

SLUTTRAPPORT – ARBEIDSPAKKE 2.2, NASJONAL DIGITAL SIKRINGSKONTRAKT



SAMMENDRAG

Målet med arbeidspakke 2.2 er å etablere en felles nasjonal standard for bruk av sikringskontrakt i ISPS-havneanlegg. Siden ISPS-koden ble innført i Norge i juli 2004, har havneselskap benyttet sine egne, og ulike former for sikringskontrakt uten mulighet for at samme kontrakt kan gjelde for flere havneselskap. Gjennom standardisering og digitalisering skal prosjektet utforme en standard, hvor minste felles multiplum ivaretas på et nasjonalt nivå, mens lokale tillegg for særegenheter ivaretas av havneselskap lokalt.

Bransjeorganisasjonen Norske Havner tok eierskap til forprosjektet og midler er tildelt gjennom Digital havn prosjektet. Grieg Connect AS har påtatt seg utvikling og driftsansvaret for datasystemet, uten øvrige kommersielle forpliktelser for havneselskap og virksomheter som vil benytte seg av nasjonal digital sikringskontrakt. Havneselskapene vil inngå i styret for Norske Havners enhet.

En bransjestandard er etablert med informasjon, ansvar og plikter som partene anerkjenner ved å benytte systemet. Bransjestandarden har fått navnet: «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg». Nasjonal sikringskontrakt skal forenkle, digitalisere og oppnå bedre sikringseffekt for inngåelse, administrasjon og oppfølging av virksomheter som gis fast adgang til ISPS-havneanlegg. Kystverkets avdeling for maritim sikring har vært orientert underveis i prosjektet, og har gitt positiv respons med tanke på oversiktlighet, oppfølging og forbedret sikkerhet.

Prosjektet har 20 deltakende havneselskap som alle har bidratt på ulike måter. Tre arbeidsgrupper ble etablert innledningsvis, hvor Arbeidsgruppe 1 har stått for projektering og utvikling, arbeidsgruppe 2 har bistått med tekniske løsninger og arbeidsgruppe 3 har vært referansegruppe.

Totalt er det gjennomført i underkant av 20 arbeidsmøter siden oppstartsmøtet den 3. november 2023. Delprosjektet har hatt fem faser som listet under.

1. Oppstartsfasen
2. Designfasen
3. Utviklingsfasen
4. Testfasen
5. Implementeringsfasen

Nasjonal sikringskontrakt skal kunne benyttes av både offentlige og private havneselskap, og forhåpentlig vil så mange som 60 % av de 630 havneanleggene i Norge benytte seg av løsningen.

Arbeidspakke 2.2, Nasjonal digital sikringskontrakt

Emne: Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg og datasystem for digitalisering av sikringskontrakt

Dato: 20.12.2024

Leder av arbeidsgruppe: Hans-Petter Bakke

Utarbeidelse av rapport: Hans-Petter Bakke

Deltakere i workshops i arbeidsgruppe 1:

- Stavangerregionen Havn IKS – Arvid B. Nygaard og Steffen Mikalsen
- Oslo Havn KF – Emilie Groth og Rune Aarset
- Bodø Havn KF – Morten Nydal
- Trondheim Havn IKS – Kurt Kristiansen
- Bergen Havn AS – Christian Hafstad
- Karmsund Havn IKS – Tor Arne Ulsund Hansen
- Kristiansand Havn IKS – Matthias Eder
- Norske Havner – Arnt-Einar Litsheim
- Grieg Connect – Tord Svanqvist og Konrad Boehm
- Security Risk AS – Hans-Petter Bakke

Kvalitetskontroll: Arvid B. Nygaard og Steffen Mikalsen

Bilder: Skjermdumper fra Grieg Connect (Figma- og datasystem), figurer utviklet av arbeidsgruppen, figurer utviklet av Melvær & Co.

