# Uppdrag om ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn

I Slutrapport för regeringsuppdragen *Fi2018/02150/DF, Fi2018/03037/DF och I2019/01061/DF* har Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet och Skatteverket tillsammans med DIGG analyserat och tagit fram förslag till åtgärder för att skapa ökad säkerhet och effektivitet i samband med elektroniska informationsutbyten inom och med den offentliga sektorn, bland annat genom ökad standardisering.

Inom uppdraget har samråd skett med aktörer som till exempel Datainspektionen, Försvarsmakten, Länsstyrelsen i Västra Götaland, Myndigheten för samhällsskydd och beredskap, Riksarkivet, Sveriges standardiseringsinstitut, Statistiska centralbyrån, Säkerhetspolisen, eSamverkansprogrammet och Sveriges Kommuner och Landsting.

Hänsyn har tagits till det arbete som pågår inom Vision e-hälsa 2025 och inom uppdraget om att utveckla rättsväsendets informationsförsörjning (Ju 2012/6639/SI). Arbetet har även beaktat Lantmäteriets uppdrag om att verka för en smartare samhällsbyggnadsprocess (Fi2018/00396/DF).

Uppdraget slutredovisas till Infrastrukturdepartementet den 15 augusti 2019.

Stockholm 190626
Ort datum

Anna Eriksson
Myndigheten för
digital förvaltning

Stockholm 190626
Ort datum

Annika Stenberg
Bolagsverket

Stockholm 190626
Ort datum

Martin Holmgren
Domstolsverket

Kalmar 24/7-2019
Ort datum

Janna Valik
E-hälsomyndigheten

Stockholm 190626
Ort datum

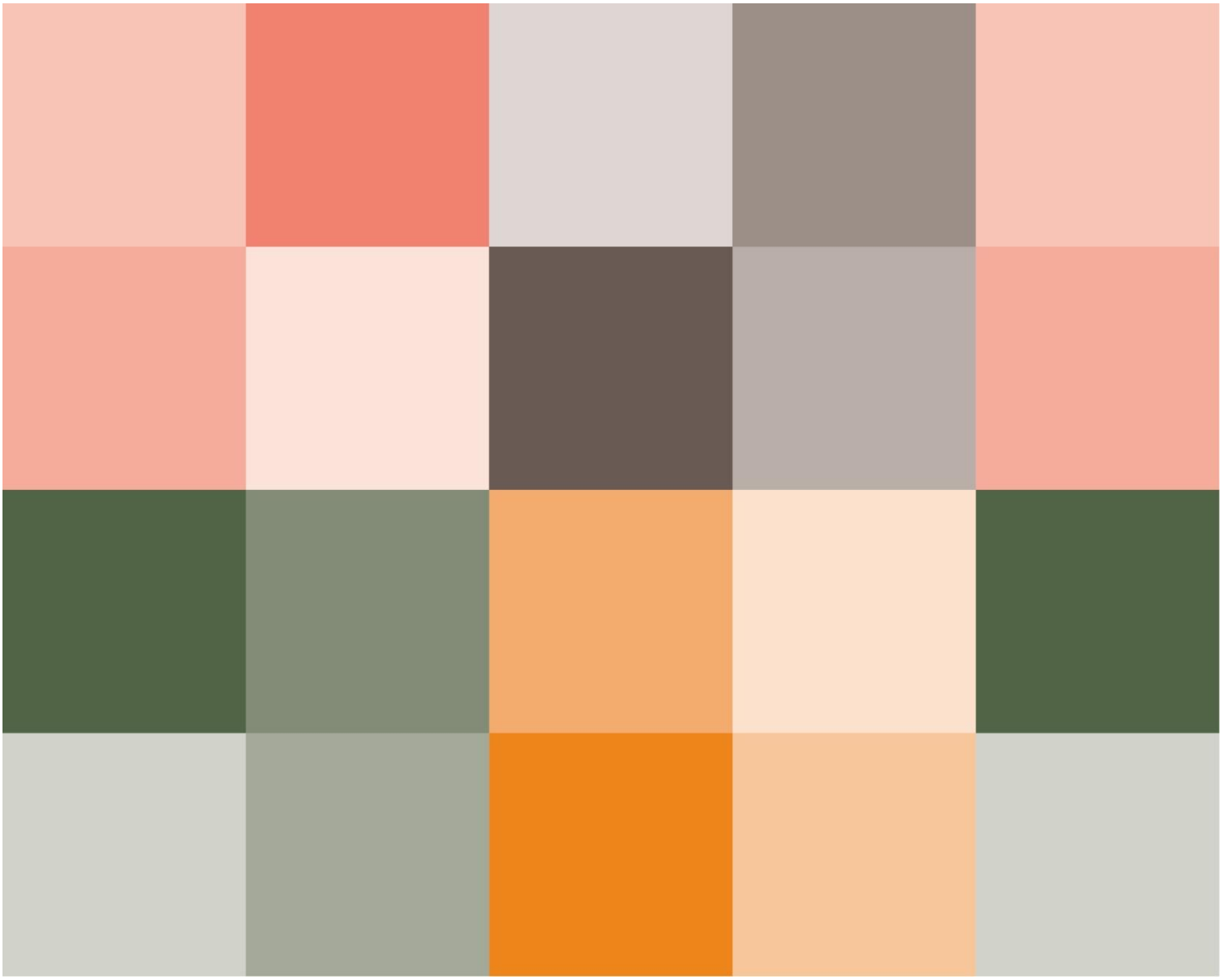
Nils Öberg
Försäkringskassan

Stockholm
Ort datum 190626

Susanne Ås Sivborg
Lantmäteriet

Solna 26/6 2019
Ort datum

Katrin Westling Palm
Skatteverket



# *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn*

Slutrapport i regeringsuppdraget Fi2018/02150/DF, FI2018/03037/DF och I2019/01061/DF

DIGG Dnr: 2019-100

# Sammanfattning

Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Skatteverket och Myndigheten för digital förvaltning (DIGG) har haft i uppdrag att tillsammans analysera och lämna förslag som syftar till att skapa ökad säkerhet och effektivitet i samband med elektroniska informationsutbyten inom och med den offentliga sektorn.

Myndigheterna har genomfört en behovsanalys där man har identifierat och prioriterat förvaltningsgemensamma behov. Behovsanalysen lyfter prioriterade behov kopplade till informationshantering, tillit och säkerhet, informationsutbyte och digitala tjänster.

Myndigheterna har genomfört en omvärldsanalys där befintliga nationella lösningar för informationsutbyte och lösningar från omvärlden har beskrivits och analyserats för att ta tillvara på lärdomar och insikter. Omvärldsanalysen visar att de nationella befintliga lösningarna behöver kompletteras med gemensamma regelverk, standarder och förvaltningsgemensamma byggblock för att möjliggöra ett överskridande utbyte mellan sektorer i det offentliga och med privat sektor. Det bedöms inte lämpligt att ersätta dagens befintliga infrastruktur med en lösning från omvärlden.

Utifrån analyserna föreslår myndigheterna att det ska finnas fyra kategorier av förvaltningsgemensamma byggblock i ett ekosystem med förvaltningsgemensam digital infrastruktur för informationsutbyte. Lösningen beskrivs som en konceptuell arkitektur och förslag lämnas även gällande styrformer och reglering av ansvar för byggblocken. De fyra kategorierna är digitala tjänster, informationsutbyte, informationshantering samt tillit och säkerhet.

För att realisera byggblocken föreslår myndigheterna ett antal förutsättningsskapande åtgärder som bedöms vara nödvändiga första steg mot ett säkrare och effektivare informationsutbyte. Myndigheterna föreslår att regeringen säkerställer en nationell styrform för att kunna besluta om aktiviteter för utveckling och realisering av en förvaltningsgemensam digital infrastruktur för informationsutbyte. Vidare föreslås nya regeringsuppdrag och finansiering för att analysera, utveckla och realisera en färdplan och realisera de prioriterade byggblocken. Slutligen föreslås inrättande av ett rättsligt beredningsorgan, för att säkerställa att det finns långsiktiga rättsliga förutsättningar för byggblocken att tas fram.

# Innehållsförteckning

# 1 Inledning

## 1.1 Uppdraget och bakgrund

Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Skatteverket och Myndigheten för digital förvaltning (DIGG) fick under våren 2018 i uppdrag[1] att tillsammans analysera och lämna förslag som syftar till att skapa ökad säkerhet och effektivitet i samband med elektroniska informationsutbyten inom och med den offentliga sektorn, bland annat genom en ökad standardisering.

Med elektroniskt informationsutbyte i detta sammanhang avses ett systematiserat tillgängliggörande av grunddata, samt annat utbyte av strukturerad och ostrukturerad information, exempelvis ärendestatus och meddelanden mellan aktörer.

