Slutrapport
Branschgemensamt Digitalt Anlöp - Fas 1

Förberedande arbete för effektivare anlöp genom digitalisering

Forskning och Innovation

Rapporten finns tillgänglig på Sjöfartsverkets webbplats www.sjofartsverket.se

Dnr/Beteckning	21-00156
Författare	Sjöfartsverket
Månad År	December 2021

Sammanfattning

Detta projekt har haft som mål att lägga grunden till fortsatt utveckling och implementation av digitala och automatiserade lösningar samt tjänster bland aktörerna i anlöpsprocessen. Effektivisering av anlöpsprocessen genom digitalisering förväntas på sikt resultera i en minskad kostnad för transportköparna och en ökad konkurrenskraft för sjötransporter, vilket bidrar till det övergripande transportpolitiska målet om överflyttning av gods från land till sjö. Dessutom bidrar en effektiviserad anlöpsprocess till en minskad miljöpåverkan från sjöfarten eftersom bränsleförbrukning optimeras.

Arbetet har genomförts i fem arbetspaket. I det första arbetspaketet har branschens aktörer gått samman för att gemensamt ta fram en översiktlig beskrivning av anlöpsprocessen och identifiera dess största utvecklingsbehov. Det andra arbetspaketet har fokuserat på att utreda förutsättningar för att etablera en digital infrastruktur, som kan stödja utvecklingen av nya digitala tjänster. Ett exempel på en sådan ny digital tjänst har behandlats i arbetspaket tre, som genomfört en förstudie kring hur en ny tjänst för tillhandahållande av samlad nautisk tilläggsinformation kan etableras. Emedan de första tre arbetspaketen genomförts som förstudier, har det fjärde arbetspaketet varit av praktisk karaktär. I detta fjärde arbetspaket har en kommande internationell standard av stor vikt för sjöfartens fortsatta digitalisering testats genom integrationstester mellan deltagande projektparters system. Det femte arbetspaketet har utgjorts av projektledning och resultatspridning.

För att realisera ovan nämnda nyttor av digitalisering behöver utvecklingen stödja en förflyttning mot automatiserade processer. Eftersom anlöpsprocessen består av en kedja av tjänster, som tillhandahålls av ett stort antal aktörer, krävs samverkan för att undvika lokala särlösningar. Sjöfarten är global, varför nya tjänster behöver utvecklas med beaktande av internationella standarder, så att framtagna lösningar är interoperabla med andra system. Denna förflyttning underlättas om branschens aktörer förmår att bibehålla den samverkansplattform som etablerats genom projektet och fortsatt utveckling inom ramen för branschprogrammet bör beakta slutsatserna från respektive arbetspaket. Sammantaget har projektet skapat bärkraftiga förutsättningar för fortsatt gemensam utveckling av branschprogrammet Smarta Anlöp och bidragit med insikter om branschens prioriteringar för Sjöfartsverkets fortsatta digitala transformation.

Norrköping, december 2021

Carina Stål

Programchef Digitalt Anlöp

Innehåll

1 Slutsats och rekommendationer

Incitamenten för ett starkt digitalt anlöp är ökad effektivitet och konkurrenskraft, ökad sjösäkerhet, kortare omloppstider och ökad leveranssäkerhet, reducerad miljöpåverkan och lägre produktionskostnader. För att realisera dessa nyttor för sjöfartsnäringen och för transportsystemet som helhet krävs stora investeringar i digital infrastruktur och systemstöd, nya processer, anpassade regelverk och gemensamma standarder. Denna förstudie har haft som ansats att skapa fördjupad förståelse för hur dessa nyttor ska kunna realiseras i en process som involverar många aktörer.

För att etablera en gemensam bild av anlöpsprocessen och dess utvecklingsbehov har ett stort antal representanter från sjöfartsnäringen samverkat inom ramen för projektet. Projektresultatet innefattar identifierade utvecklingsbehov för att minska administration av fartygsanlöp och för att underlätta tillgång till uppdaterad information genom informationsdelning. I sin roll som förvaltare av Sveriges portal för myndighetsrapportering kopplad till fartygsanlöp och som en tjänsteleverantör i anlöpsprocessen bör Sjöfartsverket verka för effektivare informationsdelning.

Tillgång till tillförlitlig information i rätt tid är en förutsättning för att anlöpsprocessen ska fortlöpa smidigt, vilket inte bara ställer krav på ansvariga myndigheter att hitta nya lösningar för att ta emot och dela information, utan även på flertalet aktörer i anlöpsprocessen. Exempelvis lyfte tillfrågade i branschen behovet av tillgång till lots vid rätt tidpunkt som det enskilt viktigaste utvecklingsområdet för att öka sjöfartens konkurrenskraft. Ett sätt att adressera behovet är att genom ett digitaliserat, automatiserat informationsutbyte mellan anlöpets aktörer skapa ökad transparens i anlöpsprocessen, som underlättar planering och ömsesidig processkontroll. Med tillgång till mer tillförlitlig information, i ett tidigare skede, kan lotsplaneringen underlättas, vilket i sin tur skapar bättre förutsättningar för att tillhandahålla lots vid en överenskommen tid, inom rimliga kostnadsramar. På samma sätt kan respektive aktör genom kännedom om övriga aktörers planering få en mer överskådlig planeringshorisont och bättre förutsättningar att optimera sina respektive tjänster i anlöpsprocessen. För det enskilda fartyget innebär det att hastigheten kan anpassas för att ankomma ’just in time’, vilket i sin tur bidrar till minskad miljöpåverkan och lägre kostnader för bränsleförbrukning.

Sverige är en liten nation och sjöfarten är global, varför framtida projekt måste beakta internationell utveckling. För ett säkert informationsutbyte och som en grund för nya S-100[1]-produkter bedöms SECOM[2] komma att rekommenderas av IMO att utgöra standard för informationsutbyte mellan fartyg och land. För kommande utveckling av nya digitala tjänster, såsom Sjöfartsverkets utveckling av en lösning för att tillhandahålla nautisk tilläggsinformation, behöver SECOM och S-100 beaktas.

Projektets övergripande slutsats är att effektivisering av anlöpsprocessen genom digitalisering behöver ske i nära samverkan mellan anlöpets aktörer för att möjliggöra kompatibla lösningar för informationsdelning över organisationsgränser och processautomation. Målbilden för arbetet bör vara att kunna realisera ’just in time’-anlöp, dvs. anlöp som minimerar icke värdeskapande stillestånd i anlöpsprocessen. Eftersom sjöfarten är global behöver arbetet undvika regionala och nationella särlösningar, varför internationella samarbeten är av stor vikt, liksom deltagande aktörers förmåga att sprida projektresultat nationellt till stöd för det övergripande transportpolitiska målet om överflyttning av gods från land till sjö.

[1] Se bilaga 3, Förstudie nautisk tilläggsinformation.
[2] Se bilaga 4, SECOM Test Project – Final report.

2 Behov av kraftsamling och koordinering

Eftersom sjöfarten är global behöver investeringar i digital utveckling ske med stor hänsyn till internationell och regional utveckling. Standardiseringsarbetet inom IMO[3] och IHO[4] där Sverige deltar är styrande, liksom det arbete som bedrivs inom EU för harmoniserad myndighetsrapportering av fartyganlöp. För att skapa synliga nyttor för de aktörer som är involverade i ett fartygsanlöp och öka respektive aktörs interna effektivitet behöver förekommande digitala initiativ runt ett fartygsanlöp synkroniseras och fås att samverka. Denna utveckling kräver en dramatiskt höjd digital förmåga och en vilja hos aktörerna att dela processpecifik information via överenskomna internationella standarder.

Under senare år har Sjöfartsverket, flera svenska hamnar, redare och andra aktörer arbetat för att förenkla fartygens anlöp till och från svenska hamnar. Digitalisering har här varit ett viktigt verktyg för att minska kostnader och öka kundnyttan. Förbättringarna har i regel utgått från varje aktörs egna tjänster, vilket även gäller även Sjöfartsverkets digitaliseringsarbete. Enskilda aktörers projekt kan ge ett intressant resultat, men genom att ensa och koppla samman dem uppnår man en helhet som är större än de individuella delarna. Hur ska det gå till?

I början av år 2020 har ett branschgemensamt program för Smarta Anlöp etablerats för långsiktig samverkan och utifrån ambitionen att skapa en branschgemensam process för anlöp oberoende av hamn- eller rederitillhörighet. Mot bakgrund av anlöpsaktörernas gemensamma vilja att realisera nyttan av digitala anlöp har det här projektet haft en explorativ ansats för att bättre förstå hur fartygets resa till och från svenska hamnar kan effektiviseras genom digitalisering. Utgångspunkten för det här arbetet har därför varit att identifiera vilka utvecklingsbehov som finns i nuvarande anlöpsprocess och vilka förutsättningar som behöver finnas på plats för att stötta en digitalisering och automatisering av det informationsutbyte som idag till största delen sker manuellt.

2.1 Projektmål

Projektmålet har varit att lägga grunden till fortsatt utveckling och implementation av digitala och automatiserade lösningar och tjänster hos aktörerna i anlöpsprocessen. Ökad digitalisering och automatisering i anlöpsprocessen bedöms skapa ökad förutsägbarhet, förbättrad planeringshorisont, minskad administration och minskade kostnader i anlöpsprocessen. Dessa effektiviseringar förväntas resultera i en minskad kostnad för transportköparna och en ökad konkurrenskraft samt minskad miljöpåverkan för sjötransporter. En digitalisering av fartygsanlöpet skapar också förutsättningar att kunna koppla samman informationsflödet med väg- och järnvägstransporter och skapa förutsättningar för bättre integration mellan trafikslagen och till en högre transportkvalitet för transportköparna.

Projektet har arbetat för realisering av nedan mål:

- Att aktörerna i anlöpsprocessen genom gemensam kartläggning av anlöpsprocessen och den digitala infrastrukturen skapar bärkraftiga förutsättningar för en branschgemensam utveckling av Smarta Anlöp.
- Bidra till att påskynda digital transformation av olika delar av anlöpsprocessen samt att omsätta olika utvecklingsinsatser inom sjöfartsområdet till realiserad nytta med stöd av digital teknik.
- Att leverera en förstudie kring en branschgemensam tjänst av nautisk tilläggsinformation.
- Att testa och utvärdera en utvecklad branschöverskridande standard (SECOM) för att mogna standarden inför IEC[5]-omröstningen 2021.

[3] International Maritime Organization
[4] International Hydrographic Organization
[5] International Electrotechnical Commission

2.2 Metoder och modeller

Projektet har genomförts under perioden mars 2020 – december 2021 genom tre förstudier som analyserat förutsättningar för det digitala anlöpets kärnområden samt ett praktiskt testarbete inom ramen för IMO:s arbete med utveckling av globala standarder. Då frågan är komplex och involverar flera parter med varierande digital förmåga har arbetet till stor del bedrivits genom interaktiva workshops och litteratursökning. Detta har även bidragit till att uppfylla ett av projektets viktigaste generella syften, att etablera ett samarbetskluster inom den svenska sjöfartsnäringen kring digitalisering.

Den modell för projektstyrning som använts för projektet är PPS[6].

3 Tre förstudier och ett praktiskt testförfarande

Arbetet har indelats i fem arbetspaket, varav fyra beskrivs översiktligt i detta avsnitt. För vart och ett av dessa fyra arbetspaket har en slutrapport författats som bifogas i sin helhet, se bilagor:

5.1 Förstudie anlöpsprocessen och identifiering av utvecklingsbehov
5.2 Förstudie infrastruktur för digitalisering
5.3 Förstudie nautisk tilläggsinformationstjänst
5.4 Test av interface för säkert utbyte av maritim information

Det femte arbetspaketet har utgjorts av projektledning och resultatspridning och redovisas inte närmare i denna rapport.

3.1 Förstudie anlöpsprocessen och identifiering av utvecklingsbehov

Anlöpsprocessen involverar ett stort antal aktörer i ett flöde som präglas av höga krav på samordning, informationsdelning och effektiv planering. Detta gör det till en mycket komplex process, där oväntade avbrott eller förändringar får stora konsekvenser för inblandade aktörer och i förlängningen även för Sjöfartens konkurrenskraft i stort. Detta uppdrag har genomförts under perioden mars 2020-januari 2021 och syftade till att, tillsammans med branschens aktörer, göra en kartläggning av dagens anlöpsprocess samt identifiera vilka delar av processen som behöver utvecklas.

Arbetet projektleddes av Sjöfartsverket, med branschaktörerna som aktiva deltagare under såväl workshops som enskilda möten. Förstudien syftade till att ta fram och komma överens om en processbeskrivning för anlöp till svenska hamnar, vilken spänner över många organisationer, roller och ansvarsområden. Arbetet tog sin utgångspunkt i flera befintliga arbeten på området, både svenska och internationella. Det finns sedan tidigare underlag om anlöpsprocessen hos Sjöfartsverket genom Gothenburg Approach-samarbetet, från PortCDM-arbetet i STM Validation Project och hos Port Call Optimization Taskforce som leds av Rotterdams hamn och inkluderar stora hamnar och rederier på global basis. Baserat på tidigare arbete, informationsflödesanalys och genom workshops med aktörer i anlöpsprocessen har projektet levererat en beskrivning av anlöpsprocessen och identifierat utvecklingsbehov som kommer att utgöra ett fundament för kommande projekt för i Smarta Anlöp.

[6] Modell för praktisk projektstyrning

3.2 Förstudie infrastruktur för digitalisering

I takt med att samhällets intresse för att digitalisera ökar, stiger förväntningen om snabb och effektiv informationsdelning och tillgång till nya, digitala tjänster. Här utgör informationsdelning i sig en grundläggande förutsättning för en lyckad digitalisering. I samband med detta ökar också kraven på den underliggande infrastrukturen. Precis som för annan typ av infrastruktur som farleder, vägar, bredband eller elnät kommer det att krävas en infrastruktur för att hantera sjöfartens digitalisering. Inom ramen för IMO har en strategisk implementationsplan för maritima tjänster tagits fram och denna erbjuder vägledning kring vilka tjänster en maritim digital infrastruktur ska kunna leverera i en framtid. Ett digitalt anlöp behöver en infrastruktur för att klara av att leverera det framtidens sjöfart kräver i form av digitala tjänster.

I denna förstudie har Sjöfartsverket under perioden mars 2020 – december 2021 utrett vilka förutsättningar som behöver skapas för att möjliggöra implementation av det arbete som görs inom IMO. Till viss del utreddes även förutsättningar för den nationella EMSW[7]-plattformen som ska implementeras till 2025 enligt Europaparlamentets och rådets förordning (EU) 2019/1239. Den senare förutsätter att etablera en infrastruktur där digitala tjänster kan publiceras och konsumeras av olika aktörer inom sjöfartsnäringen, men också av andra transportslag för att effektivisera transporter av gods. I en sådan infrastruktur ingår komponenter för autentisering, informationsdelning, loggning, standarder och så vidare.

Förstudien har utrett nuläge och börläge avseende Sjöfartsverkets möjligheter till informationsdelning, inklusive framtagande av disparata användarfall i syfte att utröna olika kravbilder ur ett informationsdelningsperspektiv. En stor del av arbetet har fokuserat på komponentanalys med syfte att fastställa krav på ingående komponenter såsom autentisering, informationssäkerhet och relevanta standarder etc. Vidare har förstudien genom ett användarfall för informationsdelning med hamnar utvärderat affärsmodell och affärslogik för att stödja affärsmässigheten i Sjöfartsverkets framtida lösning för informationsdelning. Slutligen har förstudien tagit fram ett förslag på IT-arkitektur för att stödja en säker och hållbar informationsdelning över tid, inklusive en konceptvalidering för infrastrukturen med syftet att stödja publicering och konsumtion av digitala tjänster.

3.3 Förstudie nautisk tilläggsinformationstjänst

Nautisk Tilläggsinformation (NTI) behövs av fartyg och rederier i planeringen och genomförandet av hamnanlöp. Det finns säkerhetsrelaterad och praktisk information som behöver komma anlöpande fartyg till del och som hamnmyndigheterna svarar för. Anlöpande fartygs skyldigheter gentemot hamnen kan exempelvis stipuleras i hamnordning, hamnföreskrifter eller driftsföreskrifter.

SOLAS[8]-konventionens kapitel 5 stipulerar att de länder som ratificerat konventionen ska tillhandhålla nödvändig information för att tillgodose behoven för säker navigering. Historiskt har detta uppfyllts bl.a. genom tillhandahållandet av publikationen Svensk Lots som innehöll information om hamnar och deras tjänster, lämpliga fartygsrutter, nautiska tjänster såsom lotsning, isbrytning, bogsering och VTS[9] samt restriktioner gällande t.ex. farter, vindgränser, lotsningsrestriktioner och bogserbåtskrav. Sjöfartsverket kommer fortsättningsvis att uppfylla detta behov inom sitt ansvarsområde genom digitaliserade lösningar, vilket är ett avgränsat arbete som har påbörjats och som finansieras av Sjöfartsverkets egna medel. Den här förstudien har haft som ansats att utreda hur en ny och utvidgad samordning mellan hamnar och Sjöfartsverket gällande informationsförvaltning, digitalisering av information och digitala tjänster för distribution till anlöpande fartyg kan förväntas ge en ökad kundnytta. Arbetet har pågått under perioden mars 2020 – december 2021.

[7] European Maritime Single Window
[8] Internationell konvention för säkerhet till sjöss (Safety of Life at Sea)
[9] Sjöfartsverkets trafikcentraler (Vessel Traffic Service)

Förstudien har utrett förutsättningar för strukturering och digitalisering av masterdata som omfattas av begreppet nautisk tilläggsinformation. Förstudien omfattar kartläggning av alternativ för att åskådliggöra denna masterdata i sjökort, elektroniska publikationer eller digitaliserade tjänster. Förstudiens ansats har varit att analysera vilken informationsmängd som kan sägas avses med SOLAS kapitel 5 gällande information för säker navigering samt övrig information från hamnar och myndigheter som kan tänkas ingå in en ny digital NTI-tjänst. Vidare har en juridisk bedömning av den överenskomna definitionen genomförts, liksom identifiering av informationsägarskap och nuläge med avseende på informationskvalitet, ansvar och distribution.

3.4 Test av interface för säkert utbyte av maritim information

Till skillnad från övriga arbetspaket i projektet har detta arbete varit praktiskt inriktat i form av tester för att införa, prova ut och verifiera IEC-standardens lämplighet för utbyte av maritim information i ett gemensamt gränssnitt.

Test av gränssnitt för säkert informationsutbyte har genomförts i partnerskap mellan följande organisationer;

- StormGeo,
- Saab Transpondertech,
- Sjöfartsverket (koordinerande projektpart)

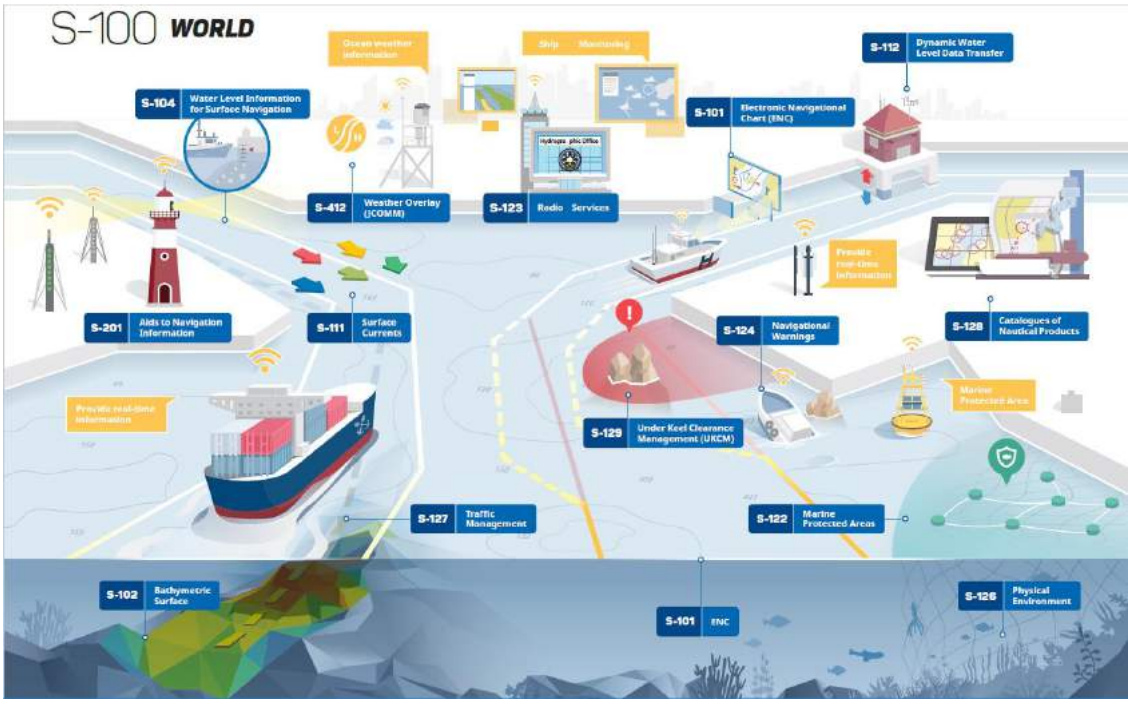
Arbetet har pågått under perioden mars 2020- juni 2021 och har letts av Sjöfartsverket, i nära samverkan med Saab Transpondertech och StormGeo. Testarbetet har levererat ett viktigt bidrag till IEC[10]:s arbete med att utveckla SECOM, en standard för säkert informationsutbyte mellan fartyg och land, som är av stor vikt för sjöfartens fortsatta digitalisering.

3.4.1 En global standard för säkert informationsutbyte

Sjöfartsverket leder arbetet i den internationella standardiseringsorganisationen International Electrotechnical Commission (IEC), WG17[11] (arbetsgrupp nr 17), med att ta fram en internationell standard, SECOM, för utbyte mellan oberoende IT-system av maritim information, t.ex. färdplaner, navigationsvarningar och hamninformation. Detta interface bygger på arbetet med Sea Traffic Management (trafikledning till sjöss) och görs nu till en internationellt fastställd standard som kommer att bidra till interoperabilitet mellan tillverkare av IT-system för fartyg, hamnar, myndigheter och tjänsteleverantörer. SECOM är en förutsättningsskapare för operativa tillämpningar av en maritim digital infrastruktur.

Standardiseringsarbetet har pågått under 2019 och har nu kommit så långt att en första version går att implementera och prova ut. Testprojektet har således syftat till att prova ut och verifiera standardens lämplighet för utbyte av maritim information. Operativa tillämpningar omfattar exempelvis att skapa möjligheter för sjöfartsnäringen att abonnera på information (att kunna hämta information och skicka information) och att kunna lokalisera relevanta tjänster baserat på geografisk position. Detta kräver säkert utbyte av information, exempelvis bibehållen dataintegritet (att data inte kan manipuleras). Funktioner för behörighetshantering ingår också i arbetet med standarden, vilket är en förutsättning för att kunna styra utbytet av information. SECOM är ett initiativ som möjliggör ett standardiserat informationsutbyte av S-100 produkter som omfattar bl.a. nya generationens sjökort, navigationsvarningar och tjänster för ruttutbyte (se bild Figur 1 nedan från IHO).

[10] International Electrotechnical Commission
[11] Working Group 17



Figur 1: Informationsutbyte genom S-100, Källa: IHO.

3.4.2 Metod

Projektets syfte var att testa och återkoppla förbättringsförslag på SECOM-standardens utformning. Arbetet har genomförts genom integrationstester mellan samtliga partners för att testa de gränssnitt som inkluderats i standarden. Sjöfartsverket har ansvarat för rapportering av resultatet av integrationstesterna till IEC, WG 17.

Metoden som använts är att respektive partner implementerat standarden i eget system, varpå deltagande partners testat att utbyta information mellan varandra i ett strukturerat testförfarande med loggning av resultat och dokumentation av slutsatser. Arbetet har genomförts iterativt och planerats och följts upp på veckobasis.

Intresset för projektets arbete i WG17 har varit stort och kommentarer från deltagande länder påverkar utvecklingen av standarden och vilka testfall som projektet behövt testa. Med anledning av projektets och SECOM-arbetets iterativa karaktär har flera nya testfall (interface) tillkommit under projektets gång.

3.4.3 Resultat

Arbetspaketet har bidragit till att standarden når teknisk interoperabilitet, så att system från olika tillverkare sömlöst kan utbyta information mellan varandra. Det som nu återstår är tester för att uppnå operationell interoperabilitet (affärslogik/semantik), vilket ligger utanför projektets ursprungliga ambition. Testfall av operationell karaktär återstår efter att projektet avslutats och kommer att vara föremål för andra, kommande projekt.

I IEC:s standardframtagningsprocess har SECOM nu varit ute på CDV-omröstning (Committe Draft Voting) vilket innebär att WG17 formellt lämnat ifrån sig standarden och kommentarer i omröstningen hanteras av sekreteraren för TC80[12] där WG17 ingår. Omröstningen gav gott resultat och nästa steg efter sammanställning och bemötande av kommentarer är att SECOM skickas ut som Final Draft International Standard (FDIS) för att därefter, vid positivt utfall, släppas som fastställd Internationell Standard (IS).

Testrapporten i sin helhet är författad på engelska och bifogas rapporten i bilaga 5.4 SECOM Test Project – Final report.

4 Nästa steg

Den gemensamt framtagna anlöpsprocessen och identifierade utvecklingsområden bör användas som utgångspunkt i framtida arbete. Under arbetet etablerades en gemensam förståelse för de olika aktörernas prioriteringar kopplat till anlöpsprocessen samt utvecklingsbehov som behöver omhändertas genom framtida samarbetsprojekt. Högst prioriterat av sjöfartsnäringen var tillgång till lots i rätt tid, följt av effektiv informationsdelning. Tillgång till tillförlitlig information, i rätt tid, skapar bättre planeringsförutsättningar för alla aktörer i anlöpsprocessen och digitalisering är ett strategiskt verktyg för att underlätta informationsutbyte aktörerna emellan. Digital informationsdelning är t.ex. en viktig del i att möjliggöra tillgång till lots i rätt tid. Fortsatt branschgemensamt arbete är därmed en nyckelfaktor för att fortsätta resan mot ett mer integrerat och effektivare anlöp. Det branschgemensamma programmet Effektivare anlöp genom digitalisering (Smarta Anlöp) är ett viktigt instrument där Sjöfartsverket, föreningen Svensk Sjöfart, Sveriges Hamnar, Sveriges Skeppsmäklareförening och Näringslivets Transportråd samarbetar för att med digitalisering, automatisering och informationsdelning effektivisera fartygens anlöp till svenska hamnar.

För att möjliggöra ett digitaliserat informationsutbyte krävs investeringar i digital infrastruktur och att nationell utveckling sker med stor lyhördhet för IMO:s och IHO:s internationella standardiseringsarbete. Sjöfartsverket har en viktig roll som infrastrukturhållare för den nationella portalen för myndighetsrapportering, MSW, och som involverad aktör, i större eller mindre utsträckning, i alla handelssjöfartens anlöp till svensk hamn. För att följa med i den digitala utvecklingen och för att implementera förordning (EU) 2019/1239 behöver Sjöfartsverket utveckla sin förmåga till informationsdelning och i större utsträckning dela anlöpsinformation med andra aktörer i anlöpet. I takt med att den digitala mognadsgraden ökar bland anlöpets aktörer kommer automatiserade informationsutbyten att möjliggöra effektivisering av anlöpsprocessen genom processkontroll och processautomation. Det finns förutom teknisk utveckling också behov av fortsatt policyforskning och utveckling av gemensamma arbetssätt, styrningsmekanismer och affärsmodeller för att kunna ta hem effekterna av digitalisering av hamnanlöpet. Enskilda initiativ finns inom området, men mycket arbete återstår innan en effektivare anlöpsprocess finns implementerad.

Sjöfartsverket har även en central roll i att tillhandahålla tillförlitlig sjögeografisk information till handelssjöfarten, men en delmängd av informationen som krävs för säkra anlöp till svensk hamn ansvarar hamnen och inte Sjöfartsverket för. Detta belyser behovet av branschgemensamt samarbete för att skapa nytta för handelssjöfarten. Inledningsvis kommer Sjöfartsverket att verka för att etablera

[12] Technical Committee 80

en lösning för att strukturera och dela den informationsmängd som faller under Sjöfartsverkets ansvar, varpå möjligheten att även integrera hamnars information kommer att undersökas.

Sjöfartsverket fortsätter även att bidra till utveckling av internationella standarder för informationsutbyte genom sitt deltagande inom IMO, IHO och andra internationella organisationer. I kommande branschgemensamma projekt och internt på Sjöfartsverket kommer nya standarder att behöva tillämpas för att möjliggöra informationsutbyte mellan fartyg och land. Genom samverkansprogrammet Effektivare anlöp genom digitalisering kommer Sjöfartsverket även att verka för att information om nya standarder och regelverk som påverkar handelssjöfarten sprids till deltagande partnerorganisationer.

5 Bilagor

5.1 Förstudie anlöpsprocessen och identifiering av utvecklingsbehov
5.2 Förstudie infrastruktur för digitalisering
5.3 Förstudie nautisk tilläggsinformationstjänst
5.4 SECOM Test Project – Final report

5.1 Förstudie anlöpsprocessen och identifiering av utvecklingsbehov

Slutrapport AP1 – Förstudie anlöpsprocessen

Dnr/Beteckning	Rapport
Författare	Sjöfartsverket
Månad År	Januari 2021

Sammanfattning

Anlöpsprocessen involverar ett stort antal aktörer i ett flöde som präglas av höga krav på samordning, informationsdelning och effektiv planering. Detta gör det till en mycket komplex process, där oväntade avbrott eller förändringar får stora konsekvenser för inblandade aktörer och i förlängningen även för Sjöfartens konkurrenskraft i stort. Detta uppdrag syftade till att, tillsammans med branschens aktörer, göra en kartläggning av dagens anlöpsprocess samt identifiera vilka delar av processen som behöver utvecklas.

Arbetet projektleddes av Sjöfartsverket, med branschaktörerna som aktiva deltagare under såväl workshops som enskilda möten. Under arbetet etablerades en gemensam förståelse för de olika aktörernas prioriteringar kopplat till anlöpsprocessen samt utvecklingsbehov. Fortsatt branschgemensamt arbete är en nyckelfaktor för att fortsätta resan mot ett mer integrerat och effektivare anlöp. Den gemensamt framtagna anlöpsprocessen och identifierade utvecklingsområden bör användas som utgångspunkt i framtida arbete. Detta arbetspaket har skapat en samsyn om utgångsläget samt en förväntan bland branschens aktörer om ett gemensamt arbete framåt.

Uppdraget pågick från mars 2020 till januari 2021

Norrköping, januari 2021

Maria Filipsson

Chef Anlöpstjänster

Innehåll

1 Inledning

I avsnitt 1 beskrivs uppdragets bakgrund, syfte och mål, avgränsningar samt leveranser.

1.1 Bakgrund

Detta arbetspaket ingår tillsammans med tre andra arbetspaket i Branschgemensamt digitalt anlöp - fas 1. Trafikverket är huvudsaklig finansiär av arbetspaketen. Sjöfartsverket är projektledare för arbetspaketen och bidrar med ytterligare resurser för arbetet i dem. Externa partners har också utlovat sin tid för arbete i vissa av arbetspaketen, att så sker är en förutsättning för genomförande av Arbetspaket 1.

Arbetspaketet ska ta fram en överenskommen processbeskrivning för anlöp till svenska hamnar, vilken spänner över många organisationer, roller och ansvarsområden.

Arbetet tar sin utgångspunkt i flera befintliga arbeten på området:

- Det finns underlag om anlöpsprocessen hos Sjöfartsverket genom Gothenburg Approach-samarbetet,
- Från PortCDM-arbetet i STM Validation Project och hos
- Port Call Optimization Taskforce som leds av Rotterdams hamn och inkluderar stora hamnar och rederier på global basis.
- Sannolikt finns också anlöpsprocessen och dess olika delar kartlagda av olika hamnar och aktörer.

Befintligt underlag behöver konsolideras och vidareutvecklas för svenska förhållanden där roller och ansvar samt informationsägarskap och informationsflöden beskrivs på ett strukturerat sätt.

Anlöpstjänster driver ett omfattande utvecklingsarbete inom ramen för Vision 2030. Detta arbetspaket är ett fundament för fortsatt utveckling och arbete mot visionen.

1.2 Syfte och mål

Projektmål: Ta fram en översiktlig beskrivning av dagens anlöpsprocess till svenska hamnar. Processen ska vara förankrad hos intressenter och utvecklingsbehov i densamma tydliggjorda.

Effektmål: Nå en ökad kunskap om anlöpsprocessen hos aktörer i processen som möjliggör fortsatt arbete inom Digitalt Anlöp och branschprogrammet Effektivare anlöp genom digitalisering.

1.3 Avgränsningar

I arbetspaketet ingår ej att:

- Ta fram en framtida anlöpsprocess
- Kartlägga eller analysera processer kopplade till anlöpsprocessen som t.ex. den affärsuppgörelse som görs mellan rederi och lastägare eller en terminals godshantering på land efter fartygs last-/lossoperation.

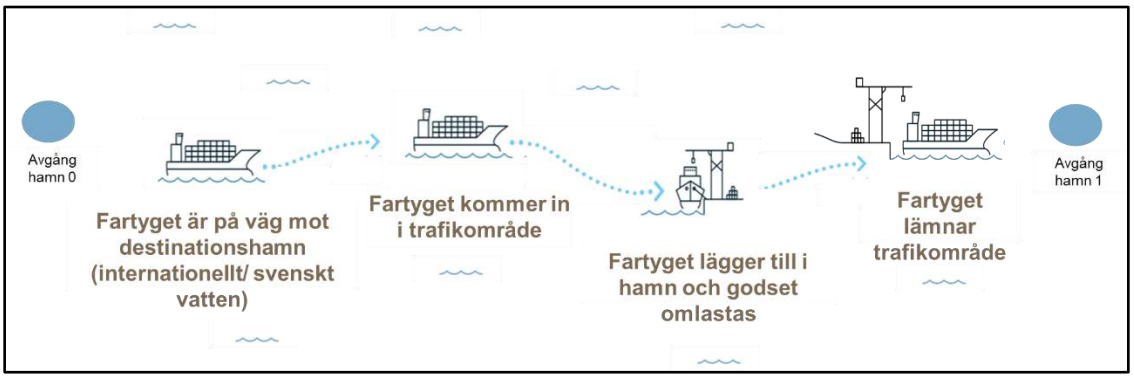
1.4 Leveranser

En förstudie innefattande:

1. Identifiering och tillgång till befintligt material från olika källor som beskriver anlöpsprocessen. Konsolidering och analys av befintligt material.
2. Ta fram en sammanhållen processbeskrivning av nuläget. Processen beskrivs på svenska med engelska begrepp där sådana är fastställda.
3. Informationsflödesanalys av vilka data som används, när och av vem. Beskrivning av roller, ansvarsområden och befogenheter i anlöpsprocessen.
4. Sammanställ utvecklingsbehov i processen
5. Verifiering av anlöpsprocess med flera svenska hamnar, rederier och andra relevanta aktörer för att säkerställa generaliserbarhet och utvecklingsbehov.

1.5 Definition av anlöpsprocessen

Anlöpsprocessen start är ett fartygs avgång från föregående hamn, kallat ”hamn 0” i processen, processen slutar i samband med ett fartygs avgång från innevarande hamn, ”hamn 1”.



Figur 1: Anlöpsprocessens omfattning och avgränsning

2 Genomförande

I detta avsnitt beskrivs vilka som deltagit i arbetet, under vilken tidsperiod det genomförts samt översiktligt vilka aktiviteter som utförts i respektive fas.

2.1 Deltagare Sjöfartsverket

Uppdraget har letts och genomförts av medarbetare inom Sjöfartsverkets enhet Anlöpstjänster samt affärsområde Lotsning. Medarbetare från enheten för Forskning och Innovation har också bidragit, däribland programchefen för Digitalt Anlöp. Enhetschef Anlöpstjänster har varit projektledare. Konsulter från Ekan Management har bidragit med planering och genomförande av uppdraget.

2.2 Externa branschaktörer

Nedan listas de partners och övriga intressenter som involveras i arbetspaketets genomförande. Aktörerna har bidragit genom informationsinsamling kring dagens anlöpsprocess och/eller genom att delta på minst ett av workshop-tillfällena.

- Sveriges Hamnar
- Gävle Hamn

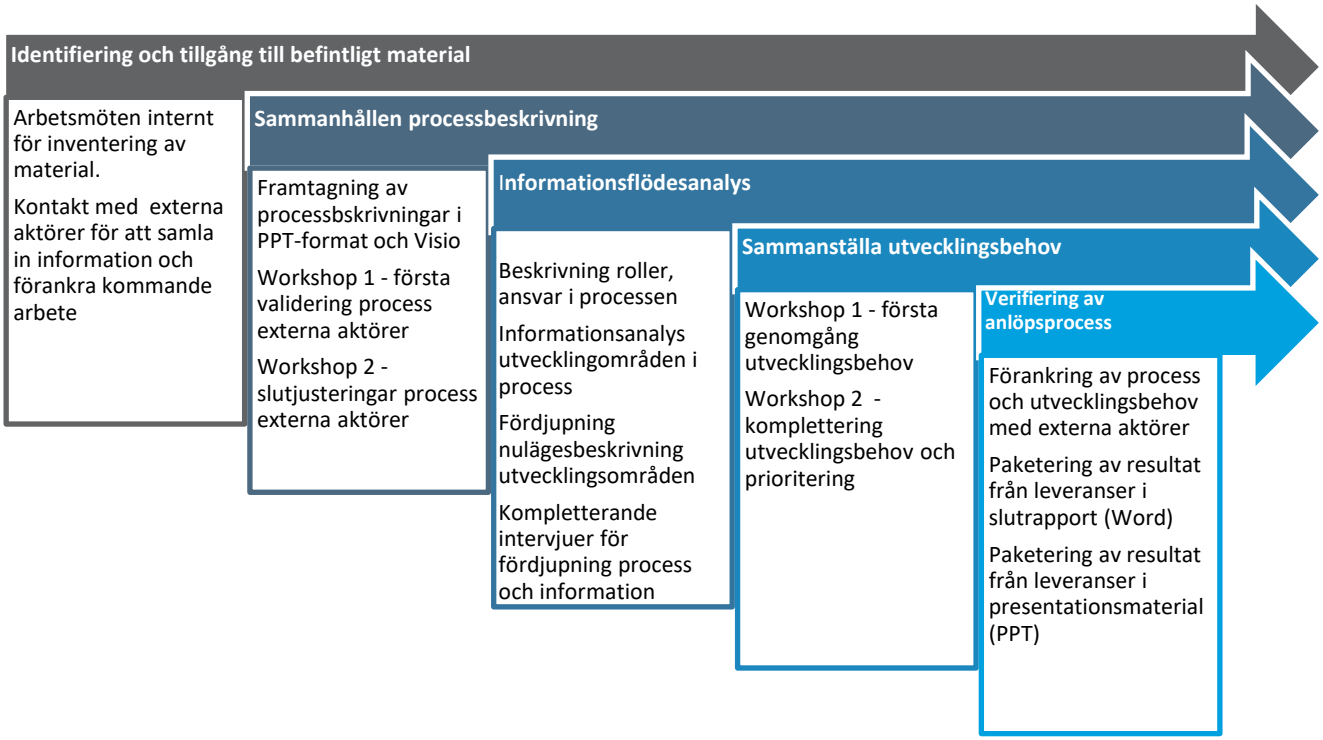
- Stockholms Hamnar
- Göteborgs Hamn
- Norrköpings Hamn
- Preem
- Sveriges Skeppsmäklarförening
- Shorelink Shipping
- Sjöfartsverket
- Näringslivets transportråd
- Metsä Board Sverige
- Bror Andrén
- TSA Agency Sweden
- Valdemar Andersson Skeppsmäkleri
- Ocean Network Express (ONE)
- SDK Shipping
- Haegerstrands
- OP Ship

2.3 Tidsramar

Uppdraget genomfördes 2020-04 till 2021-01. Tidplanen och arbetspaketets leveranser illustreras i figuren nedan.

2.4 Faser, aktiviteter och metodik

På bilden nedan illustreras vilka aktiviteter som genomfördes kopplat till respektive leverans.

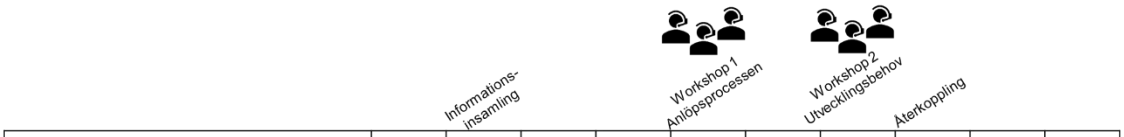


Figur 2: Översikt aktiviteter i respektive fas.

I juni samlades befintligt material kring anlöpsprocessen in. I september genomfördes workshops med dessa aktörer, med syfte att etablera en gemensam bild av anlöpsprocessen. I

november bjöds samma deltagare in till en uppföljning med temat utvecklingsbehov i processen.

Workshoptillfällena genomfördes i digital form, där det lades stor vikt vid att samtliga deltagare tillfrågades om sina respektive förväntningar, funderingar, synpunkter och konkret input till såväl anlöpsprocessen som utvecklingsbehov. Under mötets gång dokumenterades synpunkter och tankar direkt i materialet, så att deltagarnas egna ord skulle få forma analysen. Materialet skickades ut till deltagarna, för att möjliggöra ytterligare synpunkter. Ett antal kompletterande enskilda intervjuer genomfördes också för att fördjupa kunskapen om nuläget och utvecklingsbehov. I december genomfördes ett Skype-möte där deltagarna fick möjlighet att ge ytterligare återkoppling utifrån det samlade materialet kring anlöpsprocessen och utvecklingsbehov. I januari sammanställdes slutrapport och presentationsmaterial (se bilaga Presentationsmaterial AP1).



Aktiviteter	Maj	Juni	Juli	Aug	Sep	Okt	Nov	Dec	Jan	Feb
Skicka in ev. befintliga beskrivning av arbetssätt/ processer kring anlöpsprocessen										
Workshop 1: Anlöpsprocessen • Syftar till att skapa en gemensam översiktlig bild av anlöpsprocessen • Bidra med förslag på utvecklingsbehov										
Workshop 2: Utvecklingsbehov • Sammanställa utvecklingsbehov • Förankra beskrivning av anlöpsprocessen										
Remiss och återkoppling										
Ta del av resultat och förslag handlingsplan										

Figur 3: Involvering av externa aktörer i genomförandet

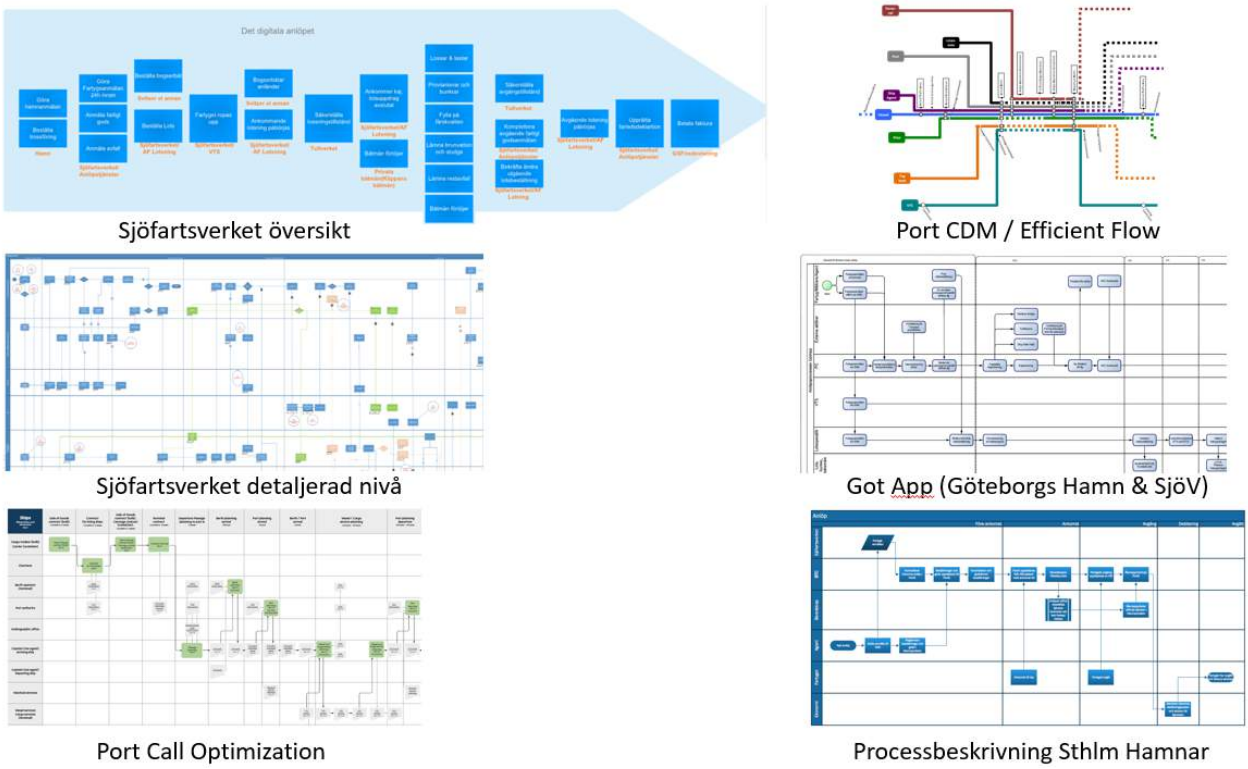
3 Resultat och analys

I detta kapitel redovisas resultaten, grupperat utifrån de leveranser som är beskrivna i uppdragsplanen.

3.1 Leverans 1: Identifiering och tillgång till befintligt material

Det har tidigare genomförts ett antal arbeten på temat effektivisering av anlöpsprocessen, både i Sjöfartsverkets egen regi men också i olika branschgemensamma samarbetsformer. För att säkerställa att tidigare insikter och kunskaper tas om hand, så har befintligt material använts under projektets gång, se punktlista och figur nedan.

- Sjöfartsverket-projekt anlöpsprocessen
- Port CDM & EfficientFlow
- Gothenburg Approach
- Port Call Optimization
- Processbeskrivning från Stockholms hamnar
- Beskrivningar av dagens arbetssätt i löptext, från ett fåtal hamnar, mäklare, godsägare



Figur 4. Exempel på resultat från inventering av befintligt material kring anlöpsprocessen.

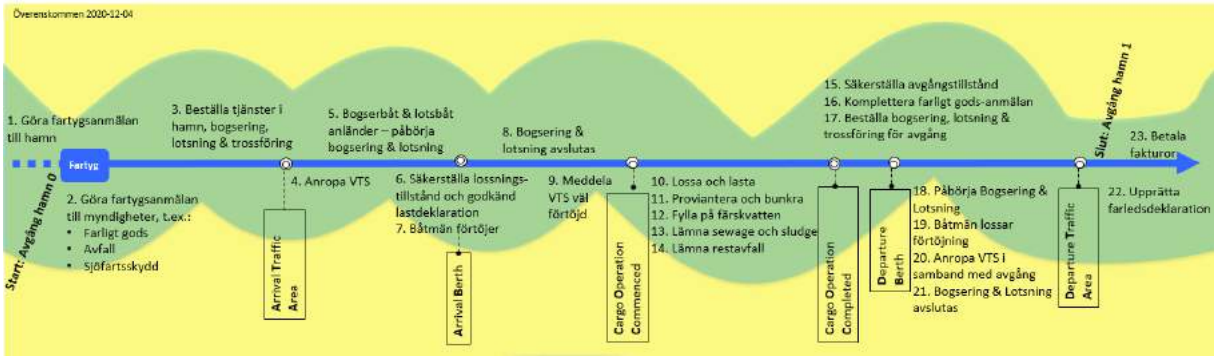
3.1.1 Analys befintligt material

Det befintliga materialet har alla olika utgångspunkter, i linje med syftet som respektive aktör har haft under arbetet med framtagningen av beskrivningarna. Detaljeringsnivån varierar och vissa av beskrivningarna har någon särskilt aktör i huvudfokus, vilket också färgar utformningen. Processernas avgränsningar skiljer sig också något åt vilket visas genom variationer i start- och slutpunkter. I stora drag har dock beskrivningarna mycket gemensamt, där ett kännetecken är ”fartyget i centrum”. Fartyget i centrum används som utgångspunkt i detta uppdrag liksom sättet att använda tidsstämplar i Port CDM och Efficient flow.

Sammantaget finns flertalet beskrivningar från olika utvecklingsprojekt. Dessa beskrivningar använder olika nomenklatur och har olika syften och avgränsningar, vilket medför risk för att olika aktörer pratar förbi varandra, med glasögonen slipade efter den egna processen. Däremot saknas oftast utförliga processbeskrivningar som används internt av de olika aktörerna. När aktörerna ombads att skicka in sina respektive processbeskrivningar, blev det i nästan alla fall en beskrivning i textform som togs fram till detta tillfälle, dvs. det var inte fastslagna dokument sedan tidigare. Behovet av en gemensam, överenskommen anlöpsprocess på övergripande nivå bedömdes därmed av aktörerna vara stort, och glädjande nog har arbetet mynnat ut i just det (se leverans 2).

3.2 Leverans 2: Sammanhållande processbeskrivning

I arbetet har en processbeskrivning på översiktlig nivå arbetats fram i flera steg. De externa branschaktörerna kunde vid det avslutande mötet i december bekräfta att slutresultatet i figuren nedan stämmer.



Figur 5. Övergripande beskrivning av befintlig anlöpsprocess.

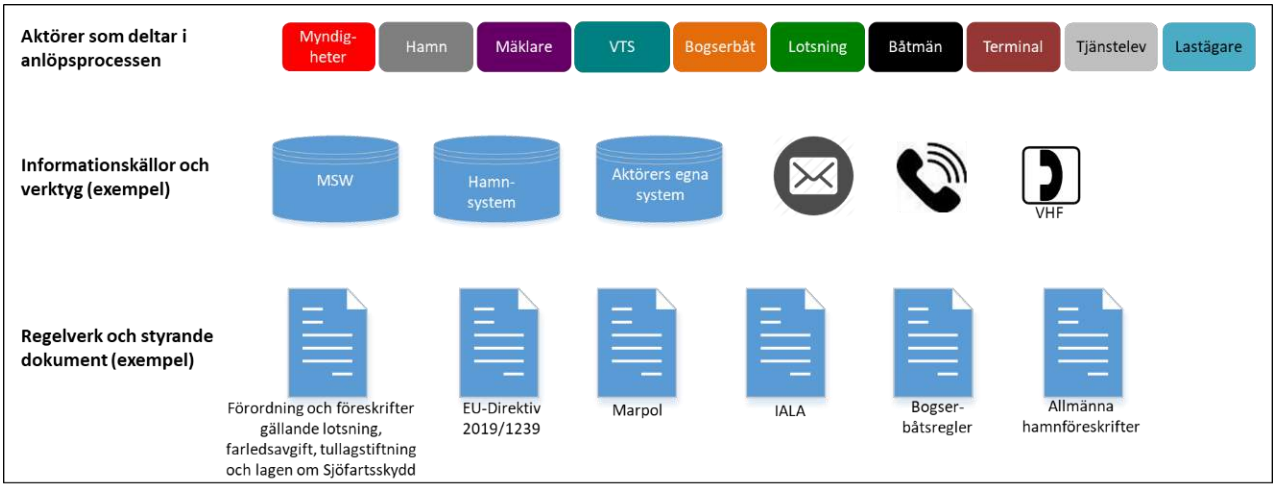
3.2.1 Förutsättningar för processbeskrivningen

Som inramning till beskrivningen finns ett antal förutsättningar:

- Affärsuppgörelse finns mellan rederi och lastägare, terminal/ hamn/ agent grovplanerar anlöpet
- Konsekvenser av ändringar i ETA visas inte. ETA uppdateras av aktör som får kännedom om nya förutsättningar.
- Anmälan och beställning av tjänster kan ske både tidigare och senare, beroende på typ av anlöp och ankommande hamn
- Aktörers interna planering beaktas ej

3.2.2 Aktörer, informationskällor och regelverk

I ett anlöp samspelar många olika aktörer, informationskällor och regelverk, vilket gör det till en komplex process. Samarbete är en framgångsfaktor för att utveckla anlöpsprocessen, skapa effektivitet och stärka Sjöfarten som transportslag.



Figur 6. Aktörer, informationskällor och regelverk i dagens anlöpsprocess.

Tabell 1. Aktörernas ansvar, befogenheter och önskade nyttor.

Aktör	Ansvar och befogenheter i anlöpsprocessen	Önskade nyttor med effektiv anlöpsprocess
Fartyg	• Transporterar gods och/eller passagerare mellan hamnar • Direkt samverkan med övriga aktörer i anlöpsprocessen • Lämnar uppgifter inför anlöpet i form av avsikt med anlöpet, last, planerade tider • Bokar tjänster som önskas i hamn	• Strömlinjeformad process, så få kontaktytor som möjligt • Optimera bränsleförbrukning till sjöss • Förkorta liggetid vid kaj
Hamnar	• Skapa förutsättningar för handel i respektive region, genom konkurrenskraftig hamnverksamhet • Motta hamnanmälan • Skapa förutsättningar för lossning och lastning • Hantera avfall, gods, passagerare • Isbrytning i hamnområdet • Uppdaterar anlöpsinformationen	• Strömlinjeformad process, möjlighet att ta emot större volymer gods och passagerare • Förkorta liggetid vid kaj • Informationsdelning i realtid • Automatiserade digitala flöden • Miljöaspekter
Mäklare	• En redares juridiska representant i en hamn/land som ser till att hamnuppehållet genomförs på ett så praktiskt sätt som möjligt vilket exempelvis innebär att kommunicera med stuverier, speditörer, lastägare och hamnmyndigheter • Den part som ”äger” anlöpet och är betalningsgarant i Sverige	• Informationsdelning i realtid • Mer standardiserat och gemensamt arbetssätt i branschen minskar arbetsbörda
Kombination hamn och godsägare	• Godsägare • Egen hamn • Säkra lastning och lossning • Motta hamnanmälan i egen hamn	• Tider, volymer och annan information är viktig för planering och effektivitet när fartyg ligger vid kaj • Informationsdelning i realtid • Optimerad planering för kritiska resurser
Kombination hamn och terminaloperatör	• Logistik och transportföretag som driver operativ verksamhet i hamnar med bland annat lastning och lossning • Mottagare och sändare av information kopplat till lossning, lastning, deklaration etc. i anlöpsprocessen	• Informationsdelning i realtid • Automatiserade digitala flöden • Ökad samverkan • Innovativa anlöpstjänster • Optimerad planering för kritiska resurser
Lotsning	• Lotsning är en tjänst som Sjöfartsverket tillhandahåller • Utifrån de lotsbeställningar som görs via MSW Reportal och direkt till Lotsplaneringscentralen • Lots ska planera, genomföra och koordinera den specifika fysiska lotsningen från bordningspunkten till kaj	• Kunna planera sina resurser på ett effektivt sätt • Få tillgång till uppgifter om fartygets ankomst- och avgångstider till kaj, i god tid innan • Framföra fartyg säkert till/från lotspliktslinjen till/från kaj • Informationsdelning i realtid

		• Automatiserade digitala flöden
Bogserbåt	• Bogsera fartyget till/från kaj	• Kunna planera sina resurser på ett effektivt sätt. Få tillgång till uppgifter om fartygets ankomst- och avgångstider till kaj, i god tid innan. Framföra fartyg säkert från hamnområde till/från kaj • Informationsdelning i realtid • Automatiserade digitala flöden
Tjänsteleverantör	• Tillhandahålla tjänster till fartyget vid kaj, som ej är möjliga till sjöss • Fylla på t.ex. färskvatten, tömma avfall	• Få tillgång till uppgifter om fartygets ankomst- och avgångstider till kaj, i god tid innan • Informationsdelning i realtid • Automatiserade digitala flöden
Terminal	• Ansvara för lossning och lastning • Bekräfta när lastning, lossning påbörjas och slutförs	• Få tillgång till uppgifter om fartygets ankomst- och avgångstider till kaj, i god tid innan • Informationsdelning i realtid • Automatiserade digitala flöden
Båtmän	• Förtöja fartyget till kaj	• Få tillgång till uppgifter om fartygets ankomst- och avgångstider till hamnområde, samt ev. ändringar • Informationsdelning i realtid • Automatiserade digitala flöden
VTS	• Övervaka och informera om aktuell sjöfart inom respektive hamnområde • Ge klartecken, dela sjötrafikinformation	• Få tillgång till alla aktörers senaste uppdateringar • Informationsdelning i realtid • Automatiserade digitala flöden
Sjöfartsverket, Tullverket, Kustbevakningen, Transportstyrelsen	• Myndighetsutövning och möjliggörare av sjöfart på svenskt vatten • Ta emot och distribuera information via systemet MSW Reportal	• Få tillgång till relevant information • Informationsdelning i realtid • Ökad samverkan • Innovativa anlöpstjänster • Automatiserade digitala flöden • Miljöaspekter
Isbrytning	• Ansvarig att lederna är seglingsbara fram till hamnområdet	• Informationsdelning i realtid för att kunna effektivisera isbrytningen och väntetider för fartyg

3.2.3 Detaljerad anlöpsprocess – 3 exempelanlöp

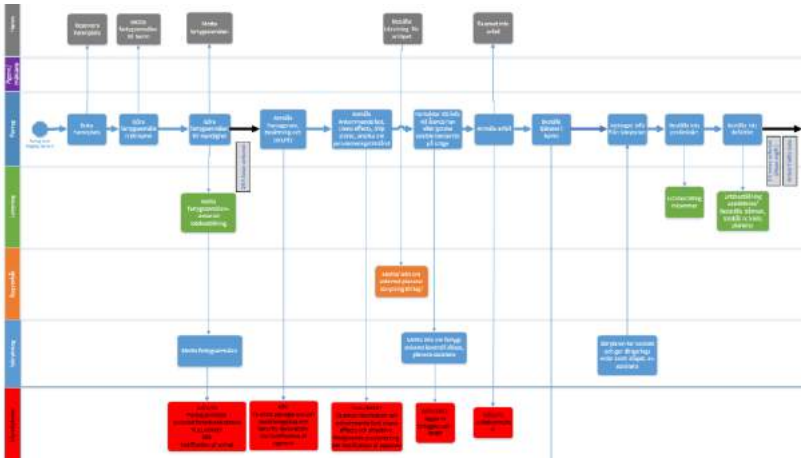
Baserat på den övergripande beskrivningen av dagens anlöpsprocess har beskrivningar av anlöpsprocessen på detaljerad nivå gjorts för tre exempelanlöp:

1. Gävle: Anlöp med isbrytning

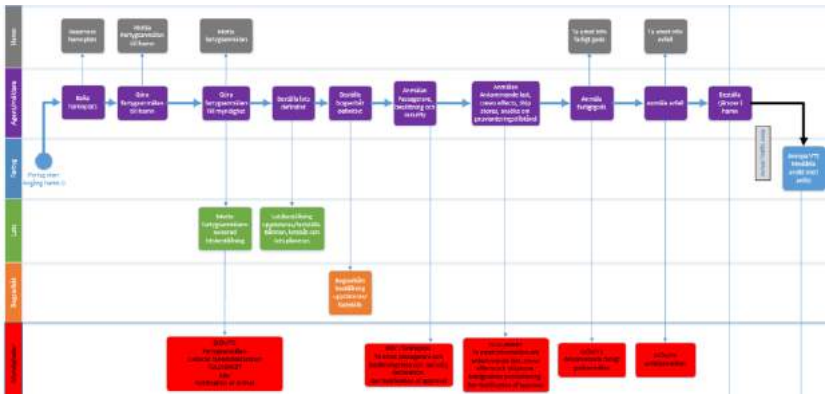
2. Stockholm: Anlöp kryssningsfartyg
3. Göteborg: Anlöp med lots och bogsering

De här beskrivningarna har tagits fram med hjälp av personer utanför arbetsgruppen med kännedom om respektive anlöpstyp och hamn. Underlagen har inte förankrats hos alla externa aktörer utan kan ses som stöd för ev. kommande gemensamt utvecklingsarbete.

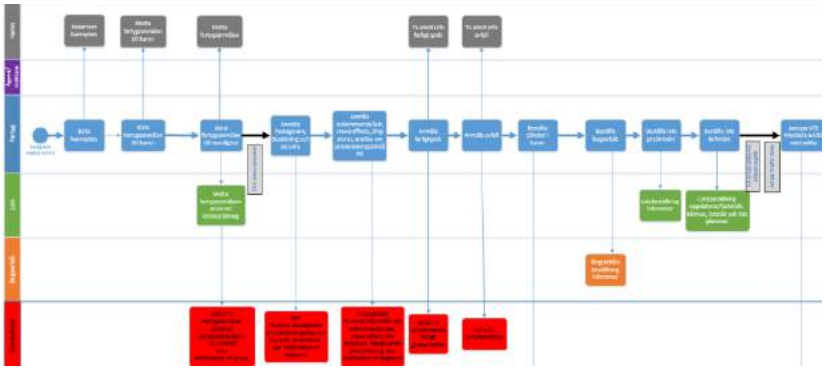
Processerna är beskrivna i flödesscheman, där originalfilerna (gjorda i programmet Visio) finns som bilagor. Delar av processerna är inklippta nedan för att ge en bild av beskrivningssätt och detaljeringsgrad. I dessa beskrivningar fångas aktiviteter mer i detalj, det framgår vilka aktörer som gör vad, vilka regelverk/rutiner som styr och stödjer liksom informationskällor som används.



Figur 7. Isbrytningsanlöp, Gävle Hamn.



Figur 8. Kryssningsanlöp, Stockholms Hamnar



Figur 9. Anlöp med bogsering och lots, Göteborgs Hamn.

3.2.4 Kostnader för ett anlöp

I syfte att få en inblick i nuläget avseende direkta kostnader förknippade med anlöpsprocessen har ett antal kostnadsposter för olika typer av anlöp studerats. Kostnaderna som inkluderats är:

- hamnavgift (som en parkeringsavgift för utnyttjandet av kaj),
- varuhamnsavgift (avgift för gods/passagerare),
- lossning- och lastningsavgifter (stuveri, kranar),
- lotsavgifter,
- bogserbåtsavgift,
- linesmen/tross,
- avgifter för olika tjänster i hamn,
- farledsavgift för fartyget,
- farledsavgift för gods/passagerare,
- bränslekostnader,
- vessel time charter,
- arvode agent

Olika poster väger olika tungt beroende på hamnens geografiska läge, t.ex. så utgör lotskostnaden en större del där lotsningen tar längre tid som i Vänern och Mälaren, medan hamnar som har kortare lotstid t.ex. Göteborg innebär en lägre lotskostnad. Under vinterhalvåret blir hamnavgiften högre i vissa hamnar då beredskap för hamnisbrytning finns. Beroende på fartygets last så tar lossning och lastning olika lång tid och är olika resurskrävande vilket gör att kostnadsandelen varierar mycket mellan olika anlöp.

Sammanfattningsvis kan konstateras att jämförelsen av kostnader i ett antal anlöp ger en tydlig bild över att kostnadsstrukturen skiljer sig åt markant. Eftersom det skiljer sig åt är det viktigt att analysera kostnader ytterligare för att förstå hur priskänsliga olika hamnar och anlöpstyper är. Dessa analyser kan också bidra till att förstå hur Sjöfarten kan stärkas i relation till andra transportslag.