INNHold

1. BAKGRUNN OG FORVENTNINGER	5
1.1 Hvor er vi nå, hva er behovene og hva skal til for å løse dem?	6
1.2 Planlagt utvikling i arbeidspakken	6
2 AKTIVITETER I ARBEIDSPAKKEN	6
2.1 Oppsummering fase 1 – Oppstart	7
2.2 Oppsummering fase 2 – Design	8
2.3 Oppsummering fase 3 – Utvikling	8
2.4 Oppsummering fase 4 – Test	9
3 OPPSUMMERING OG VEIEN VIDERE	12
4 VEDLEGG	13
4.1 Vedlegg A Oppsummering av prosjektfaser	13
4.2 Vedlegg B Barrierestrategi	13
4.3 Vedlegg C Ordliste og Liste over adgangssystemer	13
4.4 Vedlegg D Løsningsbeskrivelse datasystem	13
4.5 Vedlegg E Personvernkvadrant	13
4.5.1 Innledende personvernkvadrant	13
4.5.2 Personvernkonsekvenskvadrant	13
4.6 Vedlegg F Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg	13
4.7 Vedlegg G Testcaser for datasystemet	13
4.7.1 Manage companies	13
4.7.2 Manage Courses	13
4.7.3 Manage Port Facilities	13
4.7.4 Manage Shipping Companies	13
4.7.5 Manage Users	13
4.7.6 Onboard and Manage Ports	13
4.7.7 Security Contract Applications Flows	13

1. BAKGRUNN OG FORVENTNINGER

Målet med arbeidspakke 2.2 er å etablere en felles nasjonal standard for bruk av sikringskontrakt i ISPS-havneanlegg. Siden ISPS-koden ble innført i Norge i juli 2004, har havneselskap benyttet sine egne, og ulike former for sikringskontrakt uten mulighet for at samme kontrakt kan gjelde for flere havneselskap. Gjennom standardisering og digitalisering skal prosjektet utforme en standard, hvor minste felles multiplum ivaretas på et nasjonalt nivå, mens lokale tillegg for særegenheter ivaretas av havneselskap lokalt.

Prosjektarbeidet er organisert som et felles prosjekt mellom følgende parter:



1.1 Hvor er vi nå, hva er behovene og hva skal til for å løse dem?

Bransjeorganisasjonen Norske Havner tok eierskap til forprosjektet og midler er tildelt gjennom Digital havn prosjektet.

Oslo Havn KF står som ansvarlig for Digital havn prosjektet og gikk høsten 2023 ut med offentlig anskaffelse av delprosjektleder for AP 2.2. Valget falt på Security Risk AS og kontrakt ble signert i oktober samme år. Planlagt og gjennomført oppstart for arbeidspakken var 3. november 2023.

Grieg Connect AS har påtatt seg utviklings- og driftsansvaret for datasystemet, uten øvrige kommersielle forpliktelser for havneselskap og virksomheter som vil benytte seg av nasjonal digital sikringskontrakt. Dette ble gjort for å sikre uavhengighet for datasystemet som skal være tilgjengelig for alle havneselskap.

Det er behov for en bransjestandard som skal legge føringer for partene som er involvert. Partene er Norske Havner, deltakende havneselskap, Grieg Connect AS og virksomheter som skal kunne inngå sikringskontrakt. Videre måtte datasystemet designes og personvernlovgivning hensyntas, da nasjonal digital sikringskontrakt krever innhenting av personopplysninger.

Behovet er å etablere én sikringskontrakt som kan være gyldig for alle godkjente ISPS-havneanlegg i Norge. Nasjonal sikringskontrakt skal ivareta minste felles multiplum for krav etter ISPS-koden og til enhver tid gjeldende forskrift om sikring av havneanlegg. Lokale krav for det enkelte havneanlegg vil kunne komme i tillegg, men eventuelle lokale krav er ikke av dette delprosjektets anliggende.

1.2 Planlagt utvikling i arbeidspakken

Fremdriften skulle sikres gjennom fem faser:

1. Oppstart – resultat med informasjon til alle deltakere i arbeidspakken, etablering av mandat og etablering av arbeidsgrupper
2. Design – resultat med etablering av krav som systemet skulle ivareta, utarbeidelse av bransjestandard som skal styre ansvar, oppgaver og forpliktelser
3. Utvikling – Utvikling av datasystem, utvikling av gjennomføring av nasjonal sikringskontrakt, herunder personvern, juridiske forpliktelser og brukerveiledning
4. Test – Test av datasystem
5. Implementering – Klargjøre og implementere resultatet for overlevering til Norske Havner for idriftsettelse.