I ett tidigare uppdrag konstaterades att ansvaret för grunddata behöver tydliggöras och att ett nationellt ramverk ska etableras. Själva tillgängliggörandet av grunddata i form av tekniska tjänster och infrastruktur hanteras inom detta uppdrag, detta uppdrag är dock inte avgränsat till att bara hantera grunddata utan informationsutbyte med och inom offentlig sektor i stort.

Sverige saknar flera av de förvaltningsgemensamma grundläggande komponenterna och lösningarna som finns i jämförbara länder. Bristen på en nationell digital infrastruktur har lett till många myndighets- och sektorsspecifika lösningar, som skiljer sig från varandra, vilket i stor utsträckning har resulterat i en ineffektiv ordning för den offentliga sektorn som helhet. Statliga myndigheter och kommuner har hittills i huvudsak utvecklat lösningar för elektroniskt informationsutbyte utifrån egna verksamheters behov och förutsättningar. Avsaknaden av styrning och samordning av den förvaltnings-gemensamma nivån samt de olika utformade sektorsansvaren, har lett till att rättsliga frågor och säkerhetsfrågor fortfarande utgör hinder, som inte kan lösas mellan enskilda parter.

Problembilden kan sammanfattas i att det i dagsläget i Sverige finns:

- Lösningar för informationsutbyte inom olika sektorer och domäner som inte är heltäckande.
- Olika lösningar för informationsutbyte som fyller samma ändamål.
- Lösningar för informationsutbyte som är framtagna för specifika ändamål och ofta bilateralt mellan två aktörer. Dessa kan inte återanvändas eller skalas upp på grund av avsaknad av exempelvis rättsligt stöd.

[1] Uppdrag om ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn (Fi2018/02150/DF, FI2018/03037/DF och I2019/01061/DF).

- Avsaknad av gemensamma standarder och återanvändbara tekniska komponenter och byggblock för informationsutbyte.
- Otydlighet kring vem som ska ansvara för förvaltningsgemensamma eller nationella byggblock och standarder för informationsutbyte.
- Avsaknad av styrning och samordning av den förvaltningsgemensamma nivån och sektorsansvaret ser olika ut för olika sektorer.
- Rättsliga frågor och säkerhetsfrågor som skapar hinder som inte kan övervinnas i enskilda projekt utan informationsutbyte sker på papper, medan privatpersoner och företag får agera kurirer mellan myndigheter.

## 1.2 Målbild

Enligt regeringsuppdraget behöver styrningen och samordningen av den offentliga sektorns informationsförsörjning stärkas genom att tydliggöra ansvarsfördelningen och öka standardiseringen. Myndigheternas tolkning av målbilden enligt uppdraget är att det i Sverige ska finnas en förvaltningsgemensam digital infrastruktur med förvaltnings-gemensamma lösningar som bidrar till effektivt och säkert informationsutbyte och är tydligt reglerade avseende myndighetsansvar.

## 1.3 Metod och genomförande av uppdraget

Uppdraget har genomförts i projektform, med en projektstyrgrupp sammansatt av en representant från varje organisation som tilldelats uppdraget samt Sveriges kommuner och Landsting (SKL). DIGG har haft en samordnande projektledarroll och samtliga organisationer som tilldelats uppdraget samt SKL har tillsatt resurser i ett antal olika arbetsgrupper. Arbetsgrupperna har haft fokus på olika områden i rapporten, nämligen behovsanalys, omvärldsanalys, arkitektur, juridik, säkerhet, samt samordning och kommunikation. Månadsvis har samtliga inblandade samlats för gemensam informationsspridning, analys och planering. Styrgruppen och flera av arbetsgrupperna har delats med regeringsuppdraget Säker och effektiv tillgång till grunddata och båda uppdragen har närvarat i de ovan beskrivna månadsmöten som hållits.

## 1.4 Avgränsningar

Enligt uppdragsbeskrivningen ska de förslag som myndigheterna kommer med rymmas inom gällande rätt.

Myndigheterna har i uppdraget inte tagit höjd för hantering av säkerhetsskydds-klassificerade uppgifter. Detta, då denna typ av information ställer höga och särskilda krav på säkerhet enligt säkerhetsskyddslagen (2018:585) samt att denna information utbytes i

begränsad utsträckning mellan myndigheter och företag. När så sker, görs detta nästan uteslutande under starkt reglerade former mellan väl definierade aktörer.

## 1.5 Begrepp

En central aspekt av digitaliserad samverkan är att etablera en gemensam begreppsapparat. Genom att återanvända redan överenskomna begrepp så förstärker vi ett etablerat språkbruk för samverkan mellan olika aktörer. Begreppen nedan är de begrepp vi använder i denna rapport.

| Viktiga begrepp | Beskrivning | Källa |
|---|---|---|
| Aktör | Människa eller organisation som agerar i samverkan. | Vägledning för digital samverkan (eSamverka) |
| Asynkron kommunikation | Vid asynkron kommunikation är parterna tidsmässigt oberoende av varandra. Askynkron innebär överföring som inte är samtidig. | Terminologicentrum TNC: Basord i våra fackspråk 2012. |
| Begreppsmodell | Grafisk representation av relationen mellan begreppen i ett sammanhängande begreppssystem. | Vägledning för digital samverkan (eSamverka) |
| Byggblock | Ett byggblock är grundläggande digital service infrastruktur, som möjliggör och kan återanvändas i mer komplexa digitala tjänster.<br><br>Ett byggblock kan bestå av tekniska förmågor, men också standardiserade modeller och mönster som ska kunna återanvändas vid digitalt informationsutbyte. | CEF Definitions Regulation (EU) No 283/2014 |
| Data | Representation av fakta, idéer eller liknande i en form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel. | Rikstermbanken |
| Domänansvarig, grunddatadomän | Nationellt samordningsansvar för produktion, samverkan och tillhandahållande av grunddata inom grunddatadomän. | Jmf Delrapport Detaljplaner (Lantmäteriet) |
| Förvaltningsgemensam digital infrastruktur | Infrastruktur, som innehåller olika byggblock eller komponenter som möjliggör digital utveckling. Den används av många aktörer och sektorer inom offentliga förvaltning för att lösa gränsöverskridande och sektorsövergripande behov. | Egen definition |

| | | |
|---|---|---|
| Förvaltningsgemensamma lösningar | Lösningar, såsom byggblock eller komponenter, som kan användas av många aktörer och sektorer inom offentliga förvaltning för att lösa gränsöverskridande och sektorsövergripande behov. | Egen definition |
| Grunddatadomän | Ansvarsområde grunddata, till exempel Person, Företag, Fastighetsinformation och Geografisk information. | Egen definition |
| Information | Innebörd hos data. | Rikstermbanken |
| Informationsmodell | Grafisk representation av informationsobjekt. | Vägledning för digital samverkan (eSamverka) |
| Informationsobjekt | Bärare av information i en informationsmodell. | IRM |
| Informationsutbytesmodell | Modell som beskriver innehållet i informationsutbyte mellan två eller flera parter. | Vägledning för digital samverkan (eSamverka) |
| Informationsägare | Aktör som har ansvaret för den information som skapas och hanteras inom den egna verksamheten. | Vägledning för digital samverkan (eSamverka) |
| Interoperabilitet | Förmåga eller möjlighet hos system, organisationer eller verksamhetsprocesser att fungera tillsammans och kunna kommunicera med varandra genom att gemensamma regler följs. | Vägledning för digital samverkan (eSamverka) |
| Komponent | En avgränsad del i en infrastruktur som kan användas i olika sammanhang men som är fristående. Synonym med byggblock. | |
| Konsument | Aktör som mottar eller använder tjänst eller information. | Vägledning för digital samverkan (eSamverka) |
| Kund | Person eller organisation som har behov av en tjänst eller information. | Vägledning för digital samverkan (eSamverka) |
| Källa | Tjänst från vilken aktör kan hämta uppgifter. | Jmf Bolagsverket (begreppsmodell för sammansatt bastjänst) |
| Metadata | Data om data, till exempel datum för beslut. | Vägledning för digital samverkan (eSamverka) |

| | | |
|---|---|---|
| Producent | Aktör som tillhandahåller tjänst eller information. | Vägledning för digital samverkan (eSamverka) |
| Samverkan | Olika aktörer som samverkar mot fastställda effektmål och värden för kund. | Vägledning för digital samverkan (eSamverka) |
| SLA – Service Level Agreement | Avtal som beskriver servicenivån på en tjänst. Det kan handla om t.ex. Svarstider eller när en tjänst får stå stilla för uppdateringar. | CEF Glossary |
| Standard | En standard är en gemensam lösning på ett återkommande problem. | Svenska institutet för standarder |
| Synkron kommunikation | Synkron kommunikation sker i realtid, d.v.s. samtidig kommunikation mellan ett antal parter. | Terminologicentrum TNC. Basord i våra fackspråk 2012. |
| Tjänst | Paketerad service eller lösning som erbjuds för att tillgodose ett behov | Vägledning för digital samverkan (eSamverka) |
| Öppna data | Med öppna data menas all information som uppfyller kraven för så kallad öppen kunskap, det vill säga information som tillhandahålls fritt utan krav på avgifter och med få eller inga tekniska eller rättsliga begränsningar för hur den får användas. | Digitaliserings-rättsutredningen |