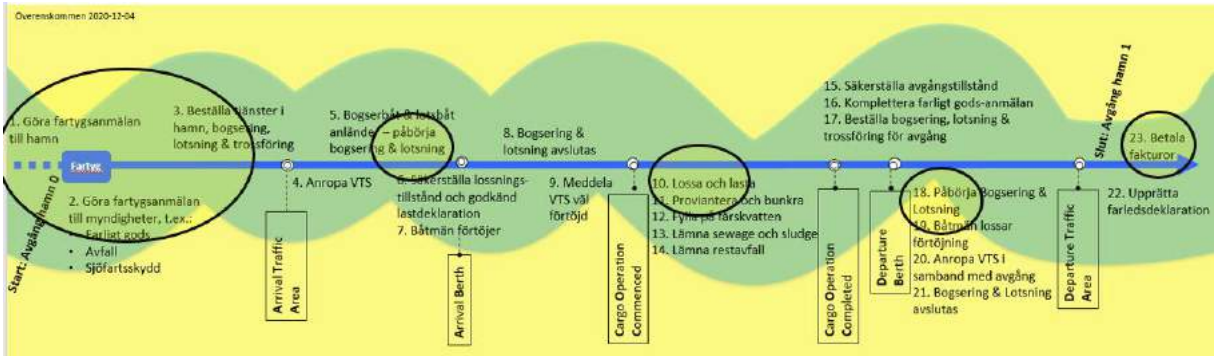
3.2.5 Analys Processbeskrivning

Under arbetet har det framkommit att olika aktörer har olika fokus. Trots detta har det gått förvånansvärt smärtfritt att hitta en enighet på en övergripande nivå. Flera aktörer har uttryckligen betonat att denna beskrivning bidrar med ett stort värde, och någon hade

omgående sett en stor nytta med underlaget och förankrat det i sin organisation med ambitionen om att lägga in i sitt ledningssystem. De mer detaljerade processbeskrivningarna bygger på den övergripande och tydliggör att olika typer av anlöp har mycket gemensamt men att ex. ordningsföljd på aktiviteter och roller i anlöpet kan skilja sig åt.

3.3 Leverans 3: Informationsflödesanalys

Informationsflödesanalysen togs fram utifrån insikter från workshoptillfällena. I bilden nedan ringas delar av processen in, där det är särskilt viktigt att information kan delas mellan aktörerna på ett tillfredsställande sätt. Mer detaljerade beskrivningar för de inringade delarna nedan återfinns i bilaga Informationsflödesanalys. Respektive område beskrivs utifrån vilken information som behövs, hur informationen delas och en nulägesbeskrivning.



Figur 10: Informationsflödesanalys i processen.

3.3.1 Fartygsanmälan till hamn och myndigheter

Under workshoptillfällena framgick att många av de problem som uppstår under anlöpsprocessen kan härledas till brist på informationsdelning tidigt i processen. Mer specifikt pekades fartygsanmälan till hamn och fartygsanmälan till myndigheter ut som en källa till problem. Det saknas ett gemensamt sätt att dela informationen mellan aktörer, vilket innebär dubbel- och trippelarbete som medför en diskrepans i informationen kring ett anlöp i olika system. Den låga användarvänligheten innebär en tröghet i ändringshanteringen då det är omständligt och tidskrävande, en part kan ha uppdaterad information, andra inte.

Utifrån denna problembeskrivning gjordes en inventering av 23 av Sveriges största hamnar. Sammanfattningsvis kan det beskrivas principiellt enligt följande:

Tabell 2. Inventering av fartygsanmälan till olika hamnar.

Antal hamnar	Fartygsanmälan via	Koppling/Integration till MSW	Hur skickas in till Hamn
2 st	MSW-formulär	MSW-integration	Via MSW → Hamn
6 st	Webb-formulär (Olika utformning)	Locode SSNS-koppling eller koppling saknas	Via hemsida
9 st	Blankett (Olika utformning och format, PDF, Word m.fl.)	Locode SSNS-koppling eller koppling saknas	Mailkorgar till olika avdelningar Fax
6 st	Ej beskrivet	Koppling saknas	Ej beskrivet

Förutsättningar för SSNS-koppling för fler hamnar

Under arbetets gång har det konstaterats att fler hamnar än idag vill ha tillgång till myndighetsinformation kring anlöpet i deras hamnsystem. Sådan koppling finns idag mellan MSW och PortIT. Det finns även möjlighet för hamnar att få tillgång till viss myndighetsinformation kring anlöpet via SSNS (Safe Sea Net Sweden). Hamnar som vill utnyttja denna möjlighet vänder sig till Sjöfartsverket och Sjötrafikservice, förvaltningen för Sjöfartsnära tjänster, för vidare hantering.

3.3.2 Lotsning

Ett område som ofta uppfattas som flaskhals i anlöpsprocessen är lotsning, där en av orsakerna kan vara att inblandade aktörer saknar information. Idag skickas information om lotsning inte vidare från MSW till exempelvis hamnsystem eller bogserbåtsbolag, vilket leder till svårigheter att optimera planeringen. På vissa håll i Sverige är dessutom tillgången på lots särskilt begränsad, vilket i kombination med avsaknad av uppdaterad information kan leda till förseningar såväl som ökade kostnader.

3.3.3 Lossa och lasta

Inför lossning och lastning behöver tillstånd och dokumentation vara godkända. Till detta godkännande behöver information hämtas in från flertalet aktörer i anlöpsprocessen. Om denna information inte kan delas i rätt tid uppstår ofta förseningar för det enskilda anlöpet, men också följdeffekter för fartyget vid nästa hamn, samt för andra fartyg i samma hamn i det fall att beläggningen är hög.

3.3.4 Betala fakturor

De olika aktörerna har en rad olika avgifter som faktureras på varierande vis. Om en mäklare är anlitad så samlar den ihop fakturorna och ser till att rätt aktörer betalar rätt fakturor. Administrationen och hanteringen av fakturor uppfattas vara ett område som kan bli mer effektivt och transparent.

3.3.5 Analys informationsflöden

Vid en närmare genomgång av anlöpsprocessen och alla inblandade aktörer så blir det uppenbart att det är ett stort informationsflöde. Det saknas en central plats för alla aktörer att hämta och lämna information på, vilket gör att antalet kontaktytor i form av system, mail, och telefonsamtal blir mycket tidskrävande och att det blir svårt att ha en gemensam uppdaterad bild av aktuellt läge. Ett citat från ett av workshoptillfällena kan lyftas fram som ett talande exempel:

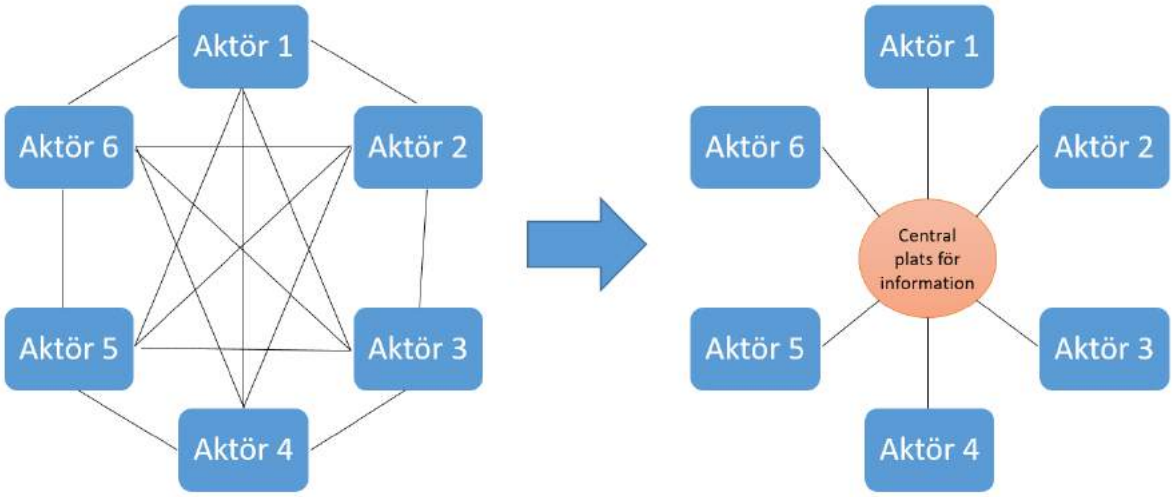
”Hela branschen ringer ihjäl sig!”

Ju fler aktörer som är inblandade, desto större är anledningen att ha en central plats för information som delas med andra, eftersom antal kontaktytor ökar exponentiellt för varje ny aktör. Detta illustreras i tabellen och figuren nedan.

Antal aktörer	**Antal kontaktytor** Om direktkontakt mellan aktörer	**Antal kontaktytor** Om central plats för information

6	15	6
10	45	10
15	105	15
20	190	20

Tabell 3. Antal kommunikationsytor vid central plats för information, jämfört med direktkontakt mellan alla aktörer.

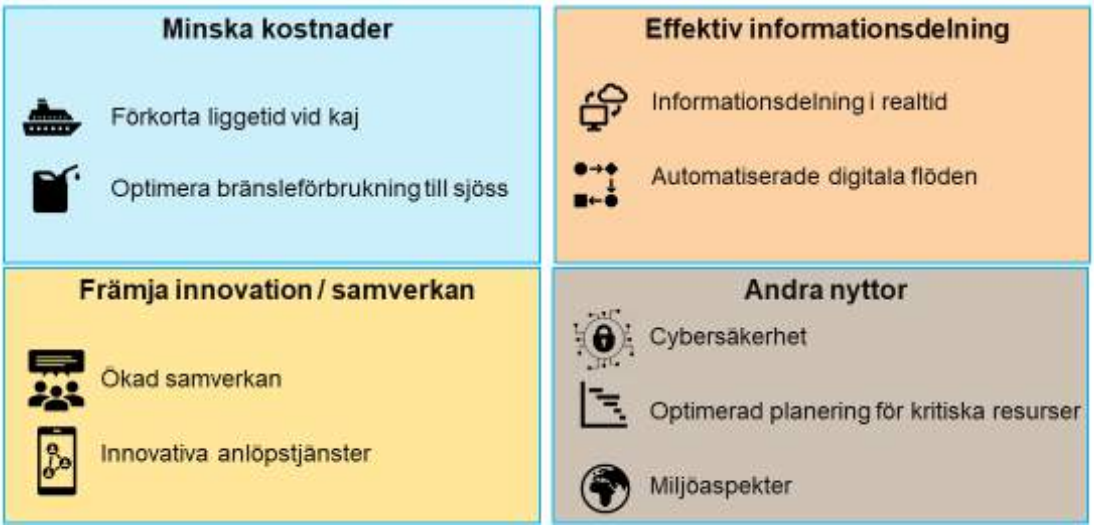


Figur 11. Principiell skiss som visar informationsflöde där informationen går direkt mellan aktörer (vänster), jämfört med ett alternativ där all information samlas på en central plats för information.

3.4 Leverans 4: Sammanställa utvecklingsbehov

Utvecklingsbehov kategoriserades enligt fyra på förhand definierade kategorier, som baserades på projektplanen för ”Branschgemensamt digitalt anlöp”, samt uppdragsplanen för detta arbetspaket. Kategorierna illustreras i figuren nedan, och sammanfattas i punktlista här:

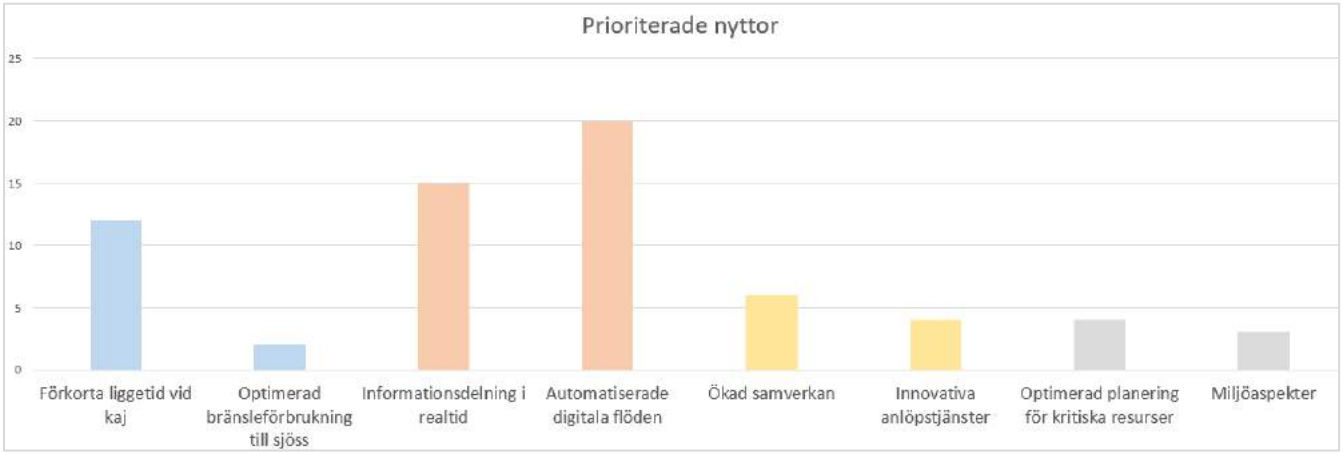
- Minska kostnader (blått)
- Effektiv informationsdelning (orange)
- Främja innovation/samverkan (gul)
- Andra nyttor (grå)



Figur 12. Långsiktiga nyttor med en utvecklad och digitaliserad anlöpsprocess.

3.4.1 Prioriterade nyttor

Under en workshop ombads aktörerna att prioritera vilka nyttor som är viktigast utifrån deras eget perspektiv. Summan av poängen visas i figuren nedan, där det framgår att nyttorna kopplat till effektiv informationsdelning fått flest poäng.



Figur 13. Summering av aktörernas prioritering av nyttor.

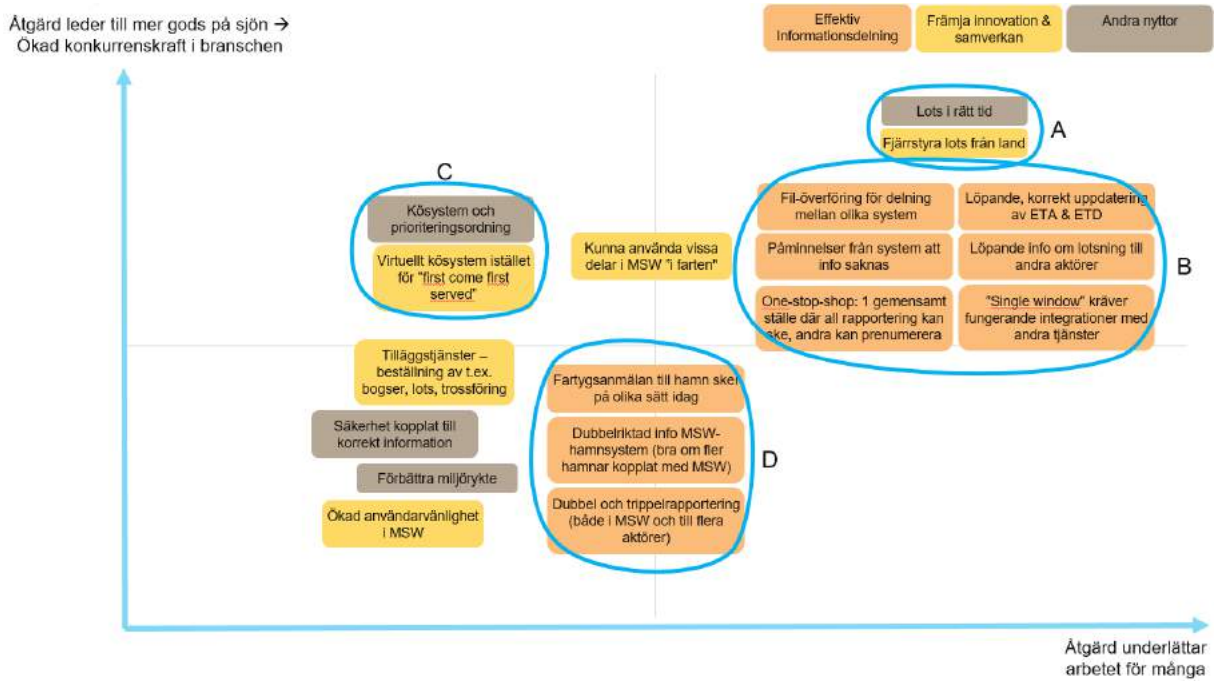
Fördelningen av poäng skilde sig mycket mellan olika aktörer, där hamnarna i huvudsak höll med varandra, godsägarna höll med varandra och agenterna höll med varandra. Godsägare hade fokus kostnaderna – det vill säga liggetid vid kaj och bränsleförbrukning, hamnarna på informationsdelning i realtid och automatiserade digitala flöden. Agenterna svarade likt hamnarna, med tillägget att de också önskad en ökad samverkan med de andra aktörerna.

3.4.2 Sammanställning utvecklingsbehov

Under workshoptillfällena och i arbetsmöten lyftes utvecklingsbehov upp av aktörerna. I figuren nedan ser vi den konsoliderade versionen, där vissa utvecklingsbehov som angränsar till varandra har grupperats (A-D), och vissa ligger ensamma. Färgkodningen från ovan hänger med här.

Placeringen i bilden beror på två faktorer. På den vågräta axeln handlar det om ifall en åtgärd i linje med utvecklingsbehovet skulle underlätta arbetet för många aktörer i anlöpsprocessen, eller få. Ju längre till höger, desto fler förväntas få en enklare vardag.

Den lodräta axeln handlar om vilken grad av nytta i form av sänkta kostnader, förbättrade intäkter, eller andra sätt som en åtgärd kan stärka konkurrenskraften för branschen. Ju högre upp, desto större nytta och möjlighet till förbättrad konkurrenskraft. Värt att poängtera är att bilden jämför åtgärderna relativt varandra, inte i förhållande till åtgärder som ligger utanför denna konstellations direkta påverkansmöjlighet såsom åtgärder kring avgifter eller skatter från politiskt håll.



Figur 14. Sammanfattning av utvecklingsbehov.

I tabellen nedan är utvecklingsbehoven fortsatt grupperade enligt A-D samt ”Övriga”. I denna tabell anges vilken del av anlöpsprocessen som utvecklingsbehoven har stark koppling till, en beskrivning av vad som skulle behöva göras samt vilken nytta en önskad åtgärd skulle leda till.

Tabell 4. Kommentarer och beskrivning utvecklingsbehov.

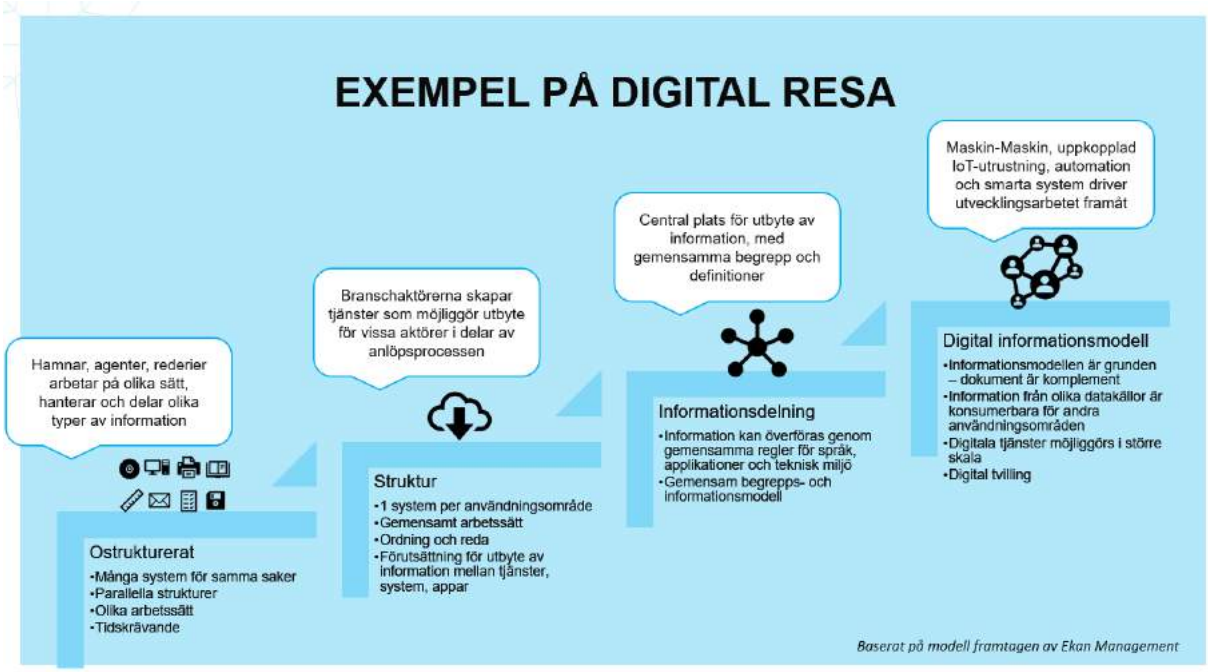
Grupp	Rubrik	Koppling processen	Beskrivning av åtgärdsbehov	Nytta/ önskad åtgärd
A	Tillgång till lots	Beställning av tjänster/lots. Påbörja lotsning, både in och ut ur hamn	• Ur en transportköpares synvinkel är pålitligheten i processen viktig, lots i rätt tid är en viktig faktor. • Kostnader för lotsning till och från Vänern och Mälaren kan uppgå till lika mycket eller mer som kostnaderna för lossning & lastning.	• Säkrare anlöpstider • Lägre kostnader • Stärkt pålitlighet för transportslaget
B	Effektiv informations-delning	Framför allt i början av process, samt ännu tidigare	• Förbättrad informationshantering är början till informationsdelning i realtid -> effektivare anlöp • Angående påminnelser från system – olika hamnar kräver olika information, kan underlätta för agent om MSW ger påminnelser om info saknas. • Turlista/planering för isbrytning skulle behöva tydliggöras • Synka rapportering av farligt gods	• Aktörer har samstämmig bild och uppdaterad info om anlöpet • Effektivare arbetssätt
C	Tydligt och tillförlitligt kösystem	Fartygsanmälan till hamn	• Möjliggöra ”slow steaming” och ”just in time” • ”Virtuell köbricka” istället för ”first come first served”	• Lägre kostnader • Mindre bunker • Lägre miljöpåverkan

D	Enhetliga förutsättningar och arbetssätt	Fartygsanmälan till hamn och myndigheter	• Varierande formulär och blanketter ställer främst till det för agenter, men försvårar även för standardisering och i förlängningen automatisk informationsdelning • Att vissa hamnar har koppling till/ prenumeration från MSW medan andra saknar orsakar brister i effektivitet och kvalitet i processen • Samarbetet mellan myndigheter (SjöV, Tullverket, Transportstyrelsen och Kustbevakningen) kring MSW behöver utvecklas	• Effektivare enhetligt arbetssätt • Minskad arbetstid
	Övriga		• Att arbeta ”i farten” ex. genom app underlättar uppdateringar av ETA och ETD och statusändring på lotsbeställning. • Förbättrat miljörykte kan uppnås genom andra effektiviseringar, se gruppering A & C • Tilläggstjänster – beställning av t.ex. bogser, lots, trossföring • Angående användarvänlighet i MSW – idag läggs ex. last och kaj in på flera ställen. • En högre användarvänlighet av MSW betyder bl.a. möjlighet att tanka ner data till enskilda verksamhetssystem	• Effektivare arbetssätt • Stärkt konkurrenskraft för transportslaget • Ökad datakvalitet genom minskad dubbelrapportering

3.4.3 Digitaliseringstrappa

Utveckling och digitalisering sker ofta stegvis. Anlöpsprocessen är inget undantag. Vissa av processens aktörer har kommit längre än andra, vissa delar av processen är helt analoga och andra har stora inslag av digital informationsdelning.

Ett sätt att beskriva utvecklingens olika steg är att se det som en trappa. Olika aktörer och delar i processer kan befinna sig på olika trappsteg. Om vi ser på anlöpsprocessen som helhet så har detta arbetspaket visat att vissa tidiga delar i processen, exempelvis fartygsanmälan till hamn (se avsnitt Informationsflödesanalys) från ett helhetsperspektiv är ***Ostrukturerat***, där det finns olika dokument och arbetssätt mellan olika hamnar, vilket försvårar för såväl agenter som för en enhetlig informationsdelning med fler aktörer. Nästa steg, ***Struktur***, kännetecknas av gemensamma arbetssätt och en mindre spretig systemflora. Där kan fartygsanmälan till Myndigheter tas upp som exempel, där rapportering till MSW sker på ett standardiserat sätt. Nästa steg är ***Informationsdelning***, vilket innebär att det finns en central plats för utbyte av information, med gemensamma begrepp och definitioner. Detta saknas idag, men kan ses som en framtida möjliggörare för Informationsdelning i realtid och flera av de nyttor som identifierats i branschprogrammet som helhet. Ett ytterligare framtida steg kan vara uppkopplad IoT-utrustning, digitala tvillingar och smarta system som kan driva utvecklingsarbete framåt. Detta steg kan benämnas på många olika sätt, men vi har valt att beskriva det som att det finns en ***Digital Informationsmodell***.



Figur 15: Digitaliseringstrappa – exempel på en digital resa inom olika delar av anlöpsprocessen.

3.4.4 Analys utvecklingsbehov

Den röda tråden i diskussionerna kring utvecklingsbehov har varit utbytet av relevant information. Det största behovet av informationsdelning uppstår tidigt i processen i samband med fartygsanmälan till hamn och myndigheter samt hantering av förändringar och uppdateringar av tider. Problem som uppstår kring tillgång till lots, onödig förbrukning av bunker på sjön eller kostnader för längre liggetid vid kaj kan i vissa fall härledas till brister i planering som beror på att information saknas.

Situationen med mörkerrestriktioner och brist på lots leder till särskilda svårigheter i de nordliga hamnarna under vintermånaderna. I och med att tidsfönstret är smalt och tillgång på lots låg finns risken att fartyg får ligga kvar vid kaj och vänta till nästkommande dag. Detta medför extrakostnader, kan kräva högre fart på sjön till nästa destination vilket påverkar kostnader och får miljöpåverkan. Navigationsstöd från land skulle vara något som kan bidra till att sänka kostnaderna för sjöfarten och därmed stärka branschens konkurrenskraft. Branschaktörerna ser att det behövs en ambitiös plan för detta, där det görs ett business case utifrån de pengar som kan sparas om detta kommer på plats.

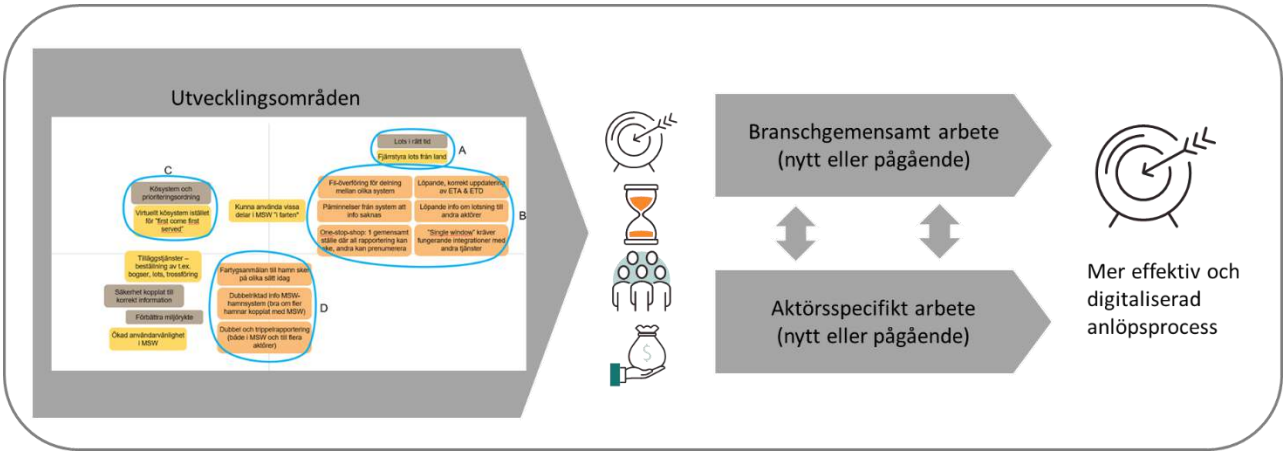
3.5 Leverans 5: Verifiering av anlöpsprocessen med aktörer

Slutresultatet av samarbetet med branschens aktörer kring anlöpsprocessen och utvecklingsbehov beskrivs under avsnitt 3.2 (Leverans 2). Det har varit en lärande och iterativ process, där projektgruppen internt har tagit fram utkast, branschaktörer har kommit med återkoppling under workshoptillfällen och slutprodukterna har successivt tagit form. Under den sista workshopen med aktörerna kunde de bekräfta att den övergripande processen stämmer och utvecklingsbehoven är vad de kan se i dagsläget. Deras bild är dock, likt arbetsgruppen och branschprogrammet, att det är viktigt att fortsätta arbeta gemensamt med dessa frågor.

Den 4 december genomfördes ett sista gemensamt Skype-möte, med möjlighet för en sista återkoppling på utskickad färdig anlöpsprocess och utvecklingsbehov (bilaga Anlöpsprocess och utvecklingsbehov). Det var en bred representation och en samsyn att anlöpsprocessen fallit på plats, samt att de relevanta utvecklingsbehoven är beskrivna.

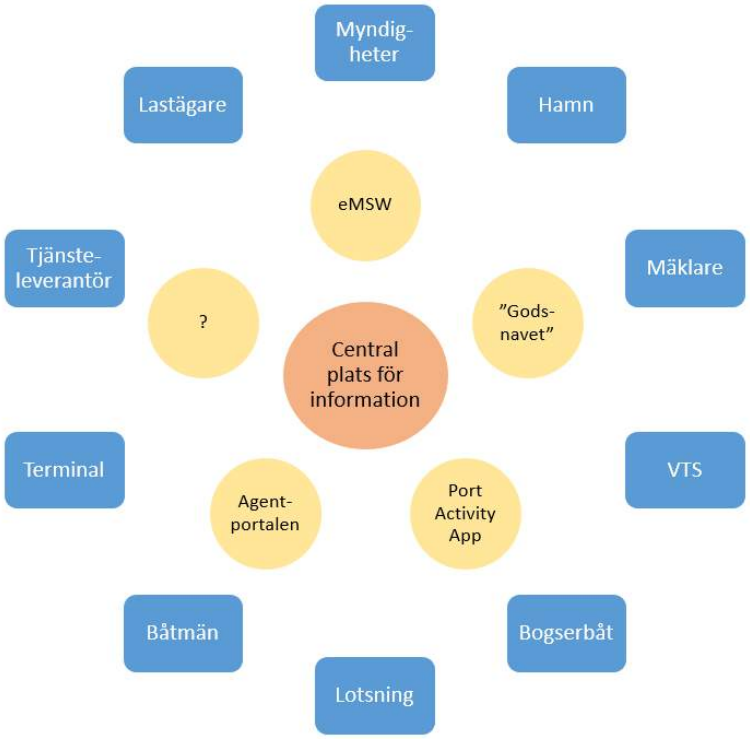
4 Slutsats och rekommendationer

Fortsatt branschgemensamt arbete är en nyckelfaktor för att fortsätta resan mot ett mer integrerat anlöp. Under arbetet etablerades en gemensam förståelse för de olika aktörernas prioriteringar kopplat till anlöpsprocessen och utvecklingsbehov. Den gemensamt framtagna anlöpsprocessen och identifierade utvecklingsområden bör användas som utgångspunkt i framtida arbete. Detta arbetspaket har skapat en samsyn om utgångsläget samt en förväntan bland branschens aktörer om ett gemensamt arbete framåt. För att det ska kunna genomföras är det viktigt att det utpekas en sammanhållande aktör som driver på arbetet. Finansiering, roller, ansvar och mandat i fortsatt arbete behöver tydliggöras. Identifierade utvecklingsområden kan tas om hand och utvärderas via nyttoanalyser och business case, för att mynna ut i handlingsplaner och så kallade Proof of Concepts för att verifiera nya lösningar.



Figur 16: Utvecklingsområden från arbetspaketet tas vidare genom såväl branschgemensamt arbete som aktörernas eget utvecklingsarbete.

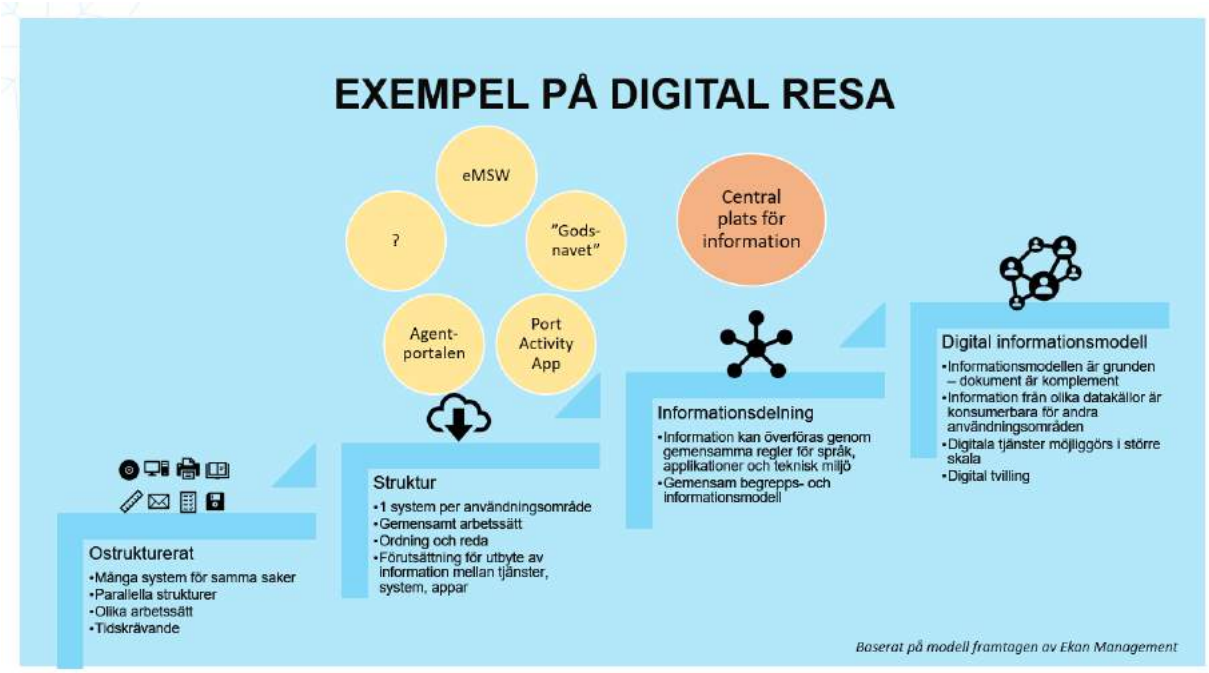
Digitalisering och mobila arbetssätt är möjliggörare för informationsdelning i realtid. Fler och fler aktörer behöver integreras med varandra, informationsmängden accelererar, artificiell intelligens och blockkedjeteknik introduceras. För att kunna svara upp mot detta och vara flexibel inför kommande system, aktörer och teknologier, så bör branschen överväga att utveckla en gemensam plats för information. Direktkontakt mellan alla aktörer blir orimligt i en framtid med accelererande mobila arbetssätt, uppkopplad utrustning och en datamängd som inte liknar det vi ser idag.



Figur 17. Figuren ovan består av tre lager, där den yttre ringen representeras av branschens aktörer. Den inre ringen representeras av olika initiativ för en förenklad delning av information. Dessa initiativ drivs av någon enskild eller några av aktörerna. I mitten finns en symbol för målbilden – en central plats för information som kan utbytas mellan aktörer och olika system eller plattformar.

Vissa av initiativen i den inre ringen kan i olika utsträckning försöka vara den centrala platsen för information, men för att nå hela vägen behöver det tas ett helhetsgrepp där branschens aktörer är delaktiga. Om vi återkopplar till digitaliseringstrappan i avsnitt 3.4. så kan de olika

initiativen betraktas som olika sätt att skapa struktur för olika delar av anlöpsprocessen, det vill säga trappsteg nummer två. Däremot saknas den centrala platsen för information för att nå det tredje trappsteget, där ”*Information kan överföras genom gemensamma regler för språk, applikationer och teknisk miljö*”.



Figur 18. Anlöpsprocessen har en bit kvar till att nå det tredje steget i den digitaliseringstrappa som arbetet har refererat till.

Sammanfattningsvis är rekommendationerna till branschgemensamt arbete att:

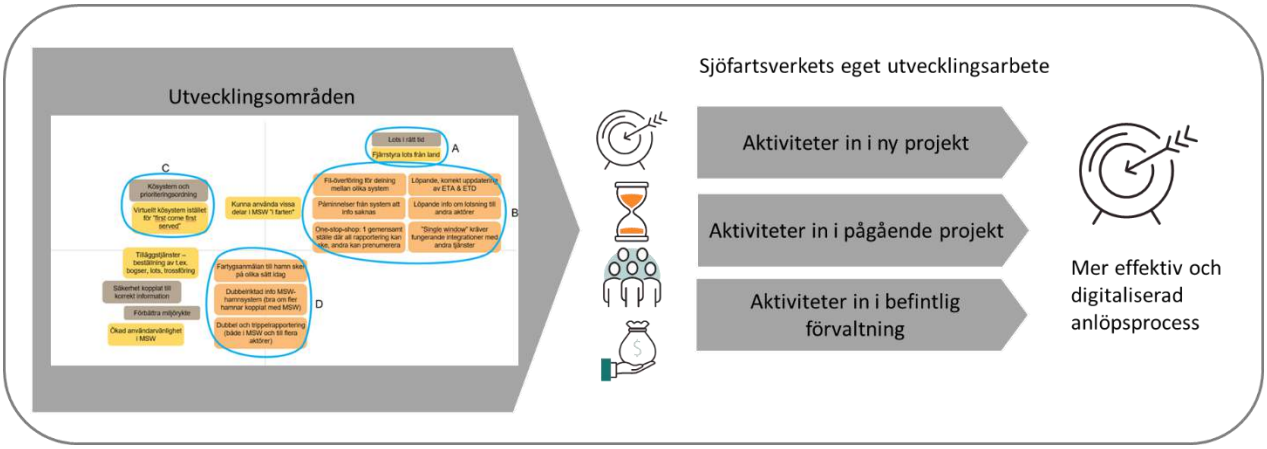
- ***Utse en sammanhållande part*** för effektivisering av anlöpsprocessen. Rekommendation att branschprogrammet lyfter fråga till branschen, Sjöfartsverket, andra inblandade myndigheter och Departementet: Är Sjöfartsverket rätt part att vara sammanhållande, och bör Sjöfartsverket i så fall få ett ökat mandat att vara sammanhållande part?
- ***Genomföra en förstudie avseende informationsdelning*** som svarar på frågorna om vilka plattformar som finns och planeras för, om plattformar kan kombineras och vilka aktörer som är inblandade. Förstudien ska resultera i en beskrivning av nuläget avseende informationsdelning samt hur branschen kan ta klivet mot ”en central plats för information”.
- ***Väva in insikter och utvecklingsbehov*** från detta arbetspaket med annat arbete som redan pågår inom branschprogrammet.

5 Förslag fortsättning, Sjöfartsverkets eget utvecklingsarbete

Vid sidan av det branschgemensamma arbetet, där Sjöfartsverket har en aktiv roll, kommer leveranser från arbetspaketet också tas vidare i det egna interna utvecklingsarbetet.

- Processbeskrivningar av dagens anlöpsprocess: Tas emot och förvaltas av *Anlöpstjänster*. Detta material består av PowerPoint- och Visio-filer, som används som bas för fortsatt utvecklingsarbete.

- Utvecklingsbehov, slutsatser och rekommendationer grovsorteras, för att bedöma vad som ska tas vidare i det branschgemensamma programmet för digitalt anlöp respektive i Sjöfartsverkets pågående eller nystartade projekt eller löpande verksamhetsutveckling/förvaltning. Denna grovsortering görs av *Anlöpstjänster*. Några av dessa områden kommer Sjöfartsverket omgående att driva internt:
    - Utreda hur tillgång till lots i rätt tidpunkt kan utvecklas
    - Beskriva och analysera kostnader för anlöp, utifrån aktörernas input till AP1
    - Ta om hand krav på förbättrad informationsdelning i pågående initiativ där så är möjligt



Figur 19: Sjöfartsverket tar om hand utvecklingsbehov från arbetspaketet i eget utvecklingsarbete.

5.2 Förstudie infrastruktur för digitalisering

SJÖFARTSVERKET

Förstudierapport
Infrastruktur för digitalisering

Forskning och Innovation

Rapporten finns tillgänglig på Sjöfartsverkets webbplats www.sjofartsverket.se

Dnr/Beteckning	21-00156
Författare	Per Löfbom
Månad År	December 2021

Sammanfattning

Målsättningen med denna förstudie är att utreda förutsättningar för att etablera en infrastruktur där digitala tjänster kan publiceras och konsumeras av olika aktörer inom sjöfartsnäringen och andra transportslag för att effektivisera transporter av gods. I tillägg till det validera förutsättningar för föreslagen infrastruktur baserad på beskrivna leveranser.

Den inledande nulägesanalysen innefattar informationsdelningstjänster för myndighetsrapportering, dynamisk rapportering till/ från fartyg samt tillhandahållande av anlöps- & avgångsinformation till svenska hamnar. I ett framtida ”börläge” måste hänsyn tas till den digitala transformation Sjöfartsverket står inför, ställa krav på att förenkla tillgången till information och tjänster för kunder och medarbetare. Vidare behöver bl.a. hänsyn tas till verksamhetens ökande förändringsbehov genom kontinuerliga mindre leveranser, ett minskat beroende till leverantörers ramverk samt att svara upp mot de säkerhetsmässiga krav som ställs på Sjöfartsverket.

Genomförd analys med avseende på informationsdelning identifierar krav på generella komponenter såsom identifiering/ autentisering, konfidentialitet, spårbarhet, skalbarhet, riktlinjer för kommunikationsprotokoll och kommunikationsmönster samt kommunikation till externa kommersiella och myndighetsgemensamma plattformar för informationsdelning. Möjligheten att ta betalt för ovan beskrivna informationsdelningstjänster bedöms som små då det saknas stöd för motsvarande uppdrag i Sjöfartsverkets instruktion. Avgiftssättning beror på hur källan till informationen finansieras. Om denna är anslagsfinansierad krävs ett uttryckligt stöd för att kunna debitera avgiften. Om tjänsten däremot finansieras genom avgifter kan avgift sannolikt motiveras genom Sjöfartsverkets allmänna uppgift att ta ut avgifter i affärsverksamheten. Vad gäller avgifter för inköpta tjänster såsom autentisering via Bank-ID kan en vidaredebitering av densamma sannolikt motiveras.

I kapitlet som beskriver framtida use-case redogörs för vidareutveckling av tjänster beskrivna i nulägesanalysen. I fallet med MSW finns EU-lagkrav på att tillhandahålla en EMSWe-tjänst. Utvecklad PAA lösning behöver kunna skalas ut till samtliga svenska hamnar och inom ramen för STM finns en stor efterfrågan på att tillhandahålla en navigationsvarningstjänst. En arkitektur som tjänar förutsättningsskapande för identifierade use-case har utformats utifrån en tolkning av MSB samt Polismyndighetens författningssamlingar. Fokus för arkitekturen är generiska tjänster såsom autentisering/ identifikation, säkerhetszoner (beroende på informationssäkerhetsklass) samt tillitsnivå (beroende av vem som konsumerar informationen). Med avstamp i föreslagen arkitektur genomfördes en PoC (Proof of Concept) i labmiljö mot den svenska identitetsfederationen Sweden Connect. Med framgång kunde Sjöfartsverket i en PoC e-tjänst; autentisera fiktiva svenska användare med korrekt tillitsnivå via (BankID, FrejaID+) samt autentisera fiktiva utländska användare via den svenska eIDAS noden med jämförbara tillitsnivåer.

Innehåll

Termer och förkortningar

Term/förkortning	Förklaring	Kommentar
API	Application Program Interface	Beskriver en anslutning för att kunna kommunicera system till system.
Azure	Microsofts plattform för molntjänster	Här återfinns tjänster för lagring, servrar eller mail bl.a.
DMZ	DeMilitarizedZone	I ett datornätverk är ett DMZ, eller demilitariserad zon, ett fysiskt eller logiskt subnät som separerar ett lokalt nätverk (LAN) från andra opålitliga nätverk - vanligtvis det publica internet.
eIDAS	electronic IDentification, Authentication and trust Services	eIDAS är en EU-förordning om elektronisk identifiering och förtroendetjänster för elektroniska transaktioner på den europeiska inre marknaden.
EMSA	European Maritime Safety Administration	EMSA tillhandahåller teknisk expertis och operativt stöd för att förbättra sjösäkerhet, beredskap och insatser vid utsläpp och sjöfartsskydd.
EMSWe	European Maritime Single Window environment	EMSWe är ett elektroniskt system för utbyte av rapporter för fartyg som ankommer till och/eller avgår från EU medlemsstaternas hamnar. Detta kommer att ersätta dagens MSW.
FTP	File Transfer Protocol	Ett sätt att överföra filer till exponerade mappar över internet.
IdP	Identity Provider	IDP är ett ”system” som skapar, underhåller och hanterar identitetsinformation för användare och tillhandahåller även autentiseringstjänster till applikationer inom en federation eller ett distribuerat nätverk.

MCP	Maritime Connectivity Platform	En plattform som består av ett identitetsregister för autentisering samt ett tjänsteregister för att möjliggöra uppslag av tjänster att kommunicera med, jfr ”Gula sidorna”.
MIG	Message Identification Guideline	Ett inom EU beslutat format som används för MSW/ EMSWe rapportering.
MSW	Maritime Single Window	MSW är ett elektroniskt system för utbyte av rapporter för fartyg som ankommer till och/eller avgår från EU medlemsstaternas hamnar.
PKI	Publik Key Infrastructure	En funktion för att garantera identiteter med utfärdade signerade certifikat
PoC	Proof Of Concept	Motsvarar en prototyp för att bevisa genomförbarheten i en utvecklad lösning.
SIG	Special Interest Group	En Special Intresse Grupp (SIG) som fokuserar på autentiseringslösningar i olika typer av användningsfall i syfte att sätta regler, policyer och referensarkitektur för dessa.
SOA	Service Oriented Architecture	Ett distribuerat IT-system organiserat som en struktur av kommunicerande tjänster
SSN	Safe Sea Net	Fartyg som transiterar EU-vatten spåras dagligen i realtid genom SafeSeaNet, EU:s övervaknings- och informationssystem för fartygstrafik.
SSNS	Safe Sea Net Sweden	Som ovan fast för svenska vatten.
STM	Sea Traffic Management	(STM) är en metod för att guida och övervaka sjötrafiken på ett liknande sätt som flygledning.
VDOM	Virtual DOMains	VDOM är en metod för logisk uppdelning av en enda brandvägg i två eller flera virtuella instanser och den fungerar som flera individuella brandväggar. Varje VDOM tillåts

		behålla sina på separata zoner, användarverifiering, säkerhetspolicyer, routing och VPN-konfigurationer.
VIS	Voyage Information Service	Et generellt API för utbyte av STM meddelanden (rutt, text, area)
WS	WebServices	XML-baserade informationsutbytessystem som använder Internet för direkt interaktion mellan applikationer
VTS	Vessel Traffic Service	En trafikcentral som bland annat ger trafikinformation och annan service till sjöfarten vid några av landets mest trafikerade eller miljökänsliga havsområden

1 Bakgrund

1.1 Om projektet och detta arbetspaket

Denna rapport beskriver resultatet av arbetspaketet Infrastruktur för digitalisering som, tillsammans med tre andra arbetspaket, är en del i projektet Branschgemensamt digitalt anlöp - fas 1, med en genomförandeperiod från och med april 2020 till och med december 2021. Trafikverket är huvudsaklig finansiär av arbetspaketen. Sjöfartsverket är projektledare för arbetspaketen och bidrar med ytterligare resurser för arbetet i dem.

Mål:

- Leverera en förstudierapport som mot bakgrund av beskrivna leveranser, utreder förutsättningar för att etablera en infrastruktur där digitala tjänster kan publiceras och konsumeras av olika aktörer inom sjöfartsnäringen men också av andra transportslag för att effektivisera transporter av gods.
- Validera förutsättningar för föreslagen infrastruktur baserad på beskrivna leveranser.

Effektmål:

- Definition av nuläge och börläge avseende Sjöfartsverkets möjligheter till informationsdelning
- Komponentanalys med syfte att fastställa krav på ingående komponenter såsom autentisering, informationssäkerhet, relevanta standarder etc.
- Affärsmodell och affärslogik för att stödja affärsmässigheten i Sjöfartsverkets framtida lösning för informationsdelning
- Framtagande av disparata use case i syfte att utröna olika kravbilder ur ett informationsdelningsperspektiv
- Framtagande av IT-arkitektur för att stödja en säker och hållbar informationsdelning över tid.
- Leverera Proof of Concept (PoC) för infrastrukturen med syftet att stödja publicering och konsumtion av digitala tjänster.

2 Informationsdelning - Nuläge

Sjöfartsverket har idag informationsutbyte med ett flertal olika intressenter inom sjöfarten såsom; agenter, mäklare, rederier, hamnar, fartyg, EMSA (European Maritime Safety Administration), SSN (Safe Sea Net), statliga myndigheter, allmänheten m.fl.

I förstudien beaktas tre initiativ för informationsdelning, MSW Maritime Single Window, STM Sea Traffic Management samt Port Activity Api.

MSW är ett system för rapportering och deklaration av information kopplat till fartygsanlöp, i huvudsak statisk information. Detta system kommer att behöva anpassas i framtiden för att harmoniera med det framtida EMSWe (European Maritime Single Window environment). EMSWe är nästa version

STM handlar om dynamisk information som förändras över tid, t ex tidsstämplar, djupgående, rutter, navigationsvarningar m.m. Där fartyg kan dela sina rutter med landbaserade centraler och tjänster.

Port Activity Api – PAA, syftar till att tillhandahålla samma information till alla partners före och under ett hamnanlöp. PAA ger förutsättningar för att öka hamnoperatörens effektivitet genom att kommunicera ankomster, avgångar samt lotsinformation till fartyg.

2.1 MSW - Maritime Single Window

Maritime Single Window (MSW) har etablerats med anledning av EU-direktiv 2010/65/EU gällande krav om samordning av administrativa förfaranden.

MSW är en gemensam webbaserad portal (MSW Reportal) för inrapportering av myndighetsinformation som är kopplat till fartygsanlöp. Systemet tillhandahålls och förvaltas av Sjöfartsverket, men är ett samarbete mellan Sjöfartsverket, Tullverket, Kustbevakningen och Transportstyrelsen.

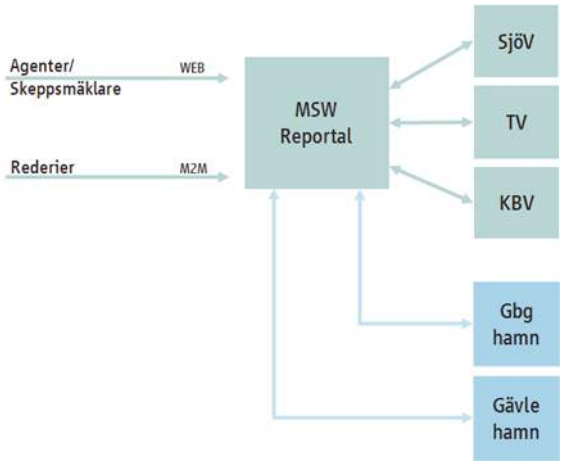
Syftet med införandet av en gemensam portal för fartygsrapportering är att underlätta för sjöfarten genom att förenkla och harmonisera rapporteringsformaliteterna samt att minska den administrativa bördan som det innebär för fartygen att rapportera uppgifter, ibland samma, till olika myndigheter.

Utöver myndigheterna har även två hamnar integrerats med systemet, Göteborgs och Gävles hamnar. Uppgifter om fartygsanlöpen som lämnas via portalen vidarebefordras sedan automatiskt till respektive myndighet och till hamnarna. De uppgifter som MSW Reportal hanterar fördelas på de olika intressenterna enligt följande:

- Kustbevakningen (KBV) – Sjöfartsskydd, besättnings- och passagerarlistor, hälsodeklaration. Har direktkoppling till MSW.
- Tullverket (TV) – Fartygsklarering. Har direktkoppling till MSW.

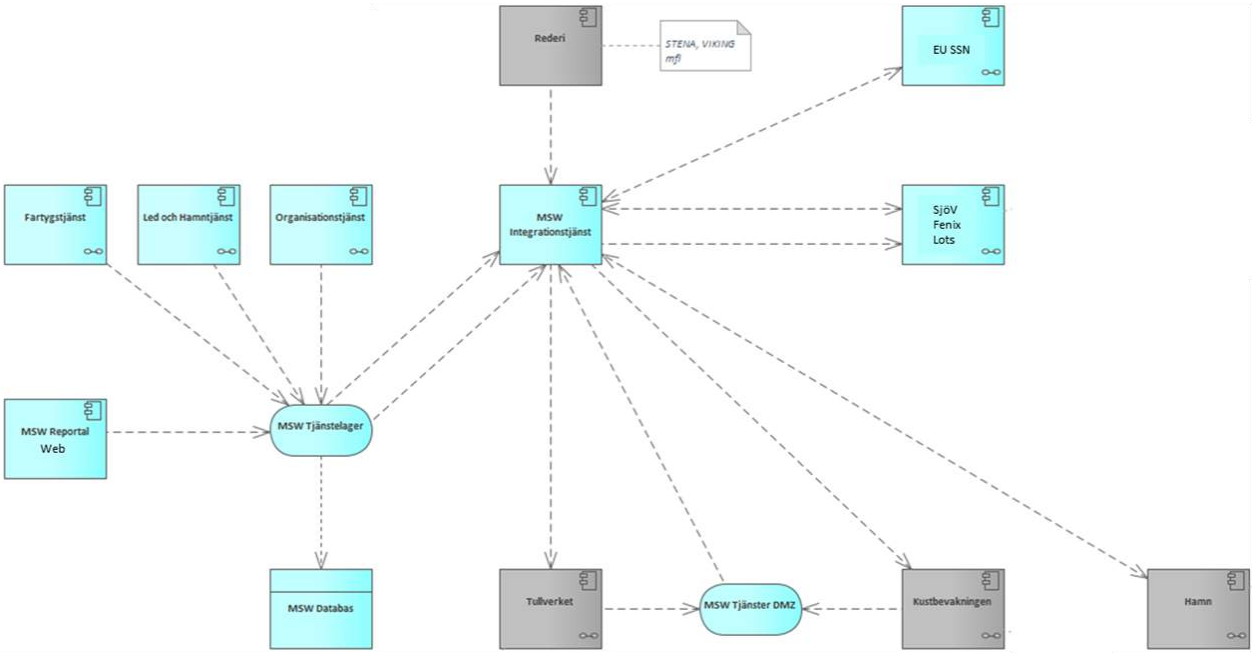
- Transportstyrelsen – Myndighetsspecifika frågor kopplat till föreskrifter. Har ingen direktkoppling till MSW, utan får sin information via andra system.
- Sjöfartsverket – Lotsbeställning och farledsdeklaration. Har direktkoppling till MSW

MSW Reportal illustreras översiktligt i nedanstående figur.



(M2M – Machine to Machine)

Övergripande arkitektur för MSW illustreras i nedanstående blockdiagram.



MSW exponerar en web portal som tillsammans med de interna informationstjänsterna för masterdata avseende fartyg, led & hamn samt organisation (kund) tillhandahåller information till MSW tjänstelager. Tjänstelagret lagrar MSW information i MSW databas samt kommunicerar med MSW integrationstjänst. MSW integrationstjänst hanterar i sin tur all intern resp. extern integration avseende maskin till maskin till och från MSW. Dessa, maskin till maskin integrationer sker antingen via FTP eller WebServices

Autentisering baseras dels på ett PKI (Publik Key Infrastructure) lösning för Webbportalen samt WebServices och dels på enkel inloggning till FTP kataloger.

2.2 STM – Sea Traffic Management

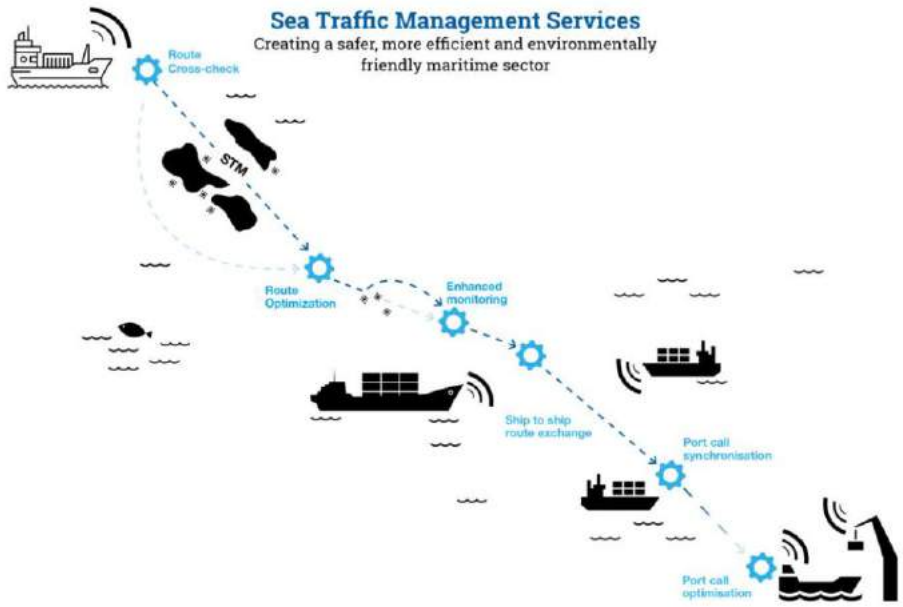
STM är ett resultat från projektet MonaLisa som var en internationell satsning med deltagare från 10 länder och som leddes av Sjöfartsverket. Utvecklingen av STM fortsätter för närvarande inom det internationella projektet STM BaltSafe som pågår under 2019 till 2021. En global utrullning och implementation av STM bedöms kunna ske fram till cirka år 2030.

STM är ett övergripande koncept som genom informationsutbyte syftar till att:

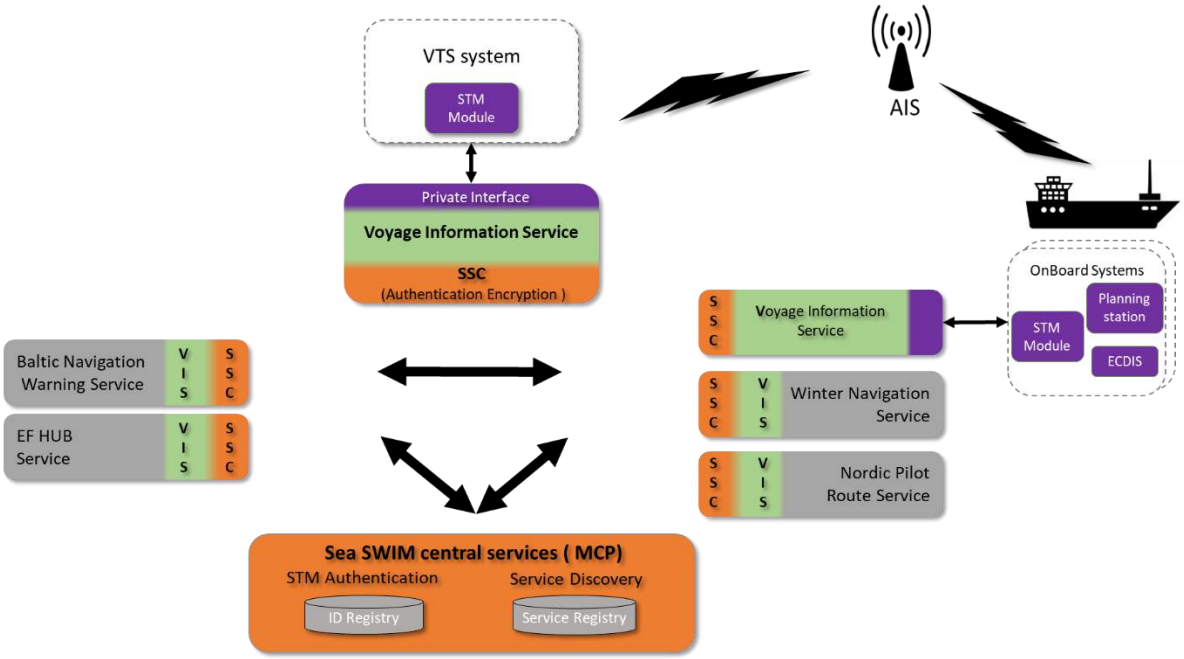
- Höja säkerheten till sjöss
- Minska miljöpåverkan
- Öka effektiviteten i resursutnyttjande

Informationsutbytet sker mellan ett flertal aktörer såsom myndigheter, redare, agenter, rederier, fartyg, hamnar, terminaler, m fl. Genom kontinuerlig uppdatering av information om rutter och tider i realtid skapas förutsättningarna för ett effektivare informationsutbyte.

Nedan illustreras konceptet och de övergripande nyttorna med STM.



Övergripande arkitektur för STM illustreras i nedanstående blockdiagram.



STM är baserad på en distribuerad tjänsteorienterad arkitektur (SOA – Service Oriented Architecture), således representeras alla maritima artefakter som en tjänst. En extern plattform MCP (Maritime Connectivity Platform) bestående av ett tjänste- och id register erbjuder funktioner för autentisering samt uppslag av publicerade tjänster. Sjöfartsverkets interna tjänster för Navigationsvarningar, VTS (Vessel Traffic Service), Isbrytning, Lotsrutter m.fl. kommunicerar med fartyg via en informationstjänst VIS (Voyage Information Service). VIS i sin tur hanterar ömsesidig autentisering via MCP vilket möjliggör kommunikation punkt till punkt med ett fartygs motsvarande VIS.

2.3 Port Activity App

Inom projektet STM Efficient Flow har en hamnlösning i Gävle utvecklats, som syftar till effektivare, säkrare och mer miljömässiga anlöp till hamnen. Den utvecklade integrationen, Port Activity App – PAA, ger samma information till alla partners före och under ett hamnanlöp. PAA syftar till att öka hamnoperatörens effektivitet genom att kommunicera ankomster och avgångar mm. till fartyg.

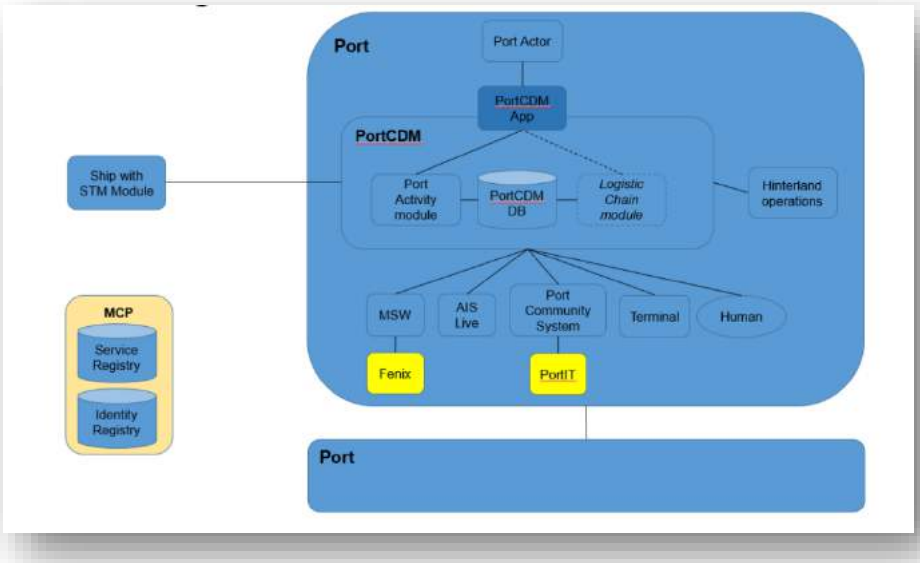
Med PAA kommer anlöps-processen för fartyg att bli effektivare och därigenom öka sjöfartens konkurrenskraft samt bidra till mindre miljöpåverkan med bättre skräddarsydda och planerade ankomster och avgångar av fartyg i hamnen. Vidare möjliggör PAA tillförlitlig information om fartygets ankomst optimering av hela transportkedjan genom vidare informationsdelning till nästa transportslag för ruttplanering av landtransporter.

Port Activity App (PAA) består av flera olika delar. En del är de API:er som matar en insamlingsplattform med data för att fylla tidslinjen med tidsstämplar. Data presenteras i presentations-gränssnittet som web-sida eller app. Sjöfartsverkets leverans består idag av de två API:er som levererar anlöps-uppgifter resp. lotsningsuppgifter.