Tildelingen av midlene ble mottatt i begynnelsen av juli 2023. Forventet tildeling var mai. I tillegg var Oslo Havn KF forpliktet å gjennomføre anbuds- og tildelingsprosesser i tråd med lov om offentlig anskaffelse. Forventet oppstart var estimert til begynnelsen av juni 2023, mens faktisk oppstart ble 3. november 2023. Dette var første grunnlag for forsinkelsen til å komme i mål til opprinnelig frist ved utgangen november 2024.

2 AKTIVITETER I ARBEIDSPAKKEN

Detaljer om arbeidsmøter og fremdrift i prosjektet er lagt til som vedlegg A i rapporten. Følgende kapitler gir en kort oppsummering for hver fase i delprosjektet.

2.1 Oppsummering fase 1 – Oppstart

Formål med fase 1 var å etablere arbeidsgrupper med havneselskap og systemutvikler som skulle gjennomføre planlegging, design og følge utviklingen av systemet til slutttest og overlevering til Norske Havner. Fem møter ble gjennomført, hvorav fire var arbeidsmøter. Størst fokus i oppstartsfasen var organisering av arbeidsgruppen, planlegging av gjennomføring og erfaringsutveksling med hva som har fungert, utfordringer og personvern hensyn.

Første møte ble gjennomført 3. november 2023 og fasen ble avsluttet 23. januar 2024. Følgende tabeller viser planlagt fremdrift og arbeidsgrupper som ble besluttet.

Oppstartsmøte ble gjennomført 3. november 2023 med orientering om prosessen, etablering av mandat og fastsettelse av arbeidsgrupper og fremdrift, ref. Tabell 1 Planlagt fremdrift. Forutsetninger for deltakere i arbeidsgrupper ble gjennomgått og arbeidsgrupper ble fastsatt, ref. Tabell 2 Arbeidsgrupper med deltakere. Endringer i sammensetning ble gjort underveis.

Tabell 1 Planlagt fremdrift

Milepæl/delmål	Dato	Leveranse (beskrivelse av leveranser)
Mandat godkjent av prosjekteier og styringsgruppe	23.11.2023	Formell godkjenning.
Etablering, forberedelse og planlegging av minimumskrav til sikringskontrakt og database	Uke 48, 2023	Etablering av arbeidsgrupper, avklaring av oppgaver og funksjoner i database. Utarbeide grunnlag for systemkrav og innhold i digital løsning.
Utvikling av systemkrav og design for database og krav til sikkerhet og sikringsaktiviteter	Uke 8, 2024	Spesifikasjoner til databasens arkitektur, funksjonalitet, sikkerhet og prosesser etablert av arbeidsgruppene 1 og 2 i fellesskap. Parallelt med systemutvikling av databasen, vil krav til minste felles multiplum for sikringsaktiviteter være etablert av arbeidsgruppe 1.
Konfigurerings og utvikling av digital løsning	Uke 35, 2024	Digital løsning skal være klar til testing av funksjonaliteter og bugfix.
Oppfølging, opplæring og testing av digital løsning	Uke 44, 2024	Korrektive tiltak i database skal være utført, opplæring og testing hos havner og aktører skal være gjennomført.
Idriftsettelse	01.11.2024	Bransjestandard og digital løsning skal være klar til idriftsettelse og bruk i havner.
Sluttrapport for arbeidspakken	15.11.2024	Rapport klar til distribusjon til aktuelle parter.