# 2 Behovsanalys

**Sammanfattning:** Myndigheterna bedömer att det behövs en tydlig styrning för följande kategorier av förvaltningsgemensamma behov:

- *Informationshantering*. Behovet är att kunna lita på informationen och kunna bedöma informationskvalitén.
- *Tillit och säkerhet*. Behovet är att bland annat kunna kontrollera att en identifierad aktör har rätt att få ta del av informationen.
- *Informationsutbyte*. Behovet är att bland annat kunna söka, sammanställa, filtrera, delge, få åtkomst till och få uppdateringar på information från flera källor (detta omfattar så kallad synkron och asynkron meddelandehantering).
- *Digitala tjänster*. Behovet är att bland annat kunna sätta villkor för informationsutbyte i till exempel Min profil.

Enligt uppdraget ska myndigheterna genomföra en behovsanalys avseende informationsutbyte inom och med offentlig sektor. Behovsanalysen har gjorts mot bakgrund av ca 260 användningsfall från Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Naturvårdsverket, Skatteverket och SKL. Behov som har redovisats i uppdraget om säker och effektiv tillgång till grunddata (Fi2018/02149/DF, Fi2018/03036DF och I2019/01060/DF) har också beaktats.

Behoven har beskrivits via användarfall och behovsmönster. Användarfallen är framtagna utifrån olika perspektiv, både med ett tydligt ”utifrån och in perspektiv” där nyttan uppstår hos part utanför den egna organisationen men också med ett ”inifrån och ut”-perspektiv vilket innebär att nyttor uppstår inom den egna organisationen. Majoriteten av de beskrivna användarfallen utgår ifrån den egna organisationens behov.

Redovisningen i denna del av uppdraget sker i avgränsad form, för fördjupat material hänvisas till projektrapporter och arbetsmaterial som tagits fram av myndigheterna inom ramen för uppdraget. Slutsatserna av behovsanalysen sammanfattas i detta kapitel utifrån de förvaltningsgemensamma behov som har identifierats och som bedöms vara prioriterade.

Syftet med behovsanalysen har varit att ta fram underlag till förslag till en konceptuell arkitektur för förvaltningsgemensamma lösningar, som beskrivs i kapitel 4.

## 2.1 Identifierade behov

Myndigheterna har, mot bakgrund av insamlade aktörspecifika användningsfall, identifierat 16 grundläggande aktörsöverskridande behov, nämligen:

*För informationshantering*

1. Kunna lita på informationen.
2. Kunna bedöma informationskvaliteten.

*För tillit och säkerhet*

3. Veta att en aktör ha rätt att få ta del av information.

*För informationsutbyte*

4. Utbyta information i enskilt ärende.
5. Utbyta information som är fakta inom ärenden.
6. Utbyta information i olika ärenden, inom samma fråga.
7. Söka, sammanställa och filtrera information från flera källor.
8. Utbyta information med tredje part.
9. Hantera gemensamma planer runt ett objekt.
10. Kunna boka möten digitalt.
11. Kunna förbereda underlag utan officiellt ärende/ Kunna ha digital dialog om icke färdigt underlag.
12. Meddela aktör om beslut/förslag/meddelande.
13. Meddela aktör om beslut/förslag/meddelande och få en kvittens tillbaka.
14. Söka, sammanställa och filtrera information från flera källor.
15. Utbyta information om verksamheten.

*För digitala tjänster*

16. Sätta villkor för informationsutbyte i t.ex. Min profil.

Myndigheterna har analyserat de aktörspecifika behoven i användningsfallen utifrån standarden för kvalitativa aspekter ISO 25010[2] för att hitta de gemensamma, aktörsöverskridande, beståndsdelarna. Standarden utgår från ett antal områden som beskriver gemensamma nämnare i ett användningsfall. Standardens områden rör följande kategorier: aktör, interaktion, betydelse/vikt, förtroende, flexibilitet och reaktionsförmåga. Följande slutsatser har dragits utifrån standarden. Slutsatserna presenteras som generella krav på en arkitektur över den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte.

*Aktör*: En arkitektur som möter behoven bör inte avgränsas till någon viss typ av aktörer. Såväl offentliga som privata aktörer omfattas av behoven. Vid ett informationsutbyte förekommer två kategorier av huvudsakliga aktörer som brukar benämnas producent och konsument.

[2] ISO/IEC 25010:2011 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models

*Interaktion*: En arkitektur som möter behoven bör omfatta informationsutbyte från en producent till en konsument, en producent till många konsumenter, många producenter till en konsument, och många producenter till många konsumenter.

*Betydelse/vikt*: En arkitektur som möter behoven bör skapa förutsättningar för förmågor och funktioner som till exempel att kunna skapa, läsa, uppdatera, söka och radera information för att utföra sina grundläggande myndighetsuppgifter.

*Förtroende*: En arkitektur som möter behoven måste omfatta förmågor och funktioner för övervakning, loggning etc. Säkra identiteter och tillit behövs för att kunna avgöra om en konsument ska få tillgång till viss information eller inte. Ökad grad av digitalisering är ett gemensamt behov som innebär att tidigare känd information ska återanvändas. Detta ligger i linje med etablerade principer för säkert och effektivt informationsutbyte som ”hämta från källan”, ”en uppgift en gång” och ”minska den administrativa bördan”. Andra aspekter inom området är att kunna genomföra kvalitetskontroller utifrån gemensamma profiler, eller ge service till olika intressenter.

Området innehåller också flera aspekter kring själva informationen såsom kvalitet, status, ursprung, känslighetsgrad etc. En konsument måste veta var informationen kommer ifrån, vilken kvalitet den har, om den är beslutad av en myndighet, om den behöver skyddas med hänsyn till regler om sekretess och integritetsskydd och vilken nivå av skydd som informationen ska omgärdas av för att kunna tas emot. En producent måste också ta hänsyn till dessa aspekter för att över huvud taget kunna lämna ut informationen till konsumenten.

Inom ramen för forskning och utveckling finns behov av att skapa så kallade testbäddar vilket ställer krav på anonymisering av information.

*Flexibilitet*: En arkitektur som möter behoven, måste vara flexibel för anpassning och utveckling. En gemensam nämnare för behoven är att det ställs krav från omvärlden och teknikutvecklingen på hög förmåga att ställa om system och ändra verksamhetsregler för ett effektivare och säkrare informationsutbyte. Omedelbar förändring mot bakgrund av incidenter gäller alla typer av informationsutbyte och kan handla om förändring inom en vecka. Nyttjande i realtid ställer krav på ökad leveranstakt som bedöms handla om förändringsförmåga inom en månad. Ny lagstiftning innebär förändring på en tidshorisont om ca 1 år.

*Reaktionsförmåga*: En arkitektur som möter behoven bör ta hänsyn till krav på hur snabb tillgång till informationen behöver vara. Självbetjäning och realtidsinformation kräver omedelbar åtkomstmöjlighet för konsumenten. Producentens behov av kontroll av en förfrågan om information kan fördröja åtkomsten upp till en timme. Komplexa bearbetningar kan ta upp till en dag.

Myndigheterna bedömer att samtliga 16 behov och krav som dessa ställer på en arkitektur tillgodoses idag i någon omfattning där behovet av digitalt informationsutbyte finns. Frågan är då vad är det som saknas för att uppnå ett mer effektivt och säkert

informationsutbyte? De huvudsakliga problemen som omgärdar behoven är att de olika befintliga lösningarna

- inte återanvänds nationellt,
- inte är heltäckande utifrån behov och
- är många och olika för samma eller liknande behov.

Det som bedöms saknas är en nationell styrning av gemensamma beståndsdelar i ett informationsutbyte som återkommer i de olika behoven.

## 2.2 Prioriterade gemensamma behov

Sammanfattningsvis kan konstateras att det övergripande gemensamma behovet är att enkelt och på ett säkert sätt, kunna dela eller få tag på relevant information inom och med offentlig förvaltning. Det ska vara enkelt att veta var, hur, när och till vem information kan tillgängliggöras.

