 564 årsverk spart
- 519 mill. i reduserte driftskostnader

Innbyggere

- 452 000 timer spart



Gevinsttype til fellesløsningene i 2025 (Totalt: 1 291 000 000 kr)



Digdir forvalter 20 digitale fellesløsninger

- Fellesløsningene dekker felles behov i forvaltningen og skaper store samfunnsøkonomiske gevinster*
- Sentrale løsninger er ID-porten, Maskinporten, Altinn, Kontakt- og reservasjonsregisteret, ELMA, eFormidling m.fl.
- Er en viktig del av offentlig digital infrastruktur

**) 1,3 mrd kr. i 2025 eks. Altinn (Oslo Economics 2026)*

Brukes av over 1500 offentlige virksomheter i over 8.000 tjenester.

Over 330 mill. innlogginger gjennom ID-porten.

(Digdirs årsrapport 2025)





Altinn
autorisasjon



Altinn
formidling



Altinn
melding



Altinn
studio



Altinn
varsling



Ansattporten



Arbeidsflate



data.altinn.no



data.norge.no



Dialogporten



Digital postkasse
til innbygger



eFormidling



elnnsyn



ELMA



eSignering



ID-porten



Kontakt- og
reservasjons-
registeret



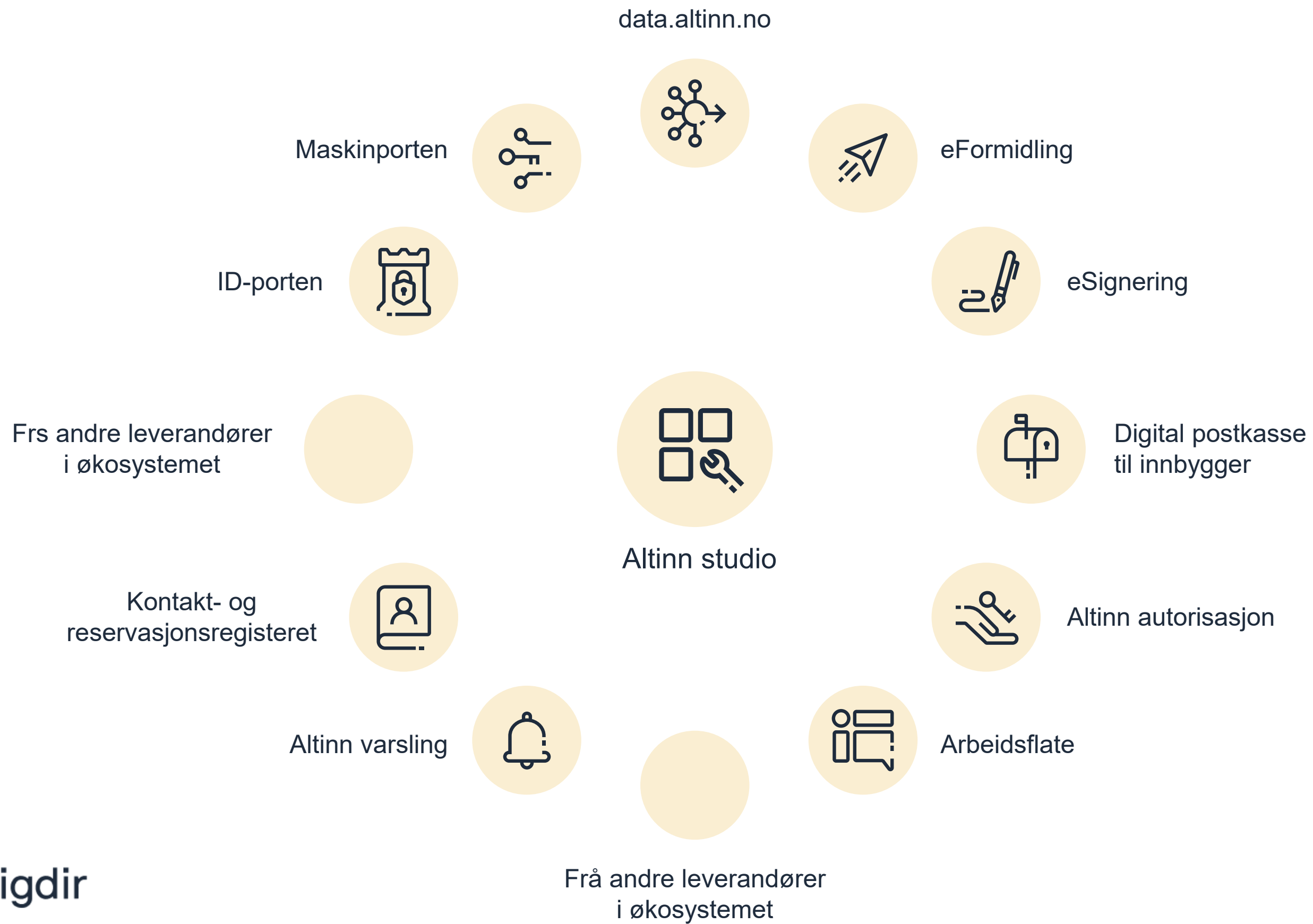
Maskinporten



MinID

Fellesløsningene en del av et økosystem







Frode Danielsen – Direktør i Digdir

Ved å gjenbruke fellesløysingane sparar forvaltninga tid og pengar fordi ein slepp å utvikle all funksjonalitet frå starten. Verksemdene kan prioritere eigen kompetanse og ressursar på å bygge gode, innovative, trygge og brukarretta tenester.

Hvor langt er vi kommet?

Hva jobber vi med nå?



Fullmakt og representasjon

- FILM
- <https://vimeo.com/1134616508/4a80d89a33?fl=pl&fe=sh>
- [Digital representasjon - Video til Samarbeidsportalen](#)