API:er i PAA:

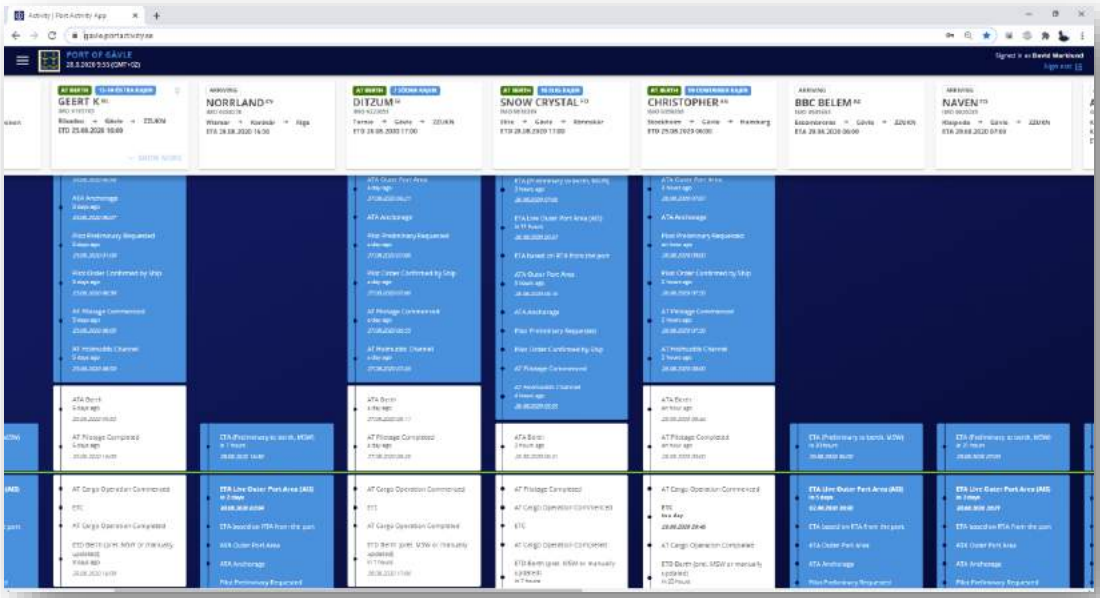
- Anlöps-anmälan, Sjöfartsverket, Källan är MSW via SSNS.
- Lotsning, Sjöfartsverket, via Fenix Lots, tex lotsning preliminärt beställd, lotsning startad, lotsning avslutad
- Grieg Connect, Live ETA (Estimated Time of Arrival), kalkylerad ETA baserad på AI/skepps-rörelser
- Shiplog, Tidsstämplar via AIS (Automatic Identification System) vid ankomst till olika ytor, tex yttre hamnområde, passage av linjer etc.
- YilPort (en terminaloperatörs system för lastning/lossning)

Insamlingsmodulen, samlar in tidsstämplar från olika API:er (se port activity module i figur)

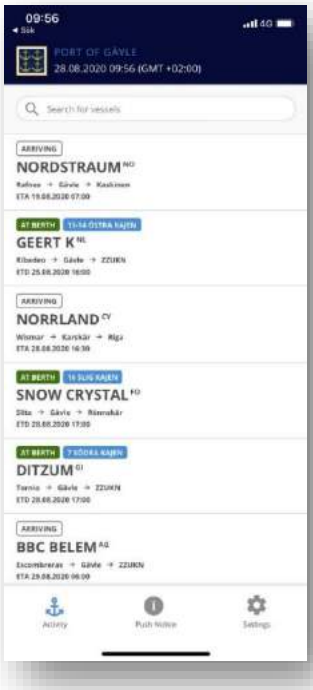


Presentations-gränssnitt

En Web-sida finns tillgänglig på denna adress, behörighet krävs.
https://gavle.portactivity.se/



En App finns på appstore / google play, se bild.



3 Informationsdelning - Börläge

Inom Sjöfartsverket finns många pågående och planerade initiativ inom området Digital transformation av Sjöfartsnära tjänster inklusive informationsdelning. För att kunna tillgodose våra kunder och verksamhetens behov behöver den tekniska plattformen som utvecklingen sker på förnyas. Befintliga system har en begränsad livslängd eftersom de bygger på teknik som inom överskådlig tid inte kommer uppdateras med nya versioner utan mer bara patchas. I ett framtida börläge ska följande områden beaktas.

- Förenkla tillgång till myndighetens information och tjänster för sjöfartsverkets kunder och medarbetare.
- En översyn av livscykelhanteringen för nya och befintliga system – så att man med rimlig insats kan tillmötesgå verksamhetens förändringsbehov (god förvaltningsbarhet)
- Förmåga att kunna leverera befintliga och nya system utan/liten nedtid CI/CD (Continuous Integration/ Continuous Deployment/Delivery)
- Minska personberoende genom att utveckla mjukvara på ett gemensamt sätt oberoende av förvaltningsobjekt
- En plattform med en arkitektur som står sig många år men minskar beroende till leverantörers ramverk och tekniska lösningar
- En plattform där data kan återanvändas samt motverkar duplicering av data
- En plattform vilken lever upp till de säkerhetsmässiga krav som ställs på Sjöfartsverket. En förutsättning för att kunna ge tillgång till information och tjänster är en tillräckligt säker lösning kring e-identiteter som skapar rätt tillit.
- Hänsyn tagen till fastslagna styrdokument i form av arkitekturprinciper, riktlinjer för utveckling samt plattformsstrategi.
- En plattform som med stöd för beslutad informationssäkerhetsklassificering. Uppskattningsvis så kommer flertalet e-tjänster behöva uppfylla kraven för tillitsnivå 3 – Internt sekretessklassad.

4 Komponentanalys

4.1 Generella komponenter

Mot bakgrund av de tre beskrivna initiativen för informationsdelning kan ett antal gemensamma komponenter identifieras som är kandidater för en generell infrastruktur avseende informationsdelning.

I samtliga fall finns krav på någon slags autentisering / identifikation, i ovanstående lösningar är dessa hårt knutna till resp. lösning (proprietära).
Utmaningar med dagens lösningar är bl.a.

- Nuvarande PKI-miljö ligger på utökad support och ska avvecklas.
- Resursläget har alltid varit ansträngt inom PKI och Sjöfartsverket har haft utmaningar att rekrytera adekvata resurser i det sammanhanget.
- Dagens PKI-miljö är för komplex.
- Nuvarande autentiseringslösningar uppfyller inte önskad indelning i olika tillitsnivåer.
- Dagens IdP (Identity Provider) lösning innefattar ett avtal som gör att enbart en leverantör får hantera miljön.
- Livcykelhanteringen och support av e-identiteter i dagens lösning är kostnadsdrivande. Hantering av klientcertifikat mm.
- Sammanfattningsvis behövs omfattande investeringar både på IT och i verksamheten för att lyckas åstadkomma e-tjänster med önskad uppdelning i olika tillitsnivåer, i egen regi.

De beskrivna lösningarna förlitar sig på en för grovt indelad nätsegmentering ur ett informationssäkerhetsperspektiv. Det saknas således en mer fingranulär indelning i zoner för att kunna stödja dedikerade funktioner för åtkomstkontroll och filtrering av nätverkstrafik, baserat på systemets skyddsvärde.

Likaså finns olika krav på tillitsnivå för den information som delas beroende på den konfidentialitetsnivå som tillskrivs delad data. DIGG har sammanställt vad tillitsramverket för Svensk e-legitimation samt ISO/IEC 29115 i korthet innebär gällande tillitsnivåer för Sverige tillsammans med EU-förordningen eIDAS. Vilket är något som behöver tas hänsyn till i utformningen av infrastrukturen för informationsdelning.

Beskrivna informationsdelningstjänster kan i någon mån betraktas som publika tjänster men saknar den enkelhet som därvid förväntas av konsumenter vare det sig rör sig om medarbetare, kunder eller andra myndigheter.
Implementationen av konsumenter behörighetsmässigt och tekniskt är inte enhetlig, det saknas en samstämmig instruktion och dokumentation för hur ett konsumerande system/ användare ska kunna ansluta till exponerade tjänster.

Funktioner för spårbarhet/ loggning och monitorering är även de unika för resp. lösning.

När det gäller riktlinjer för tillåtna kommunikationsprotokoll, kommunikationsmönster eller för den delen lagring av meddelanden, är dessa inte implementerade eller tydligt beskrivna.

I ljuset av hur digitaliseringen utvecklas kommer det sannolikt krävas utökade funktioner för s.k. inter-plattform konnektivitet (Azure, AWS, Google etc.). Nuvarande lösningar har inte tagit hänsyn till dylika krav, utan detta har skett från fall till fall.

Det saknas även möjligheter att dynamiskt skala ut en informationstjänst (till flera aktörer) och skala upp en informationstjänst (öka prestandan).
Varje ny exponerad tjänst kräver i dagsläget en leverantörsspecifik lösning och/ eller en konsumentspecifik lösning.

Sammanfattningsvis finns en hel del ytterligare att önska avseende förväntade komponenter i en tänkt framtida infrastruktur för Sjöfartsverkets e-tjänsteplattform.

4.2 e-tjänstespecifika komponenter

e-tjänsteunika komponenter innefattar de komponenter som är specifika för varje e-tjänst och därför inte kan förväntas stödjas i den gemensamma e-tjänsteplattformen, se vidare figur nedan.

- Frekvens (meddelandefrekvens)
- Informationsägarskap (definierat ansvar för exponerade informationstillgångar)
- Mottagare (stat, kommun, akademi, näringsliv, privatperson, nation, federation, union etc.)
- Affärsmodell (modell för att ta betalt om möjligt)
- Informationsklassificering (konfidentialitet, riktighet, tillgänglighet)
- Hantering av extern information (visavi internt producerad data)
- Granskning (ev. granskningsprocedur som kan komma att krävas för åtkomst till viss information)
- Informationsbehörighet (auktorisation/ behörighetshantering)
- Komplexitet (orkestrering- krav på viss meddelandesekvens)
- Aktualitet (realtid, periodiskt)
- Volymer (datastorlek)
- Skalbarhet (ur ett applikationsperspektiv)
- Uppföljning rapportering, analys
- Överföringsformat (t.ex. RTZ – ruttformat enligt CIRM standard)
- Kompatibilitet (FEDeRATED Semantic model/ Architecture masterplan)

5 Affärsmodell och affärslogik

Affärsmodell och affärslogik för att stödja affärsmässigheten i Sjöfartsverkets framtida lösning för informationsdelning omfattar vilka möjligheter som finns att utbyta anlöps- och avgångsinformation och därtill hörande tjänster ur ett affärsmässigt perspektiv.

5.1 Frågan gäller huruvida Sjöfartsverket får ta betalt för tjänster som vidareförmedlar information mellan redare och hamnar?

5.1.1 Användningsfall 1

Inom ramen för EMSWe ska Sjöfartsverket framöver förmedla viss information till hamnar. Detta krav om informationsdelning utelämnar vissa interaktioner i form av informationsutbyte. Frågan gäller i vilken mån Sjöfartsverket får genomföra sådana utelämnade informationsutbyten samt ta ut ersättning för att genomföra informationsutbyte.
Det informationsutbyte som föreslås innefattar att:

1. Publicera information - Förmedla behov ex färskvatten och sedan förmedla information om färskvattensleverantör tillbaka till fartyget (hitta tjänster)
2. Förmedla faktura
3. Genomföra betalning
4. Autentisera – förvissa sig om att man har att göra med en identifierad aktör

5.1.2 Användningsfall 2

Får Sjöfartsverket bygga ut rapporteringssystem (MSW Reportal) för att hjälpa hamnar att ta in sin anlöpsinformation? Ersätta agenters blanketter. Exempel viss detaljinformation om olja etc?

5.1.3 Avgränsning

Frågan om hur Sjöfartsverket ska förhålla sig till EMSWe och de regler som omgärdar systemet behandlas inte i denna förstudie. Skrivelsen utgår från att Sjöfartsverket vill införa tillägg till systemet utanför ramen av de krav som EU ställer på systemet och att det är möjligt att utöka systemet på det sätt som föreslås.
Flera förutsättningar vad gäller EMSWe är dessutom inte färdigutredda, exempelvis kan viss data komma att skickas till hamnarna utan Sjöfartsverket som mellanhand. Det är även oklart vilken finansieringsmodell systemet ska ha samt vilken information som omfattas av rapporteringsskyldig eller inte.
Denna förstudie förutsätter även att informationen är frivillig. För information som omfattas av rapporteringsskyldighet gäller alltid att Sjöfartsverket behöver ett lagstöd för den myndighetsuppgift som hanteringen innebär och ett uttryckligt lagstöd för eventuell avgift för den utpekade myndighetsuppgiften.

5.1.4 Slutsats

Inom ramen för frågeställningen kan informationsmängderna dels in i tre typer, information som;
1: registreras i EMSWe och sedan sparas av Sjöfartsverket,
2: registreras i EMSWe som Sjöfartsverket inte ska ta del av, samt
3: inte skickas in i EMSWe som Sjöfartsverket behöver hämta in för att förslaget ovan ska vara genomförbart.

5.1.5 Gällande rätt

Av 1 kap. 1 § 3 st. regeringsformen (1974:152) följer att den offentliga makten utövas under lagarna. Vidare följer av 5 § 1 st. förvaltningslagen (2017:900) att en myndighet endast får vidta åtgärder som har stöd i rättsordningen.
Av 2 kap. 3 § tryckfrihetsförordningen (1949:105) följer att med handling avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.
Av 2 kap. 4 § samma lag följer att en handling är allmän, om den förvaras hos en myndighet och enligt 9 eller 10 § är att anse som inkommen till eller upprättad hos en myndighet.
Av 2 kap. 6 § samma lag följer att en upptagning som avses i 3 § anses förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt. En sammanställning av uppgifter ur en upptagning för automatiserad behandling anses dock förvarad hos myndigheten endast om myndigheten kan göra sammanställningen tillgänglig med rutinbetonade åtgärder och inte annat följer av 7 §.
Av 2 kap. 9 § samma lag följer bl.a. att en handling anses ha kommit in till en myndighet, när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa. I fråga om en upptagning som avses i 3 § gäller i stället att den anses ha kommit in till myndigheten när någon annan har gjort den tillgänglig för myndigheten på det sätt som anges i 6 §. En åtgärd som någon vidtar endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en myndighet har tillhandahållit ska inte anses leda till att handlingen har kommit in till den myndigheten.
Sjöfartsverkets uppdrag framgår av förordning (2007:1161) med instruktion för Sjöfartsverket. Hur Sjöfartsverkets instruktion ser ur idag en av Sjöfartsverkets huvuduppgifter är att tillhandahålla ett system för harmonisering och samordning av rapporteringsformaliteter (MSW Reportal) och ansvara för samarbetet med Europeiska kommissionen och andra medlemsstater i fråga om att utveckla metoder för harmonisering och samordning av rapporteringsformaliteterna enligt diverse direktiv. Sjöfartsverket ska också se till att de regelverk och rutiner som myndigheten disponerar över är kostnadseffektiva och enkla för medborgare och företag.

5.1.6 Del av Sjöfartsverkets uppdrag?

För att Sjöfartsverket ska få hämta in information krävs som utgångspunkt stöd i lag. Lagstödet kan se ut på olika Sjöfartsverkets, exempel Sjöfartsverkets genom ett uppdrag att svara för fastställelse och uppbörd av en avgift. I det fallet är det klart att

Sjöfartsverket har stöd att hämta informationen som krävs för att Sjöfartsverket ska kunna fastställa avgiften. Lagstödet kan också vara i form av en registerförfattning, exempel Sjöfartsverkets lag (1998:620) om belastningsregister och förordning (1999:1134) om belastningsregister.
Sjöfartsverket har i uppdrag att tillhandahålla systemet MSW och kommer att ha uppdraget att tillhandahålla EMSWe.
För det fall regelverket runt systemet ställer krav på att Sjöfartsverkets information registreras i EMSWe och denna information sedan skickas vidare för att lagras hos Sjöfartsverket så har kravet på att hantera information uppfyllts.
Ett potentiellt problemområde är vilken information som skickas genom EMSWe till Sjöfartsverket. Beroende på hur regelverket ser ut kan det vara så att Sjöfartsverket bara ska få tillgång till information som Sjöfartsverket har nytta av i sin verksamhet. I så fall ska Sjöfartsverket med verkets nuvarande uppdrag sannolikt inte få den information som exemplifieras ovan. Samtidigt så kan det vara så att all information i EMSWe går till Sjöfartsverket i någon mån, informationen ska trots allt skickas in i systemet som förvaltas av Sjöfartsverket.
Notera att MSW i sig inte ska anses som en databas utan anses istället mer som ett ”postkontor”. Systemet ska inte lagra uppgifter utan enbart skicka dem till respektive myndighet. Därför blir handlingarna inte allmänna hos Sjöfartsverket i linje med vad som följer av 2 kap. 9 § 3 st. tryckfrihetsförordningen. Sjöfartsverket har enbart handlingarna som en del av teknisk bearbetning.
Eftersom i dagsläget saknas registerförfattningar för data som rör EMSWe så gäller istället gängse regler kring hantering av allmänna handlingar. Så snart som Viss information ligger hos Sjöfartsverket har Sjöfartsverket som regel en viss kontroll över hur informationen kan hanteras. Sjöfartsverket måste inte lämna ut handlingen digitalt eller ge någon information som inte kan sammanställas med rutinartade åtgärder, dock finns inga direkta hinder mot att göra detta om Sjöfartsverket bedömer att det är i linje med verkets uppdrag. Det är rättsligt oklart om det krävs lagstöd för att få direktåtkomst till ett system hos en myndighet. Som regel ska Sjöfartsverket dock vara mycket försiktiga om systemet behandlar personuppgifter. Desto ”känsligare” uppgifter som systemet hanterar desto mer angeläget är det att få ett uttryckligt lagstöd för att ge någon åtkomst till uppgifter i ett system.

5.2 Användningsfall 1

5.2.1 Förmedla information (ex behov av färskvatten och svar från leverantörer)

Den information som Sjöfartsverket tar emot antingen genom EMSWe eller på annat sätt och därmed har lagstöd för att hantera kan myndigheten välja att tillhandahålla. Vad gäller eventuellt svar från motpart på land saknas däremot lagstöd för Sjöfartsverket att hantera. Det skulle behövas en ändring i Sjöfartsverkets instruktion för att ge myndigheten ett uppdrag att underlätta kontakten mellan hamnarna och redarna/ skeppsmäklarna.
Det finns företag (skeppsmäklare) som ägnar sig åt sysslan och därmed en risk för konkurrensproblematik om inte uppdraget pekas ut i Sjöfartsverkets instruktion.
Avgiftssättning beror på hur EMSWe (eller annan källa till information) finansieras. Om EMSWe finansieras genom anslag krävs ett uttryckligt stöd att ta ut avgiften.

Om EMSWe finansieras genom avgifter kan avgift sannolikt motiveras genom Sjöfartsverkets allmänna uppgift att ta ut avgifter i affärsverksamheten. Eller så beslutas en särskild avgift för administration av systemet i samband med införandet i vilket fall Sjöfartsverket måste förhålla sig till denna.

5.2.2 Förmedla faktura

Att förmedla betalningstjänster är inte ett uppdrag som Sjöfartsverket har i dagsläget. Förslaget ligger långt utanför Sjöfartsverkets verksamhet och uppdraget är så renodlat marknadsmässigt att det sannolikt skulle behöva preciseras uttryckligen i Sjöfartsverkets instruktion att verket ska förmedla betalningstjänster mellan hamn och redare.
Det finns företag (faktureringsföretag, skeppsmäklare) som ägnar sig åt sysslan och därmed en risk för konkurrensproblematik om inte uppdraget pekas ut uttryckligen i Sjöfartsverkets instruktion.
Avgiftssättning beror på hur EMSWe finansieras. Om EMSWe finansieras genom anslag krävs ett uttryckligt stöd att ta ut avgiften. Om EMSWe finansieras genom avgifter kan avgift sannolikt motiveras genom Sjöfartsverkets allmänna uppgift att ta ut avgifter i affärsverksamheten. Eller så beslutas en särskild avgift för administration av systemet i samband med införandet i vilket fall Sjöfartsverket måste förhålla sig till denna.

5.2.3 Genomföra betalning

När det gäller betalningar finns ett omfattande regelverk för statliga fordringar att förhålla sig till. Staten får bl.a. som regel inte lämna kredit. Förslaget ligger långt utanför Sjöfartsverkets verksamhet och uppdraget är så renodlat marknadsmässigt att det sannolikt skulle behöva preciseras uttryckligen i Sjöfartsverkets instruktion att verket ska förmedla genomföra betalningar mellan hamn och redare.
Det finns företag (banker, faktureringsföretag) som ägnar sig åt sysslan och därmed en risk för konkurrensproblematik om inte uppdraget pekas ut uttryckligen i Sjöfartsverkets instruktion.
Avgiftssättning beror på hur EMSWe finansieras. Om EMSWe finansieras genom anslag krävs ett uttryckligt stöd att ta ut avgiften. Om EMSWe finansieras genom avgifter kan avgift sannolikt motiveras genom Sjöfartsverkets allmänna uppgift att ta ut avgifter i affärsverksamheten. Eller så beslutas en särskild avgift för administration av systemet i samband med införandet i vilket fall Sjöfartsverket måste förhålla sig till denna.

5.2.4 Autentisera

När det gäller autentisering för att skapa förtroende mellan aktörer i ett anlöp kopplar det till huruvida Sjöfartsverket besitter en dylik lösning så att identiteter kan garanteras. Eftersom Sjöfartsverket inte själva kommer att äga en autentiseringslösning utan snarare vara beroende av extern part (nationellt eller inom EU) finns antagligen små möjligheter juridiskt att ta extra betalt för en dylik tjänst utöver att vidaredebitera det Sjöfartsverket själva får betala för autentiseringslösningen.

5.3 Användningsfall 2

5.3.1 Anpassa MSW Reportal för att hjälpa hamnar att ta in sin anlöpsinformation

Det måste finnas ett lagstöd för Sjöfartsverket att hantera informationen som inkommer till myndigheten. Det saknas i dagsläget stöd att ta in den information som exemplifieras. Det skulle behövas en ändring i Sjöfartsverkets instruktion för att ge myndigheten ett uppdrag att underlätta kontakten mellan hamnarna och redarna/skeppsmäklarna.
Vad gäller själva befogenheten att genomföra ändringen i MSW Reportal måste hänsyn tas till att MSW Reportal är styrt av regelverket kring MSW. Sjöfartsverket skulle i så fall behöva samverka med Tullverket, Kustbevakningen och Transportstyrelsen innan en sådan ändring genomförs.
Det finns företag (skeppsmäklare) som ägnar sig åt sysslan och därmed en risk för konkurrensproblematik om inte uppdraget pekas ut i Sjöfartsverkets instruktion.
Avgiftssättning beror på hur EMSWe (eller annan källa till information) finansieras.
Om EMSWe finansieras genom anslag krävs ett uttryckligt stöd att ta ut avgiften.
Om EMSWe finansieras genom avgifter kan avgift sannolikt motiveras genom Sjöfartsverkets allmänna uppgift att ta ut avgifter i affärsverksamheten.

6 Framtagande av use case

Beskrivna informationsdelningstjänster i kapitel 2 kommer att vidareutvecklas i fallet med MSW finns lagkrav för att tillhandahålla en EMSWe tjänst. Utvecklad PAA lösning behöver kunna skalas ut till samtliga svenska hamnar och inom ramen för STM finns en stor efterfrågan på att tillhandahålla en navigationsvarningstjänst. I detta kapitel beskrivs dessa tjänster översiktligt tillsammans med föreslagen arkitektur i förekommande fall.

6.1 EMSWe

European Maritime Single Window Environment (EMSWe) kan ses som en vidareutveckling av dagens MSW, EMSWe innefattar ett helt nytt ekosystem för rapportering till medlemsstater i samband med ankomst- och avgång till/ från hamn. EMSWe inkluderar bl.a. ett nyckelelement som kallas Harmonized Reporting Interface Module (RIM), som ska göra det möjligt för fartygsoperatörer att tillhandahålla information på samma sätt och format, MIG (Message Interface Guideline) inom hela EU. Tack vare att ett fullt harmoniserat gränssnitt görs tillgängligt för dem. Något som MSW trots goda föresatser inte lyckades med.

Målsättningar med RIM-komponenten i EMSWe:s konceptuella arkitektur, hämtad från förordningen (EU) 2019/1239 om etablering av en gemensam miljö för inlämning av information som krävs för hamnanlöp är:

- Bidra till att främja de harmoniserade regler för inlämning av information som krävs för hamnanlöp.
- Underlätta interoperabiliteten med olika tekniker och rapporteringssystem för deklaranterna.
- Underlätta säkert elektroniskt informationsutbyte i samband med rapporteringsskyldighet för fartyg som ankommer till, vistas i och avgår från unionens hamnar.
- Minska den administrativa bördan för branschen.

6.1.1 Allmänna use case

För att beskriva möjligheten till interaktioner mellan deklarerande parter och medlemsstater identifieras tre generella användningsfall för att visa de nödvändiga komponenterna som RIM och andra domäner kommer att behöva stödja och hur de bör interagera med varandra.

Det är viktigt att notera att dessa användningsfall är enbart illustrativa exempel då definitionerna ännu inte är färdigdefinierade.

- Service Look-Up för versioner som stöds

- Syftet med detta användningsfall är att visa att det finns ett behov av att både RIM- och MIG-standardversionerna valideras och uppdateras innan en konversation mellan deklarerande parter och medlemsstater påbörjas för att kommunikation ska kunna ske via rätt adress (endpoint URL).

- Uppfyllande av krav på formaliteter
  - Syftet med detta användningsfall är att visa de nödvändiga kommunikationsstegen som behövs för att fullgöra alla formaliteter som deklarerande parter måste lämna in, i samband med interaktion med en medlemsstat före, under och efter att de lämnar hamnen.

- Begära uppdateringar av programvara/konfiguration
  - Syftet med detta användningsfall är att visa att det vid sidan av meddelandeutbyte mellan deklarerande parter och medlemsstater, krävs att RIM-konfigurationer/programvara uppdateras från en central domän.

6.1.2 Arkitektur översikt

Det föreslagna scenariot för RIM:s blivande arkitektur bygger på en onlinestrategi genom säkert utbyte av meddelanden över internet.

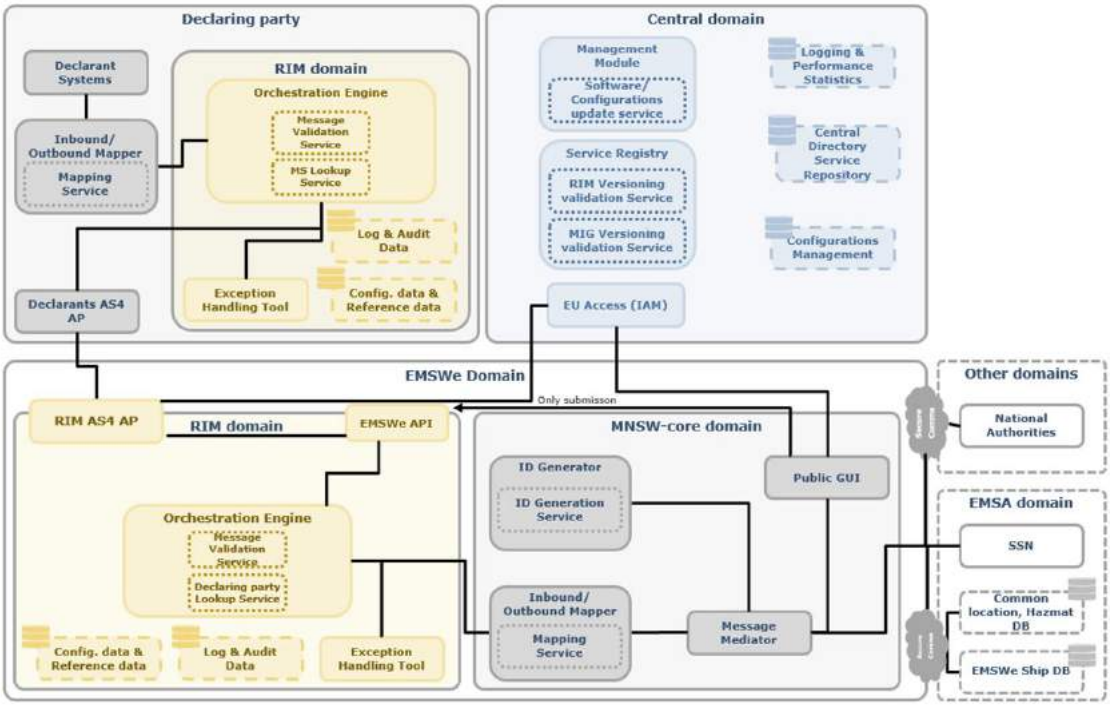
I synnerhet kommer den nya RIM-komponenten att installeras på både den deklarerande partens backoffice-system och framför medlemsstaternas MNSW-kärnor (Maritime National Single Window). Arkitekturvyn nedan möjliggör ett bättre förtydligande av de komponenter som ska implementeras på både den deklarerande partens och medlemsstatens domäner.

Det finns tre huvuddomäner som presenteras i denna högnivåarkitekturmodell. Den deklarerande parten, EMSWe-domänen och den centrala domänen.

- Den deklarerande parten representerar olika aktörer som vill lämna in formaliteter via system-till-system-kanalen genom att implementera RIM, detta kan vara deklaranten själv, en datatjänstleverantör eller en PCS som fungerar som datatjänstleverantör. En RIM-domän är belägen inom den deklarerande parten, andra komponenter, som visas i grått i figuren, har ett rent illustrativt syfte med målet att ge ett bredare sammanhang till RIM:s omfattning. Som sådan är komponenterna i den deklarerande partens domäner det fulla ansvaret för respektive aktör.

- EMSWe-domänen består av två huvudelement, MNSW-kärndomänen och RIM-domänen. MNSW-kärndomänen, presenterad i grått i figuren, har ett rent illustrativt syfte med målet att ge ett bredare sammanhang till RIM:s omfattning. Som sådan är komponenterna i MNSW-kärndomänerna respektive medlemsstats fulla ansvar.

- Den centrala domänen omfattar komponenter som inte kommer att inkapslas som en del av den distribuerade RIM, utan kommer att underhållas centralt, såsom EU Access-tjänsten och ett centralt tjänsteregister.



Applikationskomponenter

ID	Applikationskomponent	Beskrivning
1	AS4 Access Point	Säker slutpunkt för system-till-system-kommunikation som tillåter utbyte av meddelanden, genom att följa AS4-protokollet för transport och säkerhet.
2	EMSWe API	Tillhandahåller en enhetlig tjänst API Abstraktion till någon av de tillgängliga 22 ändpunkterna för kommunikation i maritima medlemsstater.
3	Orchestration Engine	Tillhandahåller syntaxvalidering för alla meddelanden som skickas och tas emot, slår upp och validerar den deklarerande partens slutpunkt som meddelanden skickas till och vidarebefordrar meddelanden till både Maritime National Single Window och den deklarerande partens slutpunkt.
4	Exception Handling Tool	Utför ett begränsat antal meddelandeleveransförsök och tillhandahåller undantagsrapporteringsloggar till MNSW-kärnan.
5	Log & Audit Database	Lagrar loggar från metadata för utbytta meddelanden för revisionsändamål och underhåll.

6	Configuration & Reference Data Database	Stores general reference data, local configurations and support for offline performance
7	EU Access (IAM)	Möjliggör en centraliserad registrering av deklarerande part/tjänsteleverantörer som ekonomiska operatörer, hanterar behörigheter och tillgång till kommunikation med olika maskin till maskin och manuell rapportering, instanser.
8	Management Module	Möjliggör central hantering av push för systemkonfigurationer och programuppdateringar till alla installerade RIM
9	Service Registry	Registrerar de MIG- och RIM-versioner som stöds för kommunikation
10	Central Directory Service Repository	Lagrar organisationsbaserad data, policys, autentiseringar, etc... och möjliggör synkronisering av EMSW-komponenter som ”hostas” på medlemsstatsnivå.
11	Configurations Management	Samlar in och hanterar all tillgänglig konfigurationsdata centralt
12	Logging & Performance Statistics	Möjliggör hantering av aktivitetsloggar och data kring prestanda
13	Inbound/Outbound Mapper	Mappar alla meddelanden/nyttolaster som tas emot från MIG-standardstrukturen till någon annan relevant standard
14	ID Generator	Genererar Visit_ID:n för deklarerande parter

Applikationstjänster

ID	Applikationstjänst	Applikationstjänstebeskrivning	Service-komponent
1	Message Validation Service	En tjänst för att tillhandahålla syntaxvaliderингar för alla meddelanden som utbyts.	Orchestration Engine (deklarerande parts och medlemsstats RIM)
2	Declaring party Look-up Service	En tjänst som tillhandahålls på medlemsstatens sida för att hitta erforderliga slutpunkter för deklarerande part till vilka meddelanden skickas.	Orchestration Engine (medlemsstats RIM)
3	Member State Look-up Service	En tjänst som tillhandahålls på den deklarerande partens sida för att hitta nödvändiga slutpunkter hos medlemsstaterna till vilka meddelanden skickas.	Orchestration Engine (deklarerande parts RIM
4	RIM Versioning Validation Service	En tjänst för att verifiera den installerade RIM-versionen och validera tillgänglig support för vidare kommunikation.	Service Registry

5	MIG Versioning Validation Service	En tjänst för att verifiera MIG-standardversionen installerad och validera tillgänglig support för vidare kommunikation.	Service Registry
6	Software/ Configuration Updates Service	En tjänst för att centralt skicka ut uppdateringar till alla lokala RIM-installationer.	Management Module
7	Mapping Service	En tjänst för att mappa meddelanden/nyttolaster till MIG-standarden och/eller andra tillämpliga standarder.	Inbound/ Outbound Mapper
9	ID Generation Service	En tjänst för att generera Visit_ID:s som svar på aviseringar om ankomst.	ID Generator

6.2 STM tjänst för navigationsvarningar

Syftet med tjänsten för navigationsvarningar är att endast tillhandahålla konsumenten, det vill säga fartyget, de varningar som är relevanta för den specifika rutten som de avser att segla/ seglar f.n. vid den tidpunkt som anges i ruttens tidplan. Dessutom kommer varningarna att visas direkt i ECDIS (Electronic Chart Display Information System) ombord och automatiskt raderas när de har gått ut och inte längre är giltiga.

Fördelarna är:

- Minskad arbetsbelastning – Inget behov av att manuellt plotta positioner/områden som tas emot av NAVTEX/röstkommunikation på ENC/pappersdiagram. Detta gör att navigatören kan koncentrera sig på att säkert navigera fartyget
- Ökad säkerhet för navigering – Enligt London P&I Club Insurance hittar inspektioner regelbundet brister i att hantera navigeringsvarningar eftersom officerare misslyckas med att implementera navigeringssäkerhetsmeddelanden.
- Minskade mänskliga fel – Eftersom varningar tillhandahålls digitalt och sömlöst visas direkt på ECDIS möjliga mänskliga fel möjliga fel i missförstånd och manuell plottning kan undvikas.
- Ökat fokus för navigeringsvarning - Eftersom endast meddelanden är relevanta för den planerade och/eller faktiska rutten kommer att skickas till ECDIS, personal ombord kan koncentrera sig på dessa och behöver inte bry sig om varningar utfärdade utanför de angränsande områdena.

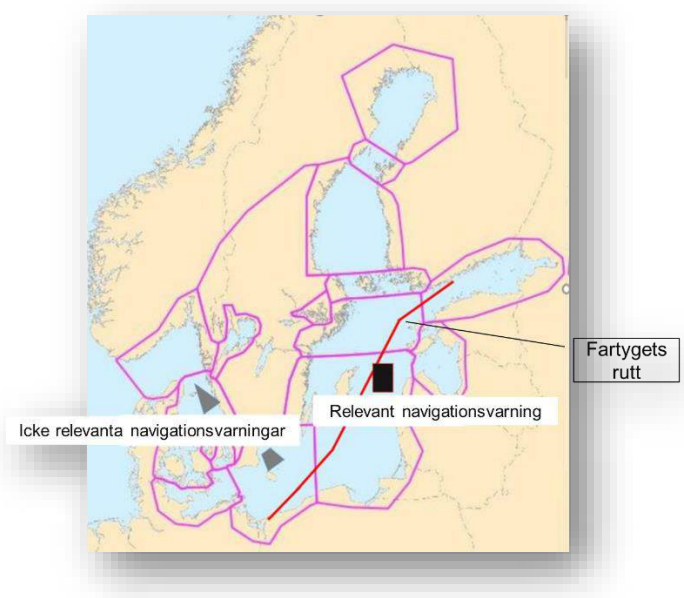
Tjänsten tillhandahåller säkerhetsmeddelanden till fartyg i S-124-format. S-124, navigationsvarningar, produktspecifikationen utvecklas av en IHO-korrespondensgrupp i syfte att skicka in den för godkännande.

Tjänsten initieras när ett fartyg delar sin rutt inklusive tidplan med navigationsvarningstjänsten. Som svar, förser navigationsvarningstjänsten initialt fartyget med alla

relaterade navigationsvarningar inom 15 nautiska mil på var sida om ruttens mittlinje och med fortlöpande uppdateringar inom ruttkorridoren.

Meddelanden utanför ruttkorridoren anses inte vara relevanta och kommer inte att skickas till fartyget.

När fartyget har lämnat tjänstens täcknings-området slutar navigationsvarningstjänsten att skicka uppdateringar till fartyget.



Navigationsvarningstjänsten tillhandahåller följande säkerhetsmeddelanden för navigering:

- Kustvarningar - Navigationsvarningar som gäller för öppet vatten klassas som kustnära. Det är samma information som idag sänds på NAVTEX.
- Lokala varningar för svenska vatten - Varningar som endast gäller vatten inomskärs är betraktas som lokala. Idag sänds endast dessa ut på VHF.

OBS: information om väder/is tillhandahålls inte av tjänsten.

6.3 Port Activity App

I en ny lösning behöver autentisering och auktorisation ses över. Ansökningsprocessen från konsumenter skall leda till en behörighet som behöver implementeras i lösningen.

Lagringen är idag gjord med Azure Storage vilket är flexibelt men har inte så bra prestanda, något som åtminstone bör utvärderas. Möjligen är det tillräckligt om man som i Arrivals-delen rensar så att bara aktiva anlöp inkl. begränsad historik finns i databasen, då blir det inte så mycket data även om man skalar upp för landets alla hamnar.

Dagens lösning är molnbaserad baserad på Microsoft Azure moln-plattform. Om Azure skall fortsätta användas bör det linjera med SjöV strategi för molntjänster.

Fördelar med en Inhouse lösning

- Full kontroll över var informationen lagras
- Oberoende av extern aktör för att tillhandhålla API:er
- Lägre kostnad över tid om drift sköts effektivt
- Enklare att få medarbetare på Sjöfartsverket att ”äga” lösningen

Nackdelar med en Inhouse lösning

- Höga API SLA – krav vilka är svåra att möta internt resursmässigt
- Exponerade API:er är inte separerade från Sjöfartsverkets infrastruktur, SLA krav på API:er blir på detta sätt beroende av SLA för interna system och infrastruktur
- Sämre möjligheter att skala upp/ ut jämfört med en molnlösning

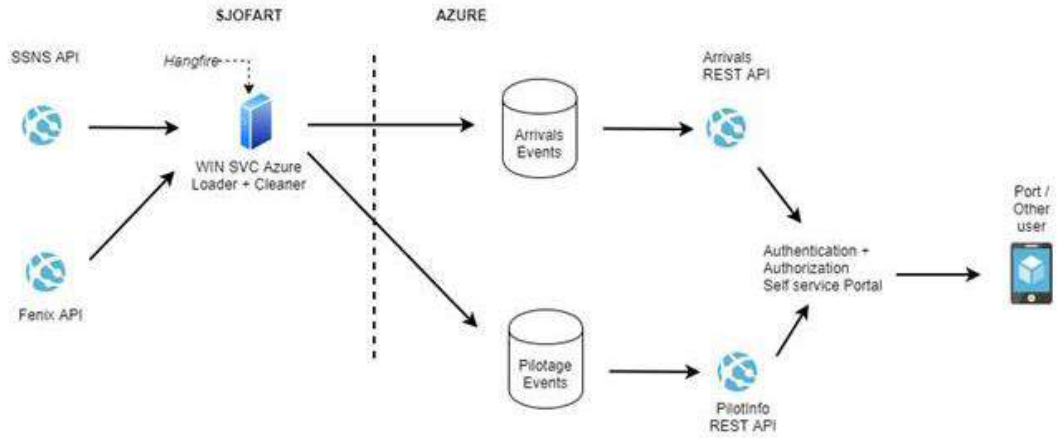
Fördelar med en molnlösning

- Helt separerad från SjöV tekniska miljöer, användarna anropar Azure-tjänsten och är aldrig i kontakt med SjöV infrastruktur
  - Fördel IT-säkerhet
  - Fördel prestanda SjöV nät, servrar
- Enkel att skala upp och ut om mer prestanda-behov uppstår
- Högt SLA på tjänster, storleksordning > 99.95%
- Etablerad på Sjöfartsverket sedan många år, bl.a. ViVa (Vind & Vatten App) driftas idag på Azure
- Tjänsten kommer fortsätta svara även om SjöV har ett servicefönster eller är nere av annat skäl

Nackdelar med en molnlösning

- Personal på Sjöfartsverket är ej inblandad i Azure i särskilt hög grad
- Informationssäkerhetsmässigt behöver detta utredas då information lagras utanför SjöV
- Riskerar kosta mer över tid jämfört med en Inhouse lösning
- Generellt svårt att byta till annan molnleverantör, då dessa generellt strävare efter s.k. vendor lock-in

En ny något omarbetad lösningsarkitektur skulle kunna se ut som i nedanstående bild.



I grova drag ingår nedanstående aktiviteter vid utveckling av en ny lösning;

- Utvärdera prestanda i Azure storage, kan ge resultatet att Azure SQL behöver införas.
- Införa automatisk rensning av lotshändelser i Azure storage
- Separera synkning av lotshändelser från Fenix infrastruktur. Idag är lösningen beroende av release av Fenix Lots för att göra en förändring i lotsdata-synkningen vilket inte blir hållbart på sikt då många aktörer blir inblandade.
- Implementera ny lösning för autentisering baserad på resultatet av en ansöknings-procedur.
- Implementera ny lösning för auktorisation (baserat på rättigheter per UnLocode ?)

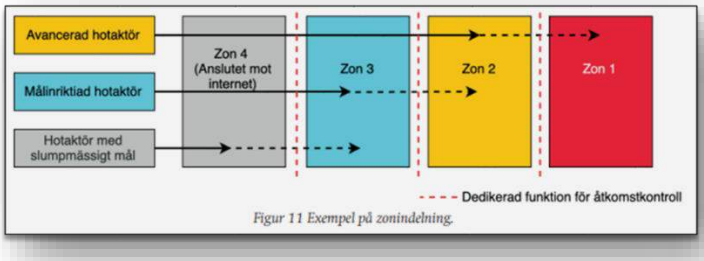
7 Framtagande av IT-arkitektur

7.1 Bakgrund

- Sjöfartsverket har behov av att kunna leverera ”generiska tjänster” i en ny plattform baserad på Linux och Open Source komponenter.
- Två grundförutsättningar som saknas för att kunna realisera detta är.
  - Nätsegmentering ur ett datacentersperspektiv.
  - Kontroll på dedikerade funktioner för åtkomstkontroll t ex IdP (Identity Provider).
- Autentisering SIG (Special Interest Group) i IT Community
- Lösningsförslaget utgår ifrån en tolkning av de krav som står omnämnda i MSBFS 2020:7 och PMFS 2019:2, se nedan bild.

7.2 Säkerhetszoner

Som utgångspunkt segmenteras nätet i fyra zoner enligt det exempel som återfinns i vägledningen kring informationssäkerhet.
Informationssystem som omfattas av motsvarande krav på säkerhetsskydd kan placeras i samma säkerhetszon.
Varje zon behöver dedikerade funktioner för åtkomstkontroll och filtrering av nätverkstrafik.



Figur 11 Exempel på zonindelning.

7.3 Säkerhetszoner och informationssystemets placering

Här definieras var informationen ligger lagrad/ vilande (”data at rest”).

- Zoner är till för att få en grov indelning av informationssystem med samma skyddsvärde.
- Zon 4 (jmf med DMZ – DeMilitarizedZone idag) är minst skyddsvärd och Zon 1 är mest skyddsvärd.
- Zon 4 har möjlig åtkomst ifrån Internet.
- Genom att undvika lagring av information i Zon 4, minskar risken kring att informationen förändras av obehöriga. (Riktighet)

Se vidare utdrag ur PMFS nedan som beskriver bestämmelser för vad som gäller för placering av informationssystem med hänsyn till olika säkerhetsskyddsklasser.

Av bestämmelserna i 4 kap. 20-21 §§ i PMFS 2019:2 framgår att: 20 §: Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller konfidentiell, logiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

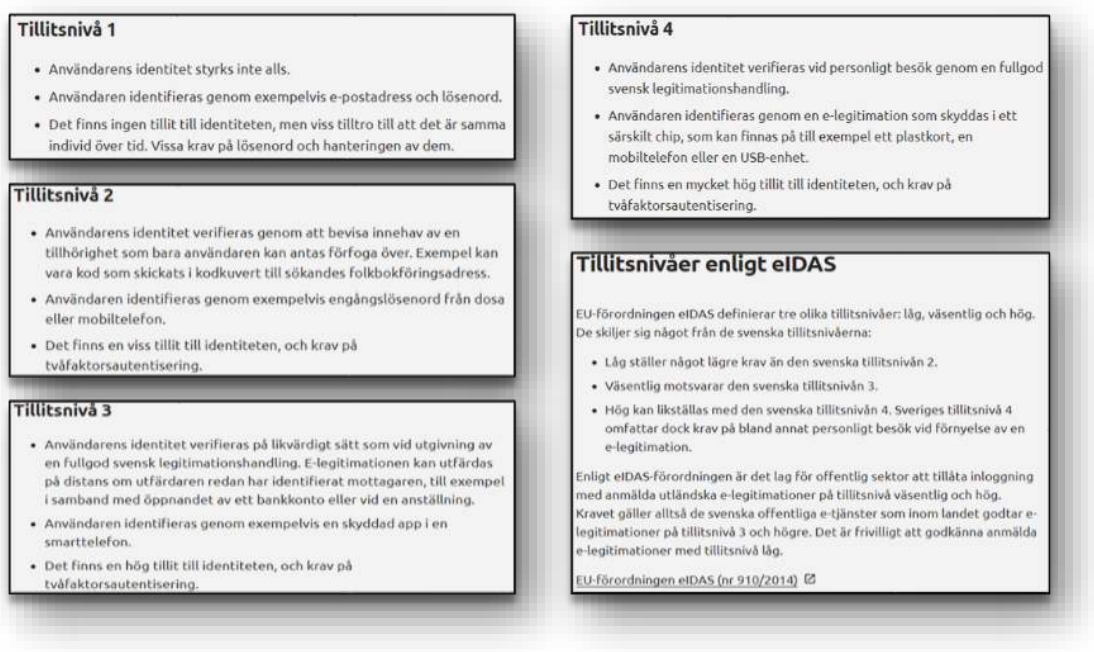
21 §: Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, fysiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd. Informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, ska tillåta endast envägskommunikation vid import respektive export av data.

7.4 Konsumtion av informationssystemets tjänster

Här definieras hur informationen kan konsumeras och av vem. ”data in transit/data in motion”

Informationssystemet behöver kunna tillgängliggöra information(tjänster) till olika konsumenter i zoner med längre skyddsvärde utan att behöva lagra informationen i zonen.
Åtkomst till tjänster i olika zoner kräver olika grad av säkerhet och tillförlitlighet som kan definieras som tillitsnivå (LoA - Level Of Assurance).

DIGG har sammanställt vad tillitsramverket för Svensk e-legitimation samt ISO/IEC 29115 i korthet innebär gällande tillitsnivåer för Sverige samt EU-förordningen eI-DAS, se vidare nedanstående figur.



I tabellen nedan definieras vilka informationsklasser en tjänst är tillåten att ställa ut i respektive Zon samt vilken tillitsnivå som krävs på konsumentens identitet.

Om tjänsten tillgängliggörs i Zon	...med information upp till säkerhetsnivå	... ställs följande krav på Tillitsnivå
Zon 4	K0 - Öppen	Tillitsnivå 1
Zon 4	K2 - Intern, känslig	Tillitsnivå 2
Zon 4	K3 - Intern, sekretess	Tillitsnivå 3
Zon 3	K3 – Intern, sekretess	Tillitsnivå 3
Zon 3	K5 – Konfidentiell	Tillitsnivå 4
Zon 2	K5 – Konfidentiell	Tillitsnivå 4
Zon 1	K6 - Hemlig	Tillitsnivå 4 med Fysisk separation
Zon 1	K7 - Kvalificerat Hemlig	Tillitsnivå 4 med Fysisk separation

7.5 Betydelse av tillitsnivå i respektive zon för Sjöfartsverket

- Baserat på vilken Zon informationstjänsten tillgängliggörs i samt vilket krav man har på tillitsnivån, kan Sjöfartsverket implementera standardlösningar för autentisering.
- För användare/individer krävs en typ av lösningar och för system/resurs krävs en annan typ av lösningar och skall vara unika över tid.
- Av bestämmelserna i 4 kap. 12-13 §§ i PMFS 2019:2 framgår att:
  12 §: Alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till individ, system eller resurs.
- Tabellen nedan innehåller exempel på en Sjöfartsverks-standard för autentiseringslösningar.

Om tjänsten tillgängliggörs i Zon	… och har krav på följande tillitsnivå	… så använder sjöfartsverket följande autentiseringslösning för användare/individer	… eller följande autentiseringslösning för system/device
Zon 4	Tillitsnivå 1	Användarnamn och lösenord.	API key
Zon 4	Tillitsnivå 2	Tvåfaktor med Användarnamn/lösenord samt App för smartphones och surfplattor	Access token.
Zon 4	Tillitsnivå 3	BankID eller FrejaID.	Access token.
Zon 3	Tillitsnivå 3	Certifikat på device samt användarnamn och lösenord.	Certifikat
Zon 3	Tillitsnivå 4	Smarta kort	Certifikat
Zon 2	Tillitsnivå 4	Smarta kort	Certifikat
Zon 1	Tillitsnivå 4 med Fysisk separation	Smarta kort	N/A
Zon 1	Tillitsnivå 4 med Fysisk separation	Smarta kort	N/A

7.6 Teknisk implementation

- En segmenteringsbrandvägg delar upp datacenternätet i Zoner och nätverkssegment inom respektive zon.
- Åtkomst till respektive Zon sker alltid via en Application Delivery Controller i separata partitioner.
- Varje Zon har en egen instans av IdP (Identity Provider), som säkerställer tillitsnivån på tjänsterna.
- Ovannämnda komponenter är separerade och med paritet mellan Utveckling, Test och Produktionsmiljö.
- Segmenteringsbrandvägg med VDOM'ar
- Active Directory Controller med partitioner (tjänster separeras i virtuellt)
- IdP i egna instanser i separata vlan (tjänster separeras i en domän).
- Varje Zon förses med en egen uppsättning tekniska hjälpmedel (förmågor) som informationsklasserna kräver.

En bild över vald målarkitektur kan av skyddsvärdesskäl inte inkluderas i denna rapport.

8 Proof of Concept (PoC) för infrastrukturen

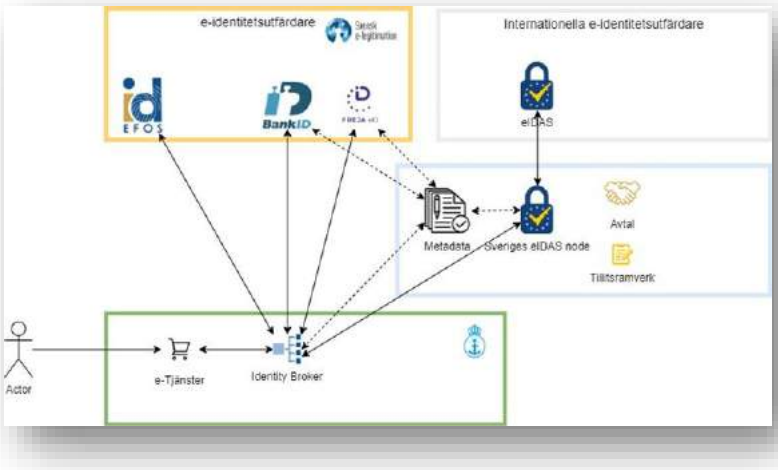
8.1 PoC med Sweden Connect (DIGG)

Med avstamp i föreslagen arkitektur genomfördes en PoC i lab-miljö mot den svenska identitetsfederationen Sweden Connect.
Med framgång kunde Sjöfartsverket i en PoC e-tjänst:

- Autentisera fiktiva svenska användare med tillitsnivå 3 och 4 via BankID, FrejaID+
- Autentisera fiktiva utländska användare med via den svenska eIDAS noden med jämförbara tillitsnivåer.

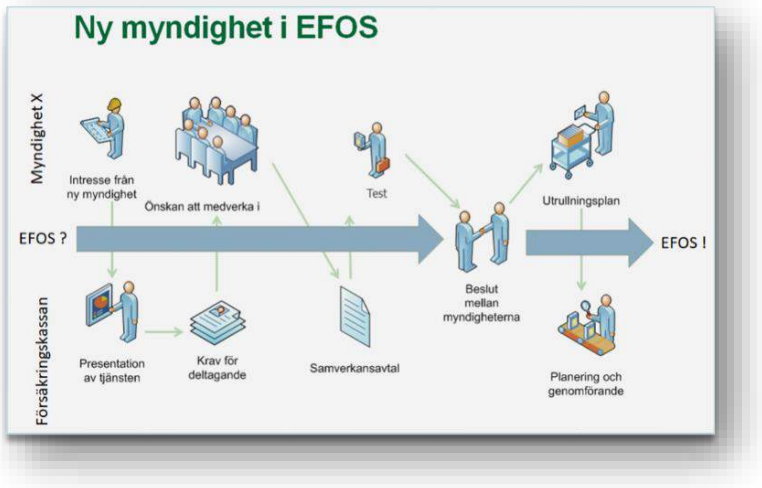
8.2 Lösningsförslag e-tjänster för kunder

- Avtal är tecknat med DIGG på Valfrihetssystemet 2017 och 2018 som ger tillgång till FrejaID+, BankID/Mobilt BankID och Telia e-legitimation.
- Genom metadatautbyte med Sweden Connect skapas en federation och en tillit mellan e-identitetsutfärdare och de e-tjänster Sjöfartsverket erbjuder.



8.3 Lösningsförslag e-tjänster för medarbetare

- Skaffa e-legitimation åt medarbetare som är godkänd för kvalitetsmärket Svensk e-legitimation.
- E-identitet För Offentlig Sektor (EFOS) är godkända för Svensk e-legitimation.
- EFOS tillhandahåller både ”smarta kort” och Mobilt EFOS.



8.4 Kontinuitetsplanering

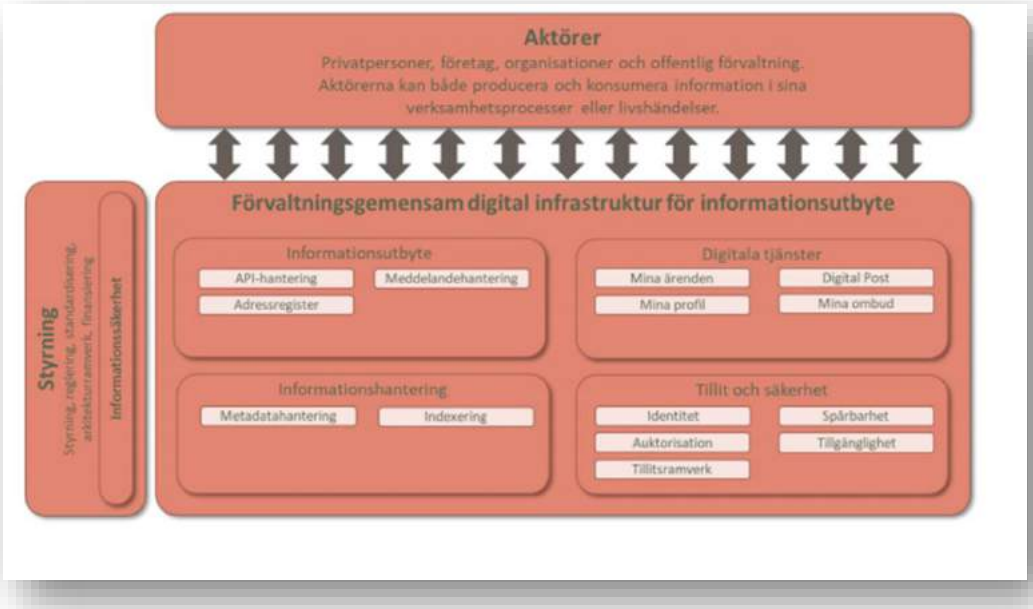
Lösningsförslaget bygger på att Sjöfartsverket använder externa tjänster för e-legitimering vilket kräver en genomtänkt kontinuitetsplanering i händelse av att dessa externa tjänster förlorar sin operativa förmåga.

En del av lösningen är att t.ex. kunderna erbjuds flera alternativa e-legitimeringstjänster (BankID, FrejaID+ mm).

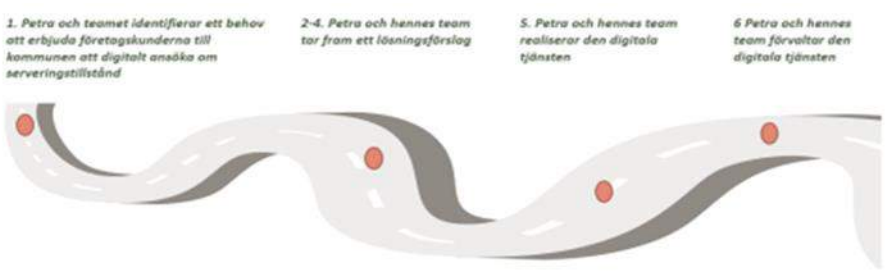
I händelse av att samtliga e-legitimeringstjänster är ur funktion kan verksamheten fatta beslut om att ta risken och sänka tillitsnivån på e-tjänsten. I detta fall kan Sjöfartsverket med lösningens komponenter erbjuda MFA (Multi Factor Authentication) med t ex användarnamn och lösenord samt engångslösenord via app som inte kräver externa tjänster.

8.5 Förvaltningsgemensam digital infrastruktur

I utvecklingen av Sjöfartsverkets IT arkitektur för informationsdelning har hänsyn tagits till den förvaltningsgemensamma digitala infrastrukturen som kommer att etableras enligt motsvarande regeringsuppdrag. I rapporten ”Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte samt uppdrag att etablera ett nationellt ramverk för grunddata inom den offentliga förvaltningen” presenteras en logisk arkitektur enligt nedan bild.



Vidare presenteras ett antal användarscenarios, varav Användarscenario – ”Petra och utvecklingsteamet ska utveckla en digital tjänst” ligger nära tillhands för att beskriva det Sjöfartsverket försöker skapa förutsättningar för i detta arbetspaket. Framförallt har byggblocken under tillit och säkerhets beaktats i Sjöfartsverkets lösning. Se inkopierad bild som beskriver användarscenariot nedan.



1. Petra och teamet har identifierat ett behov av att erbjuda en digital möjlighet för företagskunder att ansöka om serveringstillstånd.
2. Petra och teamet identifierar och analyserar de behov som kunderna till det tilltänka tjänsten har och fångar de krav som bör finnas på tjänsten för att den ska vara trygg och säker med utgångspunkt från byggblock:
   - API, där framtagna riktlinjer/rekommendationer och standarder finns att tillgå samt vilka tillgängliggjorda API:er finns att nyttja,
   - Auktorisation, där lösningsmönster och referensarkitektur finns att tillgå samt vägledning om nationella attribut som ska finnas med vid elektronisk auktorisation,
   - Tillgänglighet, där rekommendation finns gällande att säkerställa åtkomst för behörig person vid rätt tillfälle,
   - Spårbarhet, där vägledningar finns att tillgå för att kunna återskapa(utreda) händelseförlopp vid informationsutbyte,
   - Tillitsramverk, som erbjuder ramverk för ett säkert och effektivt informationsutbyte, där information finns kring hantering av tillitsnivåer, ansvar och arbetssätt.
3. Teamet analyserar vilken information som krävs i tjänsten och identifierar de informationsmängder som finns att tillgå utifrån de modeller som tidigare tagits fram av ansvariga för grunddatadomänerna Person och Företag. Eftersom informationsmodellerna beskrivs enligt grunddataramverket så kan utvecklingsteamet snabbt förstå hur informationsmängden är strukturerad och kan användas.
4. För att ta fram hela lösningsförslaget ser teamet även över vilka befintliga byggblock i infrastrukturen som går att ansluta till och återanvända i samband med realisering av den digitala tjänsten. De byggblock i infrastrukturen som teamet ser går att återanvända för denna digitala tjänst är då framförallt byggblocket Identitet, eftersom tjänster kräver säker identifiering. Kommunen har i dagsläget Mina sidor så byggblocket Mina ärenden kan användas för att generera kundhändelser som presenteras via Mina sidor. Mina ombud är en central del i denna digitala tjänst och har all funktionalitet som krävs för att hantera digitala fullmakter och notifiering via Digital Post.
5. Petra och teamet realiserar den digitala tjänsten. Programmering sker utifrån krav som tydliggjorts i de förutsättningsskapande byggblocken som nämnts ovan för att vara kompatibla med övriga delar i infrastrukturen.
6. Petra och teamet förvaltar den digitala tjänsten.

9 Referenser

Sea Traffic Management - https://www.seatrafficmanagement.info

Efficient Flow Port Activity App - https://www.seatrafficmanagement.info/projects/efficientflow/results-port-flow-optimisation/

Maritime Single Window - https://www.sjofartsverket.se/sv/tjanster/msw-reportal/

European Maritime Single Window environment - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A4407248

Polismyndighetens författningssamling - https://polisen.se/lagar-och-regler/polismyndighetens-forfattningssamling/

Myndigheten för Samhällsskydd och Beredskap författningssamling - https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-7-foreskrifter-om-sakerhetsatgarder-i-informationssystem-for-statliga-myndigheter.pdf

DIGG Förvaltningsgemensam digital infrastruktur - https://www.digg.se/4ad66f/globalassets/dokument/publicerat/publikationer/uppdrag-att-etablera-en-forvaltningsgemensam-digital-infrastruktur-for-informationsutbyte-samt-uppdrag-att-etablera-ett-nationellt-ramverk-for-grunddata.pdf

5.3 Förstudie nautisk tilläggsinformationstjänst

SJÖFARTSVERKET

Förstudierapport
Nautisk Tilläggsinformation 2

Forskning och Innovation

Rapporten finns tillgänglig på Sjöfartsverkets webbplats www.sjofartsverket.se

Dnr/Beteckning	21-00156
Författare	Tommy Skarpling
Månad År	December 2021

Sammanfattning

Slutsatsen i denna förstudierapport är att Sverige som kuststat är skyldiga att tillhandahålla aktuella seglingsbeskrivningar enligt SOLAS kapitel 5 som pekar på IHO:s publikationer, vilket i sin tur innebär att IHO:s publikation M3 är vägledande. M3 är inriktat på pappersprodukter, men publikationen godkänner också digitala produkter även om någon standard ännu inte beslutats.

IHO är styrande i arbetet med den nya standarden S-100 som i flera delar täcker den information som seglingsbeskrivning omfattar. Sjöfartsverkets sjögeografiska strategi säger att vi framgent ska inrikta oss på att producera produkter för de standarder som beskrivs inom S-100, vilket gör att det naturliga valet för framtiden är att producera seglingsbeskrivningar utifrån IHO:s M3, med inriktning att följa S-100 för digital information och distribution.

För Sveriges del som kuststat och för Sjöfartsverket betyder det att Sjöfartsverket bör distribuera seglingsbeskrivningar. Det behöver dock göras tillsammans med de svenska hamnarna som äger viss information som omfattas av detta.