Det är behovet av att det ska vara *enkelt* och *säkert* som föranleder behov av standardisering och därmed av nationella digitala lösningar som kan återanvändas vid informationsutbyte.

Myndigheterna bedömer att det behövs gemensam styrning för följande övergripande gemensamma behov, som därmed anses vara prioriterade.

Det behövs ett gemensamt ramverk som kan tillämpas på följande behov.

- *Informationsutbyte.* Behovet avser att kunna söka, sammanställa, filtrera, delge, få åtkomst till och få uppdateringar på information från flera källor, i informationens olika stadier och lägen (inkluderat meddelandehantering). Kommunikation ska kunna ske dubbelriktat. Detta övergripande mönster handlar om behovet av enklare digital åtkomst till information i ett informationsutbyte. Offentliga aktörer behöver ofta ta del av information från flera olika källor vid handläggningen av ett ärende, gemensam fråga, tillsyn eller olika rapporteringsskyldigheter. I sådana situationer uppstår behov av att på ett enkelt sätt hitta och få åtkomst till information mellan många aktörer som producerar informationen och många aktörer som behöver konsumera informationen. Exempel: ärendehandläggning inom socialtjänsten, samverkansprojekt för att motverka fel, fusk och organiserad brottslighet, rehabiliteringsärenden och detaljplaneprocessen mm. Behovet omfattar asynkron och synkron meddelandehantering.

- *Säkerhet och tillit.* Behovet avser att kunna kontrollera att en identifierad aktör har rätt att få ta del av informationen. Detta övergripande mönster är ett exempel på behovet av digitala funktioner som ger säker åtkomst till information och därmed ett säkert informationsutbyte. Exempel på sådana funktioner är säker

identifiering, gemensam behörighetshantering och klassning av information utifrån bland annat regler om dataskydd (sekretess, integritet och säkerhet).

- *Informationshantering:* Behovet handlar om att kunna lita på informationen och kunna bedöma informationskvalitén. Detta övergripande mönster är en aspekt som påverkar såväl effektiv som säker digital informationshantering hos en aktör. Mönstret ställer krav på en gemensam kvalitetsmodell för information som behöver finnas nationellt tillgänglig. Motsvarande krav på informationens innehåll har identifierats i analysen kring grunddata som gjorts i regeringsuppdraget ”säker och effektiv tillgång till grunddata”.[3]

- *Digitala tjänster*. Detta behov handlar om att kunna sätta villkor för informationsutbyte i till exempel Min profil.

De ovan identifierade behoven räcker inte utan behöver läsas tillsammans med behovsanalysen i nämnda uppdrag. Utifrån ett grunddataperspektiv behövs det ett gemensamt ramverk som möjliggör att det går att använda grunddata samt annan strukturerad eller ostrukturerad information digitalt. Detta övergripande mönster handlar om standardisering av den information som behöver vara nationellt tillgänglig. Enbart enkel och säker åtkomst är inte tillräckligt för att åstadkomma effektivitet.

Information måste också kunna vara digitalt användbar, vilket kräver att den förbereds för en standardiserad användning. Med standardisering menas att informationen är beskriven och utformad utifrån gemensamma modeller och informationsstandarder så att den exempelvis kan kombineras med andra data. Begreppet grunddata används här som ett samlingsnamn på information som är viktig i samhället och därmed är konstant efterfrågad. Behovet beskrivs närmare i regeringsrapporten till uppdraget om säker och effektiv tillgång till grunddata.

[3] Bolagsverket, Myndigheten för digital förvaltning (DIGG), Lantmäteriet och Skatteverket, *Uppdrag om säker och effektiv tillgång till grunddata – slutrapport för regeringsuppdragen (Fi2018/02149/DF och I2019/01060/DF), DIGG dnr 2018-31*

# 3 Omvärldsanalys

**Sammanfattning**: Omvärldsanalysen visar på att det finns viktiga lärdomar och insikter att ta tillvara på från EU, de analyserade länderna och från befintliga nationella lösningar och initiativ.

Den befintliga svenska infrastrukturen för informationsutbyte som finns idag uppfyller eller har åtminstone tekniska förutsättningar att uppfylla merparten av de behov som har identifierats inom olika sektorer och domäner. De befintliga lösningarna behöver kompletteras med gemensamma regelverk, standarder och förvaltningsgemensamma byggblock för att bli effektivare och säkrare och för att möjliggöra ett överskridande utbyte mellan sektorer och med privat sektor.

Det bedöms inte lämpligt att ersätta dagens befintliga infrastruktur med en lösning från omvärlden. Det finns dock flertalet komponenter i form av förvaltningsgemensamma byggblock att inspireras av och återanvända. Byggblocken behöver utformas utifrån Sveriges behov och anpassas till Sveriges rättsliga förutsättningar.

Det finns även viktiga insikter och erfarenheter kring framförallt styrning, ekonomiska effekter och lagstiftning att ta tillvara på från olika länder vid skapandet av förvaltningsgemensamma lösningar i Sverige.

De länder som har lyckats med ett förvaltningsgemensamt informationsutbyte har skapat ett överskridande utbyte (både inom och med den offentliga sektorn) genom att skapa förutsättningsskapande komponenter. Länderna har inte sett informationsutbytet primärt som en teknisk utmaning utan arbetat med översyn av lagstiftning, skapat centrala finansieringsmodeller och haft en tydlig nationell styrning och politiskt ledarskap i frågor som obligatorisk anslutning och strategier.

Enligt uppdraget ska myndigheterna genomföra en omvärldsanalys av relevanta internationella och nationella lösningar för ett säkert elektroniskt informationsutbyte. Analysen ska omfatta både nationella och internationella initiativ och lösningar för informationsutbyte. Omvärldsanalysen ska beskriva för- och nackdelar med respektive lösning, kopplat till de prioriterade behoven samt hur kompatibel den är med andra befintliga lösningar. Särskilda aspekter som ska tas hänsyn till är kostnader, ekonomiska effekter, säkerhets-, sekretess- och integritetsaspekter, samt eventuella rättsliga hinder. Uppdraget ger också utrymme för att lyfta och ta tillvara på andra relevanta erfarenheter från andra länder.

Utifrån omvärldsanalysen ska myndigheterna lämna förslag på tänkbara förvaltningsgemensamma lösningar. Lösningarna ska vara förenliga med gällande rätt, till exempel regleringen om behandling av personuppgifter, offentlighetsprincipen samt beakta säkerhetsaspekterna. Det primära syftet med omvärldsanalysen är således att

fungera som input för förslag om förvaltningsgemensamma lösningar och förslag på åtgärder inom uppdraget.

I omvärldsanalysen  har fokus främst varit på ländernas lösning för informationsförsörjning och utbyte inom den offentliga sektorn. Dessa lösningar är i grunden tekniska lösningar, men mot bakgrund av frågeställningarna i uppdraget har en bredare ansats valts för att även kunna täcka in andra aspekter och förutsättningar.

Det är sju länder som valts ut för närmare granskning (Finland, Norge, Danmark, Belgien, Singapore, Nederländerna och Estland). Störst fokus har lagts på Estland, Finland och Danmark då de specifikt nämns i uppdraget. Övriga länder har valts ut för att de ligger långt fram i arbetet med en nationell digital infrastruktur och flera av ländernas arbete lyfts upp som bästa praxis av olika EU-initiativ och internationella jämförelser och mätningar på området.

Utöver olika länders lösningar för informationsutbyte har det gjorts en genomlysning av EU-initierade projekt och initiativ som har eller kommer att ha påverkan på området. Även ett urval av befintliga nationella lösningar och initiativ beskrivs i rapporten, Spridnings och Hämtningssystemet (SHS), Ineras tjänsteplattform (baserad på RIV-TA) och projektet Säker digital kommunikation (SDK) som baseras på eDelivery lyfts särskilt.

## 3.1 Genomförande

Huvudsaklig metod för omvärldsanalysen är litteraturstudier i form av en bred initial omvärldsbevakning och inventering av befintliga analyser och rapporter på området som har bäring på uppdraget. Syftet är att ta tillvara på tidigare erfarenheter och kunskaper som finns samlat på området samt ge ledning till vilka länder, initiativ och lösningar som är lämpliga att analysera ytterligare och lyfta.

Omvärldsbevakningen har kompletterats med erfarenhetsutbyten med representanter från utvalda länder och de nationella lösningarna för att få ytterligare kunskap och en djupare beskrivning av landets lösningar för informationsutbyte. Detta för att säkerställa en nyanserad bild av genomförda analyser samt att fånga upp insikter och lärdomar som kanske inte framgår av officiella rapporter. Metod som använts för erfarenhetsutbytena är semi-strukturerade intervjuer.