Prosjekt og satsinger

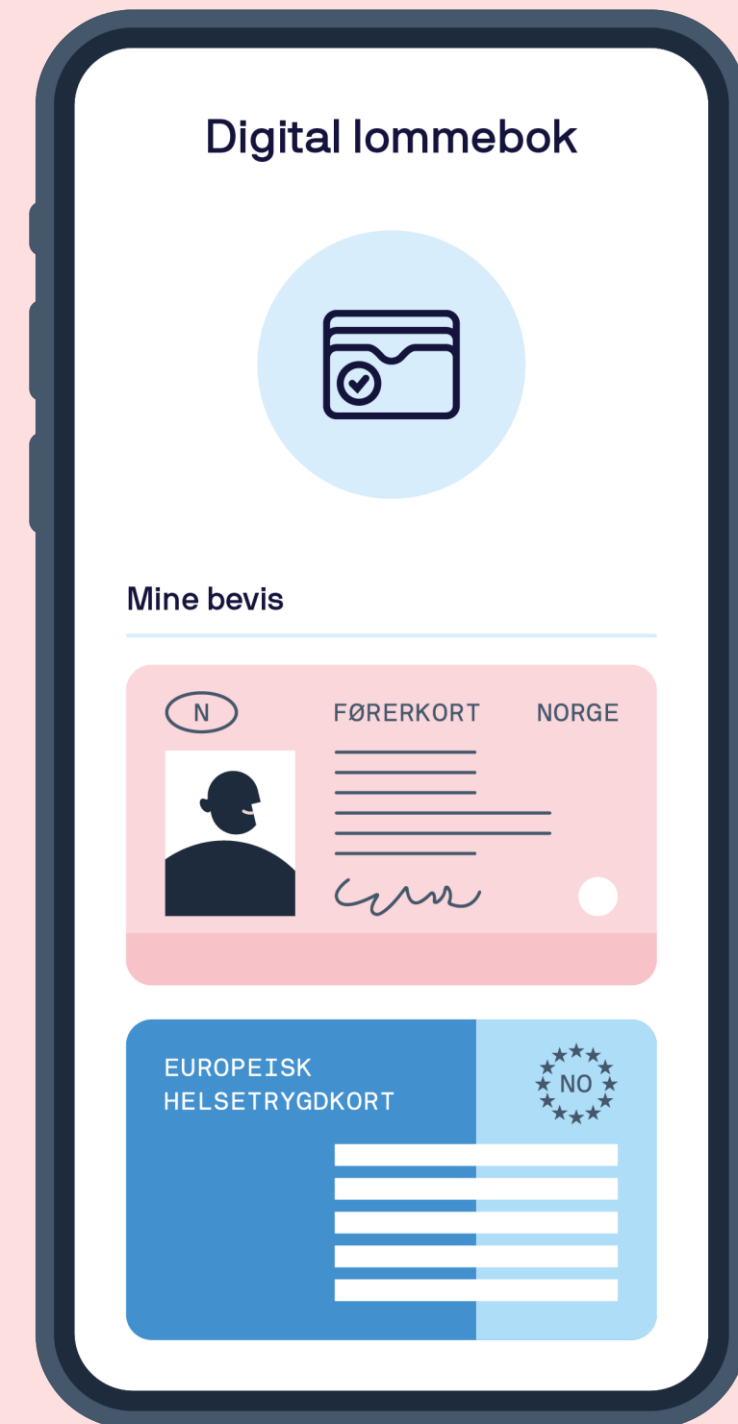
Digital Lommebok



Den europeiske digitale lommeboken kommer til Norge

Norge implementerer nå EU-forordningen eIDAS 2.0

- Alle borgere får tilgang digital lommebok og eID på høyeste sikkerhetsnivå
- Lommeboken er gratis og tilgjengelig for alle
- Sikkerhet og personvern settes i fokus
- Den skal redusere svindel og identitetstyveri
- Mange tjenester er pliktig å akseptere lommeboken som påloggingsmekanisme
- Den skal fungerer på tvers av landegrenser i Europa
- Kommunal sektor representerer et bredt spekter av tjenester og behov hvor den digitale lommeboken kan bli aktuell



Lommeboken har fire hovedfunksjonaliteter



Autentisering



Lagring



Deling



Signering

Eksempel på digital bevis i lommeboken



Sandkassen skal gjøre Norge klar for digital lommebok! Vil du være med?

Her kan du...

- Teste utstedelse, deling og verifisering av digitale bevis
- Utforske konkrete brukstilfeller og se hvordan de fungerer i praksis
- Forstå hva lommeboken kan bety for din kommune
- Utforske interoperabilitet mellom flere aktører og systemer på tvers
- Bruke Digdirs kjernekomponenter til testformål



Digital Lommebok

- FILM
- <https://vimeo.com/1173983842/f21aa17ba6?fl=pl&fe=sh>
- [Dette er digital lommebok](#)

Erfaringer fra tre DDoS- angrep mot Digdirsommeren 2026



Tre DDoS-angrep på ni uker

2026

20.-21. juni

Startet kl. 13:16.
Varighet ca. 29 timer

ID-porten og øvrige løsninger på felles driftsplattform var **utilgjengelige/svært ustabile.**