I förstudierapporten presenteras ett förslag till en teknisk lösning som möjliggör ett samarbete mellan Sjöfartsverkets olika avdelningar samt Sveriges hamnar.

Norrköping, december 2021

Tommy Skarpling

Innehåll

Termer och förkortningar

Term/förkortning	Betydelse	Kommentar
API	Application Programming Interface	Funktion för att program ska kunna kommunicera med varandra
BRM (f.d. BTM)	Bridge Resource Team (f.d. Bridge Team Management)	Branschstandard för hur de tillgängliga resurserna på en fartygsbrygga skall utnyttjas på ett effektivt/säkert sätt för reseplanering.
GMDSS	Global Maritime Distress and Safety System	Internationellt system som består av land- och rymdbaserad radioteknik samt radioutrustning på fartyg
H2M	Human To Machine	Där människan kommunicerar med en maskin (dator e.l.)
IHO	International Hydrographic Organization	
IMO	International Maritime Organization	
M2H	Machine To Human	Där maskiner (datorer e.l.) kommunicerar med en människa genom (bl. a.) ett visuellt gränssnitt.
M2M	Machine To Machine	Där maskiner (datorer e l) kommunicerar med varandra utan att människan ser innehållet.
NIPWG	Nautical Information Provision Working Group	IHO arbetsgrupp som ansvarar för standardisering av nautiska publikationer.
NTI	Nautisk Tilläggsinformation eller Sailing Directions på engelska	Information som behöver för ett anlöp som inte står i ett sjökort.
PoC	Proof of Concept	Koncepttest
S-100	IHO Universal Hydrographic Data Model	Serie med hydrografiska/marina standarder från IHO
SOLAS	IMO Safety of Life At Sea	Internationell konvention för säkerhet för människoliv till sjöss
TRL-skala	Technical Readiness Level	En beteckning för en teknologis mognadsgrad och tillhörande teknologisk risk
VTS	Vessel Traffic Services	Säkerhetssystem för sjöfarten som bygger på att fartyg i tättrafikerade leder anmäler sig och berättar om sina avsikter till en lokal myndighet
UKHO	United Kingdom Hydrographic Office	Brittiska motsvarigheten till Sjöfartsverkets avdelning Sjögeografi

1 Bakgrund

1.1 Om projektet och detta arbetspaket

Denna rapport beskriver resultatet av arbetspaketet Nautisk Tilläggsinformation 2 som, tillsammans med tre andra arbetspaket, är en del i projektet Branschgemensamt digitalt anlöp - fas 1, med genomförandeperiod april 2020 - december 2021. Trafikverket är huvudsaklig finansiär av arbetspaketen. Sjöfartsverket är projektledare för arbetspaketen och bidrar med ytterligare resurser för arbetet i dem. Externa partners har också utlovat sin tid för arbete i vissa av arbetspaketen, vilket var en förutsättning för genomförande av Arbetspaket 3.

Mål:

- Leverera en förstudierapport som mot bakgrund av beskrivna leveranser, föreslår tillvägagångssätt för Sverige som medlemsstat i IMO och IHO att tillhandahålla tillfyllest NTI-information, med avstamp i vad som levereras av Sjöfartsverkets NTI1-projekt.
- Leverera scenariobeskrivningar för möjliga NTI/Sailing Directions-lösningar.

Effektmål:

- Att skapa en väg framåt för Sverige och Sjöfartsverket att uppfylla de krav inom ämnesområdet som är ställda på oss som kuststat och medlemsstat i IMO och IHO. Där har Sjöfartsverket en roll där man i regeringens instruktion är ”samordnare av Sjögeografisk information i Sverige” och även s.k. ”Hydrographical office”.
- Framtida kundnytta genom att undersöka hur vi kan utforma en relevant och affärsmässig NTI-tjänst.
- Nytta för informationsägare/-lämnare och -distributörer genom redovisning av hur en produkt som traditionellt har getts ut i bokform, kan skapa mervärde genom digitaliserad och smart distribution.

2 Från fysisk publikation till modern NTI-tjänst

Nautisk Tilläggsinformation (NTI och på engelska: ”Sailing Directions”) behövs av fartyg och rederier i planeringen och genomförandet av hamnanlöp.

Det finns säkerhetsrelaterad och praktisk information som behöver komma anlöpande fartyg till del och som hamnmyndigheterna svarar för. Anlöpande fartygs skyldigheter gentemot hamnen kan exempelvis stipuleras i hamnordning, hamnföreskrifter eller driftsföreskrifter.

Historiskt har detta uppfyllts bl.a. genom tillhandahållandet av publikationen Svensk Lots som innehöll information om hamnar och deras tjänster, beskrivning av lämpliga fartygsrutter, nautiska tjänster såsom lotsning, isbrytning, bogsering och VTS samt restriktioner gällande t.ex. farter, vindgränser, lotsningsrestriktioner och bogserbåtskrav. Sjöfartsverket avser att fortsättningsvis uppfylla detta behov inom sitt ansvarsområde genom digitaliserade lösningar, vilket är ett avgränsat arbete som för närvarande pågår och som finansieras av Sjöfartsverkets egna medel.

Genom en ny och utvidgad samordning mellan hamnar och Sjöfartsverket gällande informationsförvaltning, digitalisering av information och distribution till anlöpande fartyg genom digitala tjänster är förväntan att en ökad kundnytta skulle kunna uppnås. Detta befinner sig fortfarande på en konceptuell nivå lågt på TRL-skalan. Förutom individuell nytta ger denna branschöverskridande tjänst också ett tillfälle att praktiskt testa och utvärdera förslagen till samordnad styrning och långsiktig planering.

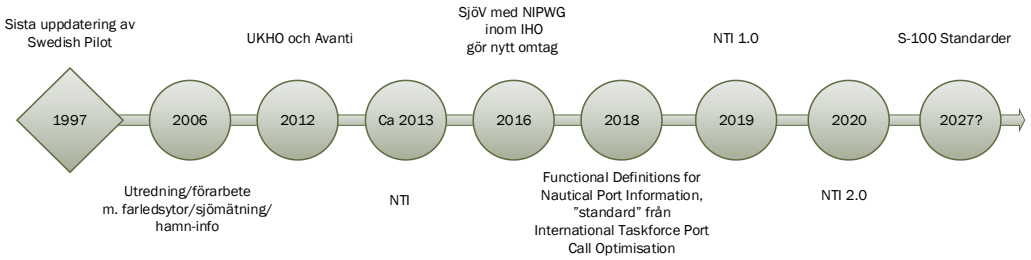
2.1 Nautiska publikationer och uppkomsten av S-100

I IMO:s konvention SOLAS kap 5 framgår det att en kuststat ska tillse att nödvändiga nautiska publikationer tillhandahålls för säker navigation genom försorg från kuststatens egen eller kontrakterade hydrografiska kontor. I konventionen[1] hänvisas till IHO:s standarder och specifikationer. Det som kan anses tillämpbart för just nautiska publikationer återfinns i Resolutions of the IHO (M-3)[2]..

Innan sjöfarten kom att domineras av navigering med elektroniska navigationssystem gav Sjöfartsverket ut nautiska publikationer som motsvaras av de som omnämns i ovan resolutioner. Det gäller Svensk Lots och Svensk Fyrlista, som gavs ut i sina sista upplagor i slutet av 1990-talet. Därefter kom informationen delvis att ersättas av att den årliga uppdaterade UFS A utökades till att omfatta mer generisk information som inte kan kommuniceras via sjökort. Dessutom publicerades också viktig information, som förr

[1] Regulation No 2 och No 9
[2] Under kapitel 2.4, Publications och mer specifikt under kapitel 2.4.6 Sailing Directions (Seglingsbeskrivningar)

återfanns i Svensk Lots, på SjöV:s externa hemsida under respektive lots-områdes undersidor som uppdateras regelbundet. Ett 10-tal år efter att Svensk Lots utgivits i sin sista upplaga slutade SjöV att sälja produkterna och man initierade då samtidigt ett arbete, kallat NTI, Nautisk Tilläggsinformation, för att utreda hur man på ett strukturerat sätt skulle kunna tillhandahålla dylik information.



Runt 2005-2006 startade SjöV ett arbete med att ta fram underlag med hamninformation som skulle ligga till grund för kommande leveranser till det som idag kallas för Nautisk Tilläggsinformation.

Fram till omkring 2012 deltog Sjöfartsverket i ett arbete tillsammans med International Harbour Masters Association (IHMA), i samarbete med UKHO, för att ta fram en prototyp eller en digital samlingsplats för att lagra information om seglingsbeskrivningar digitalt utifrån ett hamnperspektiv. Prototypen, som kallats AVANTI, skulle fungera som en databas. Då de kommersiella förhållandena till UKHO var oklara valde Sjöfartsverket att endast finnas med som observatör i AVANTI-projektet. Det arbete som gjorts lyftes in i den nybildade konstellationen International Taskforce for Port Call Optimization (ITPCO) som drivs från Rotterdams hamn i Nederländerna.

Sjöfartsverket behöll dock strukturen och tankarna runt det som formulerats i det ursprungliga Avanti-arbetet och började titta på det arbete som lagts ned för att runt 2012-2013 starta ett nytt arbete med nya fräscha ögon. Detta projekt kallades fortsatt Nautisk Tilläggsinformation (NTI). Under åren fram till 2016 arbetade Sjöfartsverket med koncept för NTI både vad gäller insamling av data, lagring, registrering och ett gränssnitt att tillgodogöra sig informationen. Ett viktigt resultat var att man kom fram till en miniminivå för vilken information som måste ingå i en framtida NTI-lösning. Denna miniminivå avstämdes också med Transportstyrelsen.

Omkring 2016 hade Sjöfartsverket lyft behoven och vårt arbete till IHO där vi arbetade tillsammans med arbetsgruppen Nautical Information Provision Working Group[3] (NIPWG)vars mål är (fritt översatt från webbplatsen): ”Att

[3] NIPWG, https://iho.int/en/nipwg

utveckla och upprätthålla vägledning, resolutioner och specifikationer för att ge fartygsanvändare nödvändig och uppdaterad information i rätt tid för att möjliggöra planering av en säker rutt för den avsedda resan och säker navigering under resan."

Under 2020 har ett samarbete inletts mellan IHO:s ansvariga arbetsgrupp NIPWG och IHMA för att inom IHO verka för att standardisera resultat från AVANTI-projektet. Vid det övergripande kommittémötet (HSSC) i oktober 2020 togs beslut om att denna produkt ska tilldelas produktspecifikationsnamnet S-131, Marine Harbour Infrastructure.

NIPWG arbetar med att få in Nautical Publications i en ramverksstandard för sjögeografiska data. Detta system kallas för S-100 och är tänkt att ersätta dagens enklare elektroniska sjökort (S-57), samt möjliggöra standardisering av andra sjögeografiska data som används för navigation och även en standardiserad beskrivning av informationstyper kopplat till den marina miljön. S-100-standarden är ett ramverk som är avsett för utveckling av digitala produkter och tjänster för digital navigation (enligt IMO:s e-navigationprinciper), men ska även kunna användas som standarder för att definiera dataformat för andra GIS-lösningar. De dataset som NIPWG ansvarar för, och som motsvaras av Nautical Publications, är:

- S-122 Marine Protected Areas s.k. MPAs
- S-123 Marine Radio Services
- S-125 Marine Navigational Services
- S-126 Marine Physical Environment
- S-127 Marine Traffic Management
- S-128 Catalogue of Nautical Products
- S-131 Marine Harbour Infrastructure

Detta kommer att ersätta det som idag beskrivs som Sailing directions, Radio Signals och List of Light.

2.2 Sailing Directions i Sveriges omvärld

Hur förhåller sig Sveriges grannländer till deras förpliktelser som kuststat och överenskomna åtaganden vad gäller Sailing Directions (seglingsbeskrivningar) och utgivning av nautiska publikationer?

Urvalet av jämförelseländer har skett med hänsyn till vissa geografiska likheter (Norge, Finland), närmsta geografiska grannskap (Norge, Finland,

Danmark) samt på grund av redan etablerade kontakter och samarbeten mellan sjöfartsmyndigheter inom olika internationella maritima projekt (Estland m.m.).

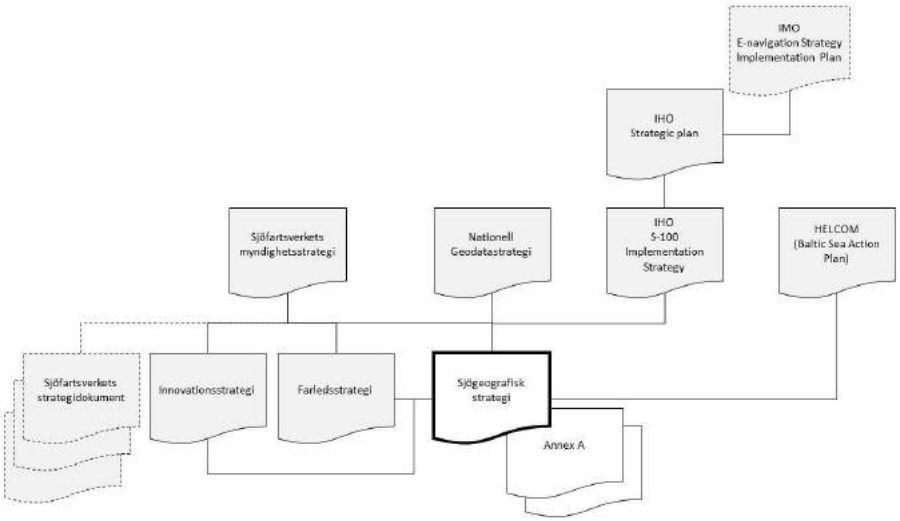
Generellt kan konstateras att andra länders arbete med att utveckla Seglingsbeskrivningar på modernt format bedöms vara på samma nivå som i Sverige, med undantag för Norge. De Östersjöländer som omfattas av denna analys tillgängliggör nautisk information i mer eller mindre elektronisk form, oftast i pdf-format eller som en interaktiv tjänst. Norge tycks ha kommit längst bland jämförda kuststater vad gäller utveckling samt implementering av interaktiva lösningar för Sailing Directions och tillhandahåller en interaktiv karttjänst och man nyttjar även Artificiell Intelligens (AI) i de utvecklade nautiska produkterna. Ansvariga myndigheter i Östersjöländerna följer upp eller deltar i arbetet med utveckling av S-100 standarderna.

Utgivare av kommersiella produkter, såsom brittiska Admiralty Sailing Directions och ”Guide to Port Entry”, utvecklar egna produkter och erbjuder olika former av tillhörande tjänster. Även dessa leverantörer bedöms arbeta mot digitalisering samt följer utvecklingen av S-100 standarden. Läs mer om Sailing Directions i vår omvärld i bilaga 7.4.

Utifrån denna nulägesbild kan det inte uteslutas att utveckling av framtida produkter för Seglingsbeskrivningar kommer att ske internationellt, men främst i samarbete med andra kuststater inom Östersjöområdet.

2.3 Sjöfartsverkets sjögeografiska strategi 2020 med S-100 och NTI

Strategier och vägledande principer för den sjögeografiska strategin måste förstås i sitt sammanhang. Den sjögeografiska strategin är associerad till internationella och nationella strategier och är underordnad dessa liksom den är underordnad Sjöfartsverkets myndighetsstrategi. Vidare finns associationssamband till myndighetens övriga strategier, till exempel farledsstrategin.



Strategier associerade till den sjögeografiska strategin

Produkter från Sjöfartsverkets avdelning Sjögeografi stödjer navigering i framtidens digitaliserade farleder bl. a. genom efterfrågade tjänster som nya generationens ENC (S-101), djupdata i ECDIS (S-102), navigationsvarningar i ECDIS (S-124) samt produkter för ruttplanering (NTI). Övriga S-100 tjänster kommer att identifieras via Sjögeografis S-100 Strategiska plan (Annex B). För att leverera framtidens sjökortsprodukter måste högupplösta djupdata finnas tillgängliga genom fortsatt sjömätning av svenska farvatten.

2.4 S100-standardens relevans för NTI

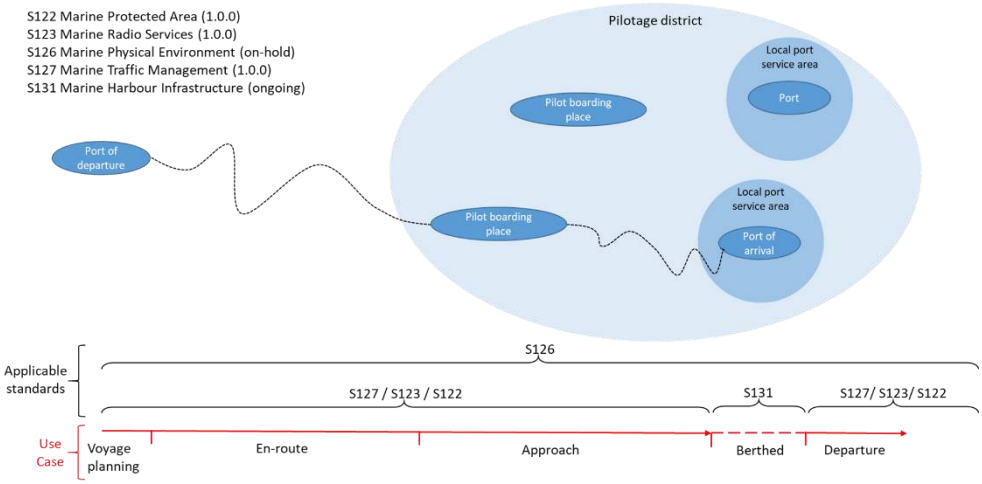
S-100 är ett ramverk som tas fram med ledning av IHO och är tänkt att skapa standarder för utveckling av digitala produkter och tjänster för hydrografiska, maritima och GIS-områden. Olika ”intresseområden” har tilldelats egna nummerserier inom S-100 där man hitta IHO:s hydrografiska data inom serien S-101 – S-199, IALA:s Light Authorities som har delen som återfinns inom spannet S-201 – S-299. Bland övriga organisationer med områden inom S-100 finns WMO (World Meteorological Organization, Inland ENC Harmonization Group (IEHG) med flera. En introduktion för mer information om standarden S-100 finns att läsa på IHO:s hemsida.[4]

För NTI så är det främst S-127 (Marine Traffic Management) som är aktuellt och förmodligen kommer användas mest. Till denna skall vi också analysera standarden S-131 (Marine Harbour Infrastructure) men inte i samma detaljeringsgrad som S-127. Det finns utöver dessa två standarder som kommer att behöva användas i NTI-systemet och nedanstående S100-standarder

[4] https://iho.int/en/introduction-0

innehåller i olika mängd delar av dess datamodeller för att tillsammans uppfylla de krav och rekommendationer som IHO:s M3 beskriver. Utöver ovan nämnda standarder skulle även S-421 kunna ha betydelse för NTI genom dess förmåga att precisera ett fartygs tänkta färdplan både geografiskt och i tid.

I nuläget är status för de olika standarderna på olika nivåer, utvecklingsmässigt, men bör vara färdiga för implementering runt 2024-2025. Då det med största sannolikhet inte kommer att vara så stora ändringar då i förhållande till version 1.0 så bör det inte vara något hinder att starta utvecklingen enligt beskrivning som återfinns senare i denna förstudie.



3 Analys av resolutioner och informationsmängd för säker navigering

Vad Sailing Directions (seglingsbeskrivningar) innehåller och vem som skall ta fram, underhålla, distribuera och ansvara för vad, har tidigare inte klargjorts på ett strukturerat sätt. Från Sjöfartsverkets sida har man ansvarat för och distribuerat bl. a. Svensk Lots fram till slutet av 90-talet. Efter det har viss information publicerats på respektive lotsområdes hemsida på www.sjofartsverket.se. Seglingsbeskrivningar innehåller dock mer än så.

Generellt brukar man definiera Seglingsbeskrivningar som den information som behövs för säker navigering, för att kunna angöra en hamn och som inte beskrivs i ett aktuellt sjökort.

3.1 Analys och definition av SOLAS kapitel fem

Internationell rätt är ett omfattande och komplicerat rättsområde. Kort kan sägas att stater genom olika typer av internationella överenskommelser förbinder sig att agera på ett visst sätt. Staternas efterlevnad av överenskommelserna och sanktioner för överträdelser hanteras också inom ramen för internationell rätt.

Överenskommelserna, eller konventionerna, införs i flera steg. Det är konventionen staten tillträder. Att tillträda innebär att man utger en avsiktsförklaring att senare underteckna och ratificera konventionen. Därefter undertecknar staten konventionen och förklarar sig därmed beredd att ratificera konventionen. Slutligen ratificerar staten konventionen och införlivar den därmed i landets egen lagstiftning, en process som ibland kräver nationella författningsändringar och ett beslut av ett nationellt styrande organ. Till konventioner knyts sällan några formella sanktioner, vid sidan om informella påtryckningar och kritik i samband med utvärderingar.

Sjöfartsverket är en svensk myndighet som arbetar under svensk lag. Myndighetens förhållningssätt i förhållande till de olika konventionerna regleras genom regeringens instruktion till myndigheten.

För att Sjöfartsverket ska vara bunden av någon internationell förpliktelse ska som regel den svenska staten ha införlivat kravet i svensk lagstiftning. I så fall finns eventuella sanktioner kopplade till den lagstiftning som landets styrande organ beslutar om.

Att internationella akter av olika slag är direkt bindande är ovanligt och i princip förbehållet EU-förordningar.

Sammanfattningsvis ska Sjöfartsverket förhålla sig till relevanta konventioner i den mån vi har uppdrag att göra detta i svensk lag.

3.1.1 Vem är skyldig att publicera Sailing directions? Är någon skyldig?

Av regelverket SOLAS kapitel 5 regel 9 följer att

1 Contracting Governments undertake to arrange for the collection and compilation of hydrographic data and the publication, dissemination and keeping up to date of all nautical information necessary for safe navigation.

2 In particular, Contracting Governments undertake to co-operate in carrying out, as far as possible, the following nautical and hydrographic services, in the manner most suitable for the purpose of aiding navigation:

> *.1 to ensure that hydrographic surveying is carried out, as far as possible, adequate to the requirements of safe navigation;*
>
> *.2 to prepare and issue nautical charts, **sailing directions**, lists of lights, tide tables and other nautical publications, where applicable, satisfying the needs of safe navigation;*
>
> *.3 to promulgate notices to mariners in order that nautical charts and publications are kept, as far as possible, up to date; and*
>
> *.4 to provide data management arrangements to support these services.*

*3 Contracting Governments undertake to ensure the greatest possible uniformity in charts and nautical publications and to take into account, whenever possible, relevant international resolutions and recommendations.**

4 Contracting Governments undertake to co-ordinate their activities to the greatest possible degree in order to ensure that hydrographic and nautical information is made available on a world-wide scale as timely, reliably, and unambiguously as possible.

** Refer to the appropriate resolutions and recommendations adopted by the International Hydrographic Organization.*

Detta är Sveriges åtagande enligt SOLAS-konventionen i de delar som berör "Hydrographic services". Det följer tydligt av avsnittet att stater som undertecknat SOLAS, däribland Sverige, enligt konventionen har en skyldighet att, under de villkor som artikeln stadgar, publicera sailing directions.

Som tidigare nämnts har detta uppfyllts bl.a. genom tillhandahållandet av publikationen Svensk Lots.

Sjöfartsverket ska enligt sin instruktion (2007:1161) svara för:

- sjögeografisk information inom Sjöfartsverkets ansvarsområde(sjökartläggning)

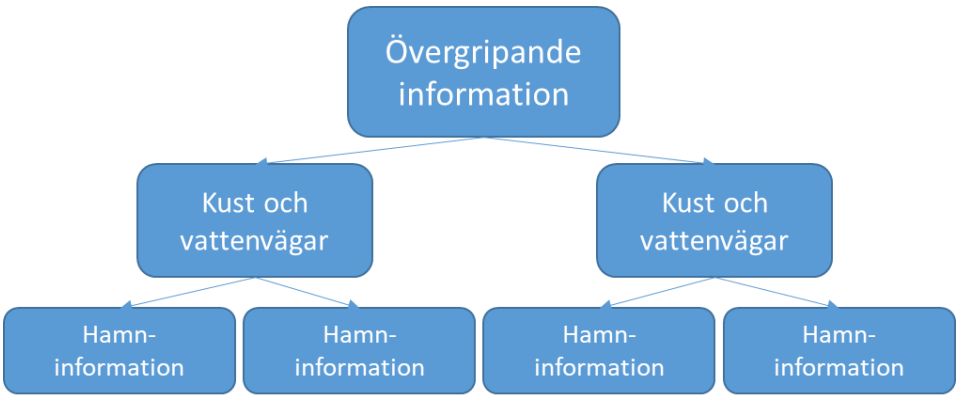
- samordning av sjögeografisk information i Sverige
- redovisning och dokumentation av Sveriges gränser till havs samt skötsel och tillsyn av dessa gränsers utmärkning.

Sjöfartsverkets bedömning är att Sveriges förpliktelser uppfylls genom tjänsten ”Underrättelse för Sjöfarare” (UFS A) samt de lotssidor som finns att hitta på Sjöfartsverkets hemsidor, www.sjofartsverket.se, men det finns en förbättringspotential i detta.

3.2 Analys av IHO:s M3

IHO:s publikation M3 är en sammanställning av ett antal resolutioner enligt resolution 13/1932 (Q3.1). Denna sammanställning av resolutioner bygger upp M3 till det dokument som beskriver hur hydrografiska tjänster och standarder bör eller skall byggas upp om de inte finns beskriva i någon särskild annan IHO-standard. I kapitel 2.4 Publications beskrivs vad som ska publiceras i nautiska beskrivningar och i vissa fall även hur. Under kapitel 2.4 beskrivs generell information som IHO-publikationer, distanstabeller, radiosignaler, tidvattenstabeller och seglingsbeskrivningar, men man tar också upp mer specifik information såsom t. ex. hur digital information skall förhålla sig till tryckt version. Det som är intressant och relevant under kapitel 2.4.2 är att IHO beskriver att nautiska publikationer kan beskrivas i två former, dels en fristående pappersversion men också en digital version av pappersformatet. Har man tagit fram en digital version av nautiska beskrivningar som är kompatibla med en ECDIS så måste man inte ha något av de två förstnämnda formaten. Redan 2002, då denna resolution fastställdes, skrev man ”*Note: Data Specifications for NP3 have yet to be finalised and therefore are not specifically referred to in this document.”*

Kapitel 2.4.6 innehåller information om Seglingsbeskrivningar (Sailing directions) i nivåer och är strukturerad så att generell information om kust och stat visas övergripande. På nästa nivå beskrivs att information om angöringen skall visas och på den tredje nivån skall eller bör information om hamnen och hamninformation beskrivas.



Då M3 är en resolution som många kuststater, med olika förutsättningar, skall godkänna så är det få tvingande punkter som beskrivs. Ett ytterst litet antal beskrivningar formuleras som ”must” eller ”strongly recommended” och de flesta formuleras istället som ”would” eller ”should”. Detta innebär att respektive kuststat har möjlighet att avgöra vilken information som är relevant att ha med i sina seglingsbeskrivningar.

Vid en analys av vilken data (information) som bör finnas i en seglingsbeskrivning i IHO:s M3 framgår att man bör göra en noggrann genomgång av informationen på respektive nivå, eftersom varje informationsdel är vag och behöver innehålla flera datadelar för att omfatta informationen som M3 tar upp. Ett exempel på detta är ”Ice conditions” under ”Waterways and coast” som med största sannolikhet måste innehålla flera datadelar för att kunna bygga strukturerad information. Struktureras inte informationen på detta sätt så innebär det att beskrivningar måste göras i fritext. Fritextinformation innebär att informationen kommer att visas för befälhavaren på olika sätt i olika geografiska områden beroende på vem som registrerat informationen.

En mycket viktig del som beskrivs i M3 är att varje informationsdel som visas också ska omfatta när informationen registrerades eller verifierades. Detta för att befälhavaren skall kunna avgöra huruvida informationen är tillförlitlig eller inte.

3.2.1 Övergripande information

I delen som handlar om övergripande information skall det finnas information om landet, i detta fall Sverige. I avsnittet ska det finnas allmän information om navigation och regler, miljöförhållanden, kust och genomfart, rutter och beskrivningar av geografiska områden.

Exempel på information som ska finnas är:

Allmän information om speciella tillstånd såsom t. ex. is och isbrytarservice, stora ansamlingar av tång m.m. Information om det finns signalsystem med bojar och sändare som inte följer IALAS riktlinjer samt information om övriga nationella regler som befälhavaren måste ha vetskap om innan inträde på nationellt vatten. I denna del bör också finnas information om förbifarter, trafikseparering, lotsning och lotsområden. Mer detaljerad information om lotsning ska visas i nästa del ”Kust och vattenvägar”.

Det bör också finnas mer detaljerad information som visar aktuella regelverk, listor över begränsade områden och andra delar som inte passar in i den normala vyn (texten). Förmodligen lägger man detta i en egen del i ett system och låter det vara sökbart eller uppdelat med hjälp av menyer.

I M3 står det i många fall att information skall visas i text eller i listor. I ett system där man ofta använder sig av kartor och sökfunktioner bör detta kunna ersätta listor och löptexter, då dessa blir överflödiga.

3.2.2 Kust och vattenvägar

Denna del beskriver i övergripande ordalag förhållanden när man har närmat sig kusten och skall stäva från öppet vatten mot hamn. Här hittar man information som återfinns inom respektive lotsområde och handlar om mer lokala fenomen som t. ex. lokala isförhållanden, fiskeaktiviteter, regler och lotsinformation. Här finns också information som kan påverka inseglingen såsom t. ex. djupinformation, rutter, tidvatten och strömmar, lokal dimma, anvisningar för vattenvägar till hamn, ankringsplatser m.m.

3.2.3 Hamninformation

Under hamninformation finns det information som också återfinns i tidigare beskrivna perspektiv. Skillnaden är att informationen som ska beskrivas på denna nivå är ur ett lokalt hamnperspektiv och därmed också mer detaljerat. Utöver att informationen ska innehålla uppgifter om hamnen och hamnledningen ska det finnas information om t. ex. vattendensitet/salinitet, väderförhållanden, regler, kontaktuppgifter till hamn och service, hamnbassänger och kajer.

Saknas information som M3 beskriver bör finnas, så skall det istället finnas information om att detta inte finns. Icke verifierad information skall inte heller finnas med i seglingsbeskrivningen.

3.2.4 Summering

I M3 rekommenderas att seglingsbeskrivningarna bör innehålla sådan information som är av betydelse för sjöfarare och inte finns beskriven i någon annan publikation. Den säger också att seglingsbeskrivningen skall vara så

enkel och tydlig som möjligt för att minimera den tidsjöfarare måste spendera på att läsa informationen. Sammanfattningsvis innebär det att seglingsbeskrivningen inte ska vara en beskrivning av sjökorten.

Seglingsbeskrivningarna i M3 utgår från sjöfararens vy där man anlöper utifrån öppet hav till kusten och i slutet av resan lägger till i hamnen. Informationen som presenteras för sjöfararen (eller annan användare) bör således på ett enkelt sätt kunna presenteras utifrån behoven som följer fartygets resa från öppet hav intill kaj med detaljeringsgrad som följer resan, d.v.s. från övergripande till detaljerad.

4 Förslag till NTI-tjänst för Sailing Directions

IMO:s SOLAS kapitel 5 hänvisar till IHO och där har man i sin tur arbetat fram resolutionen M3 för att beskriva hur en kuststat ska tillhandahålla seglingsbeskrivningar till hjälp för fartyg som ska angöra hamn. IHO har, som beskrivits tidigare i denna rapport, arbetat fram en utökad ersättning till standarden S-57 som heter S-100 och är en ny universell hydrografisk datamodell som bl. a. täcker de områden som också innefattar seglingsbeskrivningar. I nuläget har man fastslagit ett antal standarder där de flesta är i version 1.0. Detta innebär dock inte att de är färdiga för praktisk användning men de ändringar i standarderna som kommer att genomföras antas vara av mindre karaktär vilket innebär att om ett system börjar utvecklas nu så kommer ändringar kunna hanteras inom ramen för utveckling och sedermera även inom kommande förvaltning.

Detta förslag bygger på, med utgångspunkt från IHO:s M3, de standarder och datamodeller som beskrivs i S-100.

4.1 Roller och ansvar för samordnad Nautisk Tilläggsinformation

Utifrån IHO:s M3 bör seglingsbeskrivningar delas in utifrån resans perspektiv. Den första delen innehåller generell information om Sverige och dess kustlinje med övergripande information. Nästa del i beskrivningen handlar om mer specifik information om kustavsnitten och dess vattenvägar för att i den tredje och mer (geografiskt) detaljerade nivån handla om hamninformation.

Denna indelning av information finns det i Sverige inte någon enskild organisation eller myndighet som äger eller har möjlighet att ansvara för. För Sveriges del är Sjöfartsverket utpekat att ansvara för Sjögeografisk information. Den sjögeografiska avdelningen är då således både praktiskt och juridiskt lämpad för att hantera ansvaret med att hålla ihop seglingsbeskrivningarna. För de delar som behandlar kustinformation och vattenvägar bör Sjögeografi ta hjälp av eller delegera ansvaret till de olika lotsområden som redan idag beskriver sådan information. Den befintliga informationen kan behöva kompletteras och hanteras på annat sätt än idag. Detta beroende på vad ett eventuellt projekt för att ta fram en kravspecifikation kommer till för slutsats.

Utifrån IHO:s M3 ska seglingsbeskrivningarna också beskriva hamninformation. Avdelningen Sjögeografi på Sjöfartsverket bör också ansvara för delen som beskriver hamninformation även om respektive hamnmyndighet bör ansvara för sin egen information. Utöver information som återfinns i sjökorten så är det respektive hamnmyndighet som äger och ansvarar för sin information.

Då det hos de flesta hamnarna ser ut att finnas ett behov av att sprida information till fartygen och dess rederier som är eller kan vara möjliga kunder till hamnen så har många hamnar sådan information på sina hemsidor. Det finns dock inte hos alla hamnar och den information som finns är av olika karaktär med olika struktur och kvalitet.

För alla hamnar bör det ur marknadssynpunkt vara viktigt att synas så att de inte går miste om några nya affärer. Trots att de olika hamnarna med sina hamnmyndigheter är en del av Sverige så är det inte självklart för dem att leverera information till en nationell seglingsbeskrivning. Det finns dock en kungörelse om införande av informationsdelning som bör vara gällande idag[5], men detta bör i första hand regleras genom överenskommelser.

4.2 Identifiering av informationsägarskap

Det övergripande ansvaret för Sveriges seglingsbeskrivning ligger hos Sjöfartsverket och det Hydrografiska kontoret d.v.s. avdelningen Sjögeografi.

Respektive lotsområde skall tillhandahålla och säkerställa information om den delen som beskriver vattenvägar och kust med ruttinformation. Ägarskapet för informationen ska ligga hos respektive lotsområde som tar hjälp av Sjögeografi för rimlighetsbedömning av registrerad information/data.

Hamninformation kan inte tillhandahållas eller säkerställas av Sjöfartsverket då både information och ägarskap återfinns hos respektive hamnmyndighet. Ur ett juridiskt och systemperspektiv kan och bör Sjöfartsverket endast utföra kontroller av rimlighet i data som publiceras eller tillhandahålls av tredje part.

4.3 Insamling och verifiering av data samt distribution

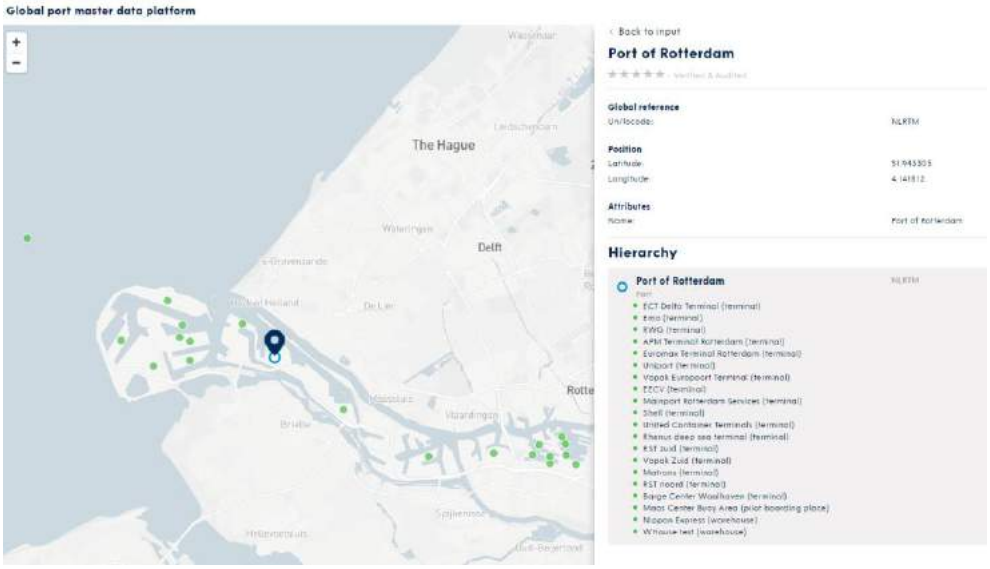
I M3 rekommenderas det att publicerad information bör revideras minst en gång varje år. I ett digitalt system bör det finnas en funktion som påminner informationsägaren om att gå igenom de delar som denne ansvarar för.

För att effektivt kunna säkerställa att data samlas in och registreras bör gränssnitt i ett digitalt system utformas utifrån respektive roll hos den ansvarige organisationen med funktioner som är anpassade utifrån typen av data med t. ex. påminnelser och enkelhet eller hjälpmedel vid ”sällananvändning”.

Övergripande information bör hanteras av en van redaktör för respektive område. Information om ”Kust och vattenvägar” bör ha en ansvarig person hos respektive lotsområde som hanterar information men vid behov tar hjälp av organisation hos avdelning Sjögeografi som ansvarar för systemet.

[5] https://www.riksdagen.se/sv/dokument-lagar/dokument/_sfs-1935-47

För hamninformation bör det tas i beaktande att hamnmyndigheten i många fall skulle kunna leja bort dessa uppgifter till en extern part såsom en agent eller IT-leverantör. Detta tillsammans med att de är ”sällananvändare” ökar behovet av ett intuitivt och lättanvänt system. I ett projekt där Rotterdams hamn har tagit fram ett testsystem (Proof of Concept, PoC) har man baserat verktyget på ett kartprogram som skulle kunna vara till hjälp för denna uppgift. Bygger man ett system för detta utifrån PoC:en kan man kanske köpa in och använda det eller så nyttjar man resultaten från PoC:en för att sedan bygga ett hamnsystem eller verktyg för denna uppgift. Detta system skall sedan kopplas till den databas där all seglingsinformation lagras. Webbadressen till en testversion av systemet är: https://portmasterdata.com/home



Verifiering av information

Redaktör, AI eller smart programmering? För att undvika höga administrationskostnader vid verifiering av registrerad data så bör gränssnittet programmeras på ett intelligent sätt så att man undviker att registrera orimliga värden.

Till en början bör man i kravhanteringen försöka hitta värden som kan innehålla numeriska värden och använda intervaller för att se rimligheten. Vid programmeringen finns det ofta möjlighet att addera inmatningshjälp i form av t. ex. rullgardinsmenyer med val så att samma text kan väljas.

Det som är svårare med intelligent ”vanlig” kod inom programmering är att verifiera löpande text så den inte innehåller data som inte är relevant. Man kan ibland se utfyllnadstext av slaget ”Lorem Ipsum…” vilket används för att kontrollera designdelar vid utveckling. Skall man skapa en funktion som

granskar att texten är relevant med hjälp av Artificiell Intelligens blir det förmodligen dyrare att utveckla detta jämfört med att låta en redaktör granska inmatad text över tid.

Förslaget är att lägga extra vikt på kravhantering, inmatningskontroller och sätta upp intervaller som högsta respektive lägsta värden för fält med siffror och låta fritext granskas av en redaktör.

Möjliga digitala distributionssätt

Beroende på mottagare och deras roll samt utrustning finns flera sätt att distribuera seglingsbeskrivningar. På ett fartyg finns möjligheter att använda flera verktyg för planering av ett anlöp. Ett ECDIS för att navigera och planera rutter, dator för att söka information på bl. a. digitala prenumerationer på Admiraltys Sailing Directions och förmodligen även en Android-platta eller Ipad som komplement. Redaren och mäklaren använder dator/plattor/mobiltelefon och i vissa fall har de också kanske byggt egna proprietära system eller så prenumererar de på Admiraltys digitala utgåva av Sailing Directions.

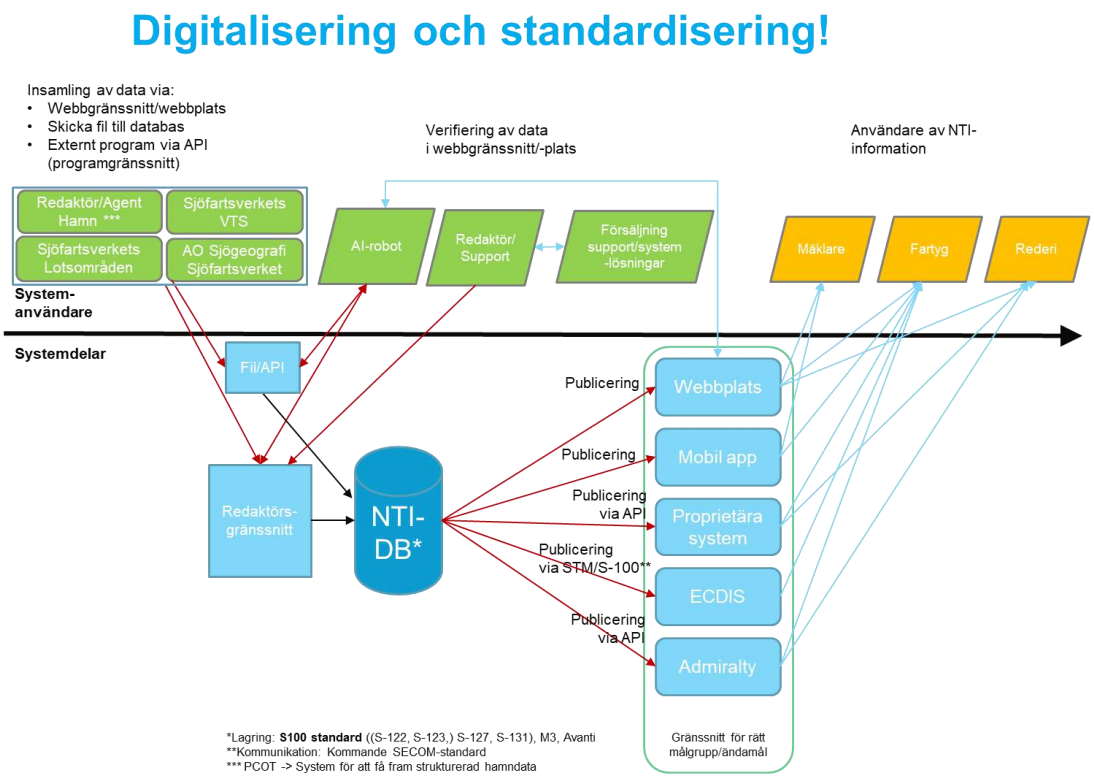
För att få en översikt över vilka möjliga distributionssätt som kan användas av olika typer av användare finns detta samlat i nedanstående tabell.

Använder/används av	**Webbplats**	**Mobil app**	**Proprietärt system**	**ECDIS**	**Admiralty**
Fartyg	X	X	X	X	X
Rederi	X		X		X
Mäklare	X	X			X

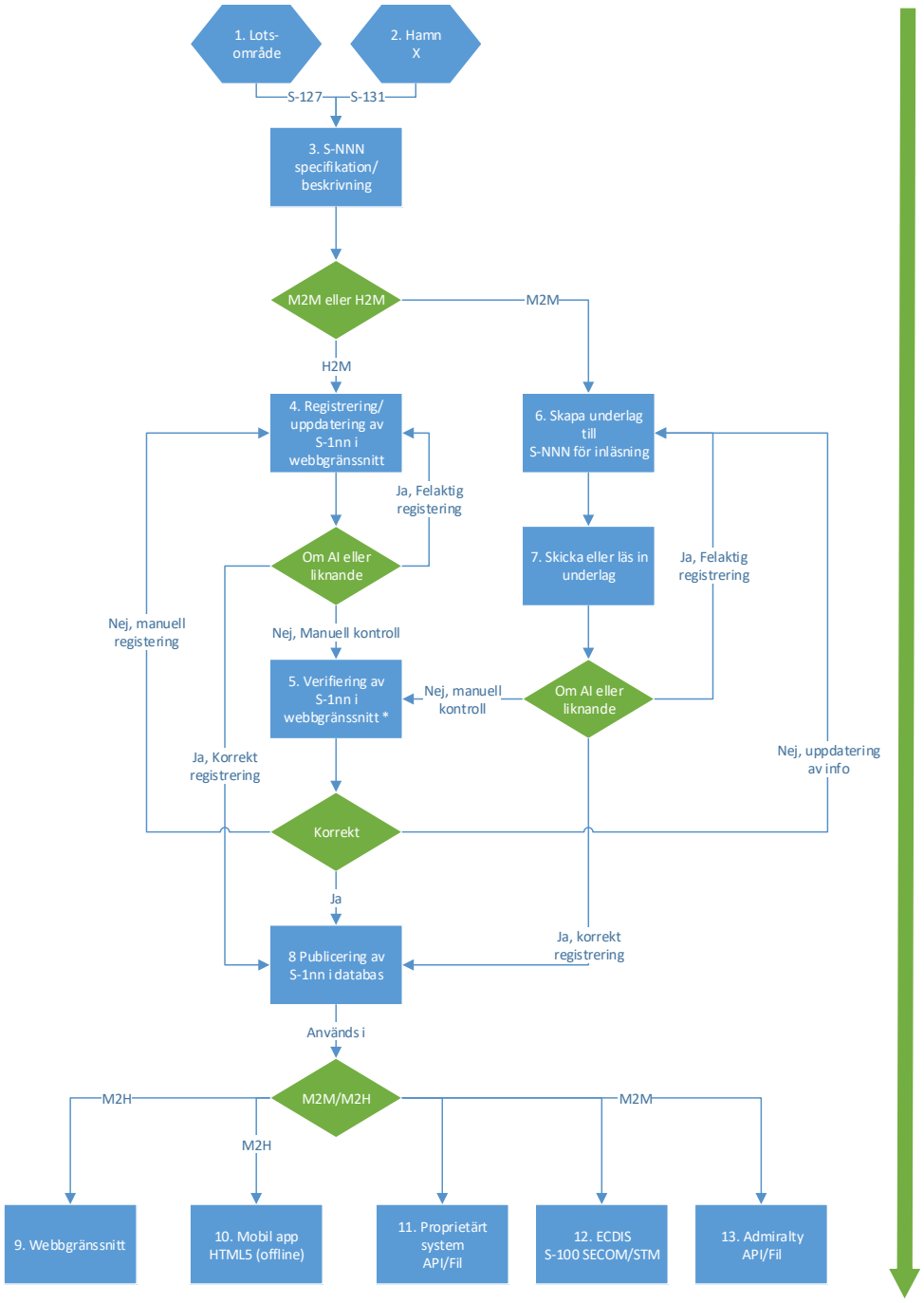
4.4 Schematisk systemlösning

En framtida systemlösning för NTI/Sailing Directions bör byggas utifrån att man skapar ett datalager som bygger på S100-standarder där informationsägare registrerar informationen via antingen egna lösningar som har kopplingar till databasen med API:er eller webbgränssnitt. Beroende på hur informationen ska användas eller vad man har för förutsättningar så bygger man lösningar för rollen som ska använda informationen. I figuren nedan så visas de olika användarrollerna ovan det vågräta svarta strecket och gränssnitten som de använder för att konsumera informationen (eller att visa informationen) visas under strecket. Ett exempel är en redaktör som går in i ett webbaserat system (gränssnitt) för att registrera information. Informationen lagras i databasen genom en (API-) koppling mellan ett administrationsgränssnitt och databas. Informationen används sedan på ett fartyg i sin

ECDIS som hämtar informationen från databasen via en annan (API-) koppling till ECDIS:en där informationen visas utifrån ECDIS-leverantörens gränssnitt för bryggpersonalen.



I nedanstående processbild förklaras hur informationen registreras fram till att den konsumeras av användaren. I denna visas vilka val som kan göras beroende på vilka förutsättningar som finns hos respektive användargrupp/roll. Begreppet S-nnn betyder att olika S100-standarder kan användas i samma process.

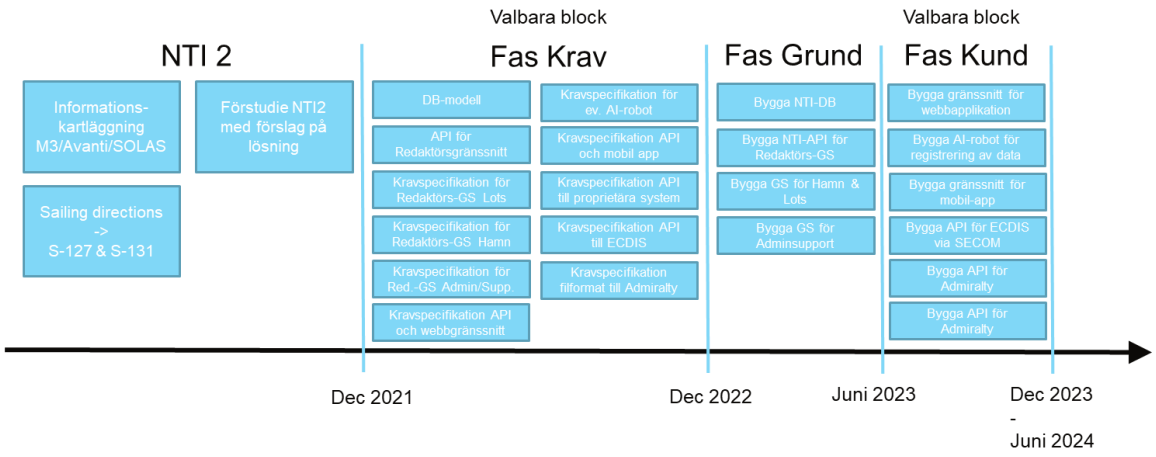


* Redaktör

4.5 Möjligt tidsperspektiv

Med den arkitektoniska utgångspunkten att systemet skall vara flexibelt både utifrån ett tekniskt perspektiv men även utifrån olika affärsmodeller så

skapar man också möjligheten att tidsperspektivet blir flexibelt. I det läget finns möjlighet att anpassa systemets uppbyggnad utifrån vilka delar som ger mest nytta eller hur man löser finansiering av uppbyggnaden. Det man inte kan rucka på är att börja med kravställningen av datamodellen som leder till databasen som är grunden i systemet.

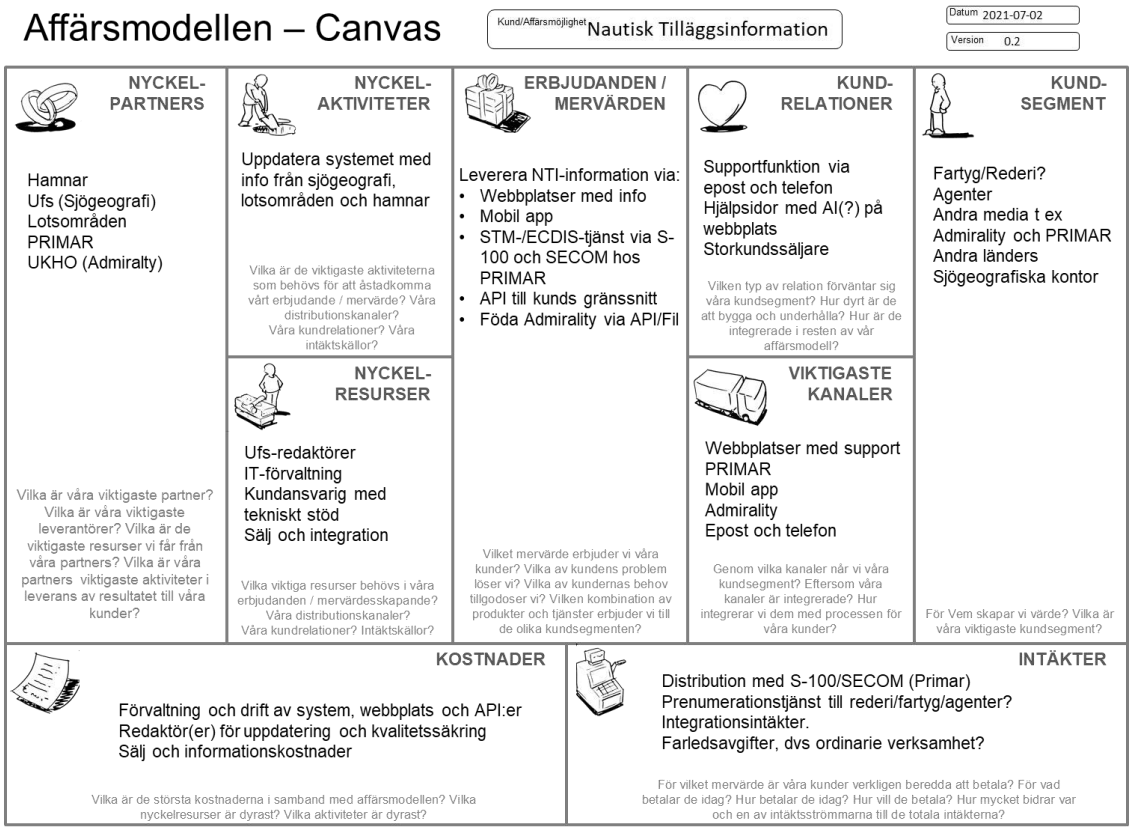


De olika delarna i fasen Krav blir då valbara förutom den ruta där det står DB-modell som leder till rutan Bygga NTI-DB i fasen Grund. Den naturliga fortsättningen blir förmodligen att gå vidare till att bygga API och gränssnitt för Redaktörer. Beroende på förutsättningar och behov väljer man sedan användargränssnitt utifrån de användare som har störst behov eller vilken finansiering som finns.

5 Affärsmodell och driftansvar

5.1 Business Model Canvas

För att beskriva hur affärsmodellen kan se ut så har vi använt oss av en modell som kallas Business Model Canvas (BMC). Denna har sedan ett antal år blivit vanlig att använda inom både privata och offentliga verksamheter för att den på ett enkelt sätt visualiserar vilka aktiviteter som utförs, vilka som är nyckelpartners och resurser, vad erbjudandet (tjänsten) är, vilka som är kunder/användare och hur man kommunicerar med dem, men också vilka kostnader och intäkter som kan förväntas i stort. Normalt så är steget efter en BMC att man arbetar vidare med en modell som kallas för Value Proposition Design (VPD) som är ett stöd för att beskriva hur tjänsten kan fungera. Med NTI och seglingsbeskrivningar är det IHO:s resolution M3 som beskriver vad tjänsten skall innehålla (med egna tolkningar och förutsättningar), därför behövs det inte tas fram VPD.



Sverige som kuststat har ratificerat (SOLAS och) M3, vilket innebär att Sjöfartsverket, där det hydrografiska kontoret hör hemma, ska uppfylla de internationella överenskommelserna. Dessa finansieras genom Sjöfartsverkets

ordinarie verksamhet. Under förstudien har vi funnit att kuststater i vår omvärld har utmaningar med seglingsbeskrivningar och flera av dem är intresserade av vad vi kommer fram till eftersom de inte har någon lösning för att digitalt dela seglingsbeskrivningar. Detta innebär att det finns möjlighet att undersöka om det antingen finns samarbetsmöjligheter där flera aktörer kan dela på utvecklingskostnaderna.

5.2 Investering i grundsystem och driftansvar

NTI-systemet bör byggas utifrån principerna om att vara så flexibel, användarvänlig och kostnadseffektiv som möjligt. Detta innebär att man bör separera delar från varandra, t. ex. en databas som bygger på standarderna i S-100, en separat del (som kan beskrivas som gränssnitt, program eller webbgränssnitt) för administration och till en början ett gemensamt webbgränssnitt för både webb och mobila applikationer utifrån strategi ”Mobile First” med HTML5 för både mobil användning i telefon eller surfplatta samt webbläsare på datorer. De olika delarna bör sedan anslutas mot databasen med separata API:er, med eller utan ett integrationssystem som t. ex. Microsoft Biztalk eller Mulesofts ”Mule”.

Eventuellt skulle den PoC, programtestet som är byggt av Rotterdams hamn m. fl., kunna användas för registrering av hamnuppgifter. Möjligheten att använda denna lösning behöver undersökas mer. . Alternativt så bygger man in funktionaliteten i ett gemensamt gränssnitt för registrering av hamnuppgifter.

Utöver att NTI-systemet blir flexibelt så skapar man också möjligheter att härleda kostnader och intäkter till respektive gränssnitt. Detta blir påtagligt vid de tillfällen som (förhoppningsvis) kopplingar kommer att göras mot rederiers proprietära (egna och företagsunika) system, kopplingar mot t. ex. PRIMAR för distribution till fartygens ECDIS:ar och till Admiralty och deras Pilot books. Utvecklingskostnader till dessa kanaler kommer inte att påverka de övriga delarna i systemet. Det går också att härleda kommande intäkter från dessa till de kostnader som uppstår.

Det kan finnas möjlighet att ta betalt för seglingsbeskrivningar även i en allmän grundversion. Utvecklingen av administratörsgränssnitt, databas och grundläggande användargränssnitt i html-miljö måste dock finansieras genom ordinarie verksamhet. De övriga gränssnitten som blir mer eller mindre unika eller anpassade finns det också möjlighet att ta separat betalt för.

Drift och förvaltning av grundsystem ansvarar Sjöfartsverket förmodligen för då vi har åtagit oss att följa resolutionen.

5.3 Externa informationsägare

Som beskrivits tidigare i denna rapport så kommer en del av informationen från tredje part och det är hamnarna med sin hamninformation. Sjöfartsverket har svårt att tvinga informationsägarna till samarbete. De flesta informationsägare kommer med största sannolikhet från början att se att arbetsinsatsen inte kommer att uppgå till den nytta (värde) som det färdiga systemet kommer att erbjuda. Nyttan uppstår i form av att säkerheten för fartygen ökar ytterligare, antalet manuella kontakter från nya anlöpande fartyg minskar och möjligheter till nya kunder och affärer. Incitamenten för hamnar att finnas med i NTI-systemet kommer förmodligen främst vara att man måste finnas med om ens konkurrenter finns där.

Även om deltagandet från hamnarna sida inte är tvingande så måste det dock skrivas avtal som reglerar rättigheter och skyldigheter. Skall informationsägaren få tillgång att dela sin information i NTI-systemet så måste vi som systemägare kunna ställa krav på informationsägarna så ansvaret för system och information blir klargjort.

5.4 Distribution till externa användarsystem

Då systemet i grunden byggs utifrån kraven i IHO:s M3 (på vad seglingsbeskrivningar är) och lagras i en databas som bygger på standarder i S-100, kommer det finnas möjlighet att på ett standardiserat sätt distribuera information till andra system än de gränssnitt eller distributionssätt som beskrivs i denna rapport. Detta öppnar upp för att kunna distribuera och ta betalt för utvecklingskostnaden vid integration och datadistributionen eftersom Sjöfartsverkets standardlösning bör vara ett webbgränssnitt eller en prenumerationslösning som alla kan ta del av.

5.4.1 ECDIS-system via en distributionstjänst

På fartygen finns ECDIS:ar från olika tillverkare. Dessa fungerar och ser ut på lite olika vis, men löser i grunden samma uppgifter. I framtiden så kommer de att kunna hantera S-100-format i olika standarder och vill fartygen komma åt NTI-informationen så kan NTI-systemet kommunicera via SECOM och/eller en distributionskanal som PRIMAR på liknande sätt som det görs med standarden S-57. Genom dessa distributioner går det att ta betalt för distributionen via prenumeration.

5.4.2 Admiralty

UKHO (United Kingdom Hydrographical Office) ger ut seglingsbeskrivningar i det som de kallar för Admiralty Sailing Directions (Pilot books) i bokform (76 volymer), men också som en e-publikation. Denna information har man tidigare skickat manuellt från Sjöfartsverkets hydrografiska kontor

(fram till 1997). Numer skickar man uppdateringar då man upptäcker rena felaktigheter, också då manuellt.

Som leverantör av information för seglingsbeskrivningar skulle man möjligen kunna avtala om royalties på försäljningen av seglingsbeskrivningarna i likhet med vad som idag sker gällande sjökortsinformation.

Dessa seglingsbeskrivningar kan också skickas i dataformat från ett befintligt system med hjälp av ett s. k. DTK (Developers Toolkit) vilket innebär att man från ett nytt NTI-system kan bygga in funktioner för kommunikation med UKHO:s system som ligger till grund för deras utgivning av Pilot books (Sailing Directions). Eftersom dessa Pilot books enligt uppskattningar från Sjöfartsverkets nautiker återfinns på över 90% av fartygen som trafikerar Sverige bör det finnas intresse att säkerställa uppdateringen av denna information och få royalties från UKHO.

5.5 Sammanfattning affärslösning

För att få en bild över vilka delar som ryms inom denna NTI-lösning har vi försökt samla detta i nedanstående tabell. I tabellen beskrivs kort vilken tjänst som avses och vem den riktar sig till, antingen som leverantör av information eller användare av densamma. I flera fall har vi inte möjlighet att ta betalt för användningen av tjänsten, då den ska finansieras av befintliga intäktskällor, men det finns flera tjänster där vi kan ta betalt. Hur den affärsmässiga uppgörelsen ser ut kan också skilja sig åt, vilket kortfattat beskrivs under rubriken Juridiskt. Övrig information kan beskriva att flera möjliga lösningar kan vara möjliga.

Tjänst	**Vem** riktar sig tjänsten till?	**Hur** tar vi betalt för tjänsten?	**Finansieringslösning**	**Juridiskt** Hur vi distribuerar tjänsten	**Övrigt**
Databas/lagring	Alla	Respektive tjänst enligt nedan	Ordinarie budget	Enligt nedan	Kan eventuellt delfinansieras eller säljas till andra stater
Registrering av Kuststatsinformation (administr.)	Internt SjöV; Sjögeografi, Lotsar	Befintlig förvaltning	Ordinarie budget	Webbplats internt	

Registrera hamninformation via webbsida	Hamnar	Gratis	Ordinarie budget	Avtal	
Registrera hamninformation via integration	Hamnar	Integration och prenumeration	Externfinansierat	Avtal	
Webbtjänst/mobil app	Alla	Gratis	Ordinarie budget	Fritt	
Proprietära system	Rederier	Integration och prenumeration	Externfinansierat	Avtal	Försäljningsansvarig på Sjögeo
ECDIS	Fartyg (Rederier)	Prenumeration via PRIMAR	Externfinansierat	Avgifter till SjöV	
Admiralty	Alla	Prenumeration via Admiralty	Externfinansierat	Royalties	

Utöver de möjligheter som beskrivs i tabellen ovan finns också möjligheten att tillsammans med våra grannländer dela på utvecklingskostnaden för de grundläggande funktionerna.

6 Rekommendationer för fortsatt arbete

Sjöfartsverket är ansvarig för att tillhandahålla Seglingsbeskrivningar utifrån de tre perspektiven Översikt angöring, kust- samt hamninformation.

Nästa steg efter denna förstudierapport är att i ett projekt utgå från IHO:s M3 för att fastslå vilken information som är viktig när man som skeppare skall angöra en hamn i Sverige. Till detta vidareutvecklas den befintliga kravspecifikationen med bilagor från 2016. Detta arbete behöver bl. a. kompletteras utifrån M3 och med fler hamnar. Systemet byggs för olika funktioner (databas, redaktör/support, användargränssnitt för olika behov) med utgångspunkt från ”S-100”-standarder även om de befinner sig i version 1.0 eller tidigare.

Grunderna finansieras genom befintliga intäkter från farledsavgifter. De olika användargränssnitten bör i flera fall kunna finansieras genom kundintäkter (licenser, utvecklingskostnader och prenumerationer).

Utvecklingen av systemet kan ske etappvis utifrån behov.

Önskvärt kan vara om Sjöfartsverket kan påverka ECDIS-tillverkare att utveckla NTI-systemet så att relevant information visas utifrån den position man befinner sig på, i planering eller verklighet, för att undvika informationsöverfyllnad.