Omvärldsanalysen genomförs utifrån de i uppdraget listade särskilda aspekterna kompletterat med andra relevanta erfarenheter. Dessa analyseras genom att övergripande mönster och gemensamma drag presenteras och belyses med exempel från de olika länderna.

Beskrivningar av lösningar och initiativ och analys utifrån särskilda aspekter och relevanta erfarenheter med exempel återfinns i bilaga 1.

## 3.2 Lärdomar från omvärldsanalysen

Dagens befintliga infrastruktur i Sverige uppfyller eller har förutsättningar att uppfylla i stora drag de identifierade behoven i behovsanalysen inom de olika sektorerna och domänerna. Det primära behovet är således där det idag saknas strukturerad samverkan och det bedöms primärt vara i form av sektorsöverskridande interoperabilitet och informationsutbyte samt nationsöverskridande informationsutbyte över landsgränserna.

Inera och SKL konstaterar och rekommenderar i ett PM[4] att man bör bygga vidare på och förstärka befintliga lösningar för informationsförsörjning inom de sektorer där det redan finns samt att man tar fram kompletterande lösningar där lösningar saknas.

Även Ramböll är i sin rapport[5] inne på ett liknande resonemang och bedömer att det sannolikt inte finns någon samhällsnytta på varken kort eller medellång sikt i att byta ut befintliga lösningar mot en annan lösning från omvärlden.

Det är framförallt inte en teknisk utmaning att lösa informationsförsörjningen inom offentlig sektor. De tekniska lösningarna går normal att anpassa efter de förutsättningar och behov som finns. Jämfört med andra analyserade länder finns vissa centrala förvaltningsgemensamma byggblock såsom lösningar för identifikation och behörighet som saknas i Sverige och som bedöms vara viktiga förutsättningar för ett effektivt informationsutbyte.

Sverige står inför ett vägval när det gäller teknisk lösning och oavsett val är det viktigt att beslut tas kring huruvida befintliga lösningar ska existera parallellt, vidareutvecklas alternativt ersättas. Något som är tydligt utifrån erfarenheterna i de andra länderna är att det inte finns ett enkelt svar på frågan, det finns inte en lösning som är att föredra över en annan utan samtliga är behäftade med respektive fördelar och nackdelar.

Erfarenheter från de analyserade länderna pekar på viktiga framgångsfaktorer i form av tidig översyn av lagstiftning, centrala finansieringsmodeller, tydlig nationell styrning och politiskt ledarskap. Obligatorisk anslutning och användning av förvaltningsgemensamma lösningar lyfts av flera länder upp som avgörande och nationell styrning kan åstadkommas på flera olika sätt, antingen genom lagstiftning eller genom samverkan och avtalslösningar. Vid avsaknad av lagstiftning krävs starka alternativa incitament för att främja användning av förvaltningsgemensamma lösningar.

I vissa fall kanske Sverige inte ens kan göra ett eget val, inom ramen för EU samarbetet är det sannolikt att författningar och regleringar kommer peka på användning av specifika byggblock och tekniska lösningar för bilateralt utbyte av data. I kommunikationen av planen för Europa 2020 pekar EU-kommissionen dock på att det är upp till medlemsstaterna att själva välja teknisk plattform och systemstöd samt även om infrastrukturen ska vara decentraliserad eller central.

[4] Ett kunskaps PM om nationell interoperabilitet, Inera 2018-09-10
[5] Rapport om X-road – Ramböll 2016-01-29

Många av de länder som vi analyserat lyder under EU-lagstiftning och har således liknande rättsliga förutsättningar som Sverige när det kommer till exempelvis personuppgiftshantering. Det finns i huvudsak ingen anledning att ifrågasätta huruvidacentrala komponenter från de analyserade länderna skulle kunna återanvändas i Sverige, speciellt eftersom de i hög grad är anpassningsbara.

Behovet av informationsutbyte inom en sektor eller domän uppfylls idag i många avseenden av de många olika myndighetsspecifika lösningar som finns framtagna. Det bedöms inte ekonomiskt försvarbart att ersätta dagens befintliga lösningar med nya. En nationell digital infrastruktur och arkitektur bestående av förvaltningsgemensamma komponenter och byggblock är ett sätt att komplettera, standardisera och effektivisera dagens situation.

Störst samhällsekonomisk nytta av att tillgängliggöra grunddata och annan typ av myndighetsdata uppstår inom den privata sektorn. Det är således av stor vikt att förvaltningsgemensamma lösningar anpassas för att utbyta information även med den privata sektorn där legala förutsättningar finns.

Användningen av förvaltningsgemensamma lösningar kan främjas antingen genom regelverk och lagar gällande obligatorisk anslutning alternativt genom ekonomiska incitament.

Flera länder nämner att användningen av förvaltningsgemensamma tjänster behöver komma upp i en kritisk nivå för att nyttan ska kunna realiseras. För att främja användning av lösningen har man i flera länder lagstiftat om obligatorisk anslutning för offentlig sektor. I exempelvis Finland fanns också ekonomiska incitament för offentliga aktörer att ansluta sig genom möjlighet till medfinansiering.

Den lösning Sverige väljer bör vara anpassad utefter de specifika behoven och den redan nu rådande befintliga infrastrukturen i de olika domänerna och sektorerna. En lösning baserad på API ’er och förvaltningsgemensamma återanvändningsbara byggblock och obligatoriska standarder och regelverk, liknande lösningarna som finns i Singapore och i Finland bedöms vara den lämpligaste vägen att gå för att standardisera och effektivisera det domän- och sektorsöverskridande informationsutbytet.

Detta möjliggör och förbereder även för ett lättare utbyte med den privata sektorn när det finns rättsliga förutsättningar på plats. Flera myndigheter (bland annat Skatteverket, E-hälsomyndigheten och Lantmäteriet) har redan börjat ta fram strategier och lösningar baserade på API:er.

# 4 Förslag till gemensamma lösningar

**Förslag:** Myndigheterna föreslår att det ska finnas fyra kategorier av förvaltningsgemensamma byggblock i ett ekosystem med förvaltningsgemensam digital infrastruktur för informationsutbyte.

1. *Digitala tjänster*. Denna kategori omfattar byggblock som möjliggör standardiserad digital service från offentlig verksamhet för företag och medborgare. Byggblocken är

- Mina ombud (prioriterat)
- Mina ärenden
- Mina meddelanden
- Min profil

2. *Informationsutbyte*. Denna kategori omfattar byggblock som innehåller standardiserade mönster och gemensamma infrastrukturtjänster för enkel digital åtkomst till och utbyte av information hos informationskällor. Denna kategori syftar bland annat till att stödja kategori 1, men möjliggör även att privata aktörer kan bygga digitala tjänster som nyttjar offentlig data och information. Byggblocken är

- API-hantering (prioriterat)
- Adressregister
- Meddelandehantering

3. *Informationshantering*. Denna kategori omfattar byggblock som möjliggör indexering samt standardiserad maskinläsbar tolkning av egenskaper hos information och informationstjänster. Dessa förmågor och komponenter syftar till att stödja kategori 2.

- Metadatahantering
- Indexering

4. *Tillit och säkerhet*. Denna kategori omfattar byggblock som möjliggör standardiserade digitala funktioner för säkert informationsutbyte och syftar till att stödja ovan nämnda kategorier 1–3.

- Identitet (prioriterat)
- Auktorisation (prioriterat)
- Tillitsregelverk (prioriterat)
- Spårbarhet

- Tillgänglighet

Myndigheterna bedömer att gällande rätt behöver utvecklas för att säkerställa rättsligt stöd för byggblocken. Initialt föreslås att nödvändiga förstudier, utredningar och utveckling av de nationella byggblocken sker med stöd av regeringsuppdrag. Fördjupade säkerhetsanalyser krävs för samtliga byggblock.

Ansvaret för byggblocken föreslås ingå i det offentliga åtagandet kring den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte (rättslig styrmodell). Det innebär att det som utgångspunkt ska ingå i relevanta statliga myndigheters ansvar att utveckla och förvalta föreslagna byggblock.

Enligt uppdraget ska myndigheterna, mot bakgrund av behovs- och omvärldsanalysen, lämna förslag till tänkbara förvaltningsgemensamma lösningar. Myndigheternas förslag till förvaltningsgemensamma lösningar presenteras i detta kapitel mot bakgrund av följande utgångspunkter.