Tabell 2 Arbeidsgrupper med deltakere

Hovedarbeidsgruppe	Teknologi og utvikling	Referanse- og testgruppe
Stavangerregionen Havn Arvid B. Nygaard	Stavangerregionen Havn Steffen Mikalsen	Stavangerregionen Havn
Trondheim Havn Kurt Kristiansen	Systemleverandør	Kristiansund og Nordmøre Havn Svein Skomsøy (Bjørnar Eresvik)
Karmsund Havn Tor Arne Ulsund Hansen	Kristiansund og Nordmøre Havn Bjørnar Eresvik (Svein Skomsøy)	Arendal Gordon Fuglestad
Bergen Havn Christian Hafstad	Arendal Havn TBC	Nord-Trøndelag Havn Svein Bondø
Kristiansand Havn Matthias Eder	Trondheim Havn Bjørnar Horsgård	Harstad Terje Johannesen
Oslo Havn Jens Petter Christiansen		Bergen Havn Silje-Olava Bruknapp
Bodø Havn Morten Nydal		Bodø Havn Johnny Harrang

2.2 Oppsummering fase 2 – Design

Formål med fase 2 var å designe systemet på grunnlag av utarbeidelse av bransjestandarden etablert gjennom fase 1. Design av datasystemet startet opp og pågikk parallelt med videre utvikling av bransjestandarden. Egen barrierestrategi ble utarbeidet, ref. 4.2 vedlegg B, sammen med ordliste og liste over adgangssystemer, ref. 4.3 vedlegg C. Ordlisten ble utviklet for å standardisere begreper som skulle benyttes, med forhåpning om at begrepslisten vil legge grunnlag for standardisering i Havne-Norge videre i fremtiden.

Design av systemet ble utført bruk av Figma, som er et program som muliggjør å vise hvordan datasystemet skal fungere. Bransjestandarden legger premisser for hva datasystemet skal løse av praktisk funksjon og informasjon. Fase 2 ble overlappet med fase 3 fra slutten av mai 2024, hvor systemleverandør utarbeidet en løsningsbeskrivelse som ble gjennomgått og forankret, ref. 4.4 vedlegg D Løsningsbeskrivelse «nasjonal sikringskontrakt».

2.3 Oppsummering fase 3 – Utvikling

Formål med fase 3 var å konfigurere datasystemet og utvikle bransjestandard for gjennomføring av nasjonal sikringskontrakt. Personvern og juridiske forpliktelser, i tillegg til brukerveiledning ble utviklet videre. Utvikling av datasystemet og oppdatering av bransjestandarden ble koordinert med tett dialog i arbeidsgruppen for oppfølging og avklaring av behov for endringer. Personvern vurderinger er lagt til rapporten, ref. 4.5 vedlegg E.

Datasystemet var klar til utførelse av testing og bugfix fra midten av oktober og frem til 15. november 2024.

Bransjestandarden ble sluttført i november og ble endret til «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg». Deltakende havneselskap i arbeidspakke 2 mottok dokumentet

for intern høring, som inkluderte Kystverkets avdeling for Maritim sikring. Høringsrunden gav ingen innvirkning på dokumentet, utover positive tilbakemeldinger.

Se kap. **Feil! Fant ikke referanse-kilden.** vedlegg F for endelig versjon av retningslinjene for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg.