7 Bilagor

7.1 Beskrivning av aktörer och dess roller: IHO, IMO, Sverige som medlemsstat, SjöV, Transportstyrelsen och hamnar

IMO

International Maritime Organisation, IMO (Internationella Sjöfartsorganisationen) är en internationell organisation inom sjöfarten som grundades efter att IMO-konventionen från 1948 trädde i kraft 1958. Organisationen, som har sitt högkvarter i London, höll formellt sitt första sammanträde året därpå och är ett fackorgan inom Förenta Nationerna (FN).

IMO ska utgöra ett forum för internationellt samarbete kring regler och praxis som styr säkerheten till sjöss. Organisationen har antagit en rad konventioner och rekommendationer om sjösäkerhet, förhindrande av föroreningar från fartyg, farliga lasttransporter samt ansvars- och skadeståndsfrågor.

Inom föregångaren till IMO tog man fram den första versionen av konventionen SOLAS (Safety of Life At Sea) år 1914, efter katastrofen med Titanic. Denna konvention hanterar och beskriver säkerhet runt handelsfartyg.

Sverige är medlemsstat i IMO och Transportstyrelsen har regeringens uppdrag att representera Sverige i IMO.

IHO

IHO, International Hydrographic Organization startade sin verksamhet i början på 1920-talet. IHO är medlemsstatsorganisation för kuststater som ansvarar för standarder för sjökortprodukter. IMO refererar till IHO-standarderna i allt vad gäller sjökortsprodukter. IHO koordinerar också aktiviteter hos medlemsstaterna genom regionala kommissioner. Antalet medlemsstater är knappt 100 i slutet av 2021. Sverige är medlemsstat i IHO och Sjöfartsverket har regeringens uppdrag att representera Sverige i IHO.

Sjöfartsverket

Av 2 § förordning (2007:1161) med instruktion för Sjöfartsverket följer att Sjöfartsverkets huvuduppgifter bl.a. är att svara för sjögeografisk information inom Sjöfartsverkets ansvarsområde (sjökartläggning) samt svara för samordning av sjögeografisk information inom Sverige.

Av 4 § samma förordning följer att Sjöfartsverket särskilt ska biträda regeringen med beredningen av ärenden i det internationella samarbetet inom Internationella hydrografiska organisationen (IHO).

Transportstyrelsen

Av 4 § förordning (2008:1300) med instruktion för Transportstyrelsen följer att Transportstyrelsen inom sitt ansvarsområde ska fullgöra uppgifter enligt EU-rättsakter och andra internationella överenskommelser.

Transportstyrelsen ska särskilt biträda regeringen med beredningen av ärenden i det internationella samarbetet inom Internationella sjöfartsorganisationen (IMO).

Hamnmyndigheter

I Sverige är de flesta allmänna hamnar ägda av kommuner genom kommunala bolag. Ungefär hälften av de allmänna hamnarna är helt kommunalt ägda medan resterande även har privata ägarintressen i varierande grad. Det finns också helt privatägda allmänna hamnar. Utöver de allmänna hamnarna finns det ett stort antal industrihamnar som i första hand är knutna till industriföretag. Begreppet hamnmyndighet har i Sverige ingen särskild rättslig innebörd, utan denna ledningsfunktion är en del av den kommunala förvaltningen eller det kommunala hamnbolaget.

Hamnars verksamhet styrs av flera EU-direktiv och andra förordningar, bl.a. lag (2006:1209) om hamnskydd, lag (1981:655) om vissa avgifter i allmän hamn och lag (2019:152) med kompletterande bestämmelser till EU:s hamntjänstförordning.

7.2 Admiralty – Sailing Directions

United Kingdom Hydrographic Office publicerar boken ”Admiralty Sailing Directions”, som fartygens befälhavare har ombord, till uppskattningsvis omkring 95% av alla fartyg. Upplägget i boken motsvarar vad som beskrivs i IHO:s M3 och innehåller 450 sidor exklusive innehållsförteckning och förkortningar för upplagan ”Baltic Pilot Volume 2” från 2018. Innehållet i boken är inte anpassat för en digital distributionskanal, men bör beaktas vid framtagandet av ett nytt (och digitalt) distributionssätt då den innehåller information som användarna/läsarna är vana att hantera.

7.3 Port Call Optimization Task Force och hamninformation

Organisationen ”International Taskforce for Port Call Optimization” (ITPCOT) arbetar utifrån ett hamnperspektiv för att standardisera hamndata. Drivande bakom organisationen står Rotterdams hamn och andra organisationer såsom UK Hydrographic Office (UKHO) och GS1, tillsammans med ett antal stora hamnar, rederier och industripartners. ITPCOT har tagit fram ett webbaserat Proof of Concept i ett projekt där även Göteborgs hamn varit involverat för att med ett grafiskt kartverktyg kartlägga och registrera data i

hamnområden och hamnbassänger. I nuläget ser det ut som att deras kommande lösning kommer att stödja registrering av information enligt standarden S-131.

7.4 Nautisk Tilläggsinformation i vår omvärld

Danmark

Den webbaserade ”Mariners' Routeing Guide Baltic Sea” publiceras av Baltic Sea Hydrographic Commission på webben och underhålls av Danish Hydrographic Office, som är del av den danska Geodatastyrelsen (Danish Geodata Agency, DGA). Innehållet i webbversionen motsvarar den nautiska informationen som anges i det tyska papperssjökort 2911 (INT1200) ”Mariners’ Routeing Guide Baltic Sea”, publicerat av Bundesamt für Seeschifffahrt und Hydrographie (BSH) och uppdateras rutinmässigt av BSH i ”Nachrichten für Seefahrer”, NFS (motsvarande svenska UFS).

Publikationen ”Mariners' Routeing Guide Baltic Sea” ersätter inte någon information i andra officiella nautiska publikationer eller sjökort utgivna av lämpliga nationella myndigheter eller dess officiella tjänster. Den innehåller allmän information som skulle kunna användas för planering av en sjöresa, t.ex. under ”Route Planning” upplyses om bl.a. fartygs ruttsystem, faror, medan man under ”Routeing” kan ta del av information om nationella regler och trafikseparerингssystem.

I kapitel ”General” sammanställs även en lista av nautiska publikationer på engelska, utgivna av andra länders relevanta myndigheter och lämpliga för Östersjön, se Tab.1.

Country	Notices to Mariners	Sailing Directions (and Supplements)	List of Lights	Other Nautical Publications
United Kingdom	Notices to Mariners (NtM)	Baltic Pilot Vol I, No. NP 18 Baltic Pilot Vol II, No. NP 19 Baltic Pilot Vol III, No. NP 20	Admiralty List of Lights Vol. C No. NP 76	Admiralty List of Radio Signals ALRS 1–6 No. NP 281–286
Denmark	Efterretninger for Søfarende Søkortrettelser (Danish Chart Corrections) (Vital elements of the Danish Chart Corrections are translated into English)	Navigation through Danish Waters		Behind the Nautical Chart
Estonia	Teadaanded Meremeestele / Notices to Mariners for Estonian Waters	Sailing Directions for Estonian Waters	List of Lights in Estonian Waters	Navigational Warnings
Finland	Tiedonantoja Merenkulkijoille/ Notices to Mariners		Finnish List of Lights	Vessel Traffic Services (VTS) Master guide's online
Germany	Nachrichten für Seefahrer (NfS) Annual enclosure to the Notices to Mariners			German Traffic Regulations for Navigable Maritime Waterways: Navigational Warnings (North) Navigational Warnings (East)

Tabell 1. Sammanställning av officiella nautiska publikationer för Östersjön. Källa: https://balticsearouteing.dk/text/

Andra uppgifter i webb-versionen av ”Mariners' Routeing Guide Baltic Sea” som är relevanta för planering eller genomförande av sjöresor är angivna i följande kapitel: Kap. 3, Miljöskydd; Kap.4 Naturliga förhållanden (vattennivå och ström, is, landhöjning); Kap.5. Information om is (praktiska råd och krav); Kap.6 Vessel Traffic Service (bl.a. VTS bevakningsområde och rapportering); Kap.7 Lotsservice (öppensjölotsning, lotsning i lotsområde); Kap.8 Maritim assistans; Kap.9 Maritim radioservice (inklusive MSI och väderprognos m.m.) samt Kap.10 Rapporteringssystem (bl. BELTREP, SOUNDREP m.m.) och Kap.11 Andra rapporter (ISPS och enligt EU dir. 2002/59/EC).

I Tabell 1 anges att Danmark publicerar nationella utgåvor av lotsböcker (Sailing Directions), så kallade ”Den danske Lods” på danska samt till en begränsad del, även på engelska. Dessa publikationer beskrivs nedan i detta kapitel.

Vem: Geodatastyrelsen

Vad: Danska Geodatastyrelsen publicerar ett antal nautiska publikationer, som kan köpas i tryckta utgåvor eller laddas ner gratis i digitala utgåvor från dess webbplats.

Hur: Följande publikationer är endast tillgängliga i tryck:

- Den danske Lots II
- Den färöiske Lots

- Hamninformation för Färöarna,

Enligt information från den danska Geodatastyrelsen, har myndigheten inte kunnat säkra resurser för att genomföra den omfattande översyn av "Den danske Lods" som krävs. Tyvärr finns det inga aktuella planer för en sådan revision av "Den danske Lods" och publikationen upphörde sedan 1990-tallet.

Nedan listade publikationer (Sailing Directions) kan laddas ner i digital version kostnadsfritt från Geodatastyrelens webbplats:

”Den danske Havnelods” på nätet (www.danskehavnelods.dk) innehåller uppdaterad information om 458 danska hamnar och 44 danska broar. Informationen om hamnarna i ”Den danske Havnelods” publiceras och underhålls av danska Geodatastyrelsen, som gör att den är en officiell nautisk publikation. Informationen i publikationen återspeglar den information som publikationens redaktion har fått om hamnarna över tid.

För varje hamn finns en text med information, hamnplaner och foto. Informationen om broarna innehåller text med angivna parametrar för specifik bro, såsom position med koordinater, segelfri höjd, segelfri bredd, utmärkning, information om ström, segling, kraftledning(ar) samt generella bestämmelser eller andra regler, gällande passage under bron och foto med brons vy. Det finns sidor med standardregler för brottsbekämpning i danska hamnar samt sidor med relevanta verkställande order angående navigering och lotsning i danska vatten. Websidan uppdateras varje onsdag kl. 1200. Efter uppdateringen införs alla korrigeringar, som har publicerats i den veckovisa "Sjökorts rättelser" in till Den danske Havnelods. För varje hamn finns information om när den senaste uppdateringen infördes.

”Den danske Lods, Generelle oplysninger” (allmän information) innehåller bakgrundsinformation, relevant för navigering i danska vatten. Syftet med denna utgåva är att göra det lättare för sjömän och andra användare att hitta uppdaterad och relevant information om navigering i danska vatten.

”Den färöiska Lods, bilaga 3” tillägget slutfördes den 21 maj 2004 och innehåller alla korrigeringar som gjorts sedan trycket av den färöiska lotsen. Tillägget har uppdaterats till och med ”Efterretninger for Søfarende” (EfS) (sv: UfS) nr 20 2004. För ytterligare korrigeringar (inklusive tillfälliga), hänvisas användarna till UfS.

”Den grönländske Havnelods” på nätet (www.gronlandskehavnelods.dk) innehåller uppdaterad information om 93 grönländska hamnar (städer, bosättningar och stationer). Informationen om hamnarna publiceras och underhålls av danska Geodatastyrelsen, som gör att den är en officiell nautisk publikation. Informationen i den publikationen återspeglar den information

som utgivaren har fått om hamnarna över tid. Websida uppdateras varje onsdag kl. 0800 Västgrönlands tid, dvs. kl. 1200 dansk tid. Efter uppdateringen införs alla korrigeringar, som har publicerats i den veckovisa "Sjökorts rättelser" in till ”Den grönländske Havnelods”. För varje hamn finns information om när den senaste uppdateringen infördes.

”Den grönländske Lods-Segelinstruktioner Västgrönland ” beskriver Grönlands västkust från Nunap Isua (Kap Farvel) till Kap Morris Jesup och har utarbetats på grundval av den information som finns tillgänglig för Geodatastyrelsen från undersökningsfartyg, statliga institutioner, handelsfartyg och kända personer och andra (källor). Denna utgåva har utarbetats, baserat på ”Den grönländske Lods I - Västgrönland, 1966”.

”Den grönländske Lods-Seglinginstruktioner Östgrönland” beskriver Grönlands östkust från Nunap Isua (Kap Farvel) till Kap Morris Jesup och har utarbetats på grundval av den information som finns tillgänglig för Geodatastyrelsen från undersökningsfartyg, statliga institutioner, handelsfartyg och kända personer och andra (källor). Denna utgåva har utarbetats, baserat på ”Den grönländske Lods, 2 del Östgrönland”.

”Den grönländske Lods, Generelle oplysninger om Grönland” (Allmän information om Grönland) innehåller information om ämnen och förhållanden, nödvändiga för kunskap om och i samband med navigering i Grönlands vatten. Angående segling (nautiska) instruktioner för Östgrönland eller Västgrönland, hänvisning görs till ”Den grönländske Lods-Seglinginstruktioner Östgrönland” respektive ”Den grönländske Lods-Segelinstruktioner Västgrönland”.

”Den grönländske Lods, Förklaringar till platsnamn”. Syftet med publiceringen av " Den grönländske Lods, Förklaringar till platsnamn" är dels att samla all information om de grönländska platsnamnen på ett ställe och dels att ge användare av nyligen publicerade västgrönländska kartor möjlighet att söka information om betydelsen av platsnamn. De nya kartorna använder ny grönländsk stavning i motsats till de äldre kartorna samt vissa publikationer, som använder gammal grönländsk stavning.

Publikationen har utarbetats på grundval av information om platsnamn i "Den grönländske piloten I, västra Grönland", "Den grönländske piloten, del 2, östra Grönland" och "Den grönländske hamnpiloten". Alla platsnamn har reviderats och uppdaterats av Oqaasileriffik - Språksekretariatet under Grönlands självstyre.

Publikationen innehåller en "översättning" till eller förklaring på danska av de grönländska platsnamnen, som anges med både ny och gammal grönländsk stavning.

https://gst.dk/soekort/nautiske-publikationer/information-om-de-nautiske-publikationer/

Följande Lotspublikationer är tillgängliga på engelska:

- Greenland Harbour Pilot- information about cities, settlements and stations;
- Greenland Pilot - General Information about Greenland;
- Greenland Pilot - Sailing Directions for West Greenland;
- Greenland Pilot - Sailing Directions for East Greenland;
- Greenland Pilot - Explanations of the placenames.

Planer eller pågående utvecklingsarbete:

Beträffande utvecklingsarbete eller planer för nya produkter/tjänster, anger Geodatastyrelsen att man är representerad vid IHO NIPWIG och deltar i dess möten, dock på grund av resurs- och kompetensbrist utan något större drivkraft. Nautiska publikationer ses inte längre som huvuduppgift, men snarare S-100 standarder diskuteras och bearbetas i NIPWIG, enligt Geodatastyrelsen.

DGA:s uppfattning är att nya S-100-standarder så småningom kommer att komplettera eller till och med ersätta de traditionella nautiska publikationerna. Data från nautiska publikationer måste integreras i dessa nya S-100-standarder. Detta kräver en strikt organisation av data och där finns ett behov av DGA att fördela resurser och förvärva kompetens i förhållande till S-100-standarderna.

DGA har genomfört en organisationsförändring där man inrättade ett team för att arbeta separat med de nya S-100-standarderna. För närvarande jobbar man på att utarbeta en huvudplan redo för detta arbete för år 2021. Förhoppningsvist skulle huvudplanen också att innehålla en plan för framtida arbete med data från nautiska publikationer.

Estland

Enligt uppgifter som är angivna i Tabell 2 nedan publicerar Estniska Sjöfartsverket nationella utgåvor av Lotsboken för estniska vattenområden.

Vem: I enlighet med direktiv Nr 55-VA från generaldirektören för Republiken Estlands Maritima Administration, dvs. Estniska Sjöfartsverket (Estonian Maritime Administration, EMA), ska Kartografiavdelningen inom Byrå (för) Hydrografi och Sjösäkerhetsanordningar utföra, bland annat, följande funktion:

"4.4.5 Compile and organise the publishing and distributing of navigational publications Notices to Mariners, Estonian Sailing Directions and Aids to Navigation in Estonian Waters;

4.4.5. Sammanställa och organisera publicering och distribution av navigationspublikationer, Underrättelser för Sjöfarande (UfS), estniska Lotsböcker och sjösäkerhetsanordningar i estniska vatten."

Vad: Estniska Lotsböcker är tillgängliga på estniska samt på engelska och kan laddas ned i PDF-format från EMAs (Estniska Sjöfartsverkets) webbsite https://veeteedeamet.ee/en/sailing-directions. Den Estniska Lotsboken är indelad i fyra områden med den femte delen bestående av bilaga enligt Tabell 2 nedan:

	Part 1: Gulf of Riga	
1.1	Sõrve poolsaar to Sääretüki lighthouse *(3.94 MB, PDF)*	Updated to 1st October 2020
1.2	Sääretüki lighthouse to Väinameri S pilot boarding place *(2.64 MB, PDF)*	Updated to 1st October 2020
1.3	Väinameri S pilot boarding place to Sorgu S buoy *(3.55 MB, PDF)*	**Updated to 1st November 2020**
1.4	Sorgu S buoy to Pärnu laht *(2.79 MB, PDF)*	**Updated to 1st November 2020**
	Part 2: Väinameri	
2.1	S part of Väinameri *(4.16 MB, PDF)*	Updated to 1st October 2020
2.2	N part of Väinameri *(3.23 MB, PDF)*	Updated to 1st October 2020
2.3	W part of Väinameri *(3.75 MB, PDF)*	**Updated to 1st November 2020**
	Part 3: Baltic Sea	
3.1	Sõrve poolsaar to Undva nina *(2.59 MB, PDF)*	**Updated to 1st November 2020**
3.2	Undva nina to Kõpu poolsaar *(2.59 MB, PDF)*	**Updated to 1st November 2020**
3.3	Kõpu poolsaar to Põõsaspea neem *(3.26 MB, PDF)*	Updated to 1st August 2020
	Part 4: Gulf of Finland	
4.1	Põõsaspea neem to Suurupi poolsaar *(3.18 MB, PDF)*	Updated to 1st September 2020
4.2	Suurupi poolsaar to Kaberneeme poolsaar *(6.73 MB, PDF)*	**Updated to 1st November 2020**
4.3	Kaberneeme poolsaar to Narva jõgi *(4.51 MB, PDF)*	**Updated to 1st November 2020**
	Appendix to Sailing Directions	
	Waypoint navigation *(178.37 KB, PDF)*	New release as of 1st June 2017
	GPX.zip *(13.16 KB, ZIP)*	New release as of 1st June 2017

GOFREP Master's Guide *(276.82 KB, PDF)*

Last updated: 30 October 2020

Tabell 2: Uppdelning av den Estniska Lotsboken Källa: https://veeteedeamet.ee/en/sailing-directions

Hur: EMA sammanställer nautisk tilläggsinformation digitalt i ett nytt format genom att all navigationsinformation sammanställs i tabeller. Till skillnad från tidigare långa beskrivande texter i Lotsboken, gör ändringen att det är lättare för användaren att hitta relevant information.

EMA konstaterar också i korrespondens som förts med Sjöfartsverket, att den tryckta beskrivande formen var svår att uppdatera och kostsam att sammanställa. Därför började man publicera Sailing Directions i denna nya tabellmall, tagen från Bundesamt für Seeschifffahrt und Hydrographie (BSH) i Tyskland enligt överenskommelse med dem.

Nautisk tilläggsinformation publiceras digitalt i fyra delar, som motsvarar geografiska regioner. Publikationen kan laddas ner gratis från https://veeteedeamet.ee/en/sailing-directions . EMA instruerar användare att skriva sidorna ut i A4-papperstorlek.

Lotsböcker uppdateras en gång i månaden i enlighet med ändringarna i Notice to Mariners, NtM.

Nautisk tilläggsinformation kompletteras i vissa fall med länkar till flygpanorama-vy på nätet, t.ex. s.2 i https://veeteedeamet.ee/sites/default/files/content-editors/SD_2.2.pdf med en länk till http://www.estonia360.ee/sadamad/.

Planer eller pågående utvecklingsarbete: För närvarande meddelar EMA inga planer på att ändra den webbaserade publikationen. Myndigheten kommer dock att följa rekommendationerna från IHO och S-100-produktspecifikationslösningen.

EMA skulle vara intresserad av att hålla kontakt med Sjöfartsverket angående eventuell lösning när man har fattat ett beslut.

Finland

Tabell 1 anges ingen information om att Finland publicerar nationella utgåvor av lotsböcker (Sailing Directions) varken på finska eller på engelska. Hydrografikontoret på det finska Transport- och kommunikationsverket, Traficom informerar att Finland inte har publicerat Sailing Directions alls, varken historiskt sett eller i dagsläget. Den information som finns tillgänglig för sjöfarare i Finland publiceras delvis i NtM och delvis i så kallat ”farledskort”.

Vem: Farledskort är en produkt som utfärdad av den finska Trafikledsverket. Den finska VTS:en är också en viktig dataleverantör för den information som farledskort samt andra nautiska publikationer vanligtvis innehåller.

Vad: Farledskort innehåller information om farleder och hamnar och är avsedda för sjömän. Publikationen utgör ett komplement till sjökort och andra nautiska publikationer. Farledskorten täcker kanaler/farleder till alla hamnar som hålls öppna under vintern, dvs. de flesta av de viktigaste sjötrafikstråken i Finland.

Hur: Ett farledskort innehåller fakta om farledens mått och navigationsförhållanden, trafikrekommendationer och begränsningar samt tillhandahållna trafiktjänster. Ritningar av farleden och hamnen är också tillgängliga men ritningarna är inte avsedda för navigationsanvändning. Dessa avbildar kanalernas orientering och utmärkning, farledsyta, säkra djupgående, kajplatser och andra platser som texten hänvisar till.

Farledskorten omfattar tre områden:

- Skärgårdshavet (Archipelago Sea), med t.ex. hamnar som: Mariehamn, Pori, Rauma eller Uusikaupunki, bland andra;
- Finska Viken (Gulf of Finland), med t.ex. följande hamnar: Hamina, Hanko, Helsinki eller Orregrund-Kotka, bland andra;
- Botniska Havet (Gulf of Bothnia), med t.ex. hamnar som: Kokkola, Kemi, Oulu, Tornio eller Raahe, bland andra.

Farledskort finns tillgängliga för att laddas ner gratis i digitala utgåvor (i PDF-format) på engelska från Trafikledsverkets websida https://vayla.fi/en/service-providers/merchant-shipping/navigating/fairway-cards

Planer eller pågående utvecklingsarbete: Informationen som farledskorten innehåller är nödvändig för sjöfarare och sjöfartens säkra navigering. De relevanta finska myndigheterna (Traficom och Trafikledsverket) upparbetar för närvarande en plan för de kommande åren som också omfattar samma aktuella fråga som i denna förstudie. I denna strategi måste man fatta beslut angående bl.a. finska Hydrografiska Myndighetens roll i framtiden för att tillhandahålla informationen som tillgängliggörs genom farledskort.

På sikt kommer informationen att tillhandahållas via S-100-produkter och det är viktigt att skapa processer för att samla in data för att kunna publicera detta i S-100-produkter. För tillfället är det inte klart om det ska göras av Traficom/Trafikledsverket eller någon annan myndighet för att få för att få relevanta krav uppfyllda.

Norge

Nautiska Publikationer utgivna av det norska Kartverket består av Etterretningar for Sjöfarare, EfS (svenska UfS), tidvattenstabeller för norska kusten och Svalbard samt den norska pilotguiden ”Den norske Los” (Sailing Directions- Den norske Lots) men även symboler och förkortningar i norska sjökort.

Vem: ”Den norske Los” är utfärdad och underhålls av det norska Kartverket.

Vad: ”Den norske Los” är en beskrivning av farbara vattenområden som täcker den norska kusten from den svenska gränsen i söder till den ryska gränsen vid Grense Jakobselv i norr och innehåller även beskrivningar för Svalbard och Jan Mayen. Publikationen är ett komplement till sjökorten och innehåller nautisk tilläggsinformation för olika farleder och kanaler men

är också en informationskälla med kartor, seglingsanvisningar för befälhavare, information om farvatten, hamnar, anlöpsanläggningar, ankarplatser, avstånd m.m. Det finns utöver detta även viktig meteorologisk information om t. ex. väder, vind och tidvattenströmmar.

Hur: Alla volymer av ”Den norske los” (Sailing Directions) kan laddas ned i PDF-format från Kartverkets webbplats: https://www.kartverket.no/global-assets/til-sjos/nautiske-publikasjoner/den-norske-los-bind1-alminnelige-opplysninger.pdf

Tabellen 3 sammanställer information om alla delar av ”Den norske los”, som är tryckt i följande delar:

Del 1	Alminnelige opplysninger (General information, 2010)	(ISBN 978-82-90-65326-7)
Del 2A	Svenskegrensen (Swedish border) – Langesund (2007)	(ISBN 978-82-90-65322-0)
Del 2B	Langesund – Jærens rev (2005)	(ISBN 978-82-90-65320-4)
Del 3	Jærens rev – Stad (2012)	(ISBN 978-82-90-65332-8)
Del 4	Stad – Rørvik (2008)	(ISBN 978-82-90-65323-9)
Del 5	Rørvik – Lødingen and Andenes (2001)	(ISBN 978-82-90-65317-4)
Del 6	Lødingen and Andenes – Grense Jakobselv (2008)	(ISBN 978-82-90-65325-0)
Del 7	Svalbard and Jan Mayen (2011)	(ISBN 978-82-90-65329-8)
Del 7 Eng	Svalbard and Jan Mayen (2012)	(ISBN 978-82-90-65330-4)
Del 7 Uppdaterade lots-skisser	Svalbard and Jan Mayen (2020)	

Tabell 3. Sammanställning av Den norske Los.Källa: Kartverket, https://www.kartverket.no/til-sjos/nautiske-publikasjoner/den-norske-los

Den Norska Los svarar på frågor som ”Hur ska resan genomföras i praktiken?”, ”Vilka faror och förhållande bör en nautiker vara medveten om?”, ”Var är närmaste säker tillflyktshamn?”. Volymerna innehåller också flygfoton, diagram över t.ex. klimat- och väderförhållande, vind- och vattenstånds- eller annan statistik samt panoramabilder över kusten. Annan information som tillhandahålls i publikationen inkluderar information om kaj- och förtöjningsplatser, bunkringsområden, varv och lokala företag.

Tidigare gavs ”Den norske los” ut, likt ”Svensk Lots”, i bokform. Det finns inga tillgängliga uppgifter om den trycks fortfarande i form av böcker. Enligt norsk lag är det lagstadgat för fartyg som går under norskt register att ”Den norske los” ska finnas ombord. I version 1.0 av ”Den norske los”, som kostnadsfritt tillgängliggörs på nätet, finns det fortfarande innehåll från PDF-utgåvorna av ”Den norske los” som inte har geo-refererats men kartverket arbetar kontinuerligt med att uppdatera detta. Följaktligen är översättning av innehåll till engelska inte fullständigt. Oavsett är den interaktiva versionen 1.0 av ”Den norske los” en mycket intressant och användbart verktyg för navigatörerna. Versionen finns tillgänglig från Kartverkets

webbplats https://www.kartverket.no/til-sjos/nautiske-publikasjoner/den-norske-los

Planer eller pågående utvecklingsarbete: För närvarande finns inga uppgifter angående utvecklingsarbete tillgängliga hos Kartverket. Genom sociala medier kan man dock konstatera att utvecklingsarbete pågår med Kartverket och några norska hamnar. Arbetet involverar även It-företag, kända för sitt engagemang i utveckling av artificiell intelligens (AI) med maskininlärningslösningar inom sjöfarten. Enligt informationen kan ”nästa generations digitala plattform för hamntillgångsdata (…) fylld med kvalitetsdata, rullas ut inom kort.”

Admiralty Sailing Directions

Vem: Det Brittiska Admiralty Sailing Directions tillför viktig information som stödjer hamnanlöp och kustnavigering för alla klasser av sjögående fartyg. Admiraltys Sailing Directions ges ut av Storbritanniens Hydrografiska Kontor (UKHO) och är en kommersiell produkt som innefattar information om hela världens hamnar och begränsar sig inte till Storbritanniens egna farvatten.

Vad: Publikationen som är fördelat på 76 volymer omfattar världens viktigaste kommersiella rutter och hamnar. Produkten är mycket väletablerad inom handelsflottan. För Östersjön publiceras Admiralty Sailing Directions (NP 18) Baltic Pilot, Vol.1, Baltic Pilot Vol.2 (NP19) samt Baltic Pilot Vol.3 (NP20) enligt bild 1 nedan:

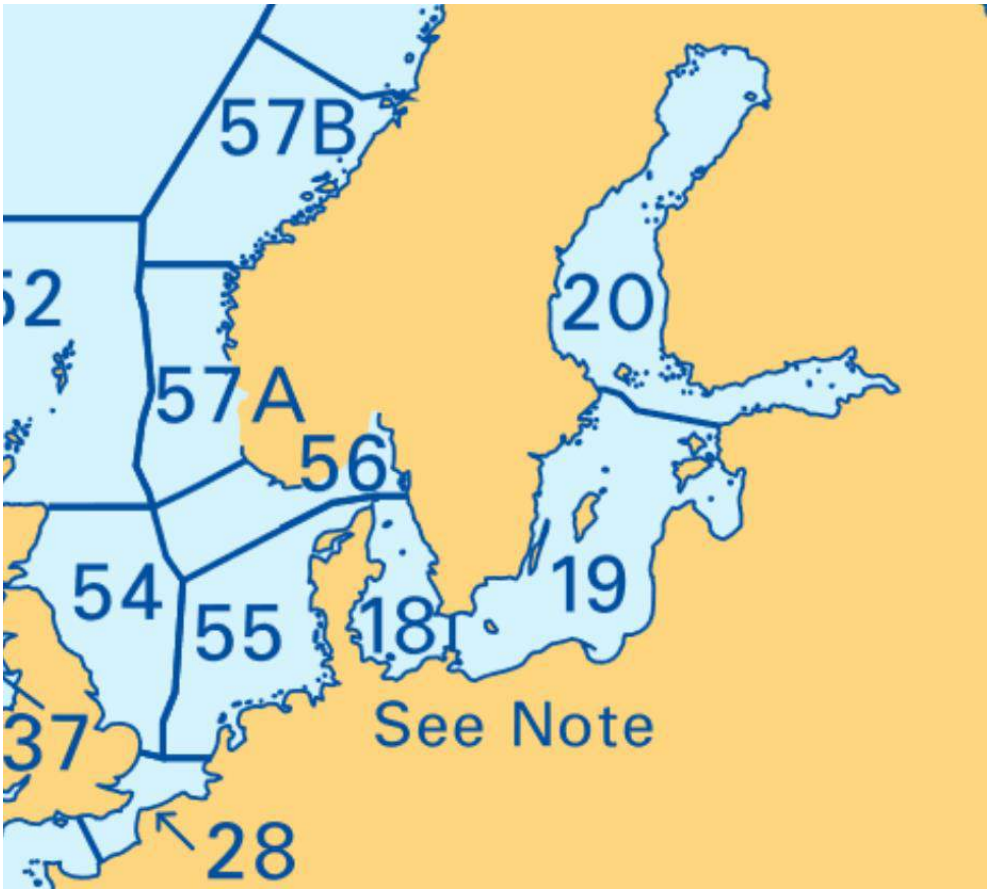


Bild 5.1 Östersjön uppdelning i Admiralty Sailing Directions .
Källa: https://www.admiralty.co.uk/publications/

Hur: Förutom i pappersformat finns varje volym av Admiralty Lots att beställa som ADMIRALTY e-Nautical Publication (AENP). AENP:er anses leda till förbättrad effektivitet, noggrannhet och tillgång till önskad information för nautiker genom elektroniska NM-uppdateringar (Notices to Mariners, motsvarande svenska UfS) samt en enkel sökfunktion. Produkter distribueras och säljs genom ett globalt nätverk av Admiralty Chart Agents

Planer eller pågående utvecklingsarbete: Inga uppgifter är tillgängliga i skrivande stund. Bedömningen görs att British Admiralty som en av de världsledande organisationerna inom Nautiska Publikationer har tillgång till ändamålsenliga resurser vad gäller kunskap, moderna teknologier, IT-lösningar samt kvalificerade medarbetare och samarbetspartners.

Guide to Port Entry

”Guide to Port Entry” är inte en officiell nautisk publikation enligt bestämmelserna i SOLAS kapitel fem eller IHO Resolution M3 som ligger till

grund för kuststaters ansvar i förhållande till tillhandahållandet av Sailing Directions-information. Genom tiderna har den dock uppskattas av sjöfarare som ett pålitligt och informationsrikt hjälpmedel vilket ligger till grund för att presentera ”Guide to Port Entry” i denna sammanställning.

Vem: ”Guide to Port Entry” ges ut av Shipping Guides Ltd. Den första upplagan släpptes 1971 och under kommande decennier har den etablerat sig väl på marknaden.

Vad: ”Guide to Port Entry” marknadsförs som den mest. exakta och omfattande resursen av portinformation, ”Guide to Port Entry” hjälper till att planera hamnanlöp till över 14700 globala kommersiella hamnar och terminaler. Utgivaren säger sig ha tillgång till marknadsledande kunskap om hamnar och terminaler och en bra kommunikation med hamnmyndigheter, agenter och operatörer som ska utgöra grunden för aktuell information.

Hur: ”Guide to Port Entry” finns till att köpa i pappersformat men erbjuds också i elektronisk form som e-bok, på CD-skivor, online på internet eller som ett applikationsprogrammeringsgränssnitt, API, vilket innebär att befogad användare har tillgång till publikationen genom mobila appar i sin mobiltelefon eller läsplatta. Information presenteras i text, kartor, bilder och skisser för att beskriva hamnar, hamnanläggningar och deras placering. Informationen kompletteras i vissa fall av rapporter och erfarenheter från faktiska besök från fartygs besättningar.

Planer eller pågående utvecklingsarbete: Inga uppgifter finns tillgängliga för närvarande.

7.5 Användarfall

Användarfallen har tagits fram utifrån en fiktiv resa med ett tankfartyg som man sedan har använt som underlag för intervjuer. I senare skede har samråd skett med andra aktörer, som ansågs involverade i fartygs hamnanlöp. Utöver en nautiker/fartygsbefäl har också intervjuer skett med ett par fartygsagenter och en skeppsmäklare.

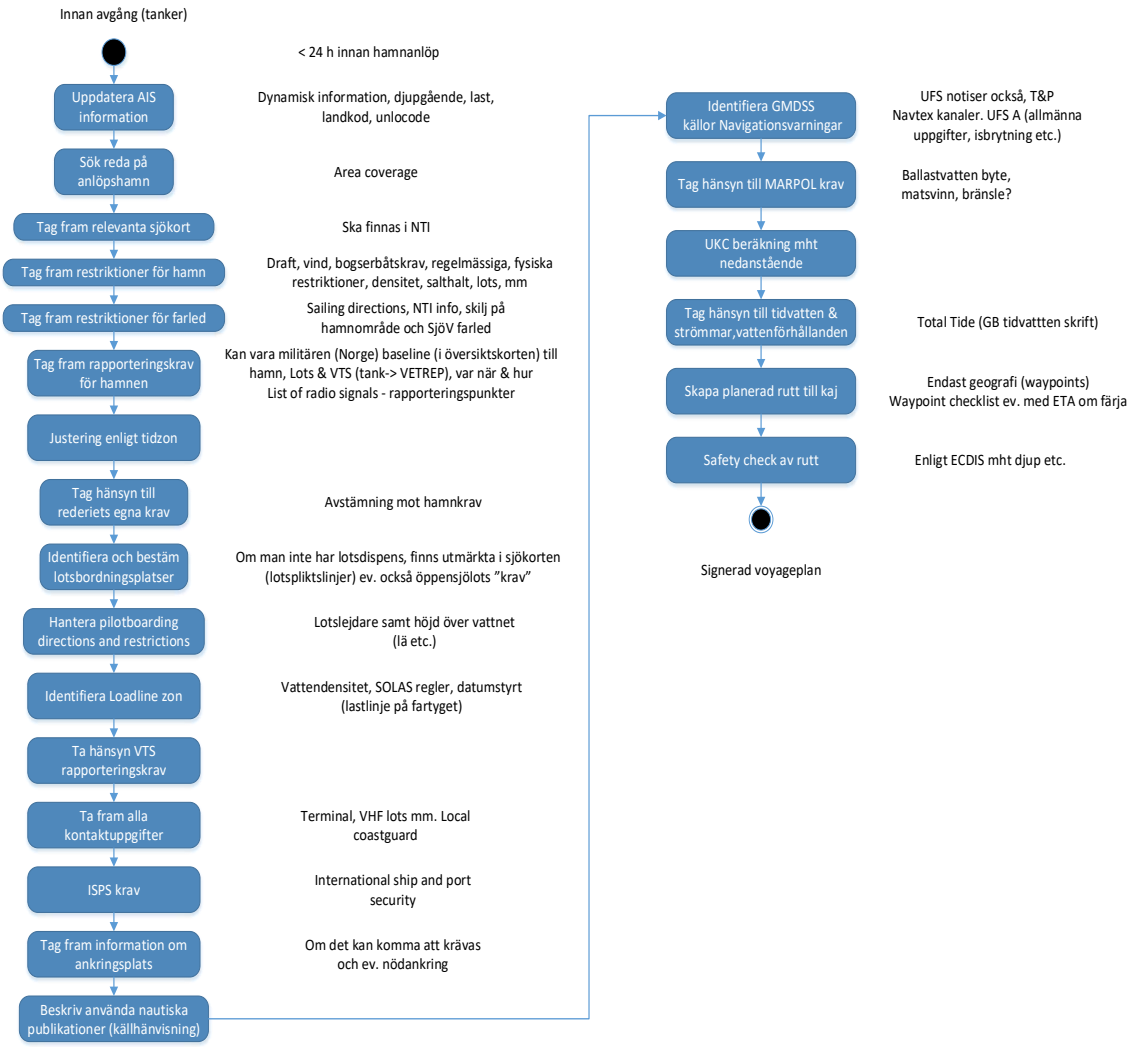
Analys

Fartygsresan delades in i 4 olika faser och nedan finns en kort sammanställning av det samlade materialet med några kommentarer eller ett förtydligande (fas 2, 3 och 4), gjort av en f.d. befälhavare och erfaren nautiker.

1. Innan avgång

Start: Reseplanering.

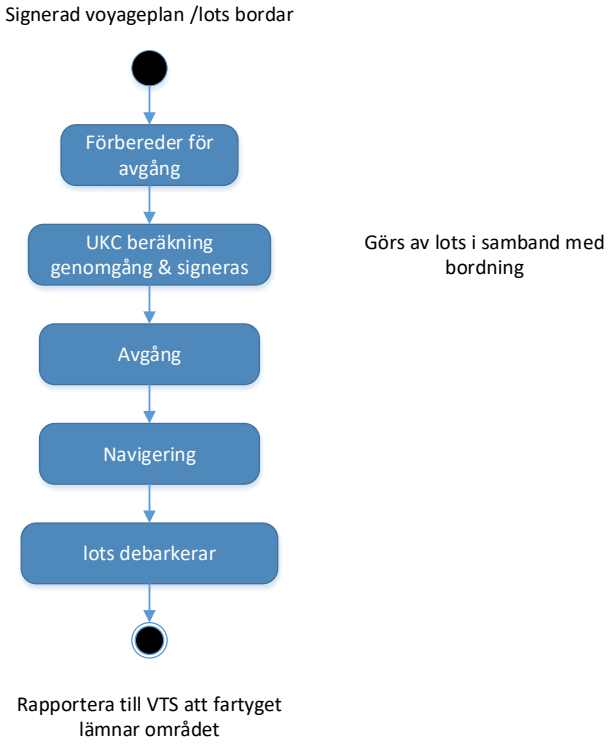
Stop: Signerad Voyage Plan.



2. Avgång

Start: Signerad Voyage Plan/Lots bordar

Stop: Rapport till VTS att fartyg lämnar området



Under denna fas av resan genomförs förberedelser för avgång, såsom start av fartygsmaskiner, radar, tester av navigationsutrustning. Bridge Resource Management (BRM) rutiner kräver genomgång av reseplaneringen vilket görs av ett bryggteam, tillsammans med lots, befälhavare och styrman. Fartygets avgång är ur nautisk synvinkel en relativt komplex process som kräver en hög grad av koncentration hos bryggteamets medlemmar och utbyte av information t.ex. rapportering och informationsutbyte med VTS, samarbete med bogserbåtar och eventuell kontakt med andra fartyg som samspelar med andra aktörer som är involverade i avgång och navigering/utkörning. Vid behov hämtas eventuellt ytterligare information direkt från en nautisk rådgivare (lots), trafikkontroll t.ex. VTS eller lämplig tjänst i hamnen eller i begränsad omfattning från fartygsagent. Debarkering av lots rapporteras av fartyget till relevanta tjänster enligt etablerade rutiner. Under avgång har vanligtvis fartygen tillgång till information genom olika kommunikationsmedel, t.ex. internet samt telefoni.

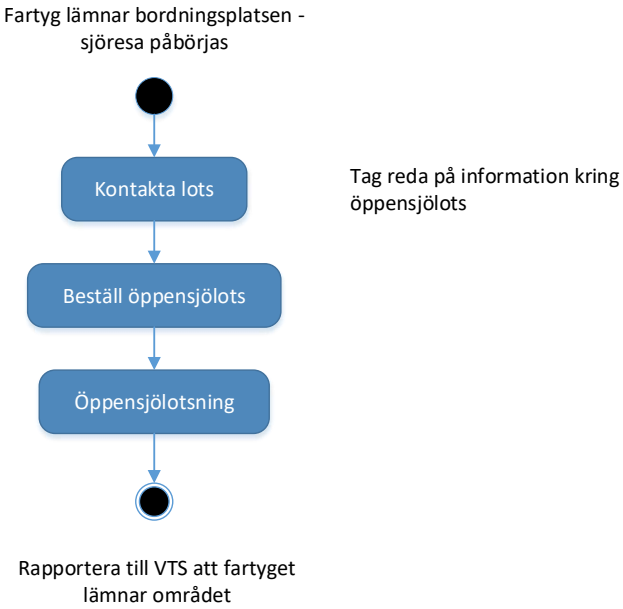
Avgång är en nautiskt intensiv process där det sällan finns utrymme för att använda sig av Seglingsbeskrivningar i dess traditionella form.

3. En Route

Start: Fartyg lämnar lots. Sjöresa påbörjas (BOSP eller COSP [6])

[6] BOSP/COSP- (eng.) beginning/commencement of sea passage

Stop: Sjöresan avslutas (EOSP [7]). Fartyg ankommer lotsbordningspunkt



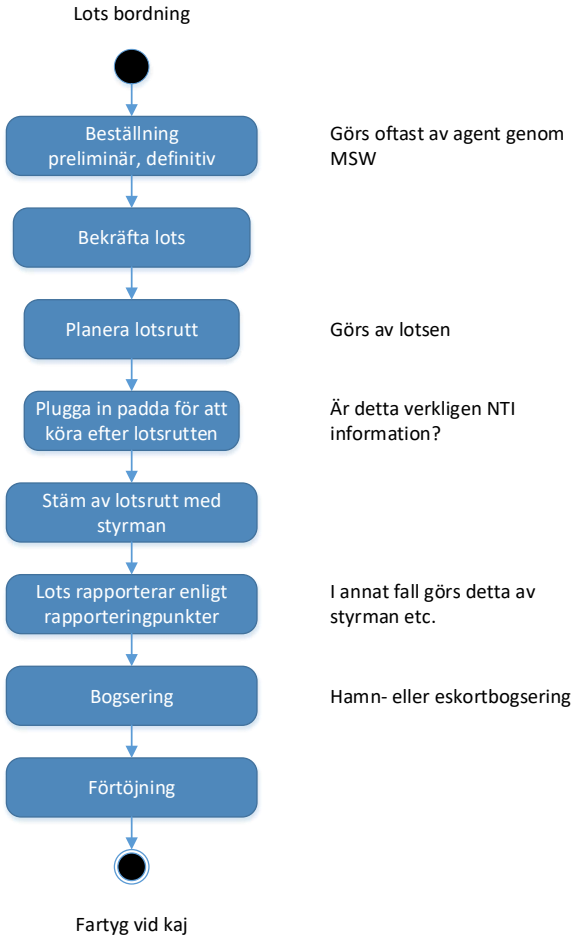
Under sjöresans fas verkställs den planerade resans ”sjö-ben” och under det använder besättningen olika nautiska hjälpmedel och publikationer för att hålla sig uppdaterade om dynamisk information, t.ex. väder, GMDSS m.m. Seglingsbeskrivningar kompletterar informationen som finns att läsa i sjökort samt andra nautiska publikationer genom dess beskrivande form (textbeskrivningar, skissar, ritningar, bilder). I de fall då ytterligare information behövs eller en del av resan omplaneras, t.ex. på grund av ändring av hamn eller terminal/angöringskaj, uppdatering av reseinstruktion m.m., används även Seglingsbeskrivningar som informationskälla.

4. Fartyg ankommer

Start: Lots bordar fartyget

Stop: Förtöjd vid kaj

[7] EOSP- (eng.) end of sea passage



I planeringsstadiet ska fartyget ha planerat sin rutt kaj till kaj. När en lots kommer ombord, kan denne ha förslag på en annan rutt. Eventuella nya uppgifter som behövs av bryggteamet inhämtas direkt från en nautisk rådgivare (lots) med kunskap om lokala förhållanden eller från lämpliga informations- och trafikkontrolltjänster (t.ex. VTS, hamn). Rapportering sker enligt bestämda rapporteringspunkter av lotsen eller fartygets styrman enligt tidigare bestämda rutiner (BTM). Kommunikation mellan fartyget och bogserbåt/bogserbåtar sköts vanligtvis av lotsen under eventuell bogsering. Detsamma gäller för kommunikationsvägar och själva kommunikationen med linesmän eller båtmän vid förtöjning.

7.6 GAP-analys

I denna förstudie har vi arbetat med att göra en GAP-analys för att identifiera skillnader mellan den information Sjöfartsverket levererar i våra seglingsbeskrivningar och kravbilden utifrån IMO:s SOLAS kapitel 5 och IHO:s M3.

Projektets ansats för GAP-analysen var att utgå från den AVANTI-mall som tagits fram tidigare av bl. a. ITPCO tillsammans med NIPWG. Efter att ha analyserat IHO:s M3 är slutsatsen att AVANTI-mallen utgår från ett hamnperspektiv där ett av målen är att jobba för att standardisera hamninformation till Seglingsbeskrivningar. Eftersom M3 är en ”heltäckande” resolution, som utöver hamninformation även innehåller information utifrån ett stats- och kustperspektiv, så kommer inte GAP-analysen skapa den nytta som förutsågs i arbetet med denna förstudie.

För att skapa ett nationellt system för seglingsbeskrivningar kommer det vara nödvändigt att arbeta vidare med den befintliga kravspecifikationen från NTI1-projektet (2016) och eventuellt ta fram ytterligare kravspecifikationer som ska ligga till grund för vad systemet skall hantera och hur det skall fungera för dess användare.

I bilagan 7.6.1 så visas den Gap-analys som gjordes under projektets början mellan IHO:s M3, Avantimall och information som finns på Sjöfartsverkets hemsidor. Bilagan finns med för att belysa skillnader mellan de tre entiteterna i fråga om ansats och innehåll.

7.6.1 GAP-analys Avanti, Lotsområdessidor och IHO M3

	MINIMINIVÅ AVANTI SJÖV/HAMN/GEMENSAM	LOTSOMRÅDESSIDOR INFO FINNS/INFO ÄR BRISTFÄLLIG/INFO FINNS EJ/ NTI-INFO PÅ LOTSHEMSI-DOR SOM EJ STÅR MED I AVANTI- MALLEN	IHO M3 TAS UPP/SKRIVET PÅ ANNAT SÄTT/TAS EJ UPP INFORMATION SOM ENLIGT M3 SKA REDOVISAS, MEN SOM EJ TAS UPP I AVANTIMALL ELLER LO-SIDOR
PORT GENERAL INFORMATION			
Port General Information			
General Information			Tas upp i många underrubriker
Location Description			
Limits Description			Limits of Port
Load			
Line			Se rad 41 i flik M3
Maximum Vessel sizes			
Time Zone			
Charts		Info finns på andra SjöV-si-dor	Se rad 17 i flik M3
Shipping announcements			

Port Information Guide Foreword

Legal Disclaimer

Contact Information

General Contact Information
Point of Contact
VHF Channel
Usage

List of Radio Signals

Weather and Tidal Information

General Hydrometeo information
Hydrometeo Phenomena

Vissa sidor länkar till ViVa se rad 54 i flik m3

Notifications

Arrival Checklists
Departure Checklists
Notifications

Reporting / Documentation

Reporting requirements Documentation Require- ments		Se rad 28 + 55 i flik M3 + Se definitions-flik, rapportering som ämne ska finnas med

Regulations and Requirements

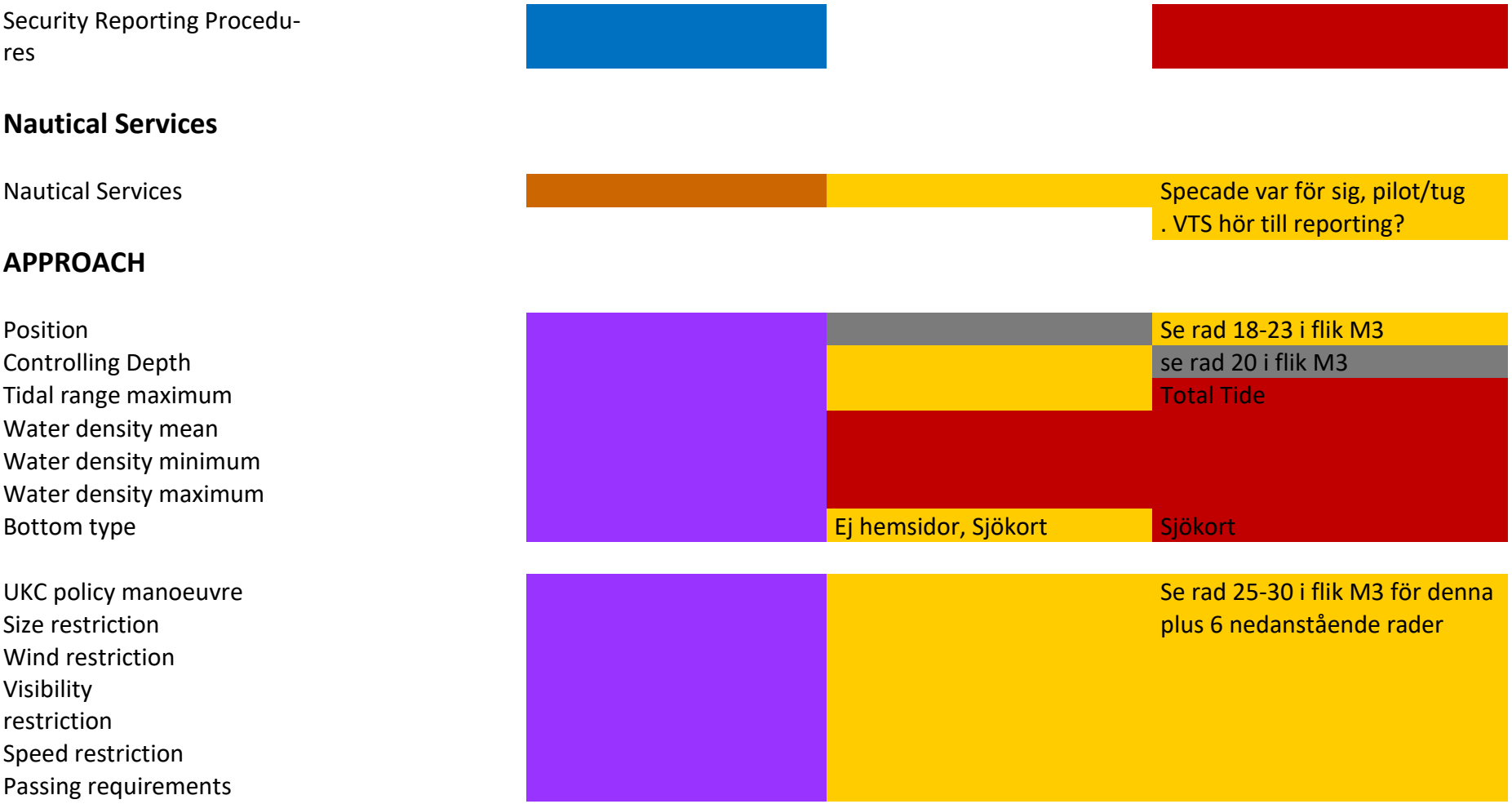
Regulations Exemptions Legal Amendments		se rad 35 + 58 i flik M3

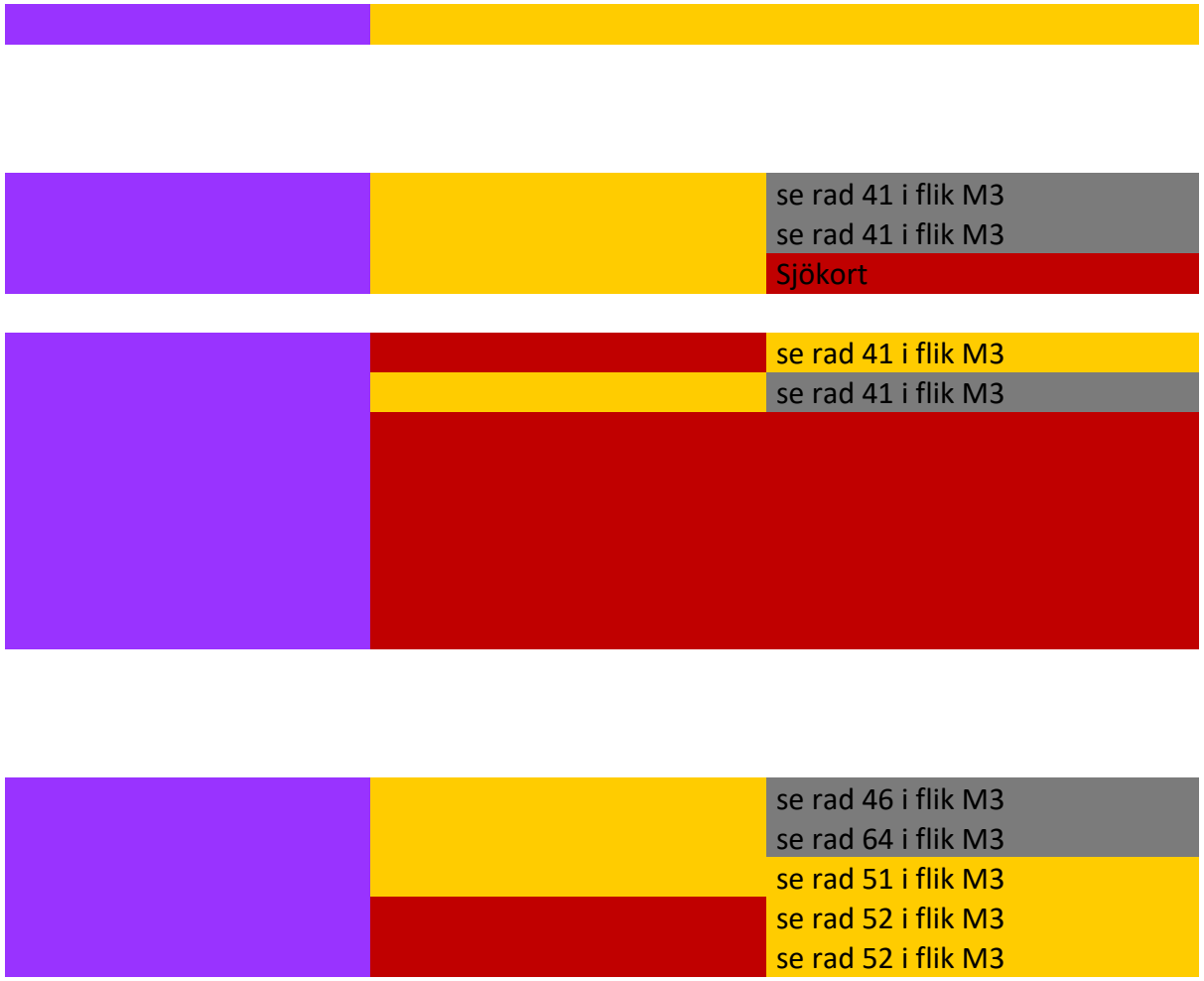
Port Safety

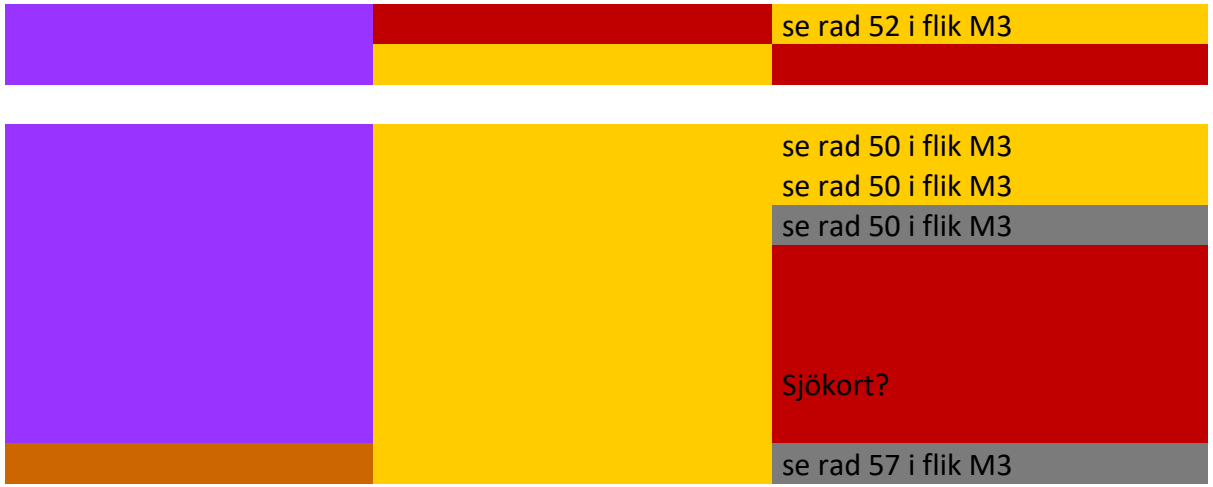
Emergency Coordination Centre Emergency Response Equipment Emergency Scenario		

Port Security

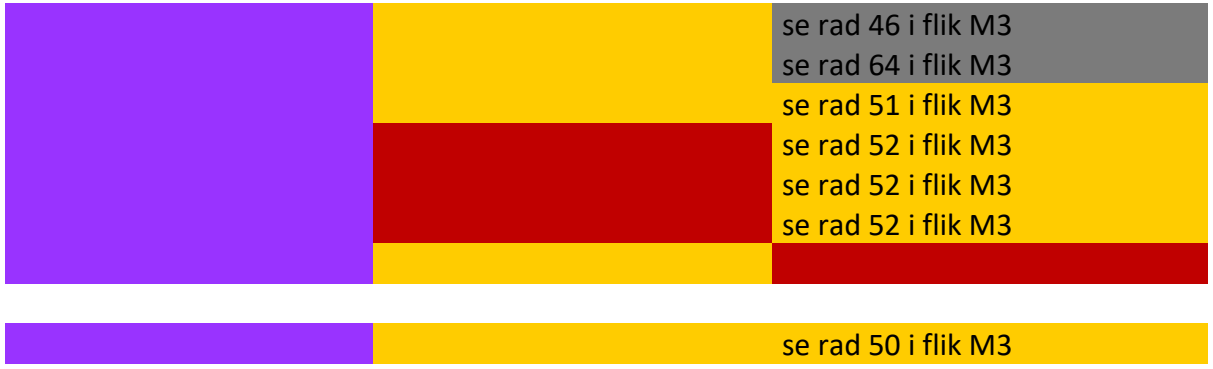
ISPS Security Level		


Security Reporting Procedu-
res
Nautical Services
Nautical Services
Specade var för sig, pilot/tug
. VTS hör till reporting?
APPROACH
Position
Controlling Depth
Tidal range maximum
Water density mean
Water density minimum
Water density maximum
Bottom type
Se rad 18-23 i flik M3
se rad 20 i flik M3
Total Tide
Ej hemsidor, Sjökort
Sjökort
UKC policy manoeuvre
Size restriction
Wind restriction
Visibility
restriction
Speed restriction
Passing requirements
Se rad 25-30 i flik M3 för denna
plus 6 nedanstående rader


Tug use
ANCHORAGE
Position
Controlling Depth
Bottom type
se rad 41 i flik M3
se rad 41 i flik M3
Sjökort
UKC policy manoeuvre
Size restriction
Wind restriction
Visibility
restriction
Speed restriction
Passing requirements
Tug use
se rad 41 i flik M3
se rad 41 i flik M3
BERTH
Position
Controlling Depth
Tidal range maximum
Water density mean
Water density minimum
se rad 46 i flik M3
se rad 64 i flik M3
se rad 51 i flik M3
se rad 52 i flik M3
se rad 52 i flik M3


Water density maximum
Bottom type
se rad 52 i flik M3
UKC policy manoeuvre
UKC policy alongside
Size restriction
Wind restriction
Visibility
restriction
Speed restriction
Passing requirements
Tug use
se rad 50 i flik M3
se rad 50 i flik M3
se rad 50 i flik M3
Sjökort?
se rad 57 i flik M3

BASIN

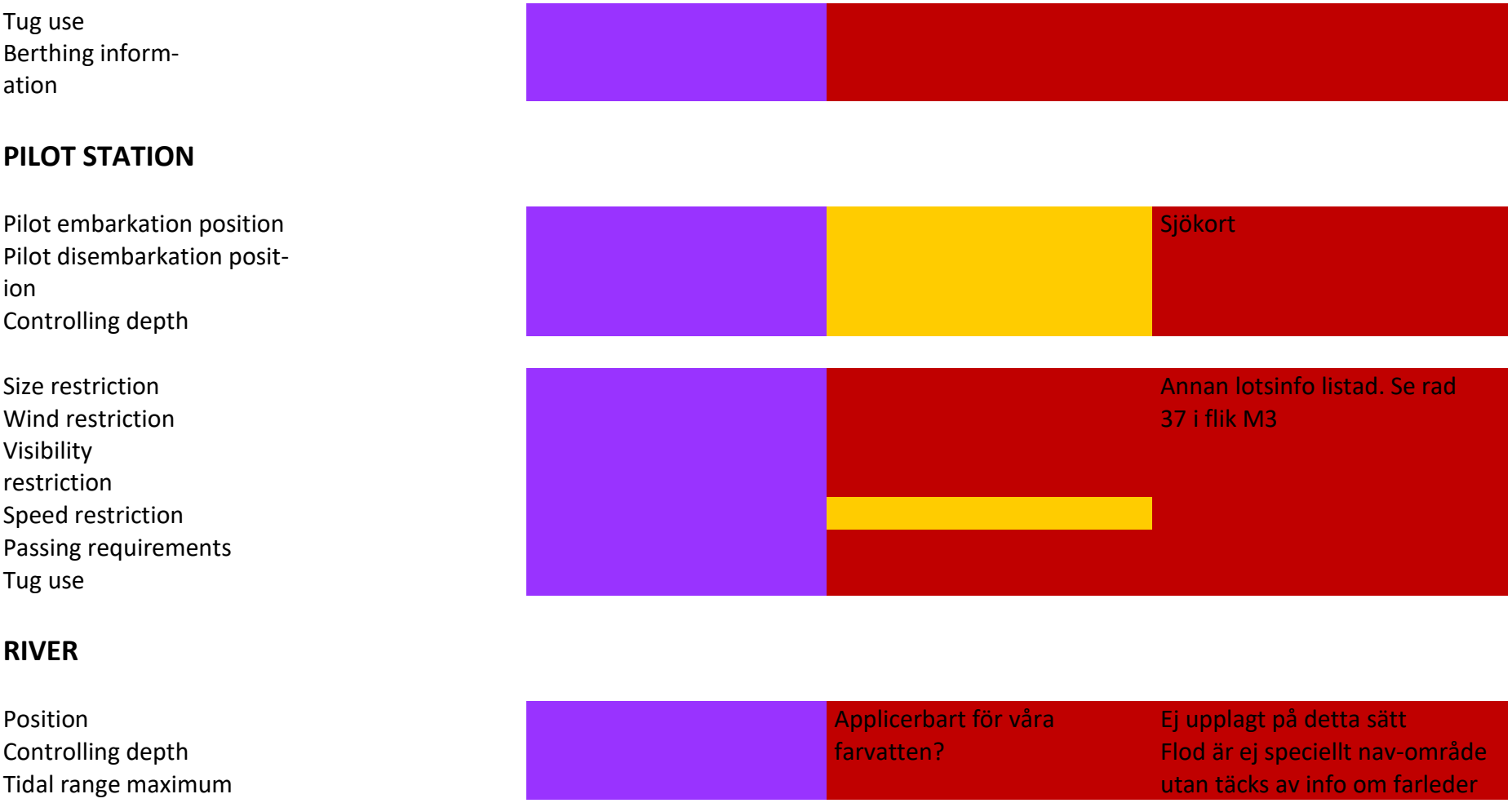

Position
Controlling Depth
Tidal range maximum
Water density mean
Water density minimum
Water density maximum
Bottom type
se rad 46 i flik M3
se rad 64 i flik M3
se rad 51 i flik M3
se rad 52 i flik M3
se rad 52 i flik M3
se rad 52 i flik M3

UKC policy manoeuvre
se rad 50 i flik M3

UKC policy alongside			se rad 50 i flik M3
Size restriction			se rad 50 i flik M3
Wind restriction			
Visibility			
restriction			
Speed restriction			Sjökort?
Passing requirements			
Tug use			se rad 57 i flik M3
Berthing information			se rad 63 + 64 i flik M3

BRIDGE

Position		Finns info om broar på web-ben	se rad 66 + 67 i flik M3
Bridge opening method		under "Sjökort och publikationer"	
Bridge pattern			
UKC policy manouvering			
Size restriction			
Wind restriction			
Visibility			
restriction			
Speed restriction			
Passing requirements			


Tug use
Berthing inform-
ation
PILOT STATION
Pilot embarkation position
Pilot disembarkation posit-
ion
Controlling depth
Sjökort
Size restriction
Wind restriction
Visibility
restriction
Speed restriction
Passing requirements
Tug use
Annan lotsinfo listad. Se rad
37 i flik M3
RIVER
Position
Controlling depth
Tidal range maximum
Applicerbart för våra
farvatten?
Ej upplagt på detta sätt
Flod är ej speciellt nav-område
utan täcks av info om farleder

Water density mean	och "waterways".
Water density minimum	
Water density maximum	
Bottom type	
UKC policy manouvering	
UKC policy alongside	
Size restriction	
Wind restriction	
Visibility	
restriction	
Speed restriction	
Passing requirements	
Tug use	
Berthing information	

INFO PÅ LOTSHEMSIDOR SOM KAN VARA NTI MEN EJ ÄR MED I AVANTIMALLEN

Isrestriktioner	se rad 32 + 53 i flik M3
Strömrestriktioner	se rad 60 i flik M3
Mörkerrestrikt-	
ioner	
Restriktioner m.h.t. fartygs utseende	
Hamninfo	se rad 41 + 45-68 i flik M3

Lotsbeställning	se rad 37+ 57 i flik M3
Lotsplikt	se rad 37+ 57 i flik M3
Bord- ning	se rad 37+ 57 i flik M3
Slussar	
Våghöjdsrestriktioner	
Tvåmanslotsning	se rad 37+ 57 i flik M3
Lotsrutter	se rad 26+ 97 i flik M3

Information som enligt M3 ska vara med men som ej står att finna eller är beskriven på samma sätt som i Avantimall eller Lotssidor.