- *Privata aktörer*, inbegripet företag och medborgare, är motorn i den digitala utvecklingen (behovsdriven utveckling). Utvecklingen av effektivare och säkrare digitalt informationsutbyte måste involvera privata aktörer och utgå från samt värna om deras behov av att påverka, ha insyn i och tillit till utvecklingen.
- *Befintliga arkitekturer och lösningar* är en utgångspunkt för utvecklingen. Det är av principiella och rationella skäl inte lämpligt att dessa byts ut mot helt nya lösningar. Istället ska de utvecklas och understödjas så att de kan fungera i ett ekosystem med förvaltningsgemensam digital infrastruktur. Modeller, internationella standarder och principer från omvärlden behöver dock återanvändas i största möjliga mån.
- *Grundläggande förvaltningsgemensamma komponenter* är, utifrån ett nationellt perspektiv, en förutsättning för att möta behoven av ett effektivt och säkert informationsutbyte.
- *Samordnad myndighetsstyrning* är en framgångsfaktor för att åstadkomma säkra och effektiva förvaltningsgemensamma lösningar. Tydligt och utpekat nationellt ansvar för förvaltningsmyndigheter, i den digitala infrastrukturen, är en del av denna framgångsfaktor.
- *Agil utveckling*, det vill säga utveckling i små steg, är en framgångsfaktor för att säkerställa nyttorealisering och för att träna upp en snabbare anpassningsförmåga hos verksamheter utifrån digitaliseringsutvecklingen i stort.

För att omvandla resultatet från behovs- och omvärldsanalysen till förslag till lösningar och åtgärder, har myndigheterna grupperat resultatet i nationella förmågor utifrån ett antal områden. Utifrån identifierade förmågor har det tagits fram en konceptuell arkitektur över nationella byggblock i ett ekosystem med förvaltningsgemensam digital infrastruktur för informationsutbyte. Syftet med den konceptuella arkitekturen är att på ett övergripande plan illustrera vad som krävs för att åstadkomma ett effektivt och säkert

digitalt informationsutbyte. Med byggblock menas i denna slutrapport sådana förvaltningsgemensamma lösningar som myndigheterna har haft i uppdrag att föreslå.

## 4.1 Förslag till konceptuell arkitektur för förvaltningsgemensamma lösningar för informationsutbyte

Dagens arkitekturer har utvecklats över tid och haft till syfte att lösa de utmaningar som uppstått vid de givna tidpunkterna. Myndigheterna ser dagens arkitekturer kring informationsutbyte som en god bas för fortsatt utveckling. Syftet med den fortsatta utvecklingen är att åstadkomma standardisering, likriktning, och flexibilitet baserat på innovation och frivillighet. Detta för att öka digitaliseringstakten och därmed snabbare få del av den nytta digitaliseringen ger.

De förvaltningsgemensamma lösningarna presenteras nedan som byggblock i en konceptuell målbild i ett ekosystem med den förvaltningsgemensamma infrastrukturen för informationsutbyte. Ett byggblock kan bestå av juridiska, organisatoriska, semantiska och tekniska förmågor[6] och standardiserade modeller och mönster som ska kunna återanvändas vid digitalt informationsutbyte.

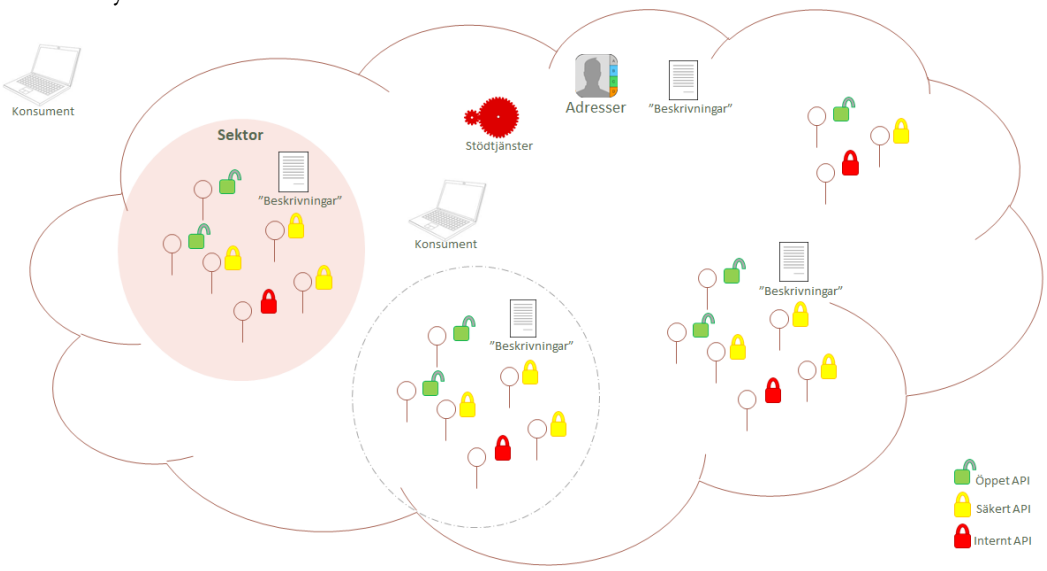
Med ekosystem avses hur aktörer och tjänster uppträder i samverkan och symbios med varandra i ett gemensamt balanserat system. Att vara en del av ekosystemet kräver en prestation av varje aktör för att bli "ekosystemredo". Den kan t.ex. vara krav att följa regelverk och standarder. Genom att definiera detta ekosystem kan lösningar och arkitekturer för säkerhet och effektivisering vidareutvecklas. Bland annat kan effektivare avtalsmodeller etableras.

En övergripande beskrivning av arkitekturen i ekosystemet är att den består av ett mönster med central tillgänglighet, baserad på löst kopplade byggblock som möjliggör utveckling hos många parallella aktörer samtidigt. Bastjänster medger åtkomst till centralt eller distribuerat lagrad information via informationsutbytesgränssnitt, API:er (Application Programming Interface), som publiceras nära informationslagringen.

Gartner beskriver hur API:er publiceras i ett ekosystem för att möjliggöra och främja serviceinnovation[7]. Även i EU:s CEF byggblock eDelivery beskrivs informationsutbyte

[6] EU, The new European Interoperability Framework, https://ec.europa.eu/isa2/eif_en - läst 2019-06-27
[7] Gartner - Government APIs Are About Delivering Outcomes, Not Technology

ske i ekosystem[8].




*Figur A, Ekosystem för informationsutbyte med och inom offentlig sektor*

Denna arkitektur tillåter löst kopplade komponenter skapas som successivt kan utvecklas med tiden. Detta ger den dynamik som krävs mellan likriktning och flexibilitet. Ett API och kan vara:

- Öppet – helt sökbara och synliga API:er för t.ex. öppna data
- Öppet säkert – sökbara och synliga API:er som kräver säker identifiering samtidigt som auktorisation mot användningsregler styr anslutning och informationsutlämnandet
- Interna – API:er som endast finns synliga och tillgängliga för intern användning

Myndigheterna föreslår att det ska finnas fyra kategorier av förvaltningsgemensamma byggblock, nämligen:

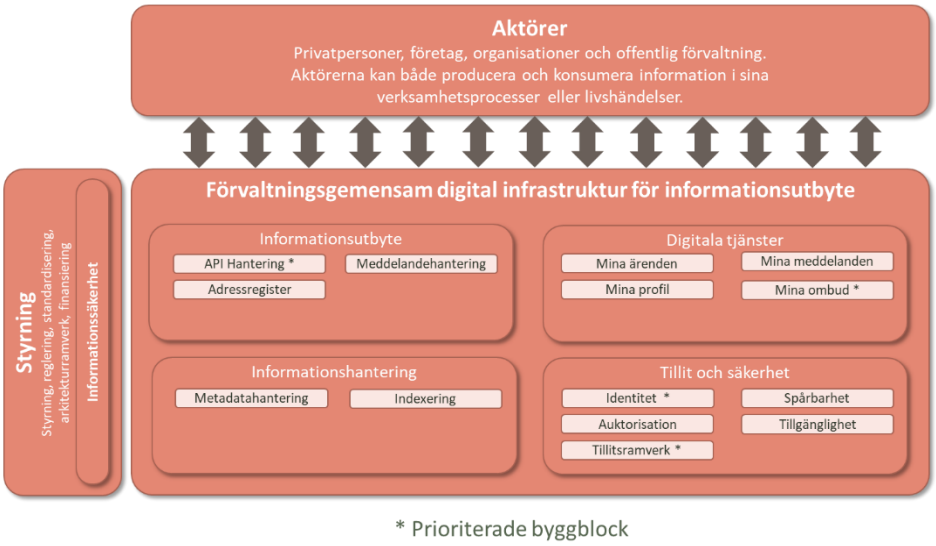
1. *Digitala tjänster*. Denna kategori samlar förmågor och byggblock som möjliggör standardiserad digital service med offentlig verksamhet för företag och medborgare. Kategorin avser inte hantera det faktiska utbytet av information mellan maskin och människa – användargränssnitt, användartjänster. Detta ligger utanför avgränsningarna för detta uppdrag.
2. *Informationsutbyte*. Denna kategori samlar förmågor och byggblock som innehåller standardiserade mönster eller gemensamma infrastrukturtjänster för enkel digital åtkomst till och utbyte av information hos informationskällor. Denna kategori syftar bland annat till att stödja kategori 1, men möjliggör även att privata aktörer kan bygga digitala tjänster som nyttjar informationen.
3. *Informationshantering*. Denna kategori samlar förmågor och byggblock som möjliggör indexering samt standardiserad maskinläsbar tolkning av egenskaper hos

[8] EU CEF-eDelivery, "The future is reuse of the CEF building blocks" 2017

information och informationstjänster. Dessa förmågor och komponenter syftar till att stödja kategori 2.