2.4 Oppsummering fase 4 – Test

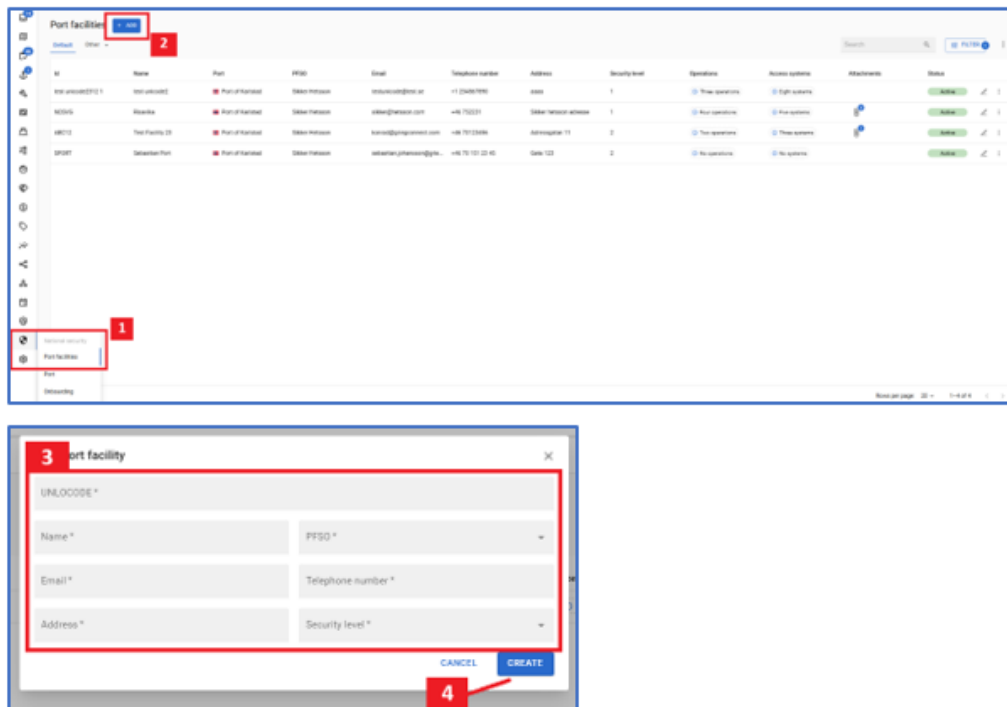
Formålet med Fase 4 var å gjennomføre test av datasystemet for å sikre at alle funksjoner er ivarettatt og fungerer etter intensjon. Egne testplaner var utviklet som ble benyttet under testingen 13, eksempel er vist i figur 8 under.

3. Creating new port facility

Test preconditions

The port has been onboarded and configured. The tester has an internal role of PORT_PFSO or higher.

Steps



1. In the sidebar menu, navigate to *Port facilities*
2. Click on *Add new* in the top left corner
3. Enter details:
 - UNLOCODE
 - Name
 - PFSO (select from a list of PFSO:s that have been registered as a key user in port configuration)
 - E-mail (name@domain.com)
 - Telephone number (country code included)
 - Address
 - Security level (select from 1–3 based on the current assessment within the port facility)
4. Click on *Save*

Expected result

The port facility is created and activated with its detail page, as well as appearing in the list view.

Figur 1 Eksempel på test av funksjon i datasystem

Testingen viste at systemet fungerte etter intensjonen, og noen bugs og mangler ble identifisert og følges opp i tråd med etablert liste.

Samtykker som utgjør digital sikringskontrakt

I forbindelse med etablering av innhold i sikringskontrakten legges samtykke til betingelser til grunn i datasystemet. Det er totalt fem samtykker som skal gis av partene før sikringskontrakten kan signeres. Alt skal i utgangspunktet være digitalt, men det skal samtidig være mulig å laste ned en PDF-versjon for eksempelvis arkivering på annet medium, jf. arkivloven.

Samtykke 1 (Søke om tilgang i datasystem)

Rolle: Ansvarlig søker hos virksomhet

Formål: Før virksomhet sender inn forespørsel om å opprette selskap og kunne søke om sikringskontrakt må juridiske forpliktelser aksepteres.

Formulering:

Ansvarlig søker bekrefter herved at virksomheten er innforstått med ansvaret og forpliktelsene som påligger virksomheten i henhold til enhver tid gjeldende lovgivning, «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg» og havneanlegget sine lokale sikringstiltak.

Dersom forespørselen godkjennes, vil oppgitte kontaktpersoner hos virksomheten motta en e-post som gir adgang til å opprette en Grieg-ID for innlogging i datasystemet og mulighet til å søke om nasjonal sikringskontakt.

Samtykke 2 (Søke om sikringskontrakt)

Rolle: Sikringsansvarlig hos virksomhet

Formål: Opplysning om virksomhetens forpliktelser, verifisering av ansvar/mandat hos søker og økonomisk forpliktelse.