Skala "General" (Lotsområdestäckande)

Coastal outline and border with latitude and longitude graduation
Limits of area
Charts: Limits and numbers of the charts for the area; Remarks on the general quality of the charts (paper and digital) available for the area, use of charts other than those of own nationality; remarks on important differences of geographical or tidal datum between charts; Limits and numbers of the charts for the area
Names of principal ports, bays, channels sea areas, headlands, islands and countries, as far as this is consistent with clarity
General aspect and remarks about the waterway and shores
Through routes and traffic separation
Buoys and beacons. *Descriptions of systems in use if differing from IALA Regions A or B*
Navigation. General remarks on navigation in *coral waters; notes on the existence of large amounts of kelp*; **ice navigation and ice-breaker service** available where these are applicable to the area; any other notes applicable to navigation throughout the area covered by the book, such as fishing and other maritime activities;
Offshore or coastal activities dangerous to shipping such as drilling platforms, military exercises, dumping grounds
Submarine cables and pipelines of a general nature (varningstext att kopiera finns i M3)
Regulations. Extracts of national regulations concerning navigation, pollution, quarantine, cables, pipelines and any other special regulations that should be known to mariners before arrival in national waters. The territorial sea and economic zones claimed should be given in general terms;
Radio services. General remarks on the availability and reliability of radio position fixing systems, radio beacons, navigational warnings, and weather forecasts. This section should not duplicate the details of times of operation and the frequencies if these are given in separate radio publications;
Pilotage. General remarks on pilotage services in the areas, national regulations regarding pilotage. Where there are standard regulations for pilots applicable to all parts of the area, these can be given to avoid repetition elsewhere in the book. Special regulations applicable only to individual ports are best given at the port concerned rather than in the first chapter;
Visual signals. *Systems of signals in use in the area for storm, weather, dredging, traffic and other special maritime activities should be described. These should not include well-known international signals; special signals only applicable to an individual port are best given with the main description of the port;*

Distress and rescue. Brief description of the sea/air rescue organisations that may be in operation for the area covered by the book;
Countries. *Brief information about the countries in the area of interest to the mariner;*
Principal ports and anchorages. A list of ports and anchorages in the area giving position, principal purpose, brief statement on limiting conditions such as depth of water, or size of vessel that can use the port, whether it is a port of entry, cross-reference to other parts of the book or other publications where further information can be obtained;
Port services*. A list of places should be given where fuel, fresh water, repairs, docking, fumigation, and diplomatic representatives are available*
Bottom topography
Seismic activity (if relevant)
Water level peculiarities and irregularities
Currents
Tidal streams
Oceanography (temperature, density, salinity)
Ice conditions with diagrams
Sea and swell
Surface meteorological information with seasonal diagrams and climatic tables for selected places on the coast
Local meteorological conditions (winds and fogs etc.)
Magnetic anomalies

Skala "Approach" (från lotsbordningspunkt till aktuellt hamnområde)

Route - general description
Controlling depth or least charted depth in the fairway
Regulations for traffic separation, movement reporting, prohibited areas
Directions for the waterway or coastal passage
Directions for approaches to harbours and anchorages
Local Pilotage
Minor side channels for small craft (less than 2m draught, or 12m in length)
Small craft anchorages, harbours and marinas not falling within larger harbours
Currents, tidal streams, overfalls;
Local winds and fogs, etc;
Principal marks and navigation aids
Anchorages and harbours
Bridges: It is resolved that minimum vertical clearance shall always be given in Sailing Directions in respect of bridges viaducts etc. It is resolved that the navigable width shall always be given for bridges and viaducts crossing navigable waters.

Channels: It is recommended that when a channel is referred to in several parts of the same volume, the complete instructions for this channel be given in a separate chapter.

Skala "Local" (hamnområde)

Name and position of port or harbour
Limits of port
General remarks on type of port, main function, and amount of traffic handled
Port authority
Limiting conditions due to draught, size of vessel
Water level and mean tidal range
Density or salinity of water if differing from normal seawater
Ice
Local meteorological conditions
Arrival information required and notice for ETA
Port information service, signal stations
Pilotage and tugs
Regulations
Outer anchorages and sea berths
Tidal streams
Entrance channel or fairway;
Traffic signals
Directions for entering
Berths, basins and depths of water
Port facilities in brief for cargo handling, ro-ro, containers, lighters, cranes, etc
Repair facilities, dry docking, and slipways
Supplies of fuel, water, etc
Transport facilities from the port by sea, road, rail, canal and nearest main airport.

7.7 Beskrivning av relevanta S-100 standarder

7.7.1 S-122 Marine Protected Areas

(https://registry.iho.int/productspec/view.do?idx=73&product_ID=S-122&statusS=5&domainS=ALL&category=product_ID&searchValue=)

Scope: S122-produktspecifikationen är avsedd att koda MPA-information (Marine Protected Area) för användning i ECDIS och andra informationssystem. MPA är skyddade områden med hav, flodmynningar eller stora sjöar. Information om marint skyddsområde kan betraktas som

kompletterande ytterligare information som kompletterar elektroniska sjökort, S-101 ENC.

Status: S-122 Edition 1.0.0 släpps endast för implementering och testning

7.7.2 S-123 Marine Radio Services

(https://registry.iho.int/productspec/view.do?idx=74&product_ID=S-123&statusS=5&domainS=ALL&category=product_ID&searchValue=)

Scope: S-123 Marinradiotjänster som anger plats, tillgänglighet, typ av radiokommunikation, frekvenser och innehåll för radiotjänster för navigeringsinformation och annan maritim radiokommunikation. Radiotjänstinformation kan betraktas som kompletterande ytterligare information som kompletterar S-101 ENC.

Status: S-123 Edition 1.0.0 släpps endast för implementering och testning.

7.7.3 S-125 Marine Navigational Services

(http://s100.iho.int/product%20specification/division-search/s-125-marine-navigational-services) som är On Hold i utvecklingen

Scope: Denna produktspecifikation beskriver sjömärken inklusive ljus och andra navigationshjälpmedel, både fysiska och virtuella; tillfälliga och säsongsbetonade märken; och lokala AIS-applikationsspecifika meddelanden. Information om navigationstjänster kan betraktas som ett utbytesformat för sjömärken för datautbyte mellan t ex hamnar och myndigheter.

Status: S-125 utveckling är för närvarande pausad.

7.7.4 S-126 Marine Physical Environment

(http://s100.iho.int/product%20specification/division-search/s-126-marine-physical-environment)

Scope: Denna produktspecifikation beskriver marin och terrestrisk topografi; rådande, säsongsbetonade och farliga strömmar; tidvatten; salinitet; väder; och andra miljöförhållanden. Fysisk miljöinformation kan betraktas som kompletterande ytterligare information som kompletterar S-101 ENC.

Status: S-126 utveckling är ej påbörjad.

7.7.5 S-127 Marine Traffic Management

(http://s100.iho.int/product%20specification/division-search/s-127-marine-traffic-management)

Scope: Produktspecifikation för fartygstrafiktjänster; lotsning; ruttsystem; och fartygsrapporteringssystem. Sjötrafikledningsinformation kan betraktas som kompletterande ytterligare information som kompletterar S-101 ENC.

Status: S-127 Edition 1.0.0 har släppts för implementering och testning.

Se bilaga för mer detaljerad beskrivning av S-127 i kapitel 7.7.8.

7.7.6 S-131 Marine Harbour Infrastructure

Webbadress saknas.

Scope: Produktspecifikation för hantering av hamninformation beskrivning av olika faciliteter och kapaciteter. Tas fram i samarbete med International Harbour masters Association (IHMA).

Status: Arbete pågår med utveckling av en första edition för testning.

7.7.7 S-421 Route Plan (IEC 63173-1)

Scope: Reseplaneringen är en viktig del av ett fartygs resa och kan användas för att optimera säkerhet och processer, samt för samspelet mellan deltagare och intressenter. Kärnan i reseplanen är rutten. Produktspecifikationen definierar alla krav som ruttplansdataprodukter ska uppfylla.

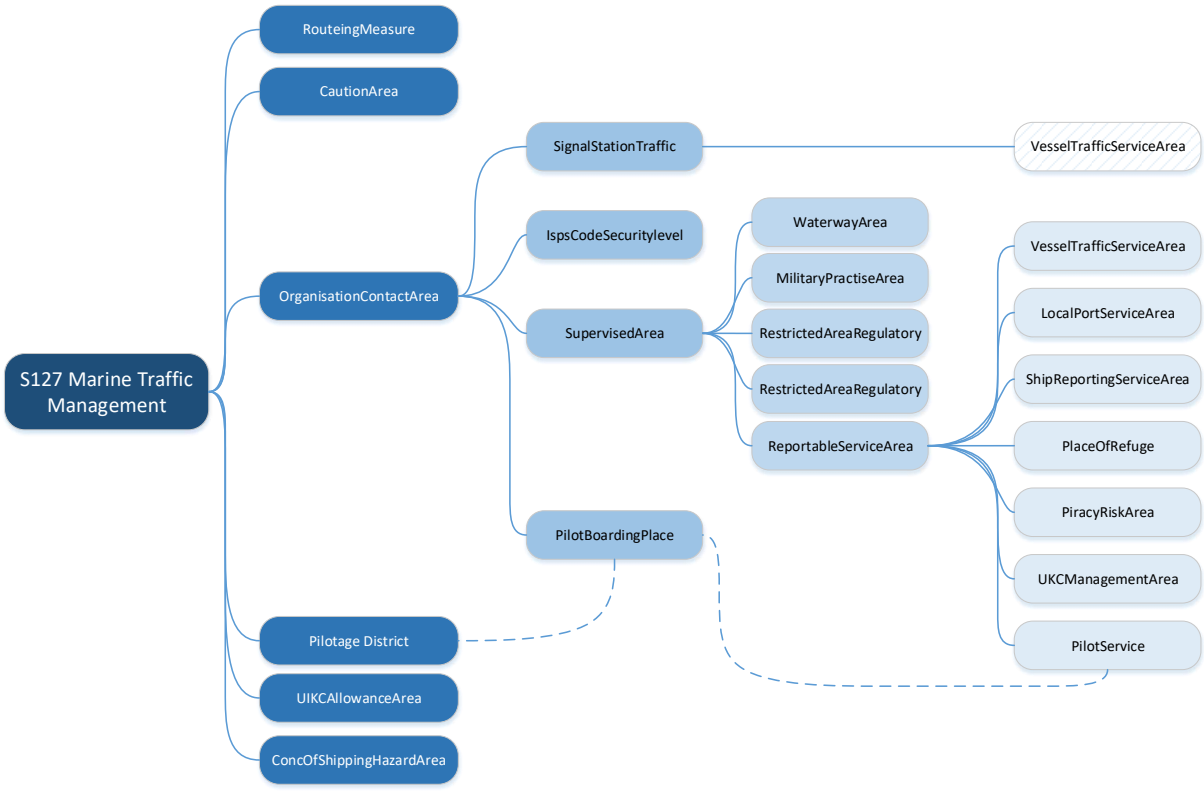
Status: S-421 för närvarande under utveckling. Se S-421 Product Specification Information

Ansvarig organization: International Electrotechnical Commission / IEC TC80

7.7.8 Beskrivning av S-127 Marine Traffic Management

S127 Marine Traffic Management (MTM) beskriver tillgängligheten och tillförlitligheten för VTS, lotsning, ruttåtgärder samt fartygsrapporteringssystem. Detta inkluderar deras serviceområden, tjänster som erbjuds och instruktioner för att kontakta eller använda dessa tjänster. MTM är avsett att vara ett komplement till ENC och beskriver därför inte den geografiska informationen i detalj såsom ENC gör. Snarare visas den som en förenklad geometri för att indikera plats och för att vara ett sätt att geolokalisera mer regulatorisk information än den som normalt återfinns i ENC.

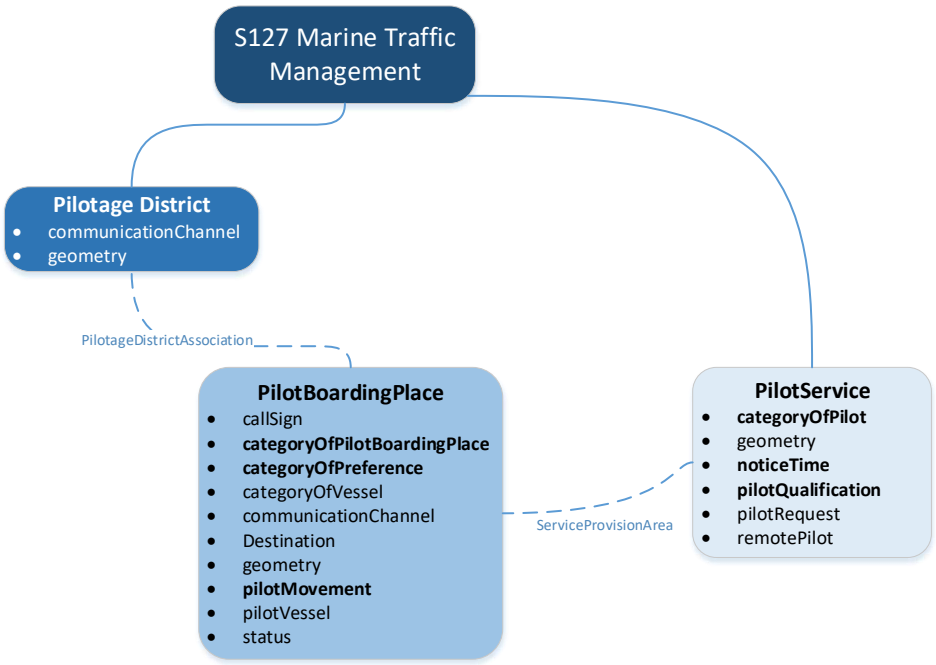
I nedanstående figur illustreras översiktligt de olika komponenter S127 standarden består av.



Utifrån Sjöfartsverkets perspektiv har sedan resp. komponent analyserats och beskrivits utifrån hur denna standard kan användas för att beskriva de informationsmängder Sjöfartsverket underhåller.

Pilotage (Lotsning)

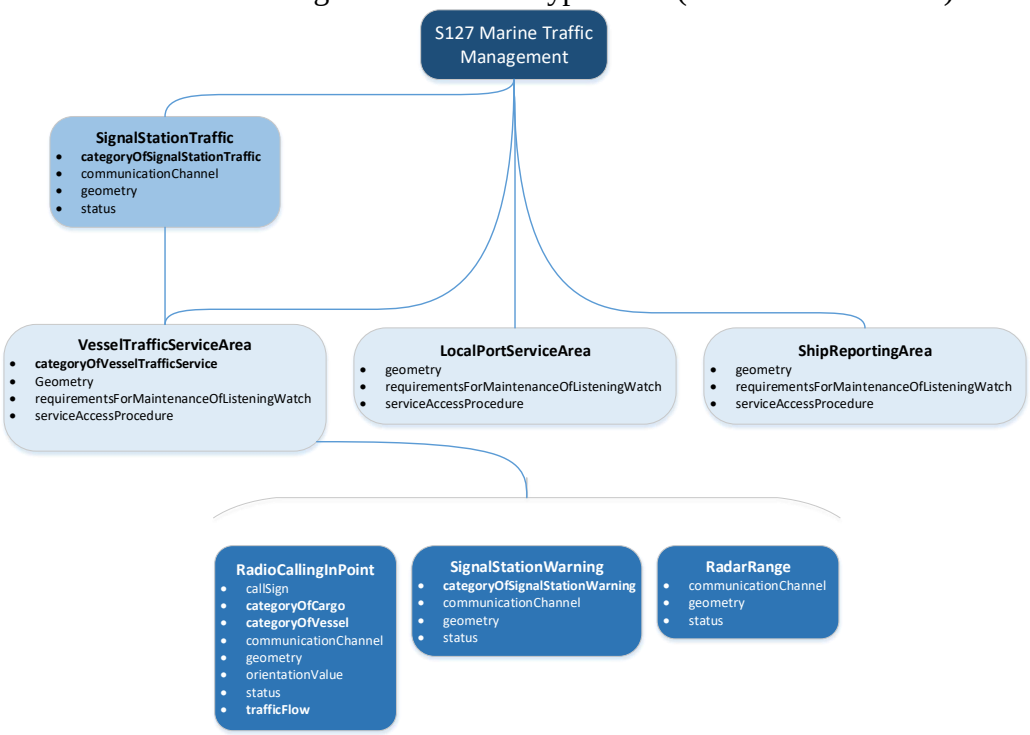
S127 föreskriver att information gällande lotsning kan hänföras till tre olika områden.
Pilotage District (motsvarar Sjöfartsverkets lotsområde) - Ett område inom vilket en lotsriktning finns. Sådana anvisningar regleras av en behörig hamnmyndighet (Sjöfartsverket har denna roll i Sverige) som dikterar de omständigheter under vilka de gäller.
Pilot Boarding Place (motsvarar lotsbordningsplats) - En plats offshore där en lots kan gå ombord på ett fartyg som förberedelse för att lotsa det genom lokala vatten.
Pilot Service (motsvarar Sjöfartsverkets lotsplanering) - Den tjänst som tillhandahålls av en person som leder ett fartygs rörelser genom lotsvatten, vanligtvis en person som har visat omfattande kunskap om kanaler, navigeringshjälpmedel, faror för navigering etc. i ett visst område och har tillstånd för det området.



VTS (Vessel Traffic Service)

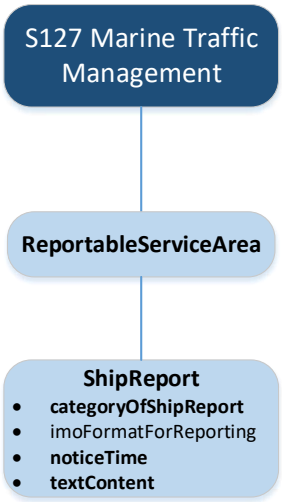
S127 föreskriver att information gällande VTS kan hänföras till tre olika områden.
Vessel Traffic Service Area (motsvarar Sjöfartsverkets VTS område) - Området för alla tjänster som genomförs av en relevant myndighet, främst utformad för att förbättra säkerheten och effektiviteten i trafikflödet och skyddet av miljön. Det kan sträcka sig från enkla informationsmeddelanden till omfattande organisation av trafiken med nationella eller regionala system.
Ship Reporting Area (motsvarar rapportering i VTS område) - En tjänst inrättad av en relevant myndighet som består av en eller flera rapporteringspunkter eller linjer där fartyg är skyldiga att rapportera sin identitet, kurs, hastighet och andra uppgifter till relevant myndighet.
Signal Station Traffic (motsvarar Sjöfartsverkets tjänst Sweden Traffic) - En trafiksignalstation är en plats på land från vilken signaler skickas för att reglera trafikens rörelse.
Local Port Service Area (lokala hamnförskrifter) - En tjänst etablerad för att tillhandahålla hamninformation utan interaktion mellan kunden och tjänsteleverantören. Denna information kan bland annat vara information om förtöjning, tillgång till hamntjänster, tidtabeller för sjöfart, meteorologiska och hydrologiska data.
Radio Calling In Point (motsvarar rapporteringspunkter inom ett VTS område) - En bestämd plats där fartyg är skyldiga att rapportera till en trafikledningscentral. Kallas även rapporteringspunkt eller radiorapporteringspunkt.

Signal Station Warning (motsvarar NavTex) - En varningssignalstation är en plats på land varifrån varningssignaler skickas till fartyg till havs.
Radar Range (ingen motsvarighet i Sverige) - Indikerar täckningen av ett havsområde för en radarövervakningsstation. Inom detta område kan ett fartyg begära landbaserad radarassistans, särskilt vid dålig sikt. Obs detta används inte i då alla Sveriges VTS:er är av typen INS (Information Service).



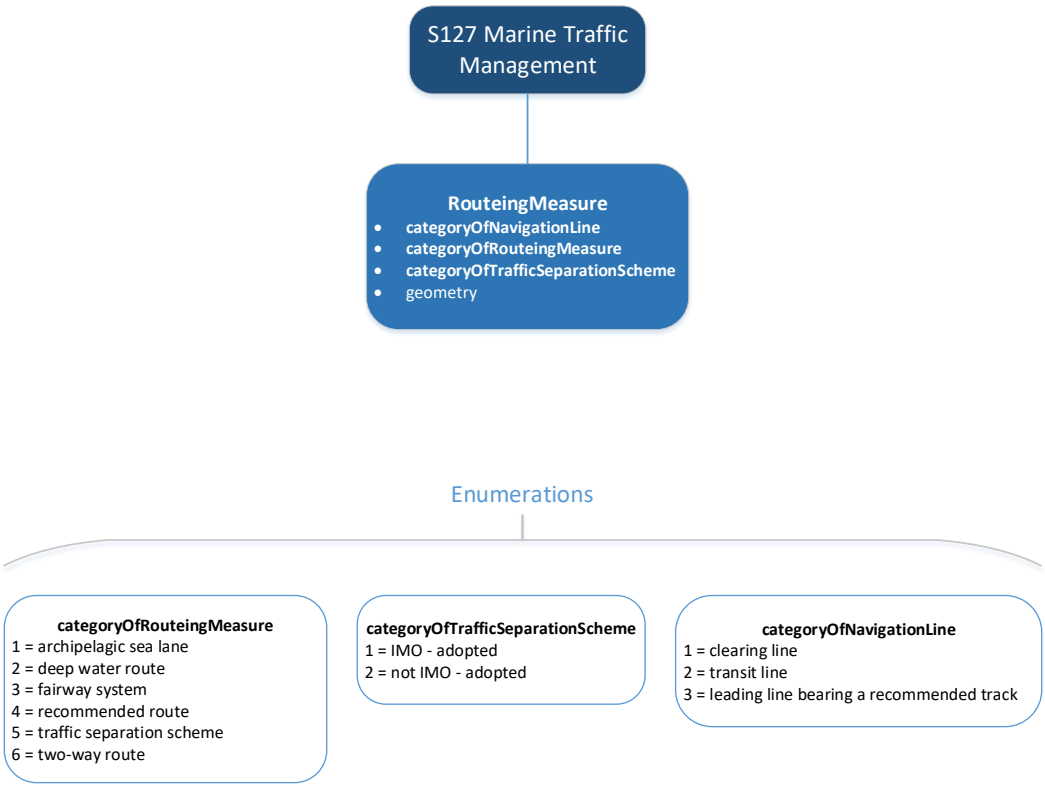
SRS (Ship Reporting Service)

S127 föreskriver att information gällande SRS kan hänföras till följande områden.
Ship Report (motsvarar) - Detta beskriver hur ett fartyg ska rapportera till en sjöfartsmyndighet, inklusive när det ska rapporteras, vad som ska rapporteras och om formatet överensstämmer med IMO-standarden för rapportering.
Reportable Service Area (motsvarar SRS område t.ex. SoundRep) - Ett tjänsteområde som i allmänhet har krav på inlämnande av information, inklusive kommunikation som inte strikt anses vara "rapportering".



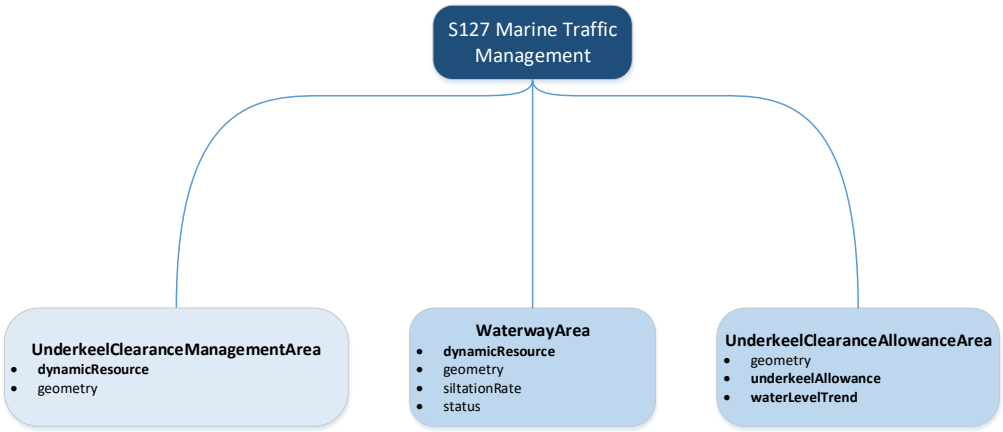
Routeingmeasure (Farleder)

S127 föreskriver att information gällande farleder kan hänföras till följande. Routeingmeasure (Klassificering av typ av yta/ farled etc.) - Ett område eller en linje som betecknar gränserna eller centrallinjen för en farled (eller en del av en farled). Farleder inkluderar trafikseparingssystem, djupvattenrutter, tvåvägsrutter, skärgårdsleder och farledssystem. Obs detta finns dock redan angivet i sjökortet i anslutning till kustlinjen. Möjligtvis kan detta komma ifråga om Sjöfartsverkets NTI i en framtid även kommer att omfatta områden längre ut från kusten.



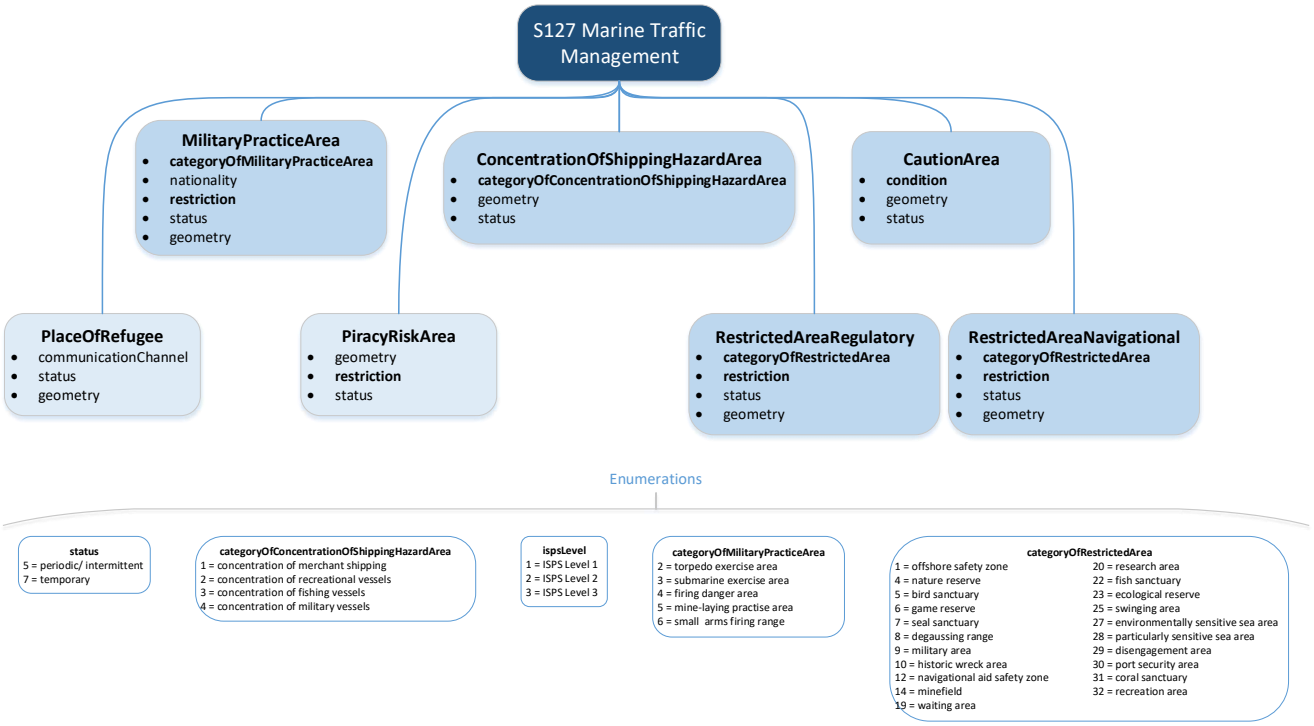
UnderkeelClearance (djup under kölen)

S127 föreskriver att information gällande UKC (Under Keel Clearance) kan hänföras till följande områden.
UnderkeelClearanceAllowanceArea (motsvara ett område för tillåtet djupgående) - Ett område för vilket en myndighet har angett krav på djup under kölen.
WaterwayArea (motsvarar en farledsyta) - Ett område där enhetlig allmän information om vattenvägen/ farleden finns.
UnderkeelClearanceManagementArea (detta finns inte i Sverige) - ett område för vilket en myndighet tillåter användning av dynamiskt underköl-djupgående eller tillhandahåller dynamisk information relaterad till underköls-djupgående.



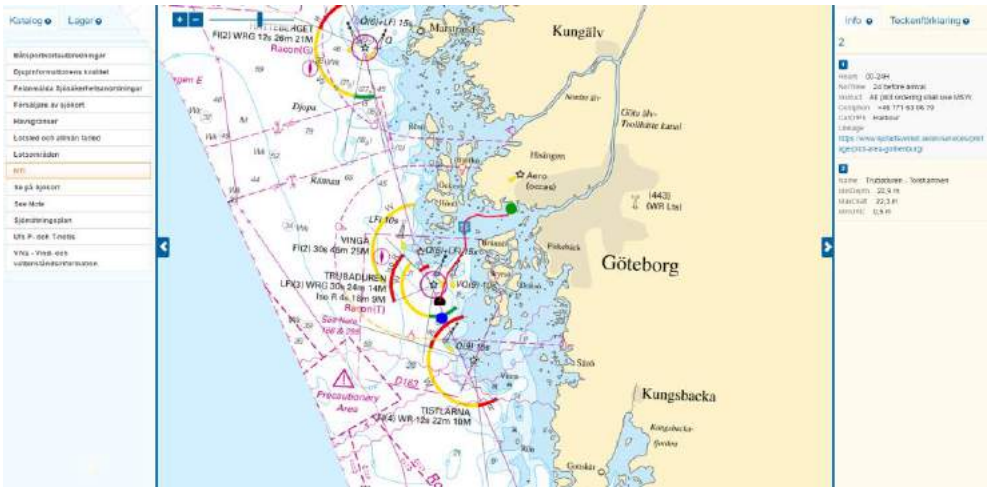
Other areas **(övriga områden)**

ConcentrationOfShippingHazardArea () - Ett område där faror, hänförliga trafikkoncentration, kan förekomma. Faror är risker för sjöfarten som härrör från andra källor än stimvatten eller hinder.
CautionArea () - I allmänhet ett område där sjöfararen måste göras medveten om omständigheter som påverkar navigeringssäkerheten.
IspsCodeSecurityLevel () - Det område för vilket en ISPS-nivå (International Ship and Port Facility Security) gäller.
MilitaryPracticeArea (motsvarar områden för relaterade navigationsvarningar) - Ett område inom vilket sjö-, militär- eller flygövningar utförs. Kallas även övningsområde.
RestrictedAreaRegulatory () - Ett specificerat land- eller vattenområde som utsetts av lämplig myndighet inom vilket tillträde eller navigering är begränsad i enlighet med vissa angivna villkor. Ett reglerat restriktionsområde är ett område där restriktionerna inte har någon direkt inverkan på ett fartygs navigering i området, utan inverkan på den verksamhet som kan ske inom området.
RestrictedAreaNavigational (motsvarar militära skyddsområden) - Ett specificerat land- eller vattenområde som utsetts av lämplig myndighet inom vilket tillträde eller navigering är begränsad i enlighet med vissa angivna villkor. Ett navigeringsområde är ett område där restriktionerna har en direkt inverkan på ett fartygs navigering i området.
PlaceOfRefugee (finns ingen motsvarighet i svenska vatten) - En plats där ett fartyg i behov av assistans kan vidta åtgärder för att det ska kunna stabilisera sitt tillstånd och minska farorna för navigering och för att skydda människors liv och miljön.
PiracyRiskArea (finns ingen motsvarighet i svenska vatten) - Ett område där det finns en ökad risk för pirater eller väpnat rån.



S-127 tillämpning

I huvudsak kan all information som omfattas av S-127 hänföras till olika verksamheter i Sjöfartsverket. S-127 är en framtida IHO standard som kan antas bli styrande för vilken information relaterat till Marine Traffic Management som förväntas exponeras från kuststater till fartyg m.fl. Av den anledningen finns det goda skäl för att inkludera föreslagna begrepp, definitioner och relationer mellan desamma, i Sjöfartsverket framtida informationsmodell för NTI. Projektet har egentligen inte funnit någon idag publicerad NTI information som inte låter sig beskrivas i S127 termer. Dock är vissa utav begreppen och definitionerna nya och kan vara svåra att förklara. S127 kommer vidare vara styrande för det meddelandeformat som en tänkt framtida NTI tjänst ska kunna leverera till andra maritima aktörer. Inte minst förväntas fartyg kunna konsumera formatet och visualisera detsamma i navigationssystemen ombord.
I detta projekt har också delar av informationen ur S127 visualiserats genom en intern karttjänst med syftet att öka förståelsen för personer som inte är bekanta med S100 standarder.
I nedanstående figur visas ett exempel på detta.



7.7.9 Mappning av S-127

Då mappningen är utförd i en arbetsbok i Excel så bifogar vi denna fil i detta dokument och distribuerar den tillsammans med filen för förstudien. Filen heter S127Mappning_draft.xlsx.

S127Mappning_draft.xlsx

7.8 Bilaga SOLAS regulation 2 samt regulation 9

" Regulation 2 - Definitions

For the purpose of this chapter:

1 Constructed in respect of a ship means a stage of construction where:

.1 the keel is laid; or

.2 construction identifiable with a specific ship begins; or

.3 assembly of the ship has commenced comprising at least 50 tonnes or 1% of the estimated mass of all structural material whichever is less.

2 Nautical chart or nautical publication is a special-purpose map or book, or a specially compiled database from which such a map or book is derived,

*that is issued officially by or on the authority of a Government, authorized Hydrographic Office or other relevant government institution and is designed to meet the requirements of marine navigation.**

3 All ships means any ship, vessel or craft irrespective of type and purpose.

** Refer to appropriate resolutions and recommendations of the International Hydrographic*

Organization concerning the authority and responsibilities of coastal States in the provision of charting in accordance with regulation 9."

"Regulation 9 - Hydrographic services

1 Contracting Governments undertake to arrange for the collection and compilation of hydrographic data and the publication, dissemination and keeping up to date of all nautical information necessary for safe navigation.

2 In particular, Contracting Governments undertake to co-operate in carrying out, as far as possible, the following nautical and hydrographic services, in the manner most suitable for the purpose of aiding navigation:

.1 to ensure that hydrographic surveying is carried out, as far as possible, adequate to the requirements of safe navigation;

.2 to prepare and issue nautical charts, sailing directions, lists of lights, tide tables and other nautical publications, where applicable, satisfying the needs of safe navigation;

.3 to promulgate notices to mariners in order that nautical charts and publications are kept, as far as possible, up to date; and

.4 to provide data management arrangements to support these services.

*3 Contracting Governments undertake to ensure the greatest possible uniformity in charts and nautical publications and to take into account, whenever possible, relevant international resolutions and recommendations.**

4 Contracting Governments undertake to co-ordinate their activities to the greatest possible degree in order to ensure that hydrographic and nautical information is made available on a world-wide scale as timely, reliably, and unambiguously as possible.

** Refer to the appropriate resolutions and recommendations adopted by the International Hydrographic Organization."*

5.4 SECOM Test Project – Final report

SECOM Test Project

Final report

Version 1.0

Content

Figures

1 SECOM Test Project

1.1 Purpose and expected outcome

The purpose is to test, validate and challenge the IEC 63173-2 SECOM standard (Maritime navigation and radiocommunication equipment and systems - Data interface - Part 2: Secure communication between ship and shore (SECOM)) draft and provide feedback to IEC TC80 WG17. The purpose is also to get more experience and example data by actually implementing the draft standard.

The expected outcomes from the project are

- feedback with recommendations to WG17 for improvement and stabilizing the SECOM standard. Completeness, Correctness, Consistency
- demonstrator, but not the primary goal
- example data and example commands
- bonus if the outcome is data and even a “simulator” or “reference service” that can support “Test methods and expected result” clauses and how a party can test if their equipment is compliant with SECOM

1.2 Interaction between SECOM Test Project and TC80 WG17

The main IEC working document (draft SECOM standard) is the common information source between the two groups. The task in SECOM Test Project is mainly to implement the latest edition of SECOM and provide feedback to WG17 for improvements. Feedback is given to WG17 in several ways; inserted in tasks before the meeting, inserted in discussion during meeting from common participants (SMA and Saab), and though written comments in IEC template.

From WG17 -> SECOM Task Project

- IEC working documenthttps://service.projectplace.com/pp/pp.cgi/r104620227
- Tasks(this document or meeting minutes from last meeting)
- Discussions items that are not tasks, but still would benefit from reality check(remarks in IEC document + questions and discussion excel)
- Timeplan(meeting minutes from last meeting)

From SECOM Test Project to WG17

- Comments and feedback on IEC Comment template. To be formally valid in WG17 they will probably need to be given by either SMA or Saab as participants in WG17.https://service.projectplace.com/pp/pp.cgi/r1622803181
- Increased knowledge and competence that is used during discussion on WG17 meetings and during WG17 tasks between meetings.

1.3 General

SECOM includes information services interfaces (APIs) for data exchange, information security measures by a SECOM PKI, communication channel security and data protection to enable secure communication. Further, SECOM includes interfaces for service discoverability as shown in Figure 1. The purpose with these included components is for SECOM to provide technical interoperability, where the same service interface is used for exchanging the information regardless of its operational use, up to the level of exchanging information securely online. Although designed for S-100 based products, SECOM is technically payload agnostic and applicable also for other types of data.

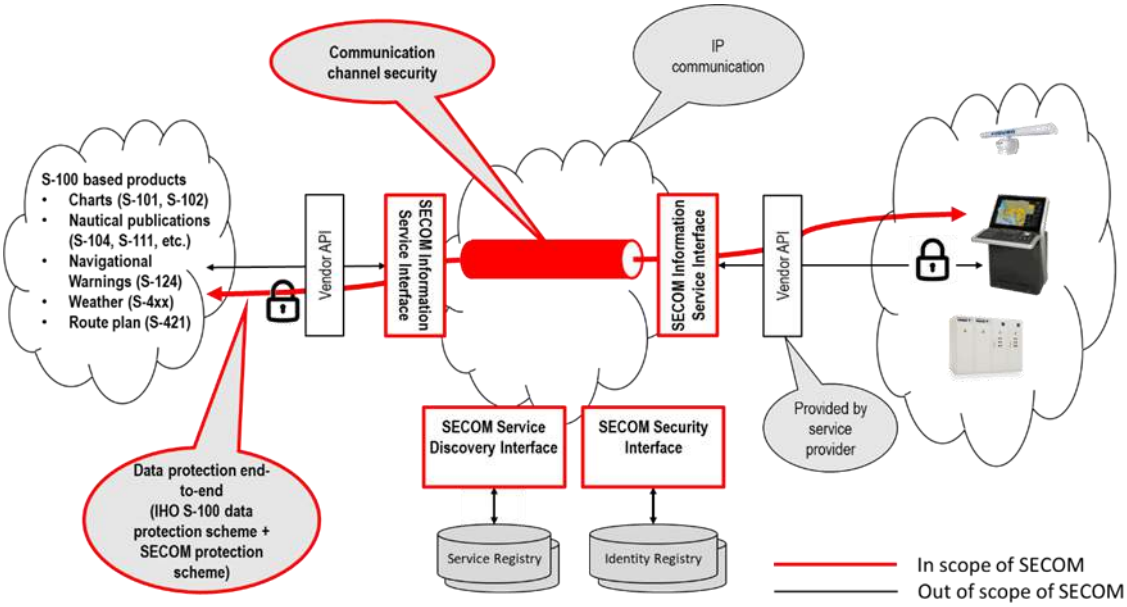


Figure 1 - Overview of SECOM

The SECOM Information service interface includes the public side exposed on the internet as depicted in Figure 1. The “last mile” links between a SECOM service instance and the end-user application is not defined and hence different solutions between the service instance and shore/ship’s system are possible.

SECOM information security contains communication channel security, a variant of PKI (Public Key Infrastructure) and data protection scheme alternatives for the information exchange with full or partial compliance with IHO S-100. The data protection scope is between end-users. SECOM PKI includes the definition of a set of service interfaces for key management.

The service discovery interface includes operations to search for service instances from a service registry to meet some criteria e.g. chart updates, navigational warnings, updated estimated time of arrival (ETA) information or route optimization services. The service discovery interface allows the user to choose a service instance to consume.

The information exchange between actors is bi-directional which means that both the ship/shipping company as well as shore authorities and private service providers can initiate the information

exchange and act as information provider. SECOM is thus applicable for both ship-to-shore and shore-to-ship communication.

1.4 Information security

1.4.1 Measures

SECOM contains several measures to meet the following quality attributes.

Authentication is a process by which a system verifies the identity of a user (human or machine) who wishes to access it (i.e. to confirm, you are who you claim to be, like a passport). This corresponds to the written signature and official stamp on paper. Authentication is achieved in SECOM on two levels; 1) Data authentication through the signature (SECOM data protection), and 2) Service authentication through the communication channel security and X.509 (RFC 5280 and RFC 2459) certificates (SECOM communication channel security). Authentication is dependent on unique identities which is achieved by SECOM PKI.

Integrity is achieved in SECOM by signing data where the checksum is part of the signature, described in SECOM data protection. The signing and verification of the signature is dependent on unique identities which is achieved by SECOM PKI.

Confidentiality is achieved in SECOM on two levels; 1) Data encryption according to SECOM data protection and S-100, and 2) Secure communication channel (transport security) for IP and HTTP through TLS and X.509 certificates, described in SECOM communication channel security.

Access control uses authorization which is the process of determining a set of permissions that is granted to a specific trusted identity. It is achieved in SECOM by the information owner authorizing access to chosen identities from the common identity registry, described in SECOM PKI. Only public interfaces are defined in SECOM (e.g. request access).

Identification is achieved in SECOM by the common registry for unique identities, bindings to asymmetric key pair and standardized API to SECOM PKI.

Non-repudiation i.e. a service intended to protect against the originator's false denial of having created the content of a message and of having sent a message, is achieved in SECOM by signing the data with the private key.

1.4.2 SECOM PKI

SECOM PKI (Public key infrastructure) describes the common interface for key management and the expected functionality to provide the binding between identity and key used for signing data and authentication in service interaction.

A SECOM PKI contains an identity registry governed by its scheme administrator. There can be several instances of SECOM PKI provided by multiple scheme administrators. An actor can participate/be registered in several instances of SECOM PKI. SECOM compatible equipment is expected to support multiple instances of SECOM PKI.

SECOM does not specify which instance of identity registry to use, and SECOM does not define or constrain number of identity registries.

1.4.3 Communication channel security

When consuming service instances according to SECOM, the internet transport shall be protected with TLS and valid certificates from trusted party as stated in SECOM communication channel security. The protection of the channel is a complement to the protection of the data itself and is necessary to be included to secure also other service requests, such as subscription request, access request and notifications. The SECOM communication channel security describes the usage of certificate obtained from a trusted identity registry and thereby enables authentication on the service interaction itself as depicted in Figure 2.

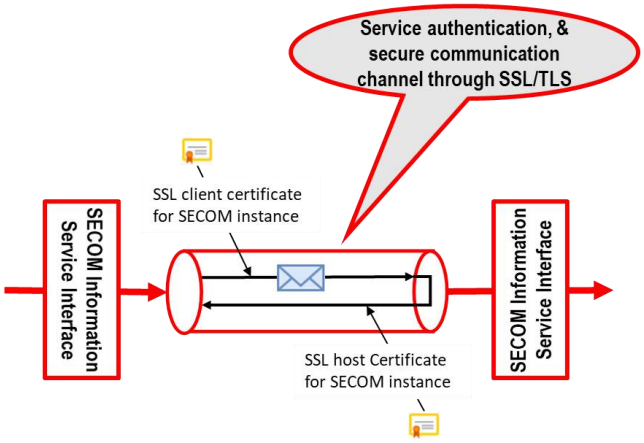


Figure 2- Secure communication channel

The SECOM communication channel security relies on a SECOM Public Key Infrastructure (SECOM PKI) or Public-Private Key management using X.509 Certificates to exchange the keys.

The SECOM communication channel security scheme does not comprise the “last mile” links between the SECOM information service interface and the end-user application.

1.4.4 Data protection

Data protection includes both signing of data for authentication and integrity (digital signature), and optionally encryption of data for confidentiality. Data protection is aligned with the IHO data protection scheme (IHO S-100 part 15).

The digital signature contains both the checksum used to check integrity of received data and claimed identity for data authentication. The verification of the signature includes access to common Public Key Infrastructure (PKI) where the public key for claimed identity can be downloaded. Whenever data is exchanged, the digital signature shall always be attached and verified as close to the end user as possible. This gives the basic data end-to-end protection, see Figure 1.

The optional encryption of data uses a common protection scheme and offers two alternatives for encryption key management: 1) the existing encryption key management with permits for ENC data, such as IHO, can be used with SECOM information service interface and 2) SECOM also includes its own encryption key management that is specially designed for more dynamic data exchange ship to shore and shore to ship, such as route plan exchange. In the SECOM data protection scheme, the sender of classified data creates a temporary encryption key which is transferred securely before the encrypted data is transferred. The temporary encryption key is encrypted with a symmetric key derived from the

sender's private key and the receiver's public key, the same key as used for authentication, thus can only be decrypted by the actor having the private key in its possession. The receiver's public key if not already present, can be retrieved from the receiver's SECOM interface PublicKey or from the SECOM PKI interface GetPublicKey. This requires a strong key pair long enough for encrypting and decrypting the encryption key.

The data protection described above only protects the data part in the message. To secure the complete message, an additional signature is added, an envelope signature that includes all information of the envelope contained in the uploadObject, including the data and its dataSignature. The parts of the message that are protected by the different signatures are illustrated in Figure 3.

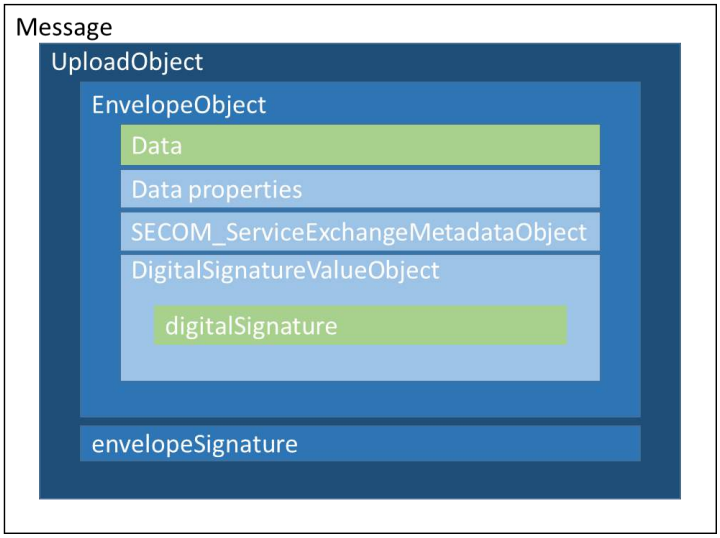


Figure 3 – Illustration of what parts of the message that are protected by the two signatures

Another rationale for introducing an envelope signature is to facilitate complete message integrity check at the receiving SECOM service instance side thus prohibiting forwarding of corrupt messages during the last mile to the receiver, see Figure 4 below.

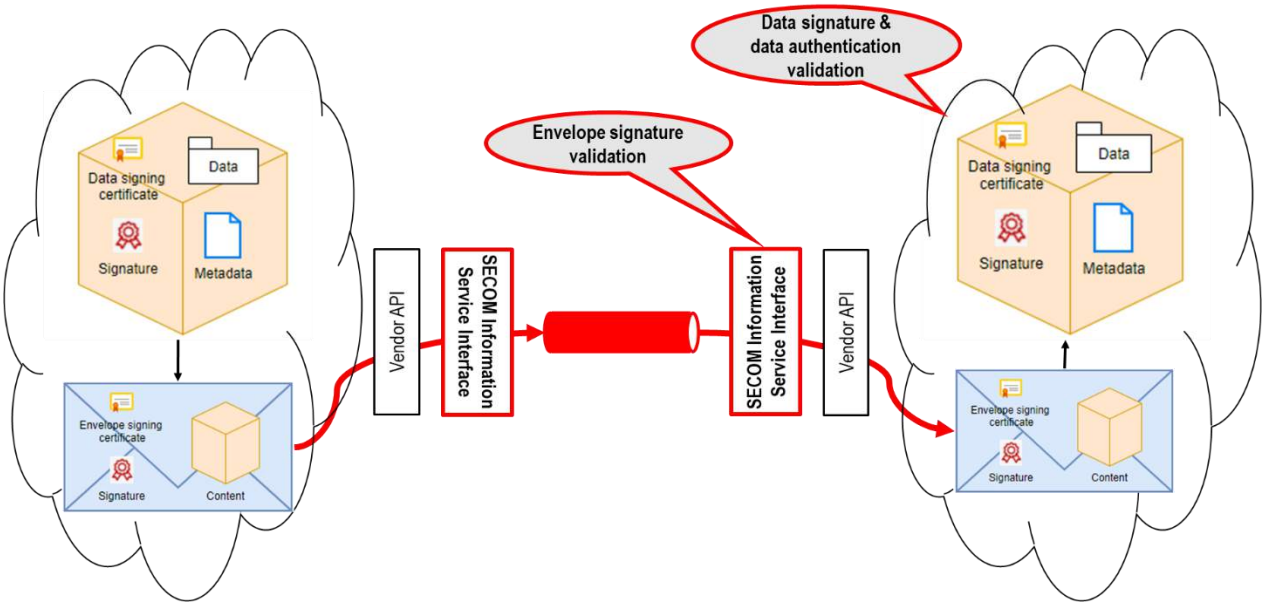


Figure 4 - Envelope and data validation

The SECOM data protection scheme relies on a SECOM public key infrastructure (SECOM PKI) using X.509 certificates to exchange the keys. The private key is generated by the actor and stored internally while the public key is securely uploaded to a SECOM PKI and attached to the identity.

The data protection scheme and the thumbprint of the root certificate indicates the identity registry used in the specific data exchange. The trusted root certificates identified with their thumbprints are expected to be stored in a local trust store.

1.4.5 Certificate revocation status

A Certificate revocation list (CRL) is a list of revoked certificates that is downloaded from the Certificate authority (CA). Online certificate status protocol (OCSP) is a protocol for checking revocation of a single certificate interactively using an online service called an OCSP responder.

1.5 Service Discoverability

To support dynamic use of services, a SECOM service discovery interface has been defined. The intended operational usage is to make it possible for both officers onboard ships and operators ashore to search for service instances to interact with. Some examples from an onboard perspective are a ship that wants to find a provider of route optimization services or a VTS along the intended route to share the route plan with or providers of navigational warnings or Electronic Navigational Charts (ENC). From a shore-based perspective it is possible to search for registered ships targeted for information requests such as required reporting information, intended route or estimated arrival time. The SECOM service discovery contains common interfaces for discovery of service instances.

A standardized interface for finding service instances reduces the need to support several different proprietary and company specific interfaces. Further it facilitates increased stability of the implementation, i.e. no new implementation and certification is necessary if a new service registry is used.

SECOM does not specify which service registry to use, and SECOM does not define or constrain the number of service registries, hence there can be several providers of service registries.

SECOM defines only the interface for discovery of service instance, not the registration of service instances in the service registry. This needs to be described by the provider of the chosen service registry.

In order for a provider of a service registry to be compliant with SECOM, SECOM's Service Discoverability interface defines the requirements on such implementation and thus, what information is expected to be exchanged.

1.6 Examples of questions

1) How does the signing request to SECOM PKI work?
2) What are the SECOM requirements for the asymmetric keys in PKI?
3) What are the SECOM requirements for the encryption key
4) How to exchange the encryption key?
5) How to use keys from e.g. PRIMAR with SECOM solution?
6) How to relate keys for signing data to keys for TLS encryption e.g. for a ship, for a VTS?
7) Shall SECOM Communication Channel Security and service authentication be based on TLS and X.509 Certificates or OpenID, HMAC or other standard using the HTTP Headers instead?
8) What are the requirements, and are they met, on SECOM Service Discovery Interface?

1.7 Overview of Test Objectives

The following Test Objectives have been identified as candidates for the SECOM Test Project.

Test Objective	Description/ rationale	SECOM solution	Test case(s)
1. Message integrity	Ensures the complete message is unchanged between SECOM services	Envelope signing	1
2. Data integrity*	Data integrity ensures the data transmitted is accurate and consistent	Data signing	1
3. Transport confidentiality	Ensure communication channel protection between SECOM services	Channel encryption (TLS)	1, 2
4. Data protection	Data protection ensures information is confidential except for the intended recipient	Data encryption (AES)	2
5. Service identity	Support SECOM service identification	Service certificate authentication (X.509 PKI)	1, 3
6. Client identity*	Support client identification	End user client certificate authentication (X.509 PKI)	1, 3
7. Client authorization	Support and facilitate client access to information	Service authorization	11
8. Bandwidth optimization	Minimize size of data package sent to reduce required bandwidth	Data compression (GZIP, Deflate)	5
9. Large message transfer	Facilitate large message transfer i.e. message sizes > 350 kB	Link to data facilitated by interfaces Upload Link, Get By Link	4
10. Closed loop communication	Notification of message received/ read etc. to ensure dialogue between end-user applications.	Acknowledgement message (acknowledgement interface)	6
11. Service discoverability	Search for services by means of service metadata. In order to locate relevant services for consumption.	Service registry lookup (Search Service interface)	12
12. Information push	Share information by uploading data to a service	Service interface to receive uploaded information (Upload interface)	2
13. Information pull	Retrieve information by downloading data from a service	Service interface to retrieve information (Get interface)	1
14. Subscribe to data	Subscribe to information to receive subsequent updates	Service interfaces for Subscription request, remove & notify	7
15. Service information	To facilitate information wrt service accepted payloads, endpoints and information objects.	Service capability interface and Get Summary interface	8
16. Service condition	Contextual service status to check service operation.	Ping interface for checking last interactionTime with end user application and SECOM service status	9

17. Payload agnostic service	Caters for exchanging payloads of different types	To be investigated	13

* Data integrity and client identity test objectives are only relevant if SECOM PKI is used for end user client certificates.

1.8 Overview of Test Cases

The following Test Cases have been identified to cover previously described test objectives.

Test Case	Name	Interface	Test objectives	Testbed target
Test Case 1	Data protection (signing) of unclassified data	Upload	1, 2, 3, 5, 6, 13	Testbed B
Test Case 2	Data protection of classified data (signing and encryption)	Get, EncryptionKey	1, 2, 3, 4, 5, 6, 12	Testbed B
Test Case 3	SECOM PKI			Testbed B
Test Case 4	Exchange Large Data	Upload Link, Get By Link	9	Testbed B
Test Case 5	Exchange compressed data	Upload	8	Testbed B
Test Case 6	Closed loop communication	Acknowledgement	10	Testbed B
Test Case 7	Subscribe to data	Subscription request, remove & notify	14	Testbed B
Test Case 8	Service information	Capability, Get Summary	15	Testbed B
Test Case 9	Service status	Ping	16	Testbed B
Test Case 10	Cyber Security Review			Testbed B
Test Case 11	White list and access request	Access	7	Testbed B
Test Case 12	Service Discovery	Search Service	11	Testbed B
Test Case 13	Exchange several different types of payloads	Capability, Upload, Get	17	Testbed C

2 Testbed

2.1 General

Three testbeds, called Testbed A, Testbed B and Testbed C, have been defined for this project. The functionality and connectivity is increased in each testbed.

The first step (Testbed A) is local implementation and email for connectivity.

Second step (Testbed B) is still local implementations with local services as intermediate step. Perhaps this testbed will be the closest design for the Test methods described in SECOM.

Third step (Testbed C) is local implementation connected through services and internet with adequate protection according to SECOM.

2.2 Testbed A

2.2.1 Description

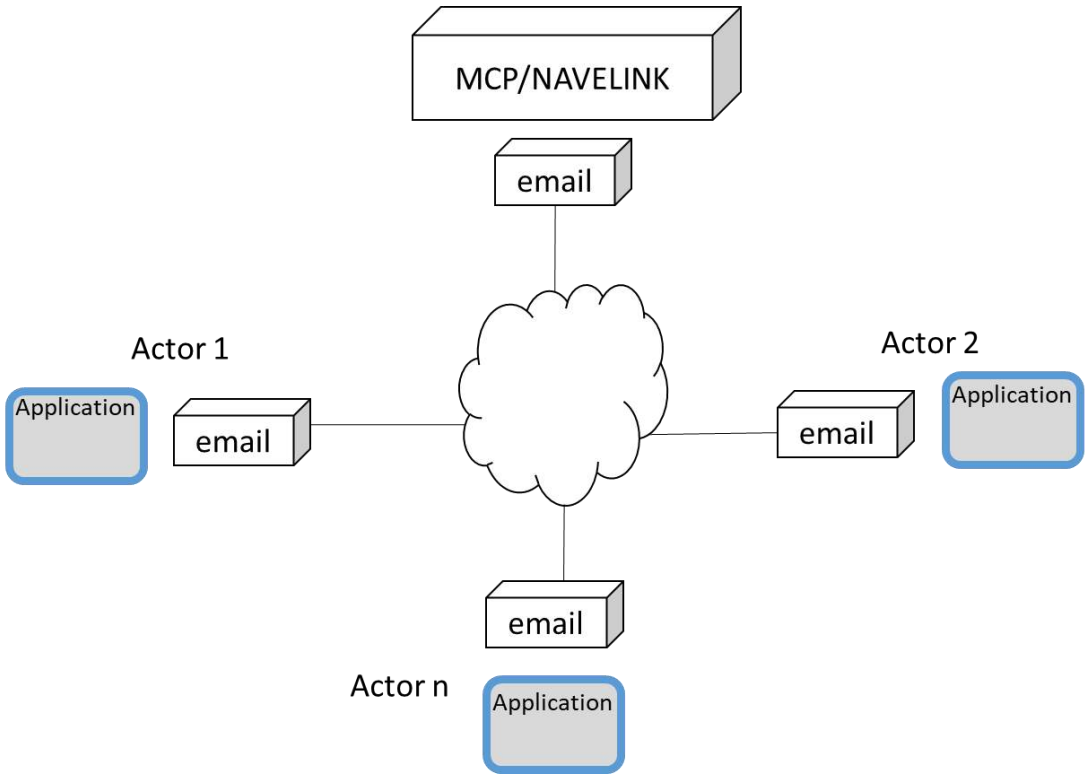
The purpose with testbed A is to test SECOM Data Protection Scheme.

PKI in the testbed

The approach is to use MCP and Navelink as far as possible as PKI system. Where SECOM goes beyond MCP/Navelink, manual commands using e.g. openssl need to be used.

- SMA creates a Service ID called “SECOM SMA Test Service ID” and issues certificate for that entity. The public certificate (Download the public part) is then emailed to Saab.
- Saab creates a Service called SECOM-SAAB and issues certificate for that entity. The public key/certificate is then emailed to SMA.

MCP/Navelink cannot today provide all public keys to other than user within same organization, hence public keys between organizations need today be mail around.