4. *Tillit och säkerhet.* Denna kategori samlar förmågor och byggblock som möjliggör standardiserade digitala funktioner för säkert informationsutbyte och syftar till att stödja ovan nämnda kategorier 1–3.

Nedan illustreras de olika kategorierna och dess byggblock som en konceptuell målbild. Med konceptuell menas att förslaget utgör en tes som kan behöva utvecklas i takt med de framsteg som görs under kommande år. Utvecklingen föreslås ske stegvis.




*Figur B. Konceptuell målbild som illustrerar vilka förvaltningsgemensamma byggblock som behövs för ett säkert och effektivt digitalt informationsutbyte.*

Följande förvaltningsgemensamma byggblock föreslås ingå i respektive kategori. Byggblock som är markerade med (*) är prioriterade och med det avses här inte vilka byggblock som är viktigare än något annat utan byggblock som är förutsättningsskapande eller grundläggande för att etablera ekosystemet. I bilaga 2 beskrivs de prioriterade byggblocken djupare. En fördjupad säkerhetsanalys behöver genomföras för vart och ett av byggblocken.

### 4.1.1 Digitala tjänster

| **Byggblock (*)** | **Mina ombud** |
|---|---|
| **Syfte** | Syftar till att en fysisk person ska kunna representera en annan fysisk eller juridisk person i en digital tjänst. Inkluderar utdelning av behörigheter baserat på företagens firmateckning och möjlighet att kontrollera vilka behörigheter som delats ut/tagits emot. |
| **Befintlig lösning** | Finns ej nationellt, men särskilda lösningar förekommer lokalt hos olika myndigheter för att hantera de egna behoven. |

| | |
|---|---|
| **Gap mot behov** | Behovsanalysens resultat kan inte mötas av någon befintlig lösning. Bolagsverket genomför förstudie som möter resultatet i behovsanalysen. |

| **Byggblock (*)** | **Mina ärenden** |
|---|---|
| **Syfte** | Byggblocket ger en samlad bild av en individs ärenden (person eller företag) i offentlig sektor. Behovet är att kunna följa ett större perspektiv på ärenden än specifika myndighetsärenden. Här avses t.ex. starta företag, rehabilitera från skada/sjukdom, etablera sig i landet. |
| **Befintlig lösning** | Finns ej nationellt, men många myndigheter och kommuner har egna lösningar. |
| **Gap mot behov** | |

| **Byggblock** | **Min profil** |
|---|---|
| **Syfte** | Syftar till att ge användaren rådighet över sin information hos offentliga aktörer så att denne kan se vilka aktörer som har tillgång till vad och har viss möjlighet att styra tillgång till informationen. Byggblocket hanterar även kontaktuppgifter och information om hur en individ vill interagera med offentlig sektor. |
| **Befintlig lösning** | Finns ej nationellt men särskilda lösningar förekommer för specifika behov exempelvis hos Bolagsverket (verksamt.se). Varje myndighet som har en funktion för ”mina sidor” har också skapat en del av detta byggblock. |
| **Gap mot behov** | Flera komponenter saknas idag eller har tveksam legal grund.<br>1. Det finns en otydlighet vem som är informationsägare för vissa gemensamma datamängder, t.ex. kontaktuppgifter<br>2. Idag saknas ofta sätt att tekniskt få åtkomst till informationen, det saknas standardiserade API:er från informationsägare för att hämta information<br>3. Som användare saknas i många fall möjlighet att agera sekretessbrytande för att kunna överföra information från en aktör till en annan (dataportabilitet) |

| | |
|---|---|
| | 4. Det saknas nationella byggblock för användare att få en översikt och möjlighet att styra informationsflöden. Det är inte enkelt för en användare att veta vart informationen om mig finns, vem som får ta del av denna information samt vem som tagit del av den?<br>5. Det saknas nationella byggblock för att följa en användares ärenden som sträcker sig över flera aktörer. |

| **Byggblock** | **Mina meddelanden** |
|---|---|
| **Syfte** | Att möjliggöra säker meddelandehantering till privatperson och företag |
| **Befintlig lösning** | Finns nationellt med möjlighet till vidareutveckling. |
| **Gap mot behov** | Verksamhetsanalys är under planering där gap och nyläge för Mina Meddelanden kommer att analyseras. |

### 4.1.2 Informationsutbyte

| **Byggblock (*)** | **API-hantering** |
|---|---|
| **Syfte** | Syftar till att likrikta funktionalitet för publicering, användning och exekvering av API:er i samband med informationsutbyte. |
| **Befintlig lösning** | Finns ej nationellt, men särskilda lösningar förekommer för specifika behov exempelvis hos Bolagsverket, Lantmäteriet, Skatteverket (Utvecklarportalen), E-hälsomyndigheten, Skogsstyrelsen med flera. |
| **Gap mot behov** | Nationell samordning och nationella lösningar saknas, exv. förutsättningar för att hitta och ansluta till API:er. |

| **Byggblock** | **Adressregister för digital kommunikation** |
|---|---|
| **Syfte** | Syftar till att säkerställa digital kommunikation utifrån digitala adresser så att meddelanden kan nå rätt adressat. Detta avser bland annat adressering till aktörer inom offentlig sektor (inkl. |

| | |
|---|---|
| | privata utförare), organisatoriska funktioner hos offentliga aktörer samt till företag och privatpersoner. |
| **Befintlig lösning** | Finns ej nationellt, men särskilda lösningar förekommer för specifika behov. Exempel: projektet SDK - Säker Digital Kommunikation[9], PEPPOL[10] - hantering av upphandlingar bl.a. gränsöverskridande. Både SDK och PEPPOL utgår i grunden från produkten eDelivery. Ytterligare exempel är HSA - hälso-och sjukvårdens adressregister, FAR – adressregister för Mina Meddelanden. |
| **Gap mot behov** | Nationell lösning saknas. |

| **Byggblock** | **Meddelandehantering** |
|---|---|
| **Syfte** | Meddelandehantering innebär att definiera gemensamma principer för utformning, transport och validering av digitala meddelanden samt för kvittens av mottagen leverans. I meddelandehantering ingår även funktion för notifiering. Exempel på behov är en myndighets behov av notifiering från en annan myndighet att en viss informationsvariabel såsom ett beslut fattats eller ändrats. |
| **Befintlig lösning** | Meddelandehantering finns nationellt för vissa specifika områden, men behöver utvecklad funktionalitet. Exempel SDK, PEPPOL. När det gäller notifiering så behövs en översyn kring möjligheterna att utveckla effektiva aviseringsfunktioner. |
| **Gap mot behov** | Idag saknas nationella principer, regler och riktlinjer för generisk meddelandehantering:<br>• Kryptera, försegla och verifiera meddelandeöverföring.<br>• Validering av meddelande (struktur och innehåll) och transportkuvert före sändning och efter mottagning.<br>• Hantera kvittenser.<br>• Spåra och övervaka.<br>För notifiering så behöver främst de juridiska förutsättningarna ses över men också utifrån behov titta på |

[9] SDK - https://www.inera.se/aktuellt/projekt/saker-digital-kommunikation/ - läst 2019-06-27
[10] PEPPOL - https://peppol.eu/ - läst 2019-06-27

| | |
|---|---|
| | hur det ska kunna skapas gemensamma principer för utformning. |