Formulering:

Ved å innlevere søknaden, bekrefter sikringsansvarlig på vegne av virksomheten at:

- Alle inngitte opplysninger er korrekte
- Oppgitte personer for de ulike rollene har fullmakt til å påta virksomheten forpliktelser som ligger den enkelte tildelte rollen
- Virksomhetens Tilganger til havnen skal kun brukes til formålet som er oppgitt i søknaden
- Opplysninger i systemet vil bli holdt kontinuerlig oppdatert
- Virksomheten plikter å holde seg oppdatert og å følge forpliktelsene som stilles i henhold til enhver tid gjeldende lovgivning, «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg» og havneanlegget sine lokale krav og sikringstiltak.
- Alminnelige personopplysninger som er nødvendige for å gjennomføre sikringskontrakten, kan lagres i datasystemet

- Havneselskap kan utføre kontroll og tilsyn med at ovennevnte er innfridd

Samtykke 3 (aksept av søknad om sikringskontrakt)

Rolle: PFSO hos havneselskap (havneanlegg)

Formål: Havneselskapet bekrefter at virksomhetens søknad godkjennes og kan signeres.

Formulering:

Havneselskapet bekrefter herved at virksomhetens søknad om aktiviteter og tilgang til omsøkte havneanlegg aksepteres. Enhver tid gjeldende lovgivning, «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg» og havneanlegget sine lokale krav og sikringstiltak, skal følges.

Samtykke 4 (signatur av sikringskontrakt, virksomhet)

Rolle: Prokura hos virksomhet

Formål: Bekrefte med signatur forpliktelser virksomheten påtar seg i tråd med «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg».

Formulering:

Undertegnede bekrefter herved å ha fullmakt til å signere sikringskontrakt på vegne av virksomheten.

Virksomheten aksepterer ansvaret for økonomiske og juridiske forpliktelser som følger av enhver tid gjeldende lovgivning, «Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg» og havneanlegget sine lokale sikringstiltak.

Virksomheten forplikter seg til å etterleve havneanleggets krav i henhold til sikringsplan, samt å sikre opplæring for ansatte som mottar fast adgang til havneanlegget.

Virksomheter aksepterer til enhver tid gjeldende prisliste ved inngåelse og årlig fornyelse av sikringskontrakten.

Undertegnede gir herved sikringsansvarlig i virksomheten tillatelse til å søke sekundærhavner å bli inkludert i sikringskontrakten, samt å holde opplysninger oppdatert i systemet.

Samtykke 5 (signatur av sikringskontrakt, havneselskap)

Rolle: Prokura hos havneselskap

Formål: Bekrefte aksept ved signatur at virksomheten godkjennes.