2.2.2 Functionality in the testbed

The following functionality is required in the testbed:

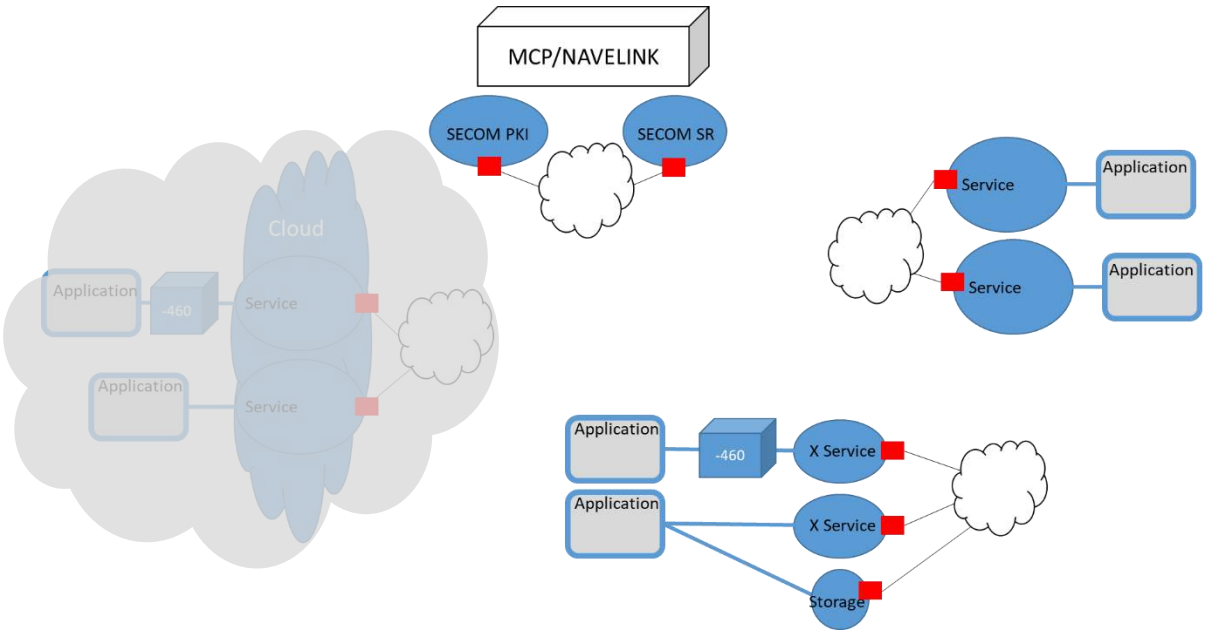
1. Create Signature on a payload
    - Calculate checksum according to SECOM (S-100)
    - Encrypt checksum with own private key
2. Exchange payload and SECOM_ExchangeMetadata objects
3. Verify signature
    - Retrieve public keys for claimed identity
4. Encrypt payload
    - Generate secret key
    - (compress data)
    - Encrypt data
5. Compress data
6. Exchange secret key
    - Encrypt secret key (RSA or ECC, diffie-hellman or similar)
    - Sign secret key
7. Decrypt payload
    - Receive secret key
    - Verify signature
    - Decrypt secret key
    - Decrypt data
    - (uncompress data)
8. Uncompress data

2.3 Testbed B

2.3.1 Description

The purpose with Testbed B is to test SECOM Data Protection in combination with SECOM transport security and SECOM service interface within each partners own environment.

Testbed B is an intermediate test bed before achieving Testbed C, but also a “plan B” if firewalls and connection between partners for some reason fails.



2.3.2 Functionality in the testbed

See Testbed C for list of functionality.

This testbed might be the testbed closest to what can/will be used in Test methods in SECOM.

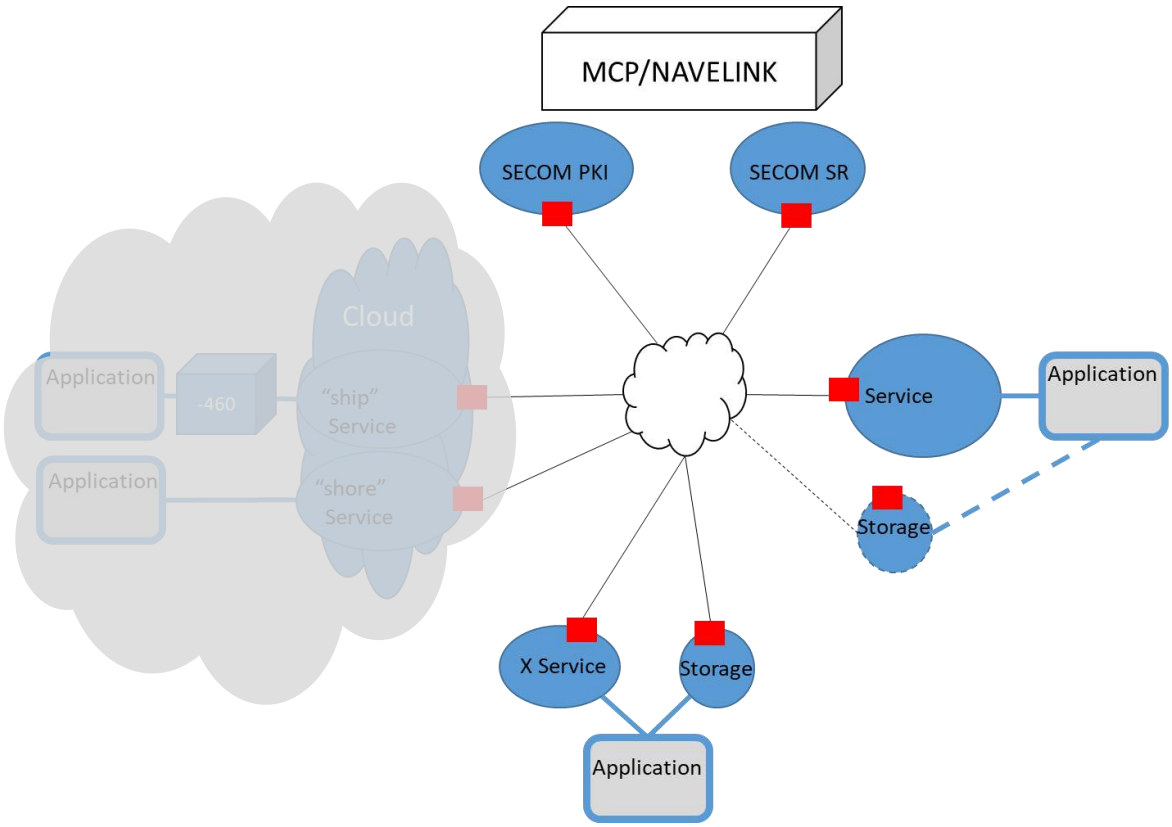
2.3.3 Requirements and input

- IEC 63173-2 SECOM
    - Annex X: OpenAPI (swagger)

2.4 Testbed C

2.4.1 Description

The purpose with Testbed C is to test SECOM Data Protection in combination with SECOM transport security and SECOM service interface and connections across different organizations networks.



2.4.2 Functionality in the testbed

The following functionality is required in the testbed:

1. *Create Signature on a payload*
    - *Calculate checksum according to SECOM (S-100)*
    - *Encrypt checksum with own private key*
2. *Exchange payload and SECOM_ExchangeMetadata objects*
3. *Verify signature*
    - *Retrieve public keys for claimed identity*
4. *Encrypt payload*
    - *Generate secret key*
    - *(compress data)*
    - *Encrypt data*
5. *Compress data*
6. *Exchange secret key*
    - *Encrypt secret key (RSA or ECC, diffie-hellman or similar)*

- *Sign secret key*

7. *Decrypt payload*
    - *Receive secret key*
    - *Verify signature*
    - *Decrypt secret key*
    - *Decrypt data*
    - *(uncompress data)*
8. *Uncompress data*
9. Expose (provide) deployed and consumable service interface **OBS! Discuss which interfaces that need logic.**
    - Upload
    - Upload Link
    - Get Summary
    - Get
    - Get by Link
    - Acknowledgement
    - Subscribe
    - Remove subscription
    - Subscription notofication
    - Request Access
    - Access Notification
    - Capability
    - Ping
    - EncryptionKey
10. Consume service interface
11. Transport Security and Service Authentication
    - Encrypt traffic
    - Authenticate client in service call
    - Decrypt traffic
12. Send Sign request
    - Create signing request
    - Call SECOM PKI Signing Request (secure, authentication)
13. Search for service to consume
14. SECOM PKI: Provide Public Keys
15. SECOM PKI: Handle Signing request
    - Authentication
    - Handle Signing request and store Public Key
16. SECOM Service Registry: Handle search request for service

3 Test Case 1 - Data protection (signing) of unclassified data

3.1 Description

The test case focus on exchange of unclassified signed data, and the verification and authentication of the signature.

3.1.1 Test objectives

- Message integrity
- Data integrity
- Transport confidentiality
- Service identity
- Information push

3.1.2 Acceptance Criteria

Message integrity verified by comparing calculated envelope signature with the corresponding received signature.

Data integrity can be validated in the SECOM instance provided the end-user application public certificate is issued by SECOM PKI. In other cases the data integrity has to be validated in the end-user application which out of scope for SECOM.

Transport confidentiality verified by establishing an encrypted channel using SECOM PKI issued SSL host certificates.

Service identity verified against SECOM PKI using provided “client” certificate received in TLS session.

Information push achieved by successful data uploaded.

3.1.3 Test Scenarios

Actor A shall send one data object (XML) to Actor B. Actor A decides that the information is unclassified. The data is encapsulated into an UploadObject ready to be exchanged as body to a SECOM Upload Service Interface.

3.1.4 Test Environment

Testbed B

3.1.5 Test tools

OpenSSL, Notepad++

3.1.6 Test data

Steps to prepare **unclassified** and **uncompressed** data.

The data in this example is one RTZ.

3.1.7 Test procedure

SENDER

Step	Commands	Result
Actor A		
Select data file		data-1.rtz
Convert to Base64	openssl base64 -A -in data-1.rtz -out data-1.rtz.base64	data-1.rtz.base64
Select Private Key		PrivateKey_SECOM_SMA_Test_Service_ID.pem
Create signature using original data file (data-1.rtz)	openssl dgst -sha256 -sign PrivateKey_SECOM_SMA_Test_Service_ID.pem data-1.rtz > data-1.rtz.sig	data-1.rtz.sig
Convert signature to HEX	xxd -u -ps -c 120 data-1.rtz.sig > data-1.rtz.sig.hex	data-1.rtz.sig.hex
Select Public Certificate for the data object		Certificate_SECOM_SMA_Test_Service_ID.pem
Select envelope public certificate		EnvelopeCertificate.pem
Set other metadata values for the EnvelopeUploadObject		Envelope.json
Sign envelope		Envelope.sig
Add envelope signature to upload object		
Create Upload Object in JSON		UploadObject-1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Upload	POST URL/v1/object {body} : return	

RECEIVER

Verify Signature(s) and restore data

Step	Commands	Result
SECOM B		
Receive …		UploadObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Parse envelope		uploadObject.Envelope
Convert to byte[]		Envelope[]
Authenticate data and claimed public key	Verify envelope signature	True/false
Store (inform Actor B OEM) incoming object		UploadObject-1.json

Actor B		
Parse and store data from object		data.rtz.base64
Parse and store signature from object		data.sig.hex
Restore signature from HEX	xxd -r -u -ps data.sig.hex > data.sig	data.sig
Parse and store public certificate from object		publicCert.pem
Identify Root Certificate through the Thumbprint		mc-ca-chain_staging.pem
Verify Certificate	openssl verify -CAfile mc-ca-chain_staging.pem publicCert.pem > publicCert.pem.verification	publicCert.pem.verification
Extract public keys from certificate	openssl x509 -in publicCert.pem" -pubkey -noout > publicCert_key.pem"	publicCert_key.pem
Restore data from Base64 to original	openssl base64 –A -d -in data.rtz.base64 -out data.rtz	data.rtz
Verify signature i.e. compare signature with original data file	openssl dgst -sha256 -verify publicCert_key.pem -keyform pem -signature data.sig data.rtz > data.sig.verification	Verified OK
Compare received data with restored data	Open received data.rtz and restored data.rtz (Notepad++ Compare Plugin)	Received data unchanged

3.1.8 Sequence diagram

Figure 5 describes the dynamic use of the Upload interface.

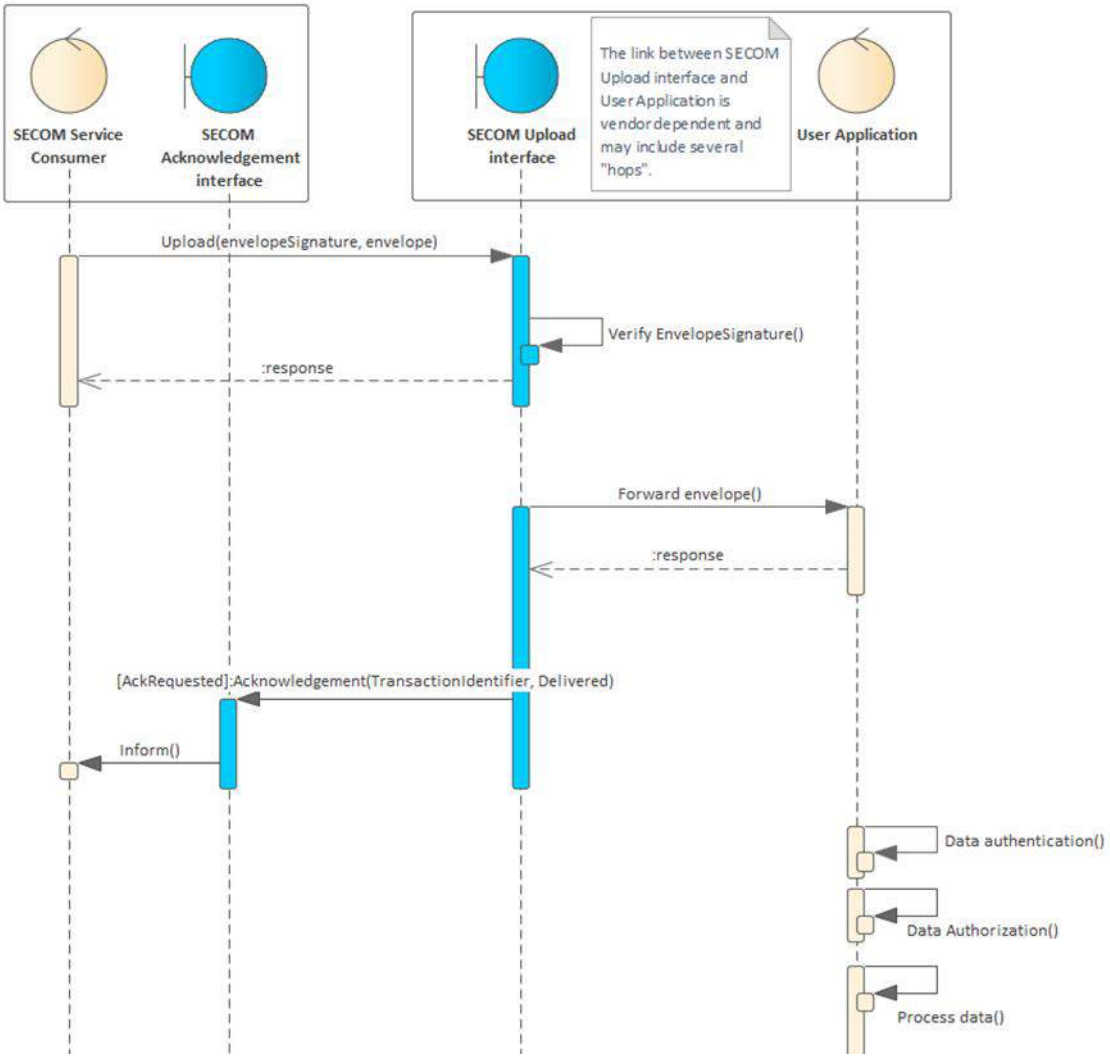


Figure 5 – Sequence diagram for upload signed unclassified data

3.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Sign envelope	Complete message integrity not implemented.	Message integrity is important to prohibit forwarding of corrupt messages in last mile communication and to reduce bandwidth usage.	Introduce message envelope with corresponding envelopeSignature.

Set other metadata values for the EnvelopeUploadObject	Timeliness of message signed is not considered.	Lacking a timestamp for when the message was signed might create confusion if messages are intentionally or unintentionally delayed on the receiver side.	Include optional envelopeSignatureTime in EnvelopeUploadObject to indicate when the envelope was signed.
Set other metadata values for the EnvelopeUploadObject	Attribute data type values might differ in various OS/ languages.	There is a need to agree on attribute data types used in SECOM to ensure interoperability.	Introduce S100 basic data types to have a common description.
Sign envelope	Signature not consistent in different implementations	Order for attributes important when creating the EnvelopeUploadObject to be signed.	The order of each added attribute is achieved by adding the attribute names in the order the attributes appear in each object.
Create UploadObject in JSON	Conversion of keys to JSON format is implementation specific.	The conversion of keys to JSON need to be agreed upon.	Minify keys to create a uniform way of sending keys in JSON format. To secure interoperability in different OS.
Receive …	Deserialization issue, not consistent between different implementations	Attribute data type issue and ordering important to be able to verify signature at the receiving end.	Introduce S100 basic data types and ordering according to the order the attributes appear in each object.

3.3 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
Message integrity	Envelope signature creation and verification	Depends on OS and implementation for consistency between services.	Introduce envelope, envelopeSignature and envelopeSignatureTime, ordering according to the order the attributes appear in the EnvelopeUploadObject,

			commonly defined data types and rules for serialization of JSON uploadObject.
Data integrity	Data signature creation and verification	If created in SECOM PKI this can be validated in the SECOM service instance.	Introduce ordering according to the order the attributes appear in each the DigitalSignatureValueObject.
Transport confidentiality	TLS using PKI issued SSL certificates	Can be an issue if SSL certificates are self-signed, hence not possible to use in certain implementations (Azure).	Suggest to use official CA issued certificates.
Service identity	Received service instance “client” certificate	Mutual authentication on service instance level by using exchanged SECOM PKI certificates.	Important to agree beforehand on entities in certificate information for “Subject distinguished name” for authentication purposes.
Information push	Upload interface	Response code if total base 64 encoded message exceeds web server maximum message size missing.	Introduce response code 413 / message if uploaded message > maximum message size (350 kB).

4 Test Case 2 - Data protection of classified data (signing and encryption)

4.1 Description

The test case focus on exchange of classified signed data. The verification and authentication of the signature is outlined in test case 1 above.

Publish and get encrypted data

4.1.1 Test objectives

- Data protection
- Information pull

4.1.2 Acceptance Criteria

Data protection can be validated in the SECOM instance provided the end-user application certificates are issued by SECOM PKI. In other cases the data protection has to be validated in the end-user application which is out of scope for SECOM.

Information pull achieved by successful data downloaded.

4.1.3 Test Scenarios

Actor A shall retrieve one data object (XML) from Actor B. Actor B decides that the information is classified. The data is encapsulated into a GetResponseObject ready to be exchanged as a response to a SECOM Get Service Interface.

Actor B requests the public certificate from Actor A for symmetric key derivation used to protect the temporary encryption key during transfer.

The data protected by an encryption key is exchanged using the SECOM EncryptionKey service interface of Actor A.

4.1.4 Test Environment

Testbed B

4.1.5 Test tools

OpenSSL, Notepad++

4.1.6 Test data

Steps to prepare **classified** and **uncompressed** data.

The data in this example is one RTZ.

4.1.7 Test procedure

4.1.7.1 Actor A requests data and Actor B responds with signed encrypted data

SENDER

Actor A issues a Get request to pull data from Actor B's published information.

Step	Commands	Result

Actor A		
Request published encrypted information		
Set filter values for the Get request	Assign values to parameters in the GetFilterObject	dataProductType = RTZ, validFrom = 20210412T101530 validTo = 20210420T101530
Create GetFilterObject in JSON		GetFilterObject -1.json
SECOM A		
Add client certificate Actor A		Certificate_ActorA.pem
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Get	GET URL/v1/object?parameters : return	

RECEIVER

Actor B decides the information requested is classified and returns the information to actor A encrypted.

Step	**Commands**	**Result**
SECOM B		
Receive …		Get request handled
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Actor B		
Retrieve and encrypt data for all available information objects authorized to actor A		
Select data file		data-1.rtz
Base64 encode, sign and HEX conversion of the signature is made according to Test case 1	…	data-1.rtz.sig.hex
Encrypt data	openssl enc -aes-256-cbc -in data-1.rtz -out data-1.rtz.enc -pass file:encryptionKey.bin -salt	data-1.rtz.enc
Convert data to Base64	openssl base64 -in data-1.rtz.enc -out data-1.rtz.enc.base64	data-1.rtz.enc.base64
Create Get response object in JSON GetResponseObject		GetResponseObject.json
Respond with response code 200 and data according to GetResponseObject		

4.1.7.2 Actor A requests the encryption key, actor B responds asynchronously with the encrypted symmetric key

SENDER

Actor A requests the encryption key by data reference id and its public certificate used for symmetric key derivation.

Step	**Commands**	**Result**
SECOM A		
Receive		GetResponseObject deserialized
Store (inform Actor A OEM) incoming object		GetResponseObject -1.json
Actor A		
Evaluate data Protection for received data	Evaluate dataProtection attribute in SECOM_ExchangeMetadataObject	dataProtection = true
Received data is protected, request encryption key from Actor B		
Set reference to received data in GetResponseObject		dataReference = UUID
Add client certificate for Actor A to the request		publicCertificate = Certificate_ActorA.pem
Set remaining attributes for the encryptionkey request	EncryptionKeyNotificationObject	EncryptionKeyNotificationObject – 1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api EncryptionKey	POST URL/v1/encryptionkey/notify {body} : return	

RECEIVER

Actor B receives the encryption key request, derives the symmetric key and responds asynchronously with the encrypted encryption key.

Step	**Commands**	**Result**
SECOM B		
Receive and acknowledge encryption key request		EncryptionKeyNotificationObject deserialized

Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Parse envelope		EncryptionKeyNotificationObject.Envelope
Convert to byte[]		Envelope[]
Authenticate data and claimed public key	Verify envelope signature	True/false
Store (inform Actor B OEM) incoming object		EncryptionKeyNotificationObject-1.json
Respond with response code 202 - Notification received		
Actor B		
Derive shared key for encryption of the encryption key and upload to actor A.		
Extract public key from Actor A public certificate	openssl x509 –in Certificate_ActorA.pem -pubkey -noout > PublicKey_ActorA.pem	PublicKey_ActorA.pem
Derive shared key for pair	$sharedKey = openssl pkeyutl -derive -inkey PrivateKey_ActorB.pem -peerkey PublicKey_ActorA.pem	$sharedKey
Create initialization vector in hex format	$iv = openssl rand -hex 128	$iv
Convert initialization vector to Base64	$ivbase64 = openssl enc -base64 <<< $iv	$ivbase64
Encrypt encryption key with derived shared key for pair and created initialization vector	openssl enc -aes-256-cbc -salt -p -K $sharedKey -iv $iv -e -in encryptionKey.bin -out encryptionKey.bin.enc	encryptionKey.bin.enc
Convert encrypted encryption key to Base64	openssl base64 -in encryptionKey.bin.enc -out encryptionKey.bin.enc.base64	encryptionKey.bin.enc.base64
Create Digital Signature for the encryption key	openssl dgst –sha256 –sign PrivateKey_ActorB.pem encryptionKey.bin > encryptionKey.bin.sign	encryptionKey.bin.sign
Convert Digital Signature for the encrypted Secret Key to hex format	xxd -u -ps encryptionKey.bin.enc.sign > encryptionKey.bin.enc.sign.hex	encryptionKey.bin.sign.hex
Set attribute encryptionKey in EnvelopeKeyObject		encryptionKey = encryptionKey.bin.enc.base64
Set attribute iv in EnvelopeKeyObject		iv = $ivBase64
Set attribute transactionIdentifier in EnvelopeKeyObject		transactionIdentifier = UUID
Set the attribute digitalSignature in DigitalSignatureValueObject		digitalSignature = encryptionKey.bin.sign.hex

Set remaining attributes in EncryptionKeyObject	EncryptionKeyObject	EncryptionKeyObject – 1.json
SECOM B		
Add client certificate Actor B		Certificate_ActorB.pem
Verify receiver host certificate SECOM A	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor A SECOM Api EncryptionKey	POST URL/v1/encryptionkey {body} : return	

4.1.7.3 Actor A receives the encryption key and decrypts received data

SENDER

Actor A receives the encryption key and decrypts the message received in 5.1.7.1

Step	**Commands**	**Result**
SECOM A		
Receive…		EncryptionKeyObject deserialized
Authenticate sender	Verify client cert for Actor B from TLS against SECOM PKI	True/false
Parse envelope		EncryptionKeyObject.Envelope
Convert to byte[]		Envelope[]
Authenticate data and claimed public key	Verify envelope signature	True/false
Store (inform Actor A OEM) incoming object		EncryptionKeyObject – 1.json
Actor A		
Identify correlating data received in Get response, verify signatures and decrypt data received in Get response		
Verify signature…		
Extract public key from Actor B public certificate	openssl x509 –in Certificate_ActorB.pem -pubkey -noout > PublicKey_ActorB.pem	PublicKey_ActorB.pem
Convert Digital Signature for the encryption key from hex format	xxd -r -u -ps encryptionKey.bin.sign.hex > encryptionKey.bin.sign	encryptionKey.bin.sign
Verify signature i.e. compare signature for encryption key with received digitalSignature	openssl dgst -sha256 -verify PublicKey_ActorB.pem -keyform pem -signature encryptionKey.bin.sign encryptionKey.bin	Verified OK

Restore and decrypt encryption key…		
Restore EncryptionKey from Base64 to original	openssl base64 –A -d -in encryptionKey.bin.enc.base64 -out encryptionKey.bin.enc	encryptionKey.bin.enc
Restore Initialization vector from Base64 to original	$iv = openssl base64 –A -d -in iv.base64	$iv
Derive shared key for pair	$sharedKey = openssl pkeyutl -derive -inkey PrivateKey_ActorA.pem -peerkey PublicKey_ActorB.pem	$sharedKey
Decrypt encryption key with derived shared key for pair and received initialization vector	openssl enc -aes-256-cbc -salt -p -K $sharedKey -iv $iv -d -in encryptionKey.bin.enc -out encryptionKey.bin	encryptionKey.bin
Decrypt received data…		
Restore received data in Get response from Base64 to original	openssl base64 –A -d -in data-1.rtz.enc.base64 -out data-1.rtz.enc	data-1.rtz.enc
Decrypt data	openssl enc -salt -aes-256-cbc -d -in data-1.rtz.enc -out data-1.rtz -pass file: encryptionKey.bin -salt	data-1.rtz
Compare received data with restored data	Open received data-1.rtz and restored data.rtz (Notepad++ Compare Plugin)	Received data unchanged

4.1.8 Sequence diagram

4.1.8.1 Actor A requests data and Actor B responds with signed encrypted data

Figure 6 and Figure 7 describe the dynamic behavior of the Get interface.

The Get interface is used to pull data from an actor's published information. The service request contains filtering parameters that allows the information owner to search and prepare data to be returned. Once the authentication of the requester has been verified, the preparation of data includes authorization check against internal access control list and packaging the data with data signatures. If access is accepted, the requested data is returned, if not, an error messages is given.

If the information owner decides to publish protected data, the consumer needs a possibility to request the encryption key if not already available, to be able to decrypt the protected data.

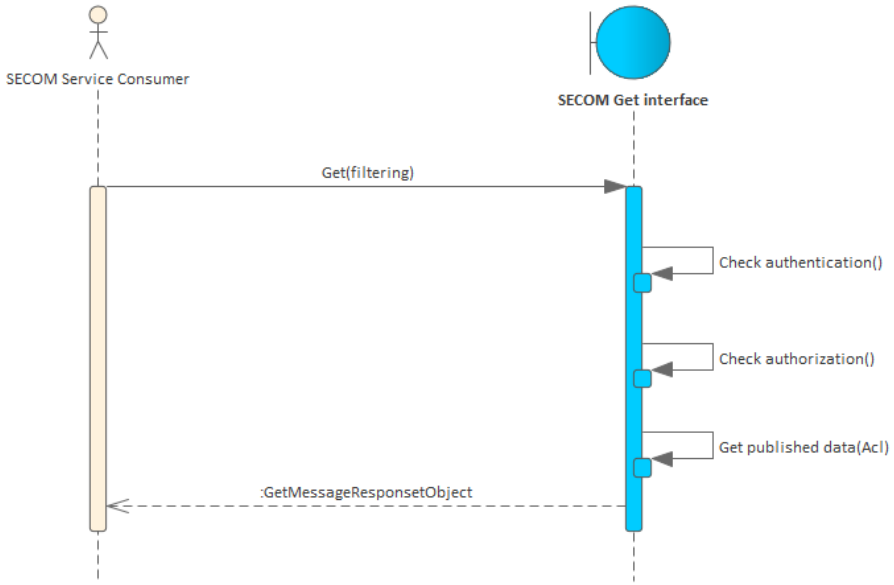


Figure 6 - Sequence diagram for Get interface

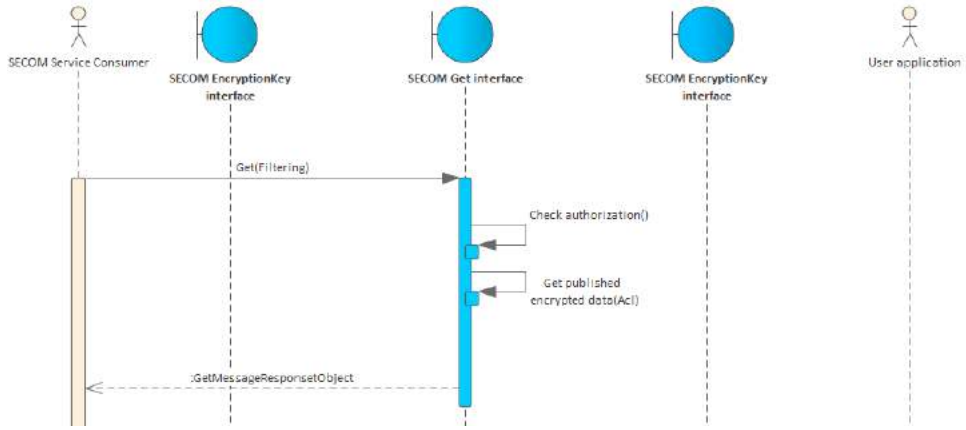


Figure 7 - Sequence diagram for Get interface and classified data

4.1.8.2 Actor A requests the encryption key, actor B responds asynchronously with the encrypted symmetric key

The consumer requests the encryption key by data reference id and its public certificate used for symmetric key derivation. The information owner encrypts the random key used when encrypting the data with a symmetric key derived from the consumer's public key and its own private key. The information owner sends the protected random key via the consumer's SECOM Encryption Key interface.

Figure 8 and Figure 9 describes the dynamic behavior of the EncryptionKey service interface.

The information owner decides to protect the information and generates a random key and initialization vector which are used to encrypt the data. In order for the information consumer to decrypt the data, the random key is protected using a derived symmetric key using the information consumer's public certificate together with the information owner's private key. The encrypted random key is signed and the random key, initialization vector, signature and the information owner's public key are put in the payload object and uploaded to the information consumer's EncryptionKey interface. See Figure 8.

The information owner decides to publish protected information and internally stores the generated random key and initialization vector. The service consumer retrieves the protected encryption key by notifying the information owner through his SECOM EncryptionKey notification interface. The information owner protects the encryption key with a derived symmetric key, derived using the publicKey from the notification request body together with its own private key. The encryption key is encrypted with the derived key and the encrypted encryption key is signed and sent to the service consumer's SECOM EncryptionKey interface. Finally the consumer gets the encryption key from its SECOM instance and can decrypt the retrieved protected information. See Figure 9.

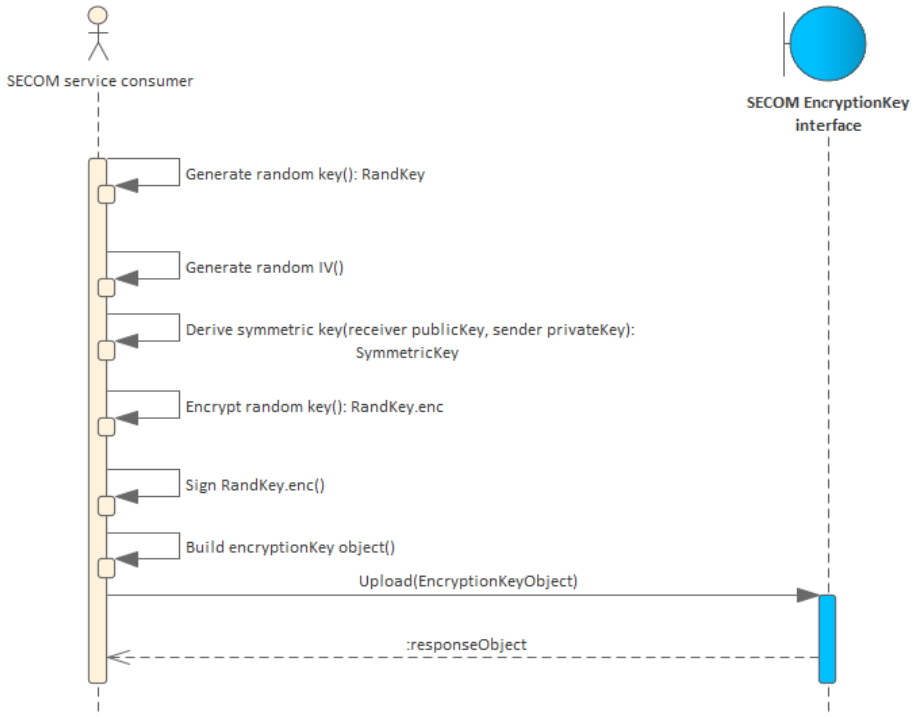


Figure 8 - Operational sequence diagram for EncryptionKey upload interface

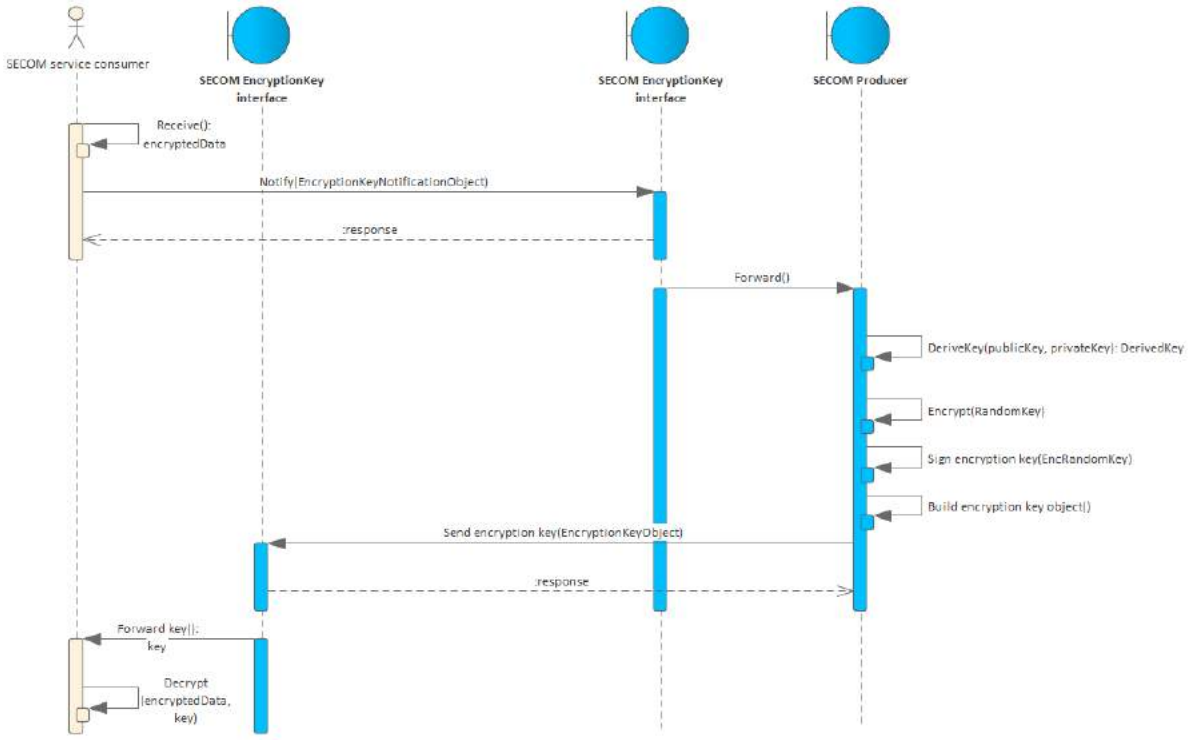


Figure 9 - Operational sequence diagram for EncryptionKey notification interface

4.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Encrypt encryption key with derived shared key for pair and created initialization vector	When working with AES encrypting the key needs to be complemented by an initialization vector.	Include initialization vector when encrypting the encryption key	Update the encryptionKeyObject to include IV value.
Request published encrypted information	How is the encryption supposed to work in a get scenario? When are the keys exchanged?	Need a way for the consumer to inform the information producer that encrypted information has been downloaded and thus, the encryption key is needed.	Add interface to request an encryption key, i.e. a notification interface.
Extract public key from Actor A public certificate	Transfer of the public key might lead to non-interoperability	There is a need to describe a consistent way of converting a	Add description of how to convert a PEM encoded key to and

	between different environments such as Unix, Windows etc. especially when it comes to line feed and carriage return characters.	PEM encoded key to and from a one line string.	from a one line string in relevant SECOM section.
Extract public key from Actor A public certificate	There should be a way to retrieve a public certificate from the SECOM PKI as an alternative to receiving the claimed public certificate from the caller.	Public certificate need to be able to request from both the service and the SECOM PKI.	Add SECOM Service interface for Get and Post PublicKey. Additionally also add a Get PublicKey interface in the SECOM PKI service interface

4.3 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
Data protection	Data encrypted with encryption key	Encryption algorithm not enough specified to ensure interoperability between different environments.	The suggestion is also to specify parameters regarding encryption such as key length, padding etc. explicitly in the SECOM standard.
Data protection	Encryption of encryption key	Initialization vector should be included in the encryption of the encryption key.	Update the encryptionKeyObject to include IV value.
Data encryption	EncryptionKey interface	Interfaces for retrieving and sending encryption keys not implemented.	Add interfaces for sending and requesting an encryption key, i.e. EncryptionKey and EncryptionKey notification interface.
Data encryption	PublicKey interface	Public key used for encryption requires interfaces to be able to retrieve.	Add SECOM Service interface for Get and Post PublicKey. Additionally also add a Get PublicKey interface in the SECOM PKI service interface
Information pull	Get interface	How is the encryption supposed to work in a get	Add interfaces for exchanging encryption keys as well as public keys.

		scenario? When are the keys exchanged?	

5 Test Case 3 – SECOM PKI

5.1 Description

The test case focus on SECOM service identification and client identification implemented as requirements on a SECOM compliant PKI.

5.1.1 Test objectives

- Service identity
- Client identity

5.1.2 Acceptance Criteria

Service identification and authentication by assigning Service X.509 certificates together with related certificate management operations.

Client identification and authentication by use of Client X.509 certificates together with related certificate management operations.

5.1.3 Test Scenarios

- Actor A sends a public key in a certificate signing request (CSR) and get them signed by the SECOM PKI provider.
- Actor A requests a signed Public Key from the SECOM PKI.
- Actor A retrieves Certificate Revocation List (CRL) from the SECOM PKI.
- Actor A checks revocation status of certificates with the Online Certificate Status Protocol (OCSP) in SECOM PKI.
- Actor A requests to revoke a certificate from SECOM PKI.

5.1.4 Test Environment

Testbed B

5.1.5 Test tools

OpenSSL, Notepad++

5.1.6 Test data

Not applicable

5.1.7 Test procedure

5.1.7.1 Certificate signing request from SECOM PKI

SENDER

Step	Commands	Result
Actor A		
Create CSR and send request to SECOM PKI. The signing request shall be according to PKCS #10 described in RFC 2986.		

Create CSR		Sign request as string, a PEM encoded PKCS#10 CSR
Create SignRequestObject in JSON		SignRequestObject – 1.json
SECOM A		
Add client certificate Actor A		Certificate_ActorA.pem
Create TLS		Encrypted channel established
Consume SECOM PKI CSR interface	POST URL/v1/csr{body} : return	

RECEIVER

Step	**Commands**	**Result**
SECOM PKI		
Receive …		SignRequestObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Store (inform SECOM PKI actor) incoming object		SignRequestObject -1.json
SECOM PKI actor		
Respond with PEM encoded signed public key after applicable vetting procedure		
Sign public key		signedPublicKey PEM encoded PKCS#10
Create POST response object in JSON SignRequestResponseObject		SignRequestResponseObject.json
Respond with response code 200 and data according to SignRequestResponseObject		

5.1.7.2 Get public key from SECOM PKI

SENDER

Step	**Commands**	**Result**
Actor A		
Create a public key Get request according to parameters		
Set filter parameter for claimed identity	Set identityId to claimed MRN	identityId = urn:mrn:org:ca:env:identity

Set filter parameter for certificate thumbprint	Set certThumbprint to thumbprint of claimed public key	certThumbprint = ddf90955832cc72d…
Create GetPublicKeyObject in JSON		GetPublicKeyObject – 1.json
SECOM A		
Add client certificate Actor A		Certificate_ActorA.pem
Create TLS		Encrypted channel established
Consume SECOM PKI GetPublicKey interface	GET URL/v1/publicKey/parameter : return	

RECEIVER

Step	**Commands**	**Result**
SECOM PKI		
Receive …		GetPublicKeyObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Store (inform SECOM PKI actor) incoming object		GetPublicKeyObject -1.json
SECOM PKI actor		
Respond with public certificate		
Retrieve corresponding public certificate		Binary PEM encoded X.509 Certificate
Create GET response object in JSON GetPublicKeyResponseObject		GetPublicKeyResponseObject.json
Respond with response code 200 and data according to GetPublicKeyResponseObject		

5.1.7.3 Request Certificate Revocation List (CRL) from SECOM PKI

SENDER

Step	**Commands**	**Result**
Actor A		
Set parameter for retrieving a CRL from SECOM PKI		
Set filter parameter for certificate authority	Set caAlias for certificate authority alias	caAlias = urn:mrn:org:ca:env:identity
SECOM A		
Add client certificate Actor A		Certificate_ActorA.pem

Create TLS		Encrypted channel established
Consume SECOM PKI CRL interface	GET URL/v1/crl/parameter : return	

RECEIVER

Step	Commands	Result
SECOM PKI		
Receive …		
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
SECOM PKI actor		
Respond with CRL		
Retrieve up to date CRL		Binary PEM encoded X.509 CRL
Respond with response code 200 and data according as described in RFC 5280		

5.1.7.4 Check certificate status in SECOM PKI

SENDER

Step	Commands	Result
Actor A		
Set parameter for checking certificate status in SECOM PKI		
Set filter parameter for certificate authority	Set caAlias for certificate authority alias	caAlias = urn:mrn:org:ca:env:identity
SECOM A		
Add client certificate Actor A		Certificate_ActorA.pem
Create TLS		Encrypted channel established
Consume SECOM PKI OCSP interface	GET URL/v1/ocsp/parameter : return	

RECEIVER

Step	Commands	Result
SECOM PKI		
Receive …		
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false

SECOM PKI actor		
Respond with OCSP response		
Retrieve certificate status		
Respond with response code 200 and data according as described in RFC 6960		

5.1.7.5 Revoke certificate in SECOM PKI

SENDER

Step	**Commands**	**Result**
Actor A		
Set attributes for revoking certificate		
Set the reason the certificate has been revoked	Set CertificateRevocation attribute RevocationReason	RevocationReason = 2 (keycompromise)
Set the date the certificate revocation should be activated	Set CertificateRevocation attribute RevokedAt	RevokedAt = DateTime
Create CertificateRevocation in JSON		CertificateRevocation – 1.json
SECOM A		
Add client certificate Actor A		Certificate_ActorA.pem
Create TLS		Encrypted channel established
Consume SECOM PKI Revoke interface	POST URL/v1/revoke/parameter {body} : return	

RECEIVER

Step	**Commands**	**Result**
SECOM PKI		
Receive …		
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
SECOM PKI actor		
Respond with revocation result		
Revoke certificate	Set certificate status and validity time	RevocationResponse = {message}
Respond with response code 200 and message according to RevocationResponse		

5.1.8 Sequence diagrams

5.1.8.1 Sequence – Certificate Signing Request (CSR)

Figure 10 shows the dynamic behaviour of a certificate signing request. Actor1 creates or updates self-signed certificates to its end application which issues a request to the SECOM PKI. The PKI returns a signed public-private key pair.

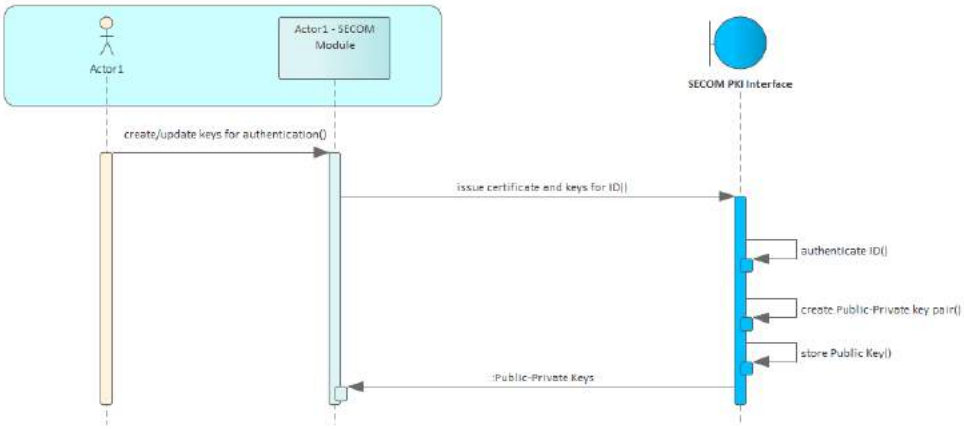


Figure 10 - Operational sequence diagram for CSR

5.1.8.2 Sequence – Get Public Key

Figure 11 shows the dynamic behaviour of a get request to retrieve a X.509 public certificate.

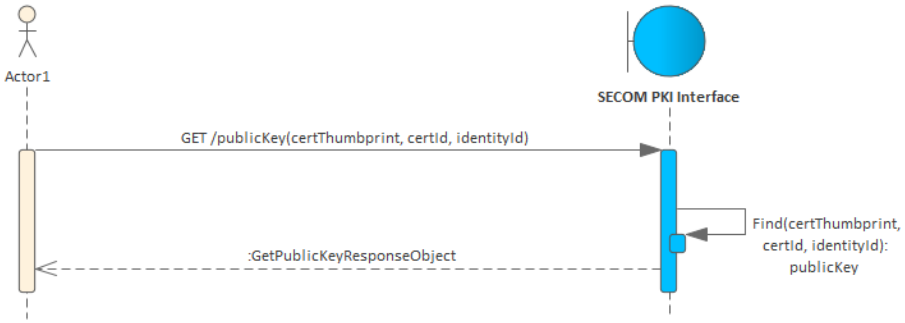


Figure 11 - Operational sequence diagram for GetPublicKey

5.1.8.3 Sequence – Certificate Revocation List (CRL)

Figure 12 shows the dynamic behaviour for retrieving a certificate revocation list.

Figure 12 - Operational sequence diagram for CRL

5.1.8.4 Sequence – Online Certificate Status Protocol (OCSP)

Figure 13 shows the dynamic behaviour of an online check of a certificate's validity.

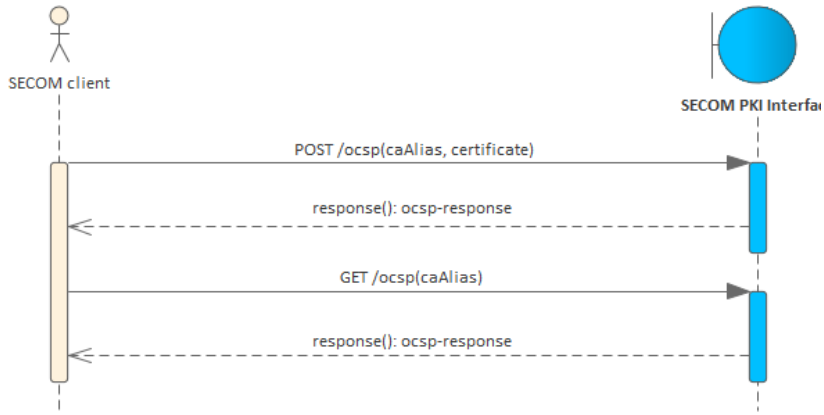


Figure 13 - Operational sequence diagram for OCSP

5.1.8.5 Sequence – Certificate revocation

Figure 14 shows the dynamic behaviour of a revoke request.

Figure 14 - Operational sequence diagram for Revoke

5.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Set filter parameter for claimed identity	SECOM lacks normative information wrt an identity registry	An identity is tied to an X.509 certificate, and the identity is expected to be registered	Propose to include a normative section in SECOM outlining requirements on an identity registry api
Set filter parameter for certificate thumbprint	Rationale behind using certificate thumbprint not clear	By referencing the thumbprint of a certificate required bandwidth is lower as	Include certThumbprint in relevant SECOM PKI interfaces

		opposed to sending the complete certificate	
All interfaces	In SECOM X.509 certificates are used, however there are implicit assumptions on what the “Subject distinguished name” should contain.	In SECOM it is assumed that the service instance identity is included in the x.509 certificate	Propose to include a normative section in SECOM wrt what attributes are required in X.509 certificate “Subject distinguished name”
Revoke certificate in SECOM PKI	The context around the need for revocation of certificates has to be described.	An organization might have multiple certificates for an entity, so we should not limit an organization’s possibility of creating a revocation request for entities with multiple certificates.	Possibly add rationale and use case around this interface in next SECOM release.

5.3 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
Service identification and authentication	Service X.509 certificates including service identity	Relies on a common use of X.509 customized attributes, together with authorization mechanisms.	Propose to include a normative section in SECOM wrt what attributes are required in X.509 certificate “Subject distinguished name”. Additionally authorization mechanisms in an expected identity registry need to be outlined in a SECOM api.
Client identification and authentication	Service X.509 certificates including client identity	As above with the following addition. Client authentication requires the client identity is included in the message.	Include recipient (client) identity in all messages where client authentication is required.
Client identification and authentication	Service X.509 certificates including client identity	To achieve end to end data protection including the last mile to the end user	Recommend to include a thumbprint of the last mile signing certificate making client authentication

		application from the SECOM instance. The message is required to be signed by the client.	possible using getPublicKey interface from sender or SECOM PKI.

6 Test Case 4 – Exchange large data

6.1 Description

This test case focuses on large message transfer when message size > 350 kb or what is possible to POST to a HTTP client, which might vary depending on webserver settings.

6.1.1 Test objectives

- Large message transfer

6.1.2 Acceptance Criteria

Large message transfer should be possible with regards to time-limited availability, correctly referenced data in related interfaces and maintained data integrity for linked data.

6.1.3 Test scenarios

Actor A decides to send a large amount of data to Actor B. Actor A consumes Actor B's Upload Link service interface and hereby sends a link to where the data can be retrieved, providing a unique transaction identifier. Actor B downloads the data using Actor A's Get By Link service interface referencing the previously received transaction identifier.

6.1.4 Test Environment

Testbed B

6.1.5 Test tools

OpenSSL, Notepad++

6.1.6 Test data

Steps to prepare **unclassified** and **uncompressed** data.

The data in this example is one very large RTZ.

6.1.7 Test procedure

SENDER

Step	**Commands**	**Result**
Actor A		
Select data file		data-1.rtz
Convert to Base64	openssl base64 -A -in data-1.zip -out data-1.rtz.base64	data-1.rtz.base64
Select Private Key		PrivateKey_SECOM_SMA_Test_Service_ID.pem
Create signature using original data file (data-1.rtz)	openssl dgst -sha256 -sign PrivateKey_SECOM_SMA_Test_Service_ID.pem data-1.rtz > data-1.rtz.sig	data-1.rtz.sig
Convert signature to HEX	xxd -u -ps -c 120 data-1.rtz.sig > data-1.rtz.sig.hex	data-1.rtz.sig.hex

Select Public Certificate for the data object		Certificate_SECOM_SMA_Test_Service_ID.pem
Select envelope public certificate		EnvelopeCertificate.pem
Temporarily store base64 converted original datafile in folder with the chosen transactionIdentifier		..\{transactionIdentifier}\data-1.rtz.base64
Set transactionIdentifier in EnvelopeLinkObject to be used in Get By Link interface		Envelope.json
Set other metadata values for the EnvelopeLinkObject		Envelope.json
Sign envelope		Envelope.sig
Add envelope signature to upload object		
Create UploadLinkObject in JSON		UploadLinkObject-1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM API Upload Link	POST URL/v1/object/link {body} : return	

RECEIVER

Verify Signature(s), retrieve linked data and restore data

Step	**Commands**	**Result**
SECOM B		
Receive …		UploadLinkObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Parse envelope		uploadLinkObject.Envelope
Convert to byte[]		Envelope[]
Authenticate data and claimed public key	Verify envelope signature	True/false

Store (inform Actor B OEM) incoming link object		UploadLinkObject-1.json
Parse and store signature from link object		data.sig.hex
Actor B		
Select transactionIdentifier referencing related large file		
Request large file by transactionIdentifier		
SECOM B		
Add client certificate Actor B		
Verify receiver host certificate SECOM A	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor A SECOM API Get By Link	GET URL/v1/object/link?transactionIdentifier : return	
Actor B		
Parse and store data from received data object		data.rtz.base64
Restore signature from HEX received in UploadLinkObject	xxd -r -u -ps data.sig.hex > data.sig	data.sig
Parse and store public certificate received in UploadLinkObject		publicCert.pem
Identify Root Certificate through the Thumbprint received in UploadLinkObject		mc-ca-chain_staging.pem
Verify Certificate	openssl verify -CAfile mc-ca-chain_staging.pem publicCert.pem > publicCert.pem.verification	publicCert.pem.verification
Extract public keys from certificate	openssl x509 -in publicCert.pem" -pubkey -noout > publicCert_key.pem"	publicCert_key.pem
Restore data from Base64 to original	openssl base64 –A -d -in data.rtz.base64 -out data.rtz	data.rtz

Verify signature i.e. compare signature with original data file	openssl dgst -sha256 -verify publicCert_key.pem -keyform pem -signature data.sig data.rtz > data.sig.verification	Verified OK
Compare received data with restored data	Open received data.rtz and restored data.rtz (Notepad++ Compare Plugin)	Received data unchanged

6.1.8 Sequence diagram

Figure 15 describes the dynamic behavior of service interfaces for large message transfer.

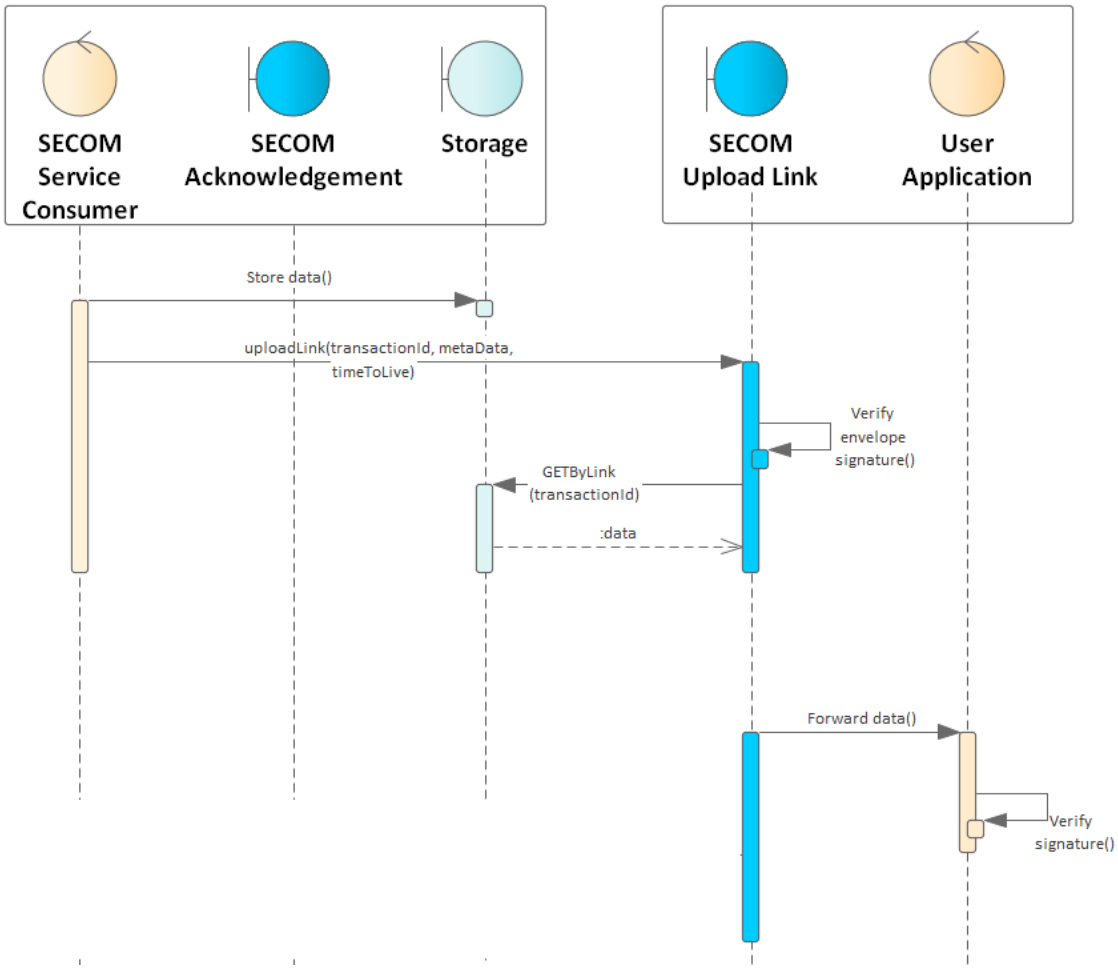


Figure 15 - Sequence diagram for large message transfer

6.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome

Verify signature i.e. compare signature with original data file	The process of uploading data in a two-step procedure (Upload Link followed by Get By Link) adds a complexity to the signature verification.	The verification of the data signature can only be done after the data has been downloaded.	The data signature has to be verified after receiving the data using the Get By Link interface.
Upload Link – Get By Link procedure	Upload Link implicitly requires a Get By Link interface	Thus more communication intense than upload object directly.	The Upload Link interface should be used for time persistent communication. To cater for message-, file- and streaming based communication.
Set other metadata values for the EnvelopeUploadObject	Data availability not constrained time-wise.	Availability to referenced data file should only be available a certain time.	Introduce timeToLive attribute to cater for this.
Set transactionIdentifier in EnvelopeLinkObject to be used in Get By Link interface	Not clear how to identify the large data file.	There is a need to supply an identity for the data file to be used as reference in subsequent communication.	Introduce a transaction identifier to be used in possible acknowledgement and when retrieving the message using Get By Link.

6.3 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
Large message transfer – time-limited availability	The sender of large data need to limit the time for availability to the linked data.	Thus creating a time-window for download of large data when the intended recipient has access to sufficient bandwidth.	Introduce a mandatory timeToLive attribute in the EnvelopeLinkObject to cater for this.
Large message transfer – correctly referenced data	An identity is required for the linked data file which is to be used as reference in	The identity shall uniquely identify the linked data to create a correlation for all subsequent	Introduce a mandatory transactionIdentifier (UUID) in the EnvelopeLinkObject.

	subsequent communication.	messaging concerning the linked data.	
Maintained data integrity for linked data.	Data signature creation and verification	If created in SECOM PKI this can be validated in the SECOM service instance.	The data signature has to be verified after receiving the data using the Get By Link interface.

7 Test Case 5 – Exchange compressed data

7.1 Description

The test case focus on exchange of compressed data.

7.1.1 Test objectives

- Bandwidth optimization

7.1.2 Acceptance Criteria

Minimized size of data package sent (individual files or files in folders), resulting in reduced required bandwidth. The extracted data package should not differ from the original package sent. The data product type of compressed file and or container type for compressed folder shall be clearly stated without having to extract the file/ folder.

7.1.3 Test Scenarios

Actor A shall send one data object in compressed format to Actor B. Actor A decides that the information is unclassified. The data is encapsulated into an UploadObject ready to be exchanged as body to a SECOM Upload Service Interface.

7.1.4 Test Environment

Testbed B

7.1.5 Test tools

OpenSSL, Notepad++, PKZIP

7.1.6 Test data

Steps to prepare **unclassified** and **compressed** data.

7.1.7 Test procedure

SENDER

Step	**Commands**	**Result**
Actor A		
Select data file		data-1.rtz
Compress data file	7z a -t7z data-1.gz data-1.rtz	data-1.gz
Convert to Base64	openssl base64 -A -in data-1.gz -out data-1.gz.base64	data-1.gz.base64

Select Private Key		PrivateKey_SECOM_SMA_Test_Service_ID.pem
Create signature using original data file (data-1.rtz)	openssl dgst -sha256 -sign PrivateKey_SECOM_SMA_Test_Service_ID.pem data-1.rtz > data-1.rtz.sig	data-1.rtz.sig
Convert signature to HEX	xxd -u -ps -c 120 data-1.rtz.sig > data-1.rtz.sig.hex	data-1.rtz.sig.hex
Select Public Certificate for the data object		Certificate_SECOM_SMA_Test_Service_ID.pem
Select envelope public certificate		EnvelopeCertificate.pem
Indicate compressed data	Set compressionFlag in SECOM_ServiceExchangeMetadataObject	compressionFlag = True
Set other metadata values for the EnvelopeUploadObject		Envelope.json
Sign envelope		Envelope.sig
Add envelope signature to upload object		
Create Upload Object in JSON		UploadObject-1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Upload	POST URL/v1/object {body} : return	

RECEIVER

Verify Signature(s) and restore data

Step	**Commands**	**Result**
SECOM B		
Receive …		UploadObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Parse envelope		uploadObject.Envelope
Convert to byte[]		Envelope[]
Authenticate data and claimed public key	Verify envelope signature	True/false
Store (inform Actor B OEM) incoming object		UploadObject-1.json
Actor B		
Parse and store data from object		data.gz.base64

Parse and store signature from object		data.rtz.sig.hex
Restore signature from HEX	xxd -r -u -ps data.rtz.sig.hex > data.rtz.sig	data.rtz.sig
Parse and store public certificate from object		publicCert.pem
Identify Root Certificate through the Thumbprint		mc-ca-chain_staging.pem
Verify Certificate	openssl verify -CAfile mc-ca-chain_staging.pem publicCert.pem > publicCert.pem.verification	publicCert.pem.verification
Extract public keys from certificate	openssl x509 -in publicCert.pem" -pubkey -noout > publicCert_key.pem"	publicCert_key.pem
Restore data from Base64 to original	openssl base64 –A -d -in data.gz.base64 -out data.gz	data.gz
Verify signature i.e. compare signature with original data file	openssl dgst -sha256 -verify publicCert_key.pem -keyform pem -signature data-1.rtz.sig data.rtz.sig > data.sig.verification	Verified OK
Extract data file	7z -e data.gz	data.rtz
Compare received data with restored data	Open received data.rtz and restored data-1.rtz (Notepad++ Compare Plugin)	Received data unchanged

7.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Compress data file	The order between base64 encoding and compression is not clear.	Decide on the order for compression vs base64 encoding.	Base 64 encoding shall be performed after compression of data.
Compress data file	It is not stated explicitly what type of compression format to use in SECOM.	Decide on compression format.	Use GZip-format as default for compressed data in SECOM.

7.3 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**

Minimize size of data package sent (individual files or files in folders)	The sender of large data shall be able to compress data.	By using compressed data less bandwidth is required.	Enable possibility to send compressed data (in ZIP format), add attribute compressionflag in SECOM_ServiceExchangeMetadataObject indicating if the data is compressed or not.
Extracted data package should not differ from sent original data package	Agree on a common compressed format.	By agreeing on a common format for compressed files/ folders facilitates interoperability.	Compression format used in SECOM shall be GZip-format. The GZip format is only compressing a byte stream and if needed it can be combined with TAR for achieving. As opposed to ZIP which is a combination of archiving and compression format requiring a filename.
Compressed file type and/ or compressed folder type shall be clearly stated.	The sender shall assign type of data and/ or type of folder in uploaded object containing the data package	By indicating the data type and/ or folder type the receiver can determine the kind of data received before extraction	Introduce mandatory enumerated attributes dataProductType – data product type of message in the data object containerType – Container type of message in the data object

8 Test Case 6 – Closed loop communication

8.1 Description

The test case focus on notification of message received/ read etc. to ensure a consistent dialogue between end-user applications. In SECOM this is implemented in the Service interface Acknowledgement which is used in conjunction with Upload, Upload Link and Get interfaces.

8.1.1 Test objectives

- Closed loop communication

8.1.2 Acceptance criteria

Notification of message received, read or not, to ensure dialogue between end-user applications shall be possible. Regardless if the receiving party (ship) is offline or online, hence the timeliness of the notification is important.