3.-4. august

Startet kl. 00:48
Varighet ca. 24 timer

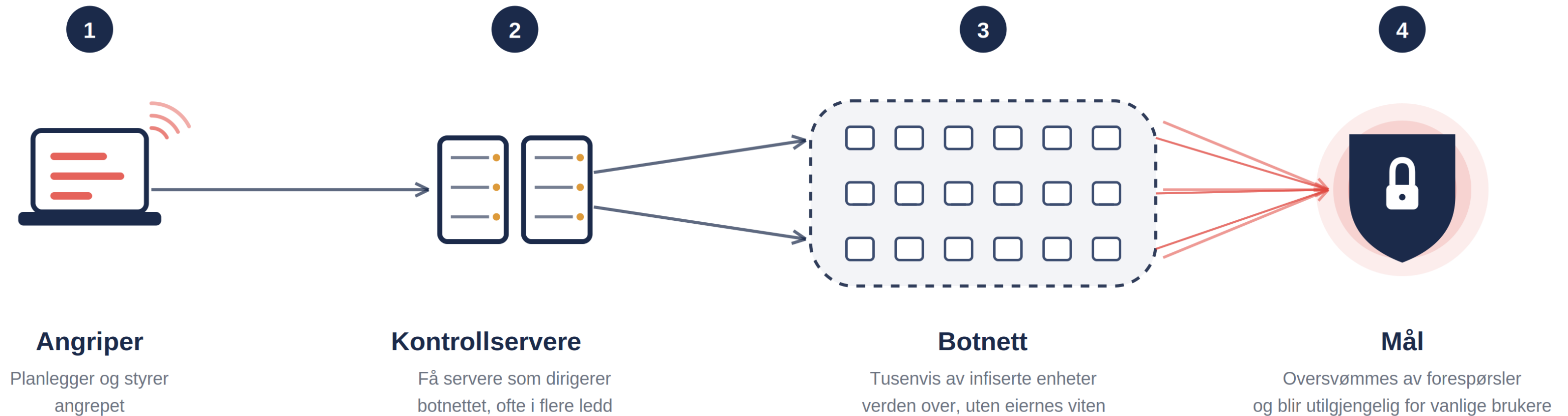
ID-porten og øvrige løsninger på felles driftsplattform var **utilgjengelige/svært ustabile.**

24.-26. august

Startet kl. 03:38
Varighet ca. 64 timer

ID-porten og løsningene var i hovedsak **tilgjengelige** under hele angrepet, bortsett fra korte perioder og på tidspunkter med lite trafikk. Unntak var innlogging fra utlandet og enkelte tjenester med avhengigheter mot andre land.

Hva er et DDoS-angrep (tjenestenektangrep)



- **Tjenestenektangrep:** DDoS-angrep (Distributed Denial of Service) skjer ved at svært mange datamaskiner sender enorme mengder trafikk mot én tjeneste. Datamaskinene er typisk infisert og befinner seg i mange land.
- **Ikke «dataangrep»:** Formålet er ikke å bryte seg inn eller hente ut data, men å overbelaste tjenestens kapasitet slik at den blir treg eller utilgjengelig for brukerne. Dette kan ramme alle som er avhengige av tjenesten.

Mer om direkte og indirekte konsekvenser

For fellesløsningene:

Periodevis utilgjengelighet og ustabilitet i ID-porten og fellesløsninger på driftsplattform.

- Hendelse 1 og 2: Løsningene i hovedsak utilgjengelige/svært ustabile.
- Hendelse 3: Nedetiden konsentrert til natt/tidlig morgen, ellers i hovedsak normal drift og mindre merkbar for innbyggere.

For tjenesteeiere og samfunn:

Periodevis utilgjengelighet og driftsforstyrrelser i tjenestene som benytter fellesløsningene.