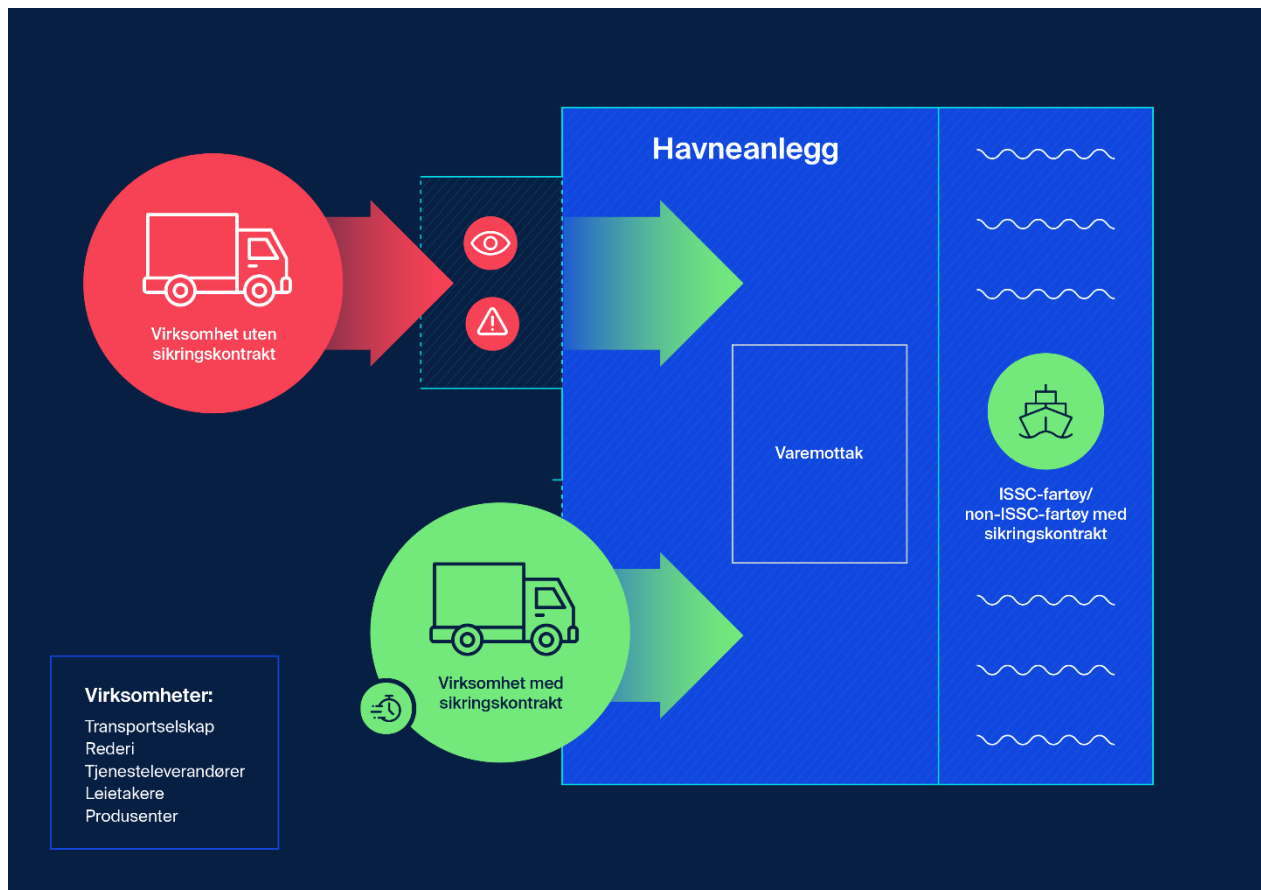
Formulering:

Undertegnede bekrefter på vegne av havneselskapet at virksomhetens søknad om aktiviteter og tilgang til omsøkte havneanlegg, godkjennes.

3 OPPSUMMERING OG VEIEN VIDERE

De siste detaljene etter gjennomført testing er slutført, og prosjektet er ferdigstilt og kan overleveres til Norske Havner for fase 5 Implementering. Endelig retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg er tilgjengeliggjort som vedlegg F. Løsningsbeskrivelse med testcaser for datasystemet er tilgjengelig, red. 4.7 vedlegg G.

Figur 1 Eksempel på test av funksjon i datasystem underbygger måloppnåelsen av prosjektet i forhold til effektivisering og bedre sikring.



Figur 2 Prinsippkisse for parter som benytter havneanlegg og utfører havnetjenester

Norske Havner, Grieg Connect og deltakende havneselskap i arbeidspakke 2.2 kan nå inngå avtaler for idriftsettelse av systemet i tråd med etablerte retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg.

4 VEDLEGG

Link til Teams side for AP2.2 Nasjonal digital løsning for sikringskontrakter er tilgjengelig for de med tilgang.

4.1 Vedlegg A Oppsummering av prosjektfaser

4.2 Vedlegg B Barrierestrategi

4.3 Vedlegg C Ordliste og Liste over adgangssystemer

4.4 Vedlegg D Løsningsbeskrivelse datasystem

4.5 Vedlegg E Personvern vurdering

4.5.1 Innledende personvern vurdering

4.5.2 Personvern konsekvens vurdering

4.5.2.1 Vedlegg personvern konsekvens vurdering - risikoanalyse

4.6 Vedlegg F Retningslinjer for bruk av nasjonal sikringskontrakt for ISPS-havneanlegg

4.7 Vedlegg G Testcaser for datasystemet

4.7.1 Manage companies

4.7.2 Manage Courses

4.7.3 Manage Port Facilities

4.7.4 Manage Shipping Companies

4.7.5 Manage Users

4.7.6 Onboard and Manage Ports

4.7.7 Security Contranct Applications Flows