8.1.3 Test scenarios

Actor A decides to request an acknowledgement from Actor B in the context of uploading data to Actor B. The acknowledgement required is twofold first to confirm message delivered in the vendor API and finally operational when the message is opened and/ or processed in the end user application.

8.1.4 Test Environment

Testbed B

8.1.5 Test tools

OpenSSL, Notepad++

8.1.6 Test data

Steps to prepare **unclassified** and **uncompressed** data.

The data in this example is one RTZ.

8.1.7 Test procedure

SENDER

Request delivered and opened acknowledgement when uploading data.

Step	**Commands**	**Result**
Actor A		
Select data file		data-1.rtz
Convert to Base64	openssl base64 -A -in data-1.rtz -out data-1.rtz.base64	data-1.rtz.base64
Select Private Key		PrivateKey_SECOM_SMA_Test_Service_ID.pem

Create signature using original data file (data-1.rtz)	openssl dgst -sha256 -sign PrivateKey_SECOM_SMA_Test_Service_ID.pem data-1.rtz > data-1.rtz.sig	data-1.rtz.sig
Convert signature to HEX	xxd -u -ps -c 120 data-1.rtz.sig > data-1.rtz.sig.hex	data-1.rtz.sig.hex
Select Public Certificate for the data object		Certificate_SECOM_SMA_Test_Service_ID.pem
Select envelope public certificate		EnvelopeCertificate.pem
Set ackRequest attribute		ackRequest = 3 (Delivered + Opened ACK Requested)
Set other metadata values for the EnvelopeUploadObject		Envelope.json
Sign envelope		Envelope.sig
Add envelope signature to upload object		
Create Upload Object in JSON		UploadObject-1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Upload	POST URL/v1/object {body} : return	

RECEIVER

Verify Signature(s), restore data and acknowledge data as requested by the sender.

Step	**Commands**	**Result**
SECOM B		
Receive …		UploadObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Parse envelope		uploadObject.Envelope
Convert to byte[]		Envelope[]
Authenticate data and claimed public key	Verify envelope signature	True/false
Store (inform Actor B OEM) incoming object		UploadObject-1.json
SECOM B		

Send delivered acknowledgement …		
Select envelope public certificate		EnvelopeCertificate.pem
Set ackType attribute		ackType = 1 (Delivered ACK – Technical acknowledgement such as delivered to end system)
Set other metadata values for the EnvelopeAckObject		Envelope.json
Sign envelope		Envelope.sig
Add envelope signature to AcknowledgementObject		
Create AcknowledgementObject in JSON		AcknowledgementObject -1.json
Add client certificate Actor B		
Verify receiver host certificate SECOM A	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor A SECOM Api Acknowledgement	POST URL/v1/acknowledgement {body} : return	
Actor B		
Parse and store data from object		data.rtz.base64
Parse and store signature from object		data.sig.hex
Restore signature from HEX	xxd -r -u -ps data.sig.hex > data.sig	data.sig
Parse and store public certificate from object		publicCert.pem
Identify Root Certificate through the Thumbprint		mc-ca-chain_staging.pem
Verify Certificate	openssl verify -CAfile mc-ca-chain_staging.pem publicCert.pem > publicCert.pem.verification	publicCert.pem.verification
Extract public keys from certificate	openssl x509 -in publicCert.pem" -pubkey -noout > publicCert_key.pem"	publicCert_key.pem
Restore data from Base64 to original	openssl base64 –A -d -in data.rtz.base64 -out data.rtz	data.rtz
Verify signature i.e. compare signature with original data file	openssl dgst -sha256 -verify publicCert_key.pem -keyform pem -signature data.sig data.rtz > data.sig.verification	Verified OK
Compare received data with restored data	Open received data.rtz and restored data.rtz (Notepad++ Compare Plugin)	Received data unchanged
SECOM B		

Send operational acknowledgement …		
Select envelope public certificate		EnvelopeCertificate.pem
Set ackType attribute		ackType = 2 (Opened ACK Operational acknowledgement such as when opened/read by end user.)
Set other metadata values for the EnvelopeAckObject		Envelope.json
Sign envelope		Envelope.sig
Add envelope signature to AcknowledgementObject		
Create AcknowledgementObject in JSON		AcknowledgementObject -2.json
Add client certificate Actor B		
Verify receiver host certificate SECOM A	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor A SECOM Api Acknowledgement	POST URL/v1/acknowledgement {body} : return	

8.2 Sequence diagram

The sequence diagram in Figure 16 describes the acknowledgement interface in conjunction with Upload. The sender (uploader) of data can request acknowledgement from the receiver enabling the sender to follow (trace) the sent data. This is especially important when uploading (sending) data to a ship that can be offline at the time for sending, but receives the data next time it is online.

NOTE When the “opened ACK” is requested in conjunction with Upload Link, the acknowledgement is sent after the data has been received using the Get By Link request.

There are two different acknowledgements defined in SECOM. The first is the “deliver ACK” that is sent by the receiver when data has been accepted and forwarded to the end-user. The second is the “opened ACK” that is sent by the end user when received data is correctly opened and processed.

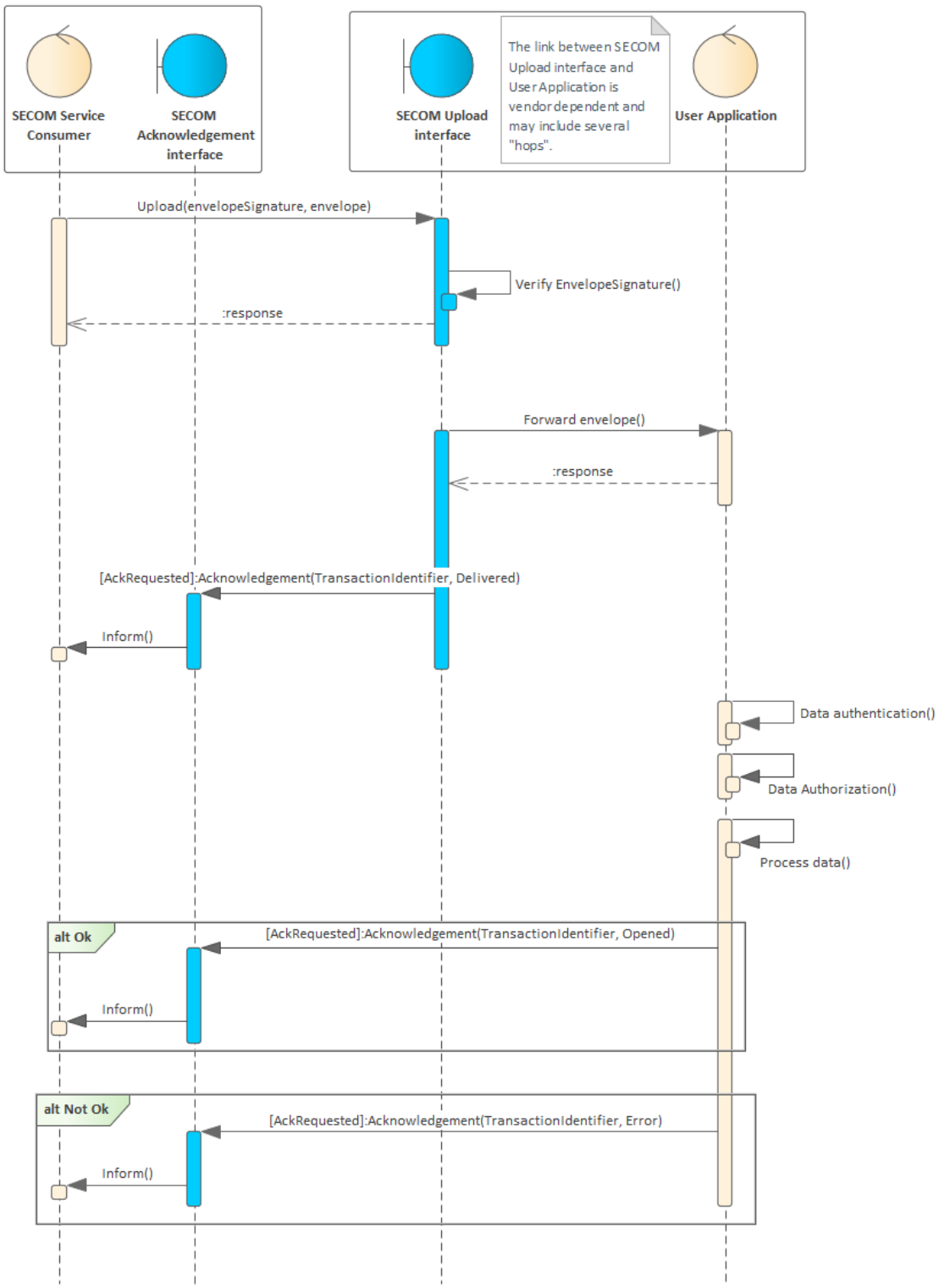


Figure 16 - Sequence diagram for Acknowledgement interface in the context of Upload

8.3 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Send delivered acknowledgement …	There might be a security risk with technical feedback, such as asynchronous technical and operational acknowledgements.	Acknowledgement data should be protected.	Introduce an envelope to protect the entire Acknowledgement message.
Set ackType attribute	Missing response messages in the AcknowledgementObject	Define the different Acknowledgement types required.	The ackType attribute should be an enumerated list: 1 – Delivered ACK 2 – Opened ACK 3 – Error
Set ackType attribute	Missing response error messages in the AcknowledgementObject	Define the different Acknowledgement errortypes required.	In case of ackType = 3 (error) the nackType attribute should be an enumerated list: 0 – XML Schema validation error 1 – Unknown data type or version 2 – Failed data signature verification 3 – Failed decryption 4 – Failed decompression
Set other metadata values for the EnvelopeAckObject	The order of received acknowledgements is important since the Acknowledgment is sent asynchronously.	The timestamp at creation of an acknowledgment is required.	Introduce an envelopeSignatureTime attribute in the EnvelopeAckObject.

8.4 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
Notification of message received, read or not received.	Messages for technical- , operational- and error-acknowledgement are required.	This facilitates closed loop communication between parties, thus facilitating communication transparency.	Introduce enumerations for attributes ackType and nackType (sent if ackType = 3 – Error). In the EnvelopeAckObject.

Ensure a consistent dialogue between end-user applications.	An identity is required for the message which is acknowledged.	The identity shall uniquely identify the transaction to create a correlation for all subsequent messaging concerning the original message.	Introduce a mandatory transactionIdentifier (UUID) in the EnvelopeAckObject.
Maintained data integrity for acknowledgement message.	Data signature creation and verification	If created in SECOM PKI this can be validated in the SECOM service instance.	Data signature of the EnvelopeAckObject has to be verified after receiving the acknowledgement message.
Timeliness of the notification is important,	The Acknowledgement is an asynchronous message which requires a timestamp for sent Acknowledgements.	This ensures the timeliness for acknowledgements received even if the ship is offline when acknowledgements are created.	Introduce an envelopeSignatureTime attribute in the EnvelopeAckObject. This timestamp should indicate when the acknowledgement is created in the end-user application.

9 Test Case 7 – Subscribe to data

9.1 Description

The test case focuses on subscription on information, either specific information according to parameters, or the information accessible upon decision by the information provider.

9.1.1 Test objectives

- Subscribe to data including creation, notification and removal of subscription

9.1.2 Acceptance Criteria

It shall be possible to subscribe on information to receive subsequent updates. Subscription shall cater for specified information needs as well as subscription on whatever information that is accessible for the requesting service. This involves both subscription requests from service consumers as well as subscriptions initiated by service producers. Removal of subscriptions shall also be possible from either party or automatically when information objects are deemed not relevant according to parameters in the subscription request. Relevant notifications in all above cases are also required.

9.1.3 Test Scenarios

Note in below scenarios steps including upload of data are omitted since these are covered in other test cases.

9.1.3.1 Subscription request

Actor A requests to subscribe on information according to attributes defined in provided SubscriptionObject from Actor B. Actor B verifies actor A access to requested information and responds with the subscription result as defined in ResponseSubscriptionObject. After which actor B sends a SubscriptionNotification message (subscription created) to actor A.

9.1.3.2 Subscription nomination

Actor B nominates actor A for subscription on information and sends a SubscriptionNotification message (subscription created) to actor A.

9.1.3.3 Subscription removal

At any point in time actor B can terminate the provided subscription by sending a SubscriptionNotification message (subscription removed) to actor A.

Alternatively the information consumer can terminate the subscription by sending a RemoveSubscription message (subscription removed) to actor A.

9.1.4 Test Environment

Testbed B

9.1.5 Test tools

OpenSSL, Notepad++

9.1.6 Test data

Steps to prepare **classified** and **uncompressed** data.

The data in this example is one RTZ.

9.1.7 Test procedure

9.1.7.1 Subscription request

SENDER

Request subscription.

Step	Commands	Result
Actor A		
Set filter values according to attributes in the SubscriptionRequestObject	Filter out routeplan for subscription	dataProductType = RTZ
Create SubscriptionRequestObject in JSON		SubscriptionRequestObject-1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Subscription	POST URL/v1/subscription {body} : return	

RECEIVER

Handle subscription request and subsequent notification of created subscription.

Step	Commands	Result
SECOM B		
Receive …		SubscriptionRequestObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Store (inform Actor B OEM) incoming object		SubscriptionRequestObject - 1.json
Actor B		
Parse and store data from object		SubscriptionRequestObject - 1.json
Verify actor A access to requested information	Validate access according to client cert for actor A	True/ false

If successful authorization		
Create subscription	Assign internal identifier for subscription	subscriptionIdentifier = UUID
Respond with response code 200 and attributes according to SubscriptionResponseObject		
Actor B		
Create subscription notification		
Set attributes in SubscriptionNotificationObject		subscriptionIdentifier = UUID eventEnum = 1 (Subscription created)
SECOM B		
Send subscription notification		
Create SubscriptionNotificationObject in JSON		SubscriptionNotificationObject - 1.json
Add client certificate Actor B		
Verify receiver host certificate SECOM A	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor A SECOM Api Subscription Notification	POST URL/v1/ subscription/notification {body} : return	

9.1.7.2 Subscription nomination

SENDER

Nominate actor A as a subscriber.

Step	**Commands**	**Result**
Actor B		
Create subscription on data deemed relevant to Actor A	Filter out specific routeplan for subscription	
Assign subscription identifier		subscriptionIdentifier = UUID
Set attributes in SubscriptionNotificationObject		subscriptionIdentifier = UUID eventEnum = 1 (Subscription created)
SECOM B		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established

Consume Actor A SECOM Api Subscription Notification	POST URL/v1/ subscription/notification {body} : return	

RECEIVER

Receive subscription nomination.

Step	Commands	Result
SECOM A		
Receive …		SubscriptionNotificationObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Store (inform Actor a OEM) incoming object		SubscriptionNotificationObject -1.json
Actor A		
Parse and store data from object		SubscriptionNotificationObject -1.json
Respond with response code 200 and attributes according to SubscriptionNotificationResponseObject		

9.1.7.3 Subscription removal

SENDER

Actor A requests removal of a subscription.

Step	Commands	Result
Actor A		
Create subscription removal		
Create RemoveSubscriptionObject in JSON	subscriptionIdentifier = UUID	RemoveSubscriptionObject -1.json
SECOM A		
Send subscription removal request to Actor B		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Subscription	DELETE URL/v1/subscription {body} : return	

RECEIVER

Notify subscriber of removed subscription.

Step	Commands	Result
Actor B		
Receive …		RemoveSubscriptionObject deserialized
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Store (inform Actor B OEM) incoming object		RemoveSubscriptionObject - 1.json
SECOM B		
Parse and store data from object		RemoveSubscriptionObject - 1.json
Respond with response code 200 and attributes according to RemoveSubscriptionResponseObject		
Actor B		
Create subscription notification		
Set attributes in SubscriptionNotificationObject		subscriptionIdentifier = UUID eventEnum = 2 (Subscription removed)
SECOM B		
Send subscription notification		
Create SubscriptionNotificationObject in JSON		SubscriptionNotificationObject - 1.json
Add client certificate Actor B		
Verify receiver host certificate SECOM A	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor A SECOM Api Subscription Notification	POST URL/v1/ subscription/notification {body} : return	

9.1.8 Sequence diagram

Figure 17, Figure 18 and Figure 19 describes the dynamic behavior of the service interface.

The Subscription interface is used to request subscription to information objects. Subscription could both be requested by the consumer (Figure 19) and nominated by the producer (Figure 18). Also removing a subscription can be initiated by the consumer as well as the producer. The requested or nominated subscription creation and removal is notified using the Subscription Notification interface seen in Figure 18 and Figure 19.

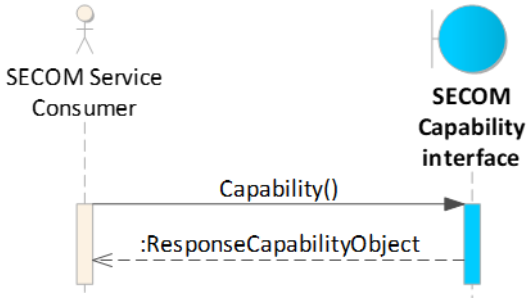


Figure 17 - Sequence diagram for Subscribe interface

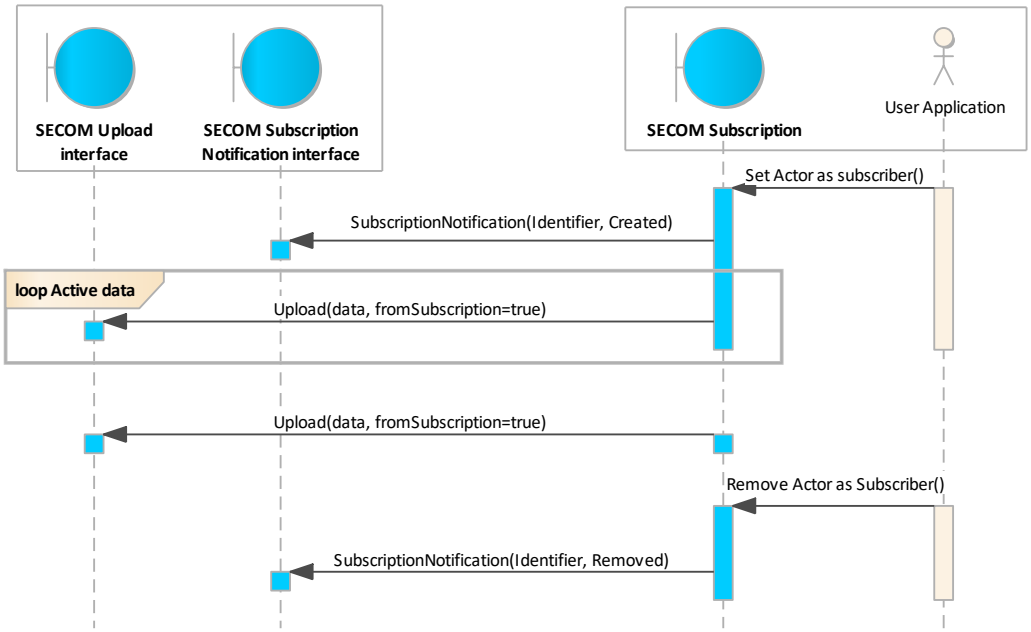


Figure 18 - Operational sequence diagram for Subscription interfaces

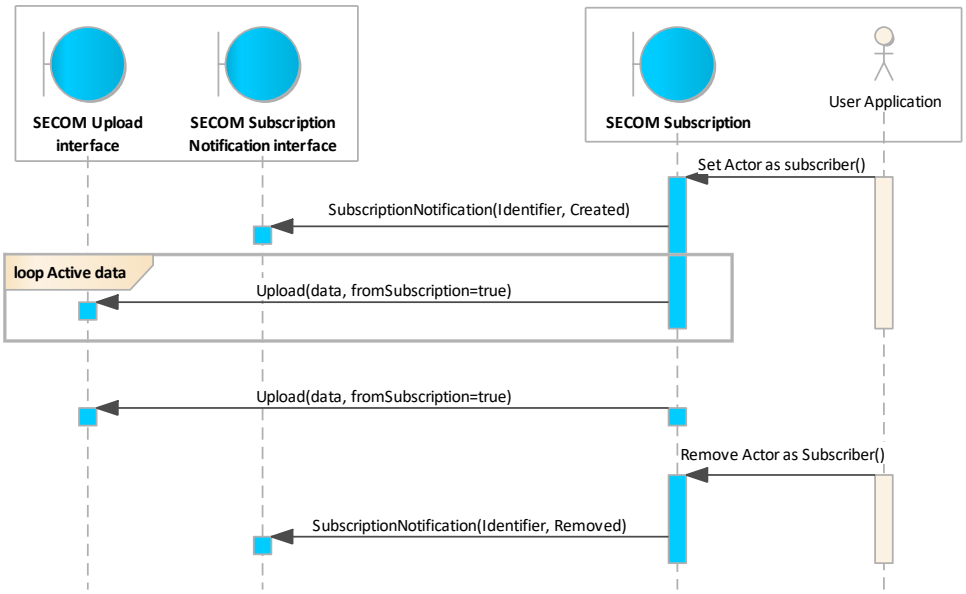


Figure 19 - Sequence diagram for Subscription interfaces with external subscription request

9.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Set filter values according to attributes in the SubscriptionRequestObject	Missing possibility to subscribe to a specific information object i.e. routeplan	We need the possibility to subscribe to specific information objects not only all objects of a certain type.	Add dataReference attribute in SubscriptionRequestObject of type UUID as a reference to data.
Set filter values according to attributes in the SubscriptionRequestObject	What is the intended behaviour if no filter attributes are provided in the SubscriptionRequestObject or if the filter results in multiple information objects?	Multiple possible information objects should return subscriptions on all information objects the requester is authorized to.	Suggest to increase the multiplicitly for SubscriptionResponseObject to 1 .. * or perhaps handle multiple subscriptions using the subscription notification interface. A workaround would instead make use of the SECOM Get Summary interface to retrieve data references

			for relevant information objects. Which in turn could be used for more specific subscription requests.
Set filter values according to attributes in the SubscriptionRequestObject	Not clear when a subscription ends if not removed by information consumer or producer.	A automatic removal of a subscription should be possible.	Suggest to add attributes subscriptionPeriodStart and subscriptionPeriodEnd in the SubscriptionRequestObject to handle automatic removal of subscription.

9.3 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
It shall be possible to subscribe on information to receive subsequent updates.	Service interface Subscription and Subscription Notification.	Interface should include request and notification of subscriptions.	The subscription should be able to initiate and by both information consumer using interface Subscription and information producer using interface Subscription Notification with eventEnum = 1 (Subscription created).
Subscription shall cater for specified information needs.	For instance it should be possible to subscribe to a specific routeplan.	Add a possibility to filter out a specific information object.	Include dataReference attribute in SubscriptionRequestObject, pointing to a specific information object.
Subscription shall cater for subscription on whatever information that is accessible for the requesting service.	Providing no filtering attributes in the SubscriptionRequestObject should return all information objects the requesting service has access to.	The interface cannot handle multiple responses in case the requests in possible subscription on more than one information object.	Suggest to increase the multiplicitly for SubscriptionResponseObject to 1 .. *.
Removal of subscriptions shall be possible	Service interface Remove Subscription and Subscription Notification.	Decision to terminate a subscription shall	The subscription should be able to initiate by both information consumer by use of interface Remove

from either party.		be possible from either party.	Subscription and information producer by use of interface Subscription Notification.
Removal of subscriptions shall also be possible automatically when information objects are deemed not relevant according to parameters in the subscription request.	Automatic termination of subscription based on optionally provided subscription validity period.	To relieve operators of manually terminating subscriptions and subscription validity period should be introduced.	Suggest to add attributes subscriptionPeriodStart and subscriptionPeriodEnd in the SubscriptionRequestObject to handle automatic removal of subscription.

10 Test Case 8 – Service information

10.1 Description

The test case focuses on information with regards to service information i.e. what interfaces are accessible for respective valid payload, formats and versions. Additionally service information regarding metadata for provided information objects.

10.1.1 Test objectives

- Service information

10.1.2 Acceptance Criteria

Service information - Verify that service information is returned correctly according to the SECOM Capability Service interface.

Additionally providing a list of metadata concerning available information objects from a service using the SECOM Get Summary interface.

10.1.3 Test Scenarios

10.1.3.1 Service capability information

Actor A shall request service information from Actor B by consuming Actor B exposed SECOM Capability Service interface. Actor B returns service information encapsulated in a CapabilityResponseObject containing a list of capability objects.

10.1.3.2 Information regarding metadata for the service provided information objects

Actor A shall request summary information from Actor B by consuming Actor B exposed SECOM Get Summary interface. Actor B returns summary of accessible information objects encapsulated in a GetSummaryResponseObject containing a list with metadata describing the provided information objects.

10.1.4 Test Environment

Testbed B

10.1.5 Test tools

Not applicable.

10.1.6 Test data

Not applicable.

10.1.7 Test procedure

10.1.7.1 SECOM Capability service interface

SENDER

Request service capability information

Step	Commands	Result
Actor A		
Request service capability information		
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Capability	GET URL/v1/capability : return	

RECEIVER

Respond with service capability information

Step	Commands	Result
SECOM B		
Receive …		Get request handled
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Actor B		
Retrieve data from table containing service information		
Respond with response code 200 and data according to CapabilityResponseObject		

10.1.7.2 SECOM Get Summary service interface

SENDER

Request metadata regarding provided information objects

Step	Commands	Result
Actor A		
Request metadata for a service provided information objects		
Set filter values for the Get Summary request	Assign values to parameters in the GetSummaryFilterObject	dataProductType = RTZ

Create GetSummaryFilterObject in JSON		GetSummaryFilterObject -1.json
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM Api Get Summary	GET URL/v1/object/summary?parameters : return	

RECEIVER

Respond with service provided information objects resp. metadata

Step	**Commands**	**Result**
SECOM B		
Receive …		Get Summary request handled
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Actor B		
Retrieve metadata for all available information objects authorized to actor A		
Create response objects for all available information objects	Set relevant attributes in GetSummaryFilterObject for all information objects	
SECOM B		
Send Get Summary response for each information object		
Create GetSummaryResponseObject in JSON		GetSummaryResponseObject -1.json
Respond with response code 200 and data according to GetSummaryResponseObject		

10.1.8 Sequence diagram

Figure 20 describes the dynamic use of the Capability interface.

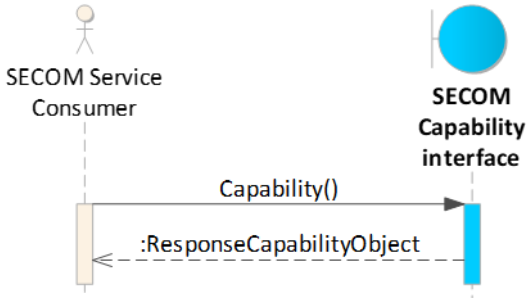


Figure 20 - Sequence diagram for Capability interface

Figure 21 describes the dynamic behaviour of the Get Summary interface.

The Get Summary interface is used to pull metadata from an actor. The received metadata response might be used for selecting which actual data to be retrieved by a new request using the Get interface. The service request contains filtering parameters that allows the information owner to search and prepare metadata to be returned. Once the authentication of the requester has been verified, the preparation of metadata includes internal judgement of information availability and packaging the metadata. If metadata is available, the requested metadata is returned, if not, an error messages is returned.

Figure 21 - Sequence diagram for Get Summary interface

10.1.9 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Respond with response code 200 and data	The distinction between payload and	Suggest to differentiate between	Introduce ContainerTypeEnum for payload containers and

according to CapabilityResponseObject	payload containers is not clear.	containers and payloads,	SECOM_DataProductType for payloads.
Respond with response code 200 and data according to CapabilityResponseObject	The interface cannot handle multiple capability objects.	Implement a list of returned objects.	Add a list of CapabilityObject to the CapabilityResponseObject.
Respond with response code 200 and data according to CapabilityResponseObject	Cannot consistently determine the payload version in returned CapabilityObject.	Suggest to add explicit attribute for payload/ payload container version.	This proved hard to standardize since versioning of various payloads may differ. Although returned attribute productSchemaUrl implicitly points to a specific version.
Set filter values for the Get Summary request	There is a need to be able to filter out actual information objects.	Suggest to include validity time period filter.	Add attributes validFrom - Time related to validity period start for information object and validTo - Time related to validity period end for information object. In GetSummaryFilterObject.
Consume Actor B SECOM Api Get Summary	Questionable if this can be handled using a synchronous messaging pattern. Since creating the available information objects might depend on end-user manual decision if the authorization cannot be handled directly in the SECOM service instance.	Suggest to make use of an asynchronous message pattern.	Replace the GET operation with POST hereby achieving reasonable time for responding to the request. Additionally message integrity can be implemented in using an envelope for the POST message.

10.2 Conclusions and Recommendations

Acceptance criteria	**Solution**	**Conclusions**	**Recommendations**
Service information	Service interface - Capability	Distinction between payload and payload containers unclear. The interface cannot handle multiple capability objects if a service supports	Introduce ContainerTypeEnum for payload containers and SECOM_DataProductType for payloads.

		more than one payload type/ payload container type.	Add a list of CapabilityObject to the CapabilityResponseObject.
Service information	Service interface - Capability	The interface cannot handle multiple capability objects if a service supports more than one payload type/ payload container type.	Add a list of CapabilityObject to the CapabilityResponseObject.
Service information	Service interface - Capability	Payload/ container version not returned in the capability response.	Rely on supplied productSchemaUrl to implicitly derive the payload version.
Service metadata information	Get Summary interface	Missing possibility to select validity period as a filter parameter	Add validTo and validFrom as filter parameters in GetSummaryFilterObject.
Service available metadata information	Get Summary interface including availability check	Suggest to use an asynchronous message pattern to allow for timely end-user availability checks. Hereby also including a message envelope for message integrity.	Suggest to use REST operation POST including message envelope instead of currently used GET operation.

11 Test Case 9 – Service status

11.1 Description

The test case focus on retrieving the contextual status of a service.

11.1.1 Test objectives

- Service condition

11.1.2 Acceptance Criteria

Service condition - Verify that service condition is returned correctly according to the SECOM Ping Service interface.

11.1.3 Test Scenarios

Actor A shall request service condition from Actor B by consuming Actor B exposed SECOM Ping Service interface. Actor B returns the service condition encapsulated in a PingResponseObject optionally containing the last interaction time with the vendor API.

11.1.4 Test Environment

Testbed B

11.1.5 Test tools

Not applicable.

11.1.6 Test data

Not applicable.

11.1.7 Test procedure

SENDER

Step	Commands	Result
Actor A		
Check service status		
SECOM A		
Add client certificate Actor A		
Verify receiver host certificate SECOM B	Check certificate against SECOM PKI	True/false
Create TLS		Encrypted channel established
Consume Actor B SECOM API Ping	GET URL/v1/ping : return	

RECEIVER

Step	Commands	Result

SECOM B		
Receive …		Get request handled
Authenticate sender	Verify client cert for Actor A from TLS against SECOM PKI	True/false
Actor B		
Retrieve data from log-table containing Vendor API last interaction time.		
Respond with response code 200 and data according to PingResponseObject		

11.1.8 Sequence diagram

Figure 22 describes the dynamic use of the Ping interface.

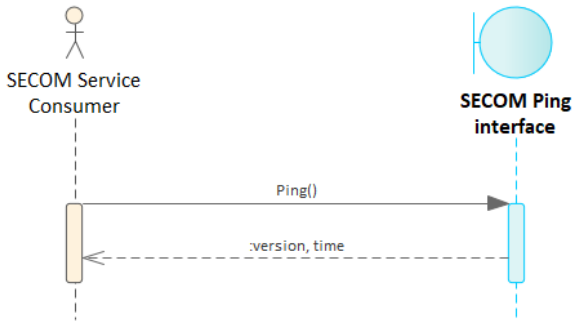


Figure 22 – Check status on service

11.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

Step	Test comments	Conclusions	Outcome
Check service status	Redundant information regarding service status.	The service status (released, provisional etc.) can be retrieved using SECOM Service Discovery service interface.	Removed service status and renamed interface from Status to Ping .

11.3 Conclusions and Recommendations

Acceptance criteria	Solution	Conclusions	Recommendations
Service condition	Service interface - Ping	The interface should only respond with the technical status of the specific service instance.	Rename interface from Status to Ping. This is to emphasize the purpose being: checking the technical status both for the service instance itself and last interaction time with Vendor API.

12 Test Case 10 - Cyber Security Review

12.1 Description

This test case is performed as a review of the SECOM document. If possible, the changes and variables made and recommended during the SECOM Test Project is also reviewed.

12.2 Targeted questions

- Review of the SECOM security solution as a whole
  - Overall description (Clause 4) of the SECOM standard
  - Overall solution of SECOM Data Protection (Clause 7)
  - Overall solution of SECOM Transport Security (Clause 6)
  - Data protection and Transport security applied on/in SECOM Information Service (REST)
- Review of specific issues
  - How exchange the secret key if SECOM Data Protection scheme is used instead of IHO and Permits?
  - What requirements does the exchange of the secret key put on the algorithm used in asymmetric keys used mainly for signing data? Will it work the same with ECC keys as for RSA keys? Or are there different procedures required for the encryption of the secret key?
  - Shall SECOM handle Nonrepudiation?
  - Is there a security risk with the Acknowledgement procedure described?
  - Exchange the digital signature in service defined attribute, PERMIT.xml, S100_DatasetDiscoveryMetadata, S100_CatalogueMetadata or in SECOM_ServiceExchangeMetadata?
  - How shall the signature be transferred?
  - Which SECOM service interfaces requires signature on the payload (all interfaces that includes payload…)?
  - How ensure authentication in those interfaces that do not exchange payload and its signature?
  - Shall SECOM describe which identity to use for signing data versus service authentication (signing transport?
  - Should SECOM support session based interaction a'la S-100/Offis examples, or MMS style in MCP?
  - Shall SECOM describe Service Authentication as normative?
  - Shall SECOM Communication Channel Security be based on TLS and Certificates or OpenID/HMAC or similar?
  - Is it/will it be accepted to mandate the use of Client Certificates from SECOM PKI?
  - Should/Shall SECOM also mandate use of host certificate from SECOM PKI? Which then becomes a selfsigned certificate? Will it work in reality?

12.3 Test Functionality

N/A

12.4 Test Variables

N/A

12.5 Testbed

N/A

12.6 Test Sequence

N/A

12.7 Test results and discussions

This chapter contains the common results and discussions around the test case. For each individual participants result see the Annexes in end of this document.

12.7.1 Observations

Num	Ref number	Observation	Consequence/Proposal	Reference in SECOM Document
001				

12.8 Conclusions and Recommendations

13 Test Case 11 – White list and access request

13.1 Description

The test case should focus on client access and client identity together with functions for white listing services. Even though this test case is not performed the underlying discussions are included below.

13.1.1 Test objectives

- Support and facilitate client access to information

13.1.2 Acceptance Criteria

Ensure client access is supported and facilitated including last mile from requesting SECOM service instance to end user application.

13.1.3 Test Scenarios

TBD

13.1.4 Test Environment

TBD

13.1.5 Test tools

TBD

13.1.6 Test data

TBD

13.1.7 Test procedure

SENDER

Step	Commands	Result
Actor A		
SECOM A		

RECEIVER

Step	Commands	Result
SECOM B		
Actor B		

13.2 Test results and discussions

This chapter contains the common results and discussions around the test case.

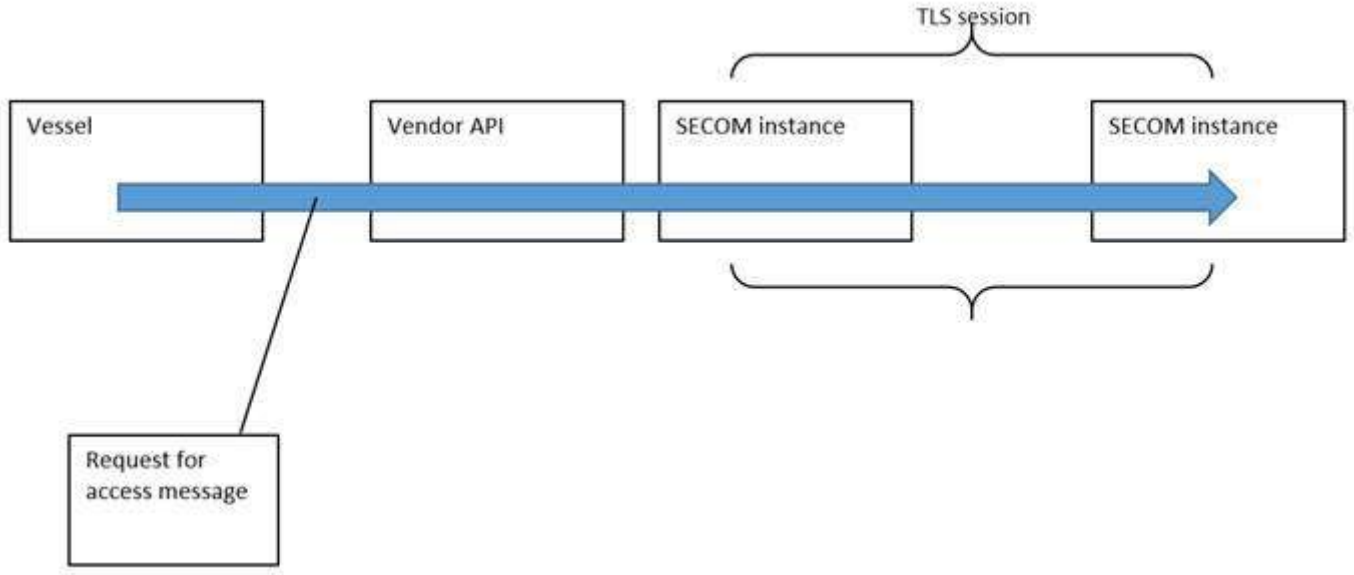
13.2.1 Request for Access

When sending information through SECOM, the communication takes place using TLS where the communicating parties exchange certificates and it is thus possible to identify a calling client by its client certificate.

The current way of requesting access does not include the identity of the party requesting access. This means that the identity available is the one available in the client certificate.

This then means that when communication need to take place in a two-step approach, example a vessel behind a vendor API, only the identity of the SECOM instance is able to request access, not the vessel identity.

(Or if a provider is hosting their SECOM instance behind a proxy, then the TLS session will terminate at the proxy, not even reaching the SECOM instance. This is common in load balancing and/or redundant setups)



A way of resolving this would be to include the identity of the vessel requesting the access in the message and signing the message. Preferably also the recipient identity and a timestamp should be included to stop playback attacks. This structure then needs to be applied to all interfaces and messages where authentication is required.

The downside of doing this would be that the request for access message would grow in size. However the new getPublicKey interface can help with that, see Minimizing message size below.

Any request that does involve authorization then should need to be signed by the sending instance to be sure of the origin of the request.

This complicated setup originates from that the data should be protected end to end. The data is protected in the TLS session, but the section between the vessel and its side of the SECOM Instance is outside the TLS session so it can only be protected using a different method like a digital signature.

13.2.2 Minimizing message size

In the current signed messages, the included public certificate takes up a lot of space. With the added GetPublicKey interface this could be reduced to only include the thumbprint of the signing certificate in the signed data. The receiver of signed data can then use the getPublicKey interface to fetch the complete public certificate from the sender (or from the PKI if possible) to verify the signature. This can be done once for the required certificate and then stored for future use until the certificate times out or is revoked.

The reduction in size due to this would be significant. A public certificate in Base64 can consist of 1600 characters. The thumbprint of the same is only 40 characters.

Suggestion is to move to use thumbprint for signature and use the getPublicKey interface towards the sender to fetch the public certificate and be able to verify the signature.

13.3 Conclusions and Recommendations

Fine granular organizationstructure, access on organizational level

Servicecertificate as a basis for access control which means attributes in the certificate would limit the granularity possible for access

14 Test Case 12 – Service Discovery

14.1 Description

The test case focus on service instance discovery.

The main purpose is to challenge

- 9 SECOM Service Discoverability.
    - Service Discovery Interface definition file (Swagger)

14.2 Targeted questions

- Fixed search parameter in interface, or dynamic query with key:value pair with recommended list of search parameters.
-

14.3 Test Functionality

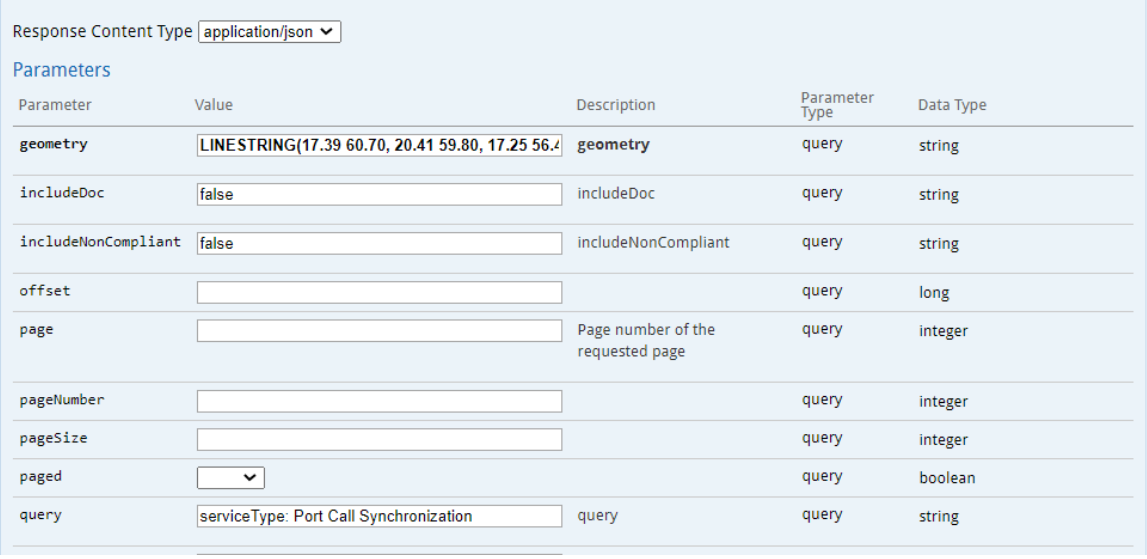
14.4 Test Variables

14.5 Testbed

Example 1: geometry combined with serviceType search

REQUEST

Search for services with provided geometry inside service coverage area and service type “Port Call Synchronization”.



Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
geometry	LINESTRING(17.39 60.70, 20.41 59.80, 17.25 56.4	geometry	query	string
includeDoc	false	includeDoc	query	string
includeNonCompliant	false	includeNonCompliant	query	string
offset			query	long
page		Page number of the requested page	query	integer
pageNumber			query	integer
pageSize			query	integer
paged			query	boolean
query	serviceType: Port Call Synchronization	query	query	string

Figur 1 - Request find service with geometry and query

https://serviceregistry.navelink.org/api/_searchGeometryWKT/serviceInstance?geometry=LINESTRING(17.39%2060.70%2C%2020.41%2059.80%2C%2017.25%2056.43)&includeDoc=false&includeNonCompliant=false&query=serviceType%3A%20Port%20Call%20Synchronization

RESPONSE

```
[
  {
    "id": 136,
    "name": "Port of Gavle",
    "version": "1.0",
    "publishedAt": "2020-11-16T10:53Z",
    "lastUpdatedAt": "2020-11-18T13:50Z",
    "comment": "This service is used to report arrival times to Port of Gävle and get confirmation or recommended RTA...",
    "geometry": {
      "type": "Polygon",
      "coordinates": [
        [
          [
            17.011284173205137,
            60.6578395558192
          ],
          [
            17.390312493517427,
            60.86243693611962
          ],
          [
            17.011284173205137,
            60.6578395558192
          ]
        ]
      ]
    },
    "geometryContentType": null,
    "keywords": "Voyageplan,Route,VIS,RTZ,ETA,SEGVX,SEKAS,Gavle",
    "status": "released",
    "unlocode": "SEGVX",
    "mmsi": "",
    "imo": "",
    "instanceAsXml": {
      "id": 147,
      "name": "SMA-MCP-PRODUCTION_Service_Instance-Port_of_Gavle_PCS.xml",
      "comment": "",
      "content": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n<ServiceInstanceSchema:serviceInstance ...",
      "contentContentType": "text/xml"
    },
    "instanceAsDoc": null,
    "implementedSpecificationVersion": null,
    "docs": null,
    "compliant": true,
    "instanceId": "urn:mrn:mcp:service:navelink:sma:instance:vis:portofgavle",
    "organizationId": "urn:mrn:mcp:org:navelink:sma",
    "endpointUri": "https://via.stm.sjofartsverket.se/portofgavle",
    "endpointType": null,
    "serviceType": "Port Call Synchronization",
    "designId": "urn:mrn:mcp:service:navelink:navelink:design:vis:rest:2.2",
    "specificationId": "urn:mrn:mcp:service:navelink:navelink:specification:vis:2.2"
  },
  {
    "id": 155,
    "name": "Facilitation of ship to shore reporting service",
    "version": "1.0.0",
    "publishedAt": "2020-11-19T13:48Z",
    "lastUpdatedAt": "2020-11-19T13:55Z",
    "comment": "The route plan of a ship must be reported to a coastal ..",
    "geometry": {
      "type": "Polygon",
      "coordinates": []
    }
  }
]
```


Figur 2 - Response from service registry

Example 2: Search with AND/ OR condition

REQUEST

Search for services with specific IMO and MMSI OR services with name containing “Baltic”.

Query = (imo: 9443255 AND mmsi: 276779000) OR name: Baltic

https://serviceregistry.navelink.org/api/_search/serviceInstance?includeDoc=false&includeNonCompliant=false&query=(imo%3A%209443255%20AND%20mmsi%3A%20276779000)%20OR%20name%3A%20Baltic

RESPONSE


```
[
  {
    "id": 62,
    "name": "Baltic Queen",
    "version": "1.0.0",
    "publishedAt": "2020-11-09T15:29Z",
    "lastUpdatedAt": "2020-11-26T15:06Z",
    "comment": "Ship voyage information mainly for meeting point calculation."
  },
  {
    "id": 61,
    "name": "Baltic Princess",
    "version": "1.0.0",
    "publishedAt": "2020-11-09T15:29Z",
    "lastUpdatedAt": "2020-11-26T15:06Z",
    "comment": "Ship voyage information mainly for meeting point calculation."
  },
  {
    "id": 148,
    "name": "Baltic Bright",
    "version": "1.0.0",
    "publishedAt": "2020-11-17T12:56Z",
    "lastUpdatedAt": "2020-12-03T09:17Z",
    "comment": "Provides voyage plans for Baltic Bright in RTZ 1.1STM."
  },
  {
    "id": 143,
    "name": "Baltic Navigational Warning Service",
    "version": "0.1",
    "publishedAt": "2020-11-16T13:51Z",
    "lastUpdatedAt": "2020-12-03T13:49Z",
    "comment": "The service provides Navigational Warnings in the Baltic region and Swedish T&P info."
  }
]
```


Figur 3 - Response from service registry

14.6 Test Sequence

TBD

14.7 Test results and discussions

TBD

14.8 Conclusions and Recommendations

TBD

15 Test Case 13 – Exchange of several different payloads

15.1 Description

The test case focus on exchanging payloads of different types. The test case is obsolete since SECOM is payload agnostic.

15.1.1 Test objectives

N/A

15.1.2 Acceptance Criteria

N/A

15.1.3 Test Scenarios

N/A

15.1.4 Test Environment

N/A

15.1.5 Test tools

N/A

15.1.6 Test data

N/A

15.1.7 Test procedure

N/A

15.2 Test results and discussions

N/A

15.3 Conclusions and Recommendations

N/A

16 ANNEX A Observations

The following table contains a compiled list of observations collected during the SECOM test project.

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-001	Converting signature to HEX may add carriage return signs, but it can also be on one line. Today not described in SECOM	Building Testbed A	affects the JSON or XML affects interoperability Need to be described in SECOM.	7 Data Protection
STPrj-002	Data may need padding if shorter than signing key. Today not described in SECOM		Amended in 7.4.	7 Data Protection
STPrj-003	SECOM v20xx is missing description of what to sign. Q: What if the data is compressed? converted to Base64? Encrypted? Shall the original data file always be signed? Or shall the file prepared for transfer be signed?	Building Testbed A	The different alternatives is elaborated in 4.7.1 Discussion: What shall be signed?	7 Data Protection 5 Information Service Interface
STPrj-004	Update Link and Get By Link is not well defined in the document	Building Testbed B and the swagger file	Impact on the swagger file	Interface Upload Link and Get By Link
STPrj-005	It may be a security risk to exchange a URL to any external storage/web page	Building Testbed B and the swagger file	One approach could be that instead of uploading a URL, an identifier is uploaded, and then Get can be used to retrieve the object attached to the identifier.	Interface Upload Link and Get By Link
STPrj-006	Should both ResponseObject and Error ResponseObject be defined for every REST interface?	Building Testbed B and the swagger file	Removed when moved to Specification part. But it may need to be defined for the REST design of the interface.	
STPrj-007	Many identifiers in the different service interfaces makes it messy.	Building Testbed B and the swagger file	Propose to clean up and make consistent, and remove unnecessary identifiers.	

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-008	What shall the REST operation be named for Upload and Get now when we removed the type of message in the URL? Object, Message	Building Testbed B and the swagger file	Included suggestion in 5.7	5.7 Service interface definitions
STPrj-009	When data is incorporated in JSON object, such as in UploadObject, it tricky to restore the data exactly to match the original, hence difficult to verify the signature.		Description should be aligned technically with the corresponding description in S-100 (ed 4.0.0 sub clause 15-8.6).	7.3.3 Creation of digital signature
STPrj-010	Is it necessary/beneficial to exchange a filename as well? If the data is compressed into a ZIP-file you need to open and see the files inside before handle it further.			7.2 Data compression and packaging
STPrj-012	Converting signature to HEX may add carriage return signs, but it can also be on one line.		Add detailed description in SECOM	7.3.3 Creation of digital signature
STPrj-013	The signature is currently described to be in HEX format when added in the JSON/XML. But the data and PEM uses Base64. Could the signature also be in Base64 instead of HEX?		Base64 is a little bit more effective and it would be more consistent to exchange both data and signature as Base64.	7.3.3 Creation of digital signature
STPrj-014	Data may need padding if shorter than signing key.		Add detailed description in SECOM	7 Data Protection
STPrj-015	SECOM don't describ what to sign. Q: What if the data is compressed? Encrypted? Converted to Base64? Shall the original data file always be signed? Or shall the data prepared for transfer be signed?		Add detailed description in SECOM	7 Data Protection
STPrj-016	Update Link and Get By Link is not well defined in the document		Add detailed description in SECOM	5.7Service interface definitions
STPrj-017	It may be a security risk to exchange a URL to any external storage/web page		One approach could be that instead of uploading a URL, an identifier is uploaded, and then Get can be used to retrieve the object attached to the identifier.	5.7.7 Service interface – Get By Link

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-018	Should both ResponseObject and Error ResponseObject be defined for every REST interface?		Removed when moved to Specification part. But it may need to be defined for the REST design of the interface.	5.6.8 SECOM_ResponseCodeEnum
STPrj-019	Many identifiers in the different service interfaces makes it messy.		Figure 1: Propose to clean up and make consistent, and remove unnecessary identifiers.	5.7 Service interface definitions
STPrj-020	Currently the UploadObject contains a SECOM_SecurityMetadata object based on S-100. Another alternative would be to always exchange an ExchangeSet ZIP containing the necessary metadata to verify the signature, filename etc. Shall SECOM define its own SecurityMetadata? Or shall SECOM always require that an ExchangeSet is sent containing the signature?		One reason why SECOM defines its own SecurityMetadata is to stay independent on S-100, although the primary goal is to exchange S-products. We know that work is ongoing on ed 5, and one of the parts that is under revision is Part 4 and the model for ExchangeSet. By defining the object in SECOM based on S-100, it remains stable also for ed 5.	5.6.3 SECOM_ExchangeMetadataObject
STPrj-021	Review:You need to add what minimum cipher requirements that is acceptable. Because the developer usually use the easiest lowest one from his perspective.		Figure 6: All ciphers that is considered ok or as deprecated by big global security associations like NIST should be named and banned. For example RC4, md5, sslv3, sha-1 to name a few. Presented in a clear list that you find in index, because of the complexity and needs for continuous updates.	7.3.2 Data formats and standards for digital signatures, keys and certificates
STPrj-022	Review:When it comes to transport encryption todays standard ask for TLS v1.2 or higher. Here you need to look at the whole picture of what support clients that is used in software today is capable of using. This could potentially shut out a lot of current users that needs to make major changes of software and hardware. An analysis of consequences for each deprecation would be important input.			6.2.1 Secure communication channel

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-023	Review:There is a standard called OWASP ASVS, Application Security Verification Standard. It's recommended to have that as reference when you building applications and functions. There is levels in that standard so you don't have to "overdo it", where Level 1 is for non-critical applications, and Level 3 is for critical.		Should be considered for future development of the standard.	N/A
STPrj-024	Review:The core of information security is Confidentiality, Integrity and Availability. Sometimes you add traceability as a forth, even if it's more of a solution to keep integrity etc. But it plays a very important role in the ecosystem, both in normal operation and when you have an intrusion, breach or likewise. Nonrepudiation is very important and should define how to get identities confirmed with good traceability. A big question mark in all this is – by who? You have covered Confidentiality and Integrity, but not Availability. Also you should describe that in what level of classification of information (see page 28: Classification) you need what level of availability in. If it's critical data the time factor when the message arrive to receiver could be crucial.		Probably more implementation specific and therefore should be left to the parent application and not part of SECOM.	N/A
STPrj-025	Review: In certificate verification process, it would be advisable to explain that it needs to reverse lookup with the issuer PKI that the certificate actually is issued and that it's still valid. Not only has that it had a valid due date.		Certificates shall be possible to revoke, hence the authentication procedure shall contain a check against the certificate revocation list (CRL) or OCSP.	8.5.2 CRL – Certificate revocation list 8.5.3 OCSP – Online certificate status protocol

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-026	Review:DSA 2048 or higher is what is recommended today (started in about year 2010).		This has to be aligned with S100 Ed 4 standard which currently relies on 1024 key length. S100 Ed 5 suggest at least 2048 key length.	N/A
STPrj-027	Review:CBC is considered deprecated. Follow NIST recommendations.		Block Ciphers: For near term use, AES-128 and for long term use, AES-256.	7.4.2 Encryption algorithm
STPrj-028	Review:A SECOM PKI, is it multiple or single? Need to be cleared out. Who is scheme administrator? Contradiction that you can buy any global accepted authority, but you need a secom certificate. Hard to understand.		A SECOM PKI should be governed by a scheme administrator (SA). There can be several instances of SECOM PKI provided by multiple SAs, and an actor can be registered in several instances of SECOM PKI. SECOM compatible equipment are expected to support multiple instances of SECOM PKI.	8 SECOM PKI
STPrj-029	Review: Requirement of having CP/CPS (Cert policy statement) for SECOM CA/PKI		Should be considered for future development of the standard.	N/A
STPrj-030	Review: Requirement that Private Key should be stored offline and have a backup copy		Implementation specific requirement.	N/A
STPrj-031	Review:If every application should be able to encrypt, every application needs its own certificate. Might clear that out, could be interpreted that you have one certificate per vessel.		Implementation specific requirement.	N/A
STPrj-032	Review:CRL could safely be cached approximate 7days, but you should always if possible prefere online checks.		Certificates shall be possible to revoke, hence the authentication procedure shall contain a check against the certificate revocation list (CRL) or OCSP.	8.5.2 CRL – Certificate revocation list 8.5.3 OCSP – Online certificate status protocol

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-033	Review:Why double encryption? As I understand you describe encryption of payload as well as in transit (TLS). This creates more bandwidth and needs more power/take longer time. Less amount of data can be sent in every packet. What is the attack vector, what do we want to protect against?		Ongoing discussion, although part of this requirement is reliant on S100.	N/A
STPrj-034	Review: Shall SECOM be referencing ISO 27001 and/or NIST as Cyber Security Framework"		Should be considered for future development of the standard. ISO 27000 referenced although the implementation should maybe not be described in SECOM.	NIST might be easier and more clearly described.
STPrj-035	Use a passphrase to create key and iv (init vector), assuming the default iteration works?		Or, as an alternative would be to provide a key + iv as the input when encrypting/decrypting.	7.5. Generate encryption key
STPrj-036	TestTool (openssl) and the newer versions differ in how they derive key and iv from the provided passphrase. Also, in the newest version, note the *** Warning, as it is now recommended to use the pbkdf2 algorithm to derive keys from a passphrase. Pbkdf2 is available in dotnet as well, and so far seems to result in identical output compared to openSSL. But, this then need to define the exact same number of iterations in hashing to work. (openSSL defaults to 10000)		Not considered.	N/A
STPrj-037	Missing details in SECOM document to implement signing of data.		Capture the required details and add detailed description in SECOM	7.3.2 Data formats and standards for digital signatures, keys and certificates

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-038	Should/will SECOM constrain number of valid algorithms/ciphers or shall/will SECOM support several/all algorithms/ciphers?		Digital signatures in SECOM (and S-100) are implementations of the Digital Signature Standard (DSS). The DSS uses the Secure Hash Algorithm (SHA256) to create a message digest (hash) of the file content that is 256 bits long.	7.3.2 Data formats and standards for digital signatures, keys and certificates
STPrj-039	The certificates (PEM) contains CR/LF and Begin + end text, but not always consistently in all examples, which may cause exception. If not standardized the implementation need to be robust enough to handle with and without trailing CR/LF.		Check the SECOM document and make recommendations that increases the interoperability for exchanging signed keys (certificates).	5.6.4 Transfer of Public Key
STPrj-040	Error messages are not fully described in SMA swagger tool, and the swagger and document is not fully consistent.		Figure 25: Error messages need to be more detailed. Swagger file and document need to be consistent	5.6.10 Common HTTP response codes 5.6.8 SECOM_ResponseCodeEnum
STPrj-041	How much information about ID and Keys are necessary to exchange together with the Signature?		If the Public Certificate is attached, the ID is redundant. It's part of the information in the certificate.	N/A
STPrj-042	How much of the Root Key need to be exchanged?		Currently there is the signed root key, hence the Root Certificate, but the Thumbprint of the root certificate has also been added in the upload object. Further discussions are needed around this.	N/A
STPrj-043	Shall SECOM exchange its own SecurityMetadata with the signature even for ExchangeSet?		To cope with other data product types this should be included.	5.6.3 SECOM_ExchangeMetadataObject

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-044	New lines and white spaces in Base64, HEX and PEM. The approach in SECOM Test Project is to exchange the data in Base64 without new lines (one single row)openssl base64 –A exchange the signed public key as base64 single line without begin and end certificate texts exchange the signature in one single line HEX (will discuss Base64 format on the SECOM meeting)		Partly considered.	5.6.4 Transfer of Public Key
STPrj-045	The public key id is not necessary to exchange in separate field. It can be extracted from the certificate (signedPublicKey)		Considered.	5.7 Service interface definitions
STPrj-046	The complete signed root key is not necessary to exchange. The thumbprint is enough. The Root Certificate (signed root keys) are expected to be downloaded be each receiver from the trusted server.		Considered.	5.7 Service interface definitions
STPrj-047	Is it necessary to exchange datatype and ProductSpecification? Currently we exchange datatype to indicate if the data is an S100_dataSet, S100_exchangeSet or other generic data (such as RTZ)? The approach in SECOM Test Project is to keep datatype, but not necessarily ProductSpecification.		Suggest to split the different datatypes into two enum types.	5.6.6 ContainerTypeEnum 5.6.7 SECOM_DataProductType
STPrj-048	Is it necessary to exchange type/length on encryption key?		Considered and removed accordingly.	5.7.15 Service interface – Encryption Key
STPrj-049	Different cryptographic libraries use different binary encodings for signature. Consequence: Possibility to have invalid signatures only because for different libraries in use.		Define expected signature binary encoding in specification so users could choose libraries accordingly. When embedded within XML files, keys shall be PEM encoded so that the plain text can be inserted as an XML element.	7.3.2 Data formats and standards for digital signatures, keys and certificates

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-050	Secom specification does not define rules regarding encoding. Consequence: Different encodings might lead to errors (ASCII, UTF-8)		Define the rules for encoding selection. To be considered in future development.	N/A
STPrj-051	Review:Without reading annex, these patterns seems to use terms that is associated with different communication protocols, such as messaging. Also word message is commonly used to describe whole http request/response (headers, body), but in this context, it is used to describe just the body (content) part.Also term 'Technical response' is questionable, if it is only http code without body (content) or some specific model to represent error state. It also requires review to check if correct Exchange patterns have been used as both upload endpoints are set as ONE_WAY, but by descriptions, REQUEST_CALLBACK would be more suitable because of ack operation. Wider discussion is needed to consider exchange patterns, need and value they bring to specification. Consequence: Exchange pattern values might be unclear and misleading.		Use clear naming and meaning for exchange patterns without collision between communication protocols as SECOM should be only REST over HTTP. Consider if those brings ant actual value to specification.	
STPrj-052	Review: UploadObject name sounds like a method/ verb. Consequence: General naming consistency.		Rename to ObjectUpload or ObjectUploadModel which naturally sounds more like a noun than a verb (REST describes resource as noun).	
STPrj-053	In case of success, same model as for errors is returnedConsequence: Not consistent with HTTP and REST.		If success scenario is not supposed to return any data, 204(NoContent) status code should be returned.	
STPrj-054	Review:In HTTP and REST context endpoint is called as a service interface, which could suggest that it contains a set of operations. Consequence: General document readability.		Call it as more familiar name: endpoint/action/operation. Personal opinion: Object upload and object upload by link could logically be called object upload interface	

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-055	Enums are passed as integers. Consequence: OpenApi contract contains integer values without actual enum meaning. Additional mapping is neccessary to know, what number actually means.		Pass enums as string, so OpenApi contract would contain actual enum values also as generated client would have full enum without additional mapping.	
STPrj-056	Encoding column seems a mix of data type and its format (encoding). Mult column without reading its description seem to represent quantity, but actually represents if it must be passed or not. Consequence: Separation of technical agnostic and Rest design might confuse.		Separate Encoding to two columns as data type and specific format if it is optional. Data type could have finite list of possible values. Multi column could just use Mandatory and Optional values as it would make more sense.	
STPrj-057	compressionFlag is not mandatory. Consequence: Not clear what state is indicated when it is not passed and why it should not be passed at all as it is part of metadata.		Change property to mandatory so it would represent clear state. Or align it with dataProtection flag so it would be consistent that such fields might not be passed and that state would mean same thing.	
STPrj-058	DigitalSignatureValueObject sounds ambigious when inside it has attribute DigitalSignature. Consequence: General naming rules.		Could be renamed to DigitalSignatureModel/DigitalSignatureObject and could have attribute Value, that would store actual signature value.	
STPrj-059	Attribute digitalSignatureReference Consequence: General naming rules.		Could be part of digitalSignatureValueObject and renamed to Alghorithm.	
STPrj-060	Custom error model Consequence: Not using general practise.		Use rfc standard: https://tools.ietf.org/html/rfc7807	
STPrj-061	Error code as enum. Consequence: Expending or changing enum would break the contract.		Use string for error code as it would be easier to extend possible error codes without breaking the contract. Consider if different implemetations might have different error codes or wider range of them (when would come back from VendorApi for example).	
STPrj-062	Resource in singular form. Consequence: Not following common resource naming practise for REST		Use resources in plural form in url.	

Ref number	Observation	Found when …	Consequence/Proposal	Reference in SECOM Document
STPrj-063	Successful response is 200 with error response model to indicate success. Consequence: Not using appropriate HTTP code		If request was successful, it should response with 204 as no content is intended to be returned.	
STPrj-064	Missing 401 http code. Consequence: Not using appropriate HTTP code		If user is not authenticated, it should return 401.	
STPrj-065	Status code 500 is used to indicate bad request. Consequence: Not using appropriate HTTP code and good API practices		For errors that is caused by request validation and client can fix them by altering request, 400 (BadRequest) should be returned with error message describing how to fix it.	
STPrj-066	Status code 403 is described incorrectly and refers to No errors status code. Consequence: Might be confusing with 401.		Associate 403 status code with forbidden message also applying correct error code if needed.	