### 4.1.3 Informationshantering

| **Byggblock** | **Metadatahantering** |
|---|---|
| **Syfte** | Syftar till att standardisera beskrivningar av information och tjänster. Det ställer krav på exempelvis likriktad versionshantering, gemensamma beskrivningar av begrepp och skyddsklassning av information. Byggblocket har mer ramverkskaraktär än tjänstekaraktär |
| **Befintlig lösning** | Finns ej nationellt men särskilda lösningar förekommer, till exempel inom geodataområdet enligt lagen och förordningen om geografisk miljöinformation. FGS – Förvaltningsgemensamma standarder[11], riksarkivets standarder för hur information ska struktureras. I dag säkras efterlevnad genom publicering av maskinläsbara tjänstebeskrivningar, hos ett antal myndigheter men inte alla. |
| **Gap mot behov** | Det saknas nationella mönster, standarder och riktlinjer för metadata. Det saknas också regler för hur dessa standarder och riktlinjer bör beskrivas i tekniska protokoll. Även verktyg kan behövas för att hantera metadata, till exempel gemensamma definitioner. |

| **Byggblock** | **Indexering** |
|---|---|
| **Syfte** | Syftar till att effektivisera tillgängligheten till lagrad information, genom att tillgängliggöra ett index gällande var information om ett specifikt objekt finns lagrat. Därmed behöver inte den specifika informationsmängden sökas för att få tillgänglighet. |
| **Befintlig lösning** | Särskilda sektorsspecifika lösningar finns idag för varje informationsutbyte. Exempel: NPÖ – Nationell Patient Översikt[12] - central funktion som indexerar hos vilka vårdgivare en patient har sjukjournaler. |

[11] Förvaltningsgemensamma specifikationer - https://riksarkivet.se/fgs-earkiv

[12] Nationell patientöversikt - https://www.vardgivarguiden.se/avtaluppdrag/it-stod-och-e-tjanster/e-tjanster-och-system-a-o/beslutsstod/nationell-patientoversikt-npo/ - läst 2019-06-27

| | |
|---|---|
| **Gap mot behov** | Behovsanalysen pekar bland annat på Tillväxtverket och arbetet med verksamt.se. För dessa behov finns inga sektorsspecifika eller nationella lösningar. |

### 4.1.4 Tillit och säkerhet

| **Byggblock (*)** | **Identitet** |
|---|---|
| **Syfte** | Består av regler och processer som syftar till att en entitet (exempelvis juridisk eller fysisk person) alltid har en unik och konsistent digital identitet. |
| **Befintlig lösning** | Privatpersoner har en naturlig identifierare via samordnings- och personnummer. På samma sätt kan organisationer identifieras med organisationsnummer. Det finns dock inget regelverk eller process för hur personer inom en organisation kan ha en unik konsistent identitet i kommunikation med andra aktörer utanför sin egen organisation. |
| **Gap mot behov** | Det saknas nationellt övergripande lösningar för till exempel användning i tjänsten med knytning till juridisk person, IOT, maskin till maskin. |

| **Byggblock (*)** | **Auktorisation** |
|---|---|
| **Syfte** | Syftar till att säkerställa tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.[13] |
| **Befintlig lösning** | Samtliga aktörer måste hantera auktorisation för att klara informationssäkerhetskraven. Det saknas nationellt övergripande lösningar. |
| **Gap mot behov** | Det saknas nationellt övergripande lösningar |

| **Byggblock (*)** | **Tillitsregelverk** |
|---|---|
| **Syfte** | Syftar till att möjliggöra samverkan och säkerställa ett förenklat informationsutbyte. |

[13] SIS TR-50:2015 Terminologi för informationssäkerhet

| | |
|---|---|
| **Befintlig lösning** | Olika lösningar finns men ingen motsvarar behoven på ett nationellt plan. Exempel svensk e-legitimation, federationslösning för e-hälsa och skola, geodatasamverkan. |
| **Gap mot behov** | Det saknas nationellt övergripande tillitsregelverk och nationell lösning. |

| **Byggblock** | **Tillgänglighet** |
|---|---|
| **Syfte** | Syftar till att säkerställa åtkomst för behörig person vid rätt tillfälle. Åtkomst innebär interaktion mellan en användare och en resurs som resulterar i överföring av information dem emellan eller nyttjande av resurser.[14] Detta genom bl.a. SLA-databas (Service Level Agreement – avtal om tillgänglighet). |
| **Befintlig lösning** | Särskilda lösningar tas idag fram för varje organisation. |
| **Gap mot behov** | Nationellt skalbar lösning saknas. |

| **Byggblock** | **Spårbarhet** |
|---|---|
| **Syfte** | Syftar till att möjliggöra att i efterhand rekonstruera händelseförlopp. |
| **Befintlig lösning** | Särskilda lösningar tas idag fram för varje informationsutbyte. |
| **Gap mot behov** | Nationellt skalbar lösning saknas. |

### 4.1.5 Byggblockens påverkan på tillgängliggörande av grunddata

I rapporten Säker och effektiv tillgång till grunddata angavs att i denna rapport återkomma med lösningsförslag för tillgängliggörande av grunddata. De exempel på behov som lyftes i slutrapporten för säker och effektiv tillgång till grunddata var att:

- det ska finnas mycket hög tillgänglighet, med kravställda svarstider,
- tillgång till grunddata ska ske via maskinläsbara gränssnitt, och
- det finns en väl fungerande förändringshantering för grunddata.

Ovan nämnda krav bör även kunna tillämpas i en bredare kontext för annan typ av myndighetsdata.

[14] SIS TR-50:2015 Terminologi för informationssäkerhet

De byggblock som föreslås i denna rapport tar höjd för att kraven från grunddata ska kunna hanteras som en naturlig del i den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte.

## 4.2 Gällande rätt

### 4.2.1 Övergripande bedömning av byggblock

Fokus vid den rättsliga bedömningen av förslagen i rapporten har varit att ringa in vad som är möjligt att genomföra för att möta identifierade behov inom ramen för gällande rätt. Behov av rättsutveckling för att stärka styrningen inom området behandlas närmare under kapitel 6 om konsekvenser.

Myndigheterna bedömer att nationella förstudier, utredningar och utveckling av de nationella byggblocken kan genomföras med stöd av regeringsuppdrag. Detta gäller för samtliga byggblock. För att driftsätta tekniska komponenter av ett byggblock på *nationell nivå* eller utfärda bindande krav för ett byggblock på nationell nivå krävs dock att den ansvariga myndigheten har författningsstöd bestående av:

1. Rättsligt stöd för att tillhandahålla den tekniska komponenten i byggblocket till andra aktörer på nationell nivå.
2. Rättsligt stöd för att utfärda bindande krav för användning av byggblocket på nationell nivå.
3. Rättsligt stöd för att hantera information i byggblocket.

De byggblock som bedöms ha ett visst rättsligt stöd på samtliga punkter ovan enligt gällande rätt är de som omfattas av förordningen med instruktion för myndigheten för digital förvaltning (DIGG), och rör den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift. Förslagen i denna rapport kan dock innebära att det rättsliga stödet i denna del behöver tydliggöras eller utvecklas, vilket behöver analyseras närmare enligt föreslagna åtgärder i kap. 5.

Myndigheterna bedömer att den första frågan kan som minimum hanteras genom att förordningar med instruktion för berörda myndigheter utökas med relevanta regler. Om ansvarig myndighet ska kunna utfärda myndighetsföreskrifter kring ett byggblock, även för kommuner, krävs dock att byggblocket regleras i lag.

Myndigheterna bedömer att byggblocken kan komma att skapa samlingar av information som i sig skapar ett informationsutbyte. Dessa samlingar kan innehålla personuppgifter och vara av känslig karaktär. För att skapa sådana samlingar, bedöms det behövas särskilt rättsligt stöd, som förutom det som nämnts ovan inte finns idag.

En särskild rättslig utmaning avseende styrningen kring varje byggblock är att ansvaret för byggblocket kan vara fördelat på flera myndigheter. Därutöver kan användningen av byggblocket träffas av upphandlingsregler för kommuner som behöver byggblocket, vilket torde motverka syftet med att byggblocket finns.

En övergripande slutsats är att det kommer att krävas utveckling av gällande rätt för att säkerställa rättsligt stöd för byggblocken. Närmare om behovet av rättsutveckling behandlas i kapitel 6 om konsekvenser. Nedanstående avsnitt beskriver närmare den rättsliga ramen för den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte.

### 4.2.2 Övergripande beskrivning av gällande rätt

Juridiken kring förvaltningsgemensamma digitala lösningar kan inordnas främst under rättsområdet offentlig IT-rätt, som spänner över traditionella rättsområden inom bland annat offentlig rätt. Myndigheterna har valt att tillämpa en metod för avgränsning enligt detta rättsområde utifrån eSam:s checklista för jurister[15] som utgör en sammanställning av rättsliga frågeställningar och relevanta författningar vid samverkan i utvecklingsinsatser.

#### *4.2.2.1 Kompetensfrågor vid rättslig utvärdering av byggblocken*

- *Myndighetens rättsliga kompetensområde*: Att delta i en digital infrastruktur innebär att myndighetsuppgifter utförs. Myndigheternas verksamhet ska