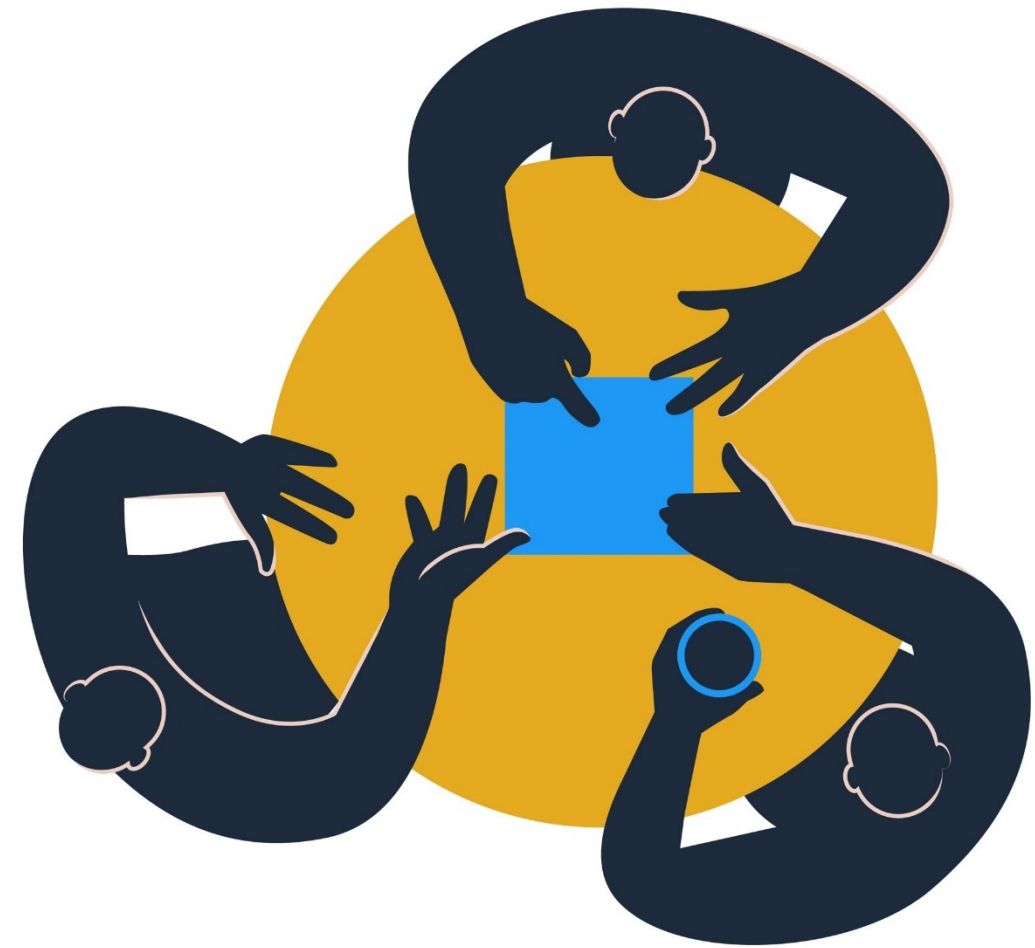
- Indirekte påvirket: Altinn, eSignering, Digital postkasse til innbygger.
- Rammet innbyggere i utlandet og enkelte (ikke-kritiske) tjenester med avhengigheter utenlands

Annet:

- Ingen indikasjoner på datainnbrudd eller at persondata er kommet på avveie.
- Langvarige eller gjentatte angrep kan få mer alvorlige følger. Det understreker betydningen av rask deteksjon og respons.

Mønster, lærdom og anbefalinger

- Gjentakelse må forventes, den nye normalen
- Planlegg for å møte angrep
- Evaluer og juster etter hendelser



Digdir har og skal ha møter med flere kunder og samarbeidspartnere i høst, og informasjon blir delt på flere relevante arenaer.

Vi opplever positiv respons på åpenhet og erfaringsutveksling om hendelsene.

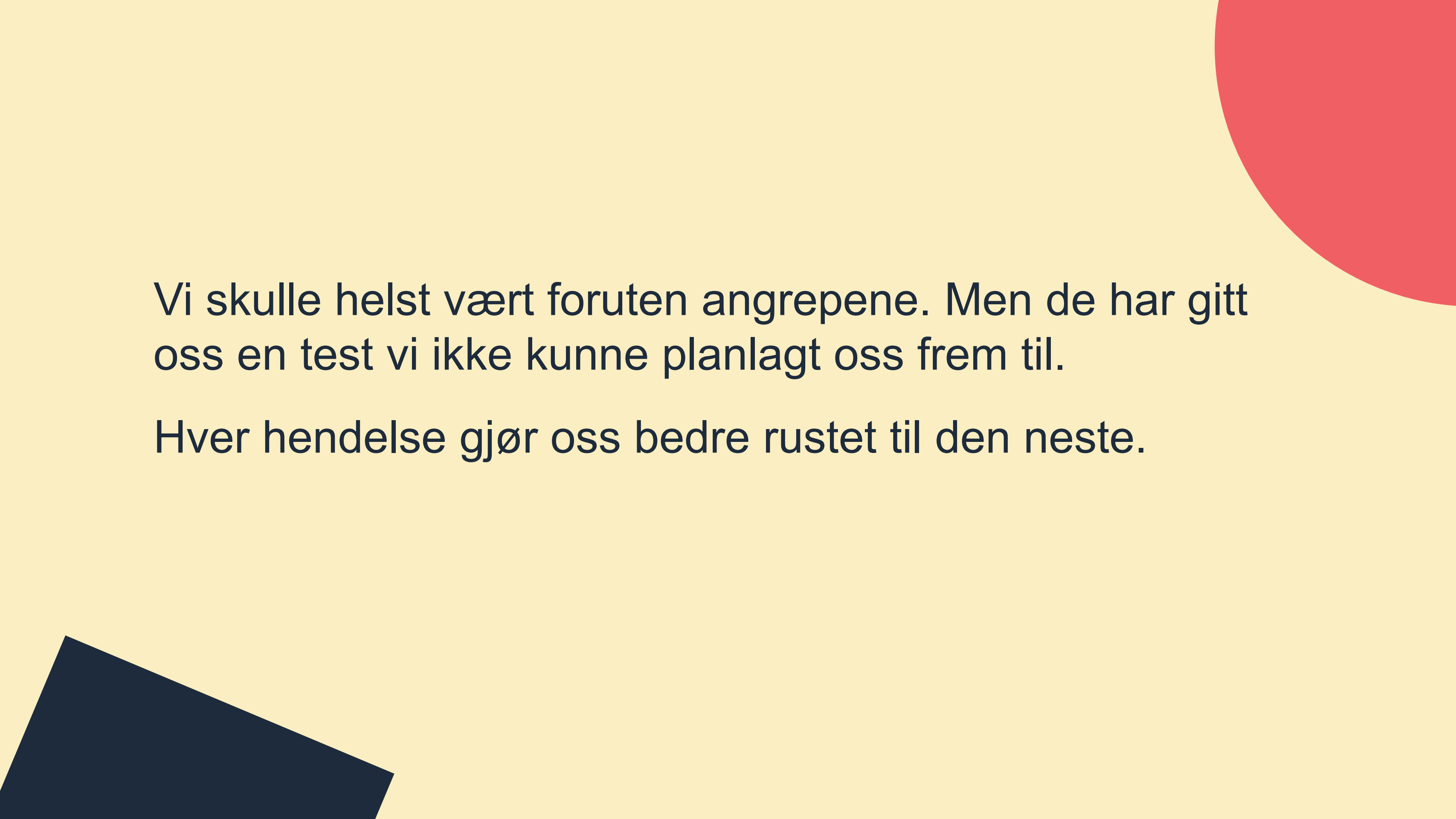
Digdir: Hva vi har gjort og hva vi jobber videre med

Dette har vi gjort

- Iverksatte mitigerende tiltak som ga effekt underveis i angrepene
- Forbedret tekniske tiltak og kommunikasjonstiltak basert på læring fra hendelse 1 og 2
- DDoS-beskyttelsen av løsningene er betydelig styrket
- Styrket dialogen med kunder om rask og tydelig informasjonsdeling

Dette jobber vi videre med

- Kortsiktige og langsiktige tiltak på ulike beskyttelsesnivå. Et sammensatt og kontinuerlig arbeid
- Intern arbeidsgruppe høsten 2026 skal sikre god oppfølging av tiltak i samarbeid med driftspartner (SOC)
- Følger opp erfaringene (varsling, beredskap, tiltak og samarbeid) i det videre arbeidet



Vi skulle helst vært foruten angrepene. Men de har gitt oss en test vi ikke kunne planlagt oss frem til.

Hver hendelse gjør oss bedre rustet til den neste.

Spørsmål?



Brukerrådet

Felles løsninger for felles gevinster

 1.–2. desember 2026

 Digital møteplass





Les mer om fellesløsningene på

samarbeid.digdir.no

eller ta kontakt på

servicedesk@digdir.no.

digdir.no

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

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



Takk for meg 😊

digdir.no

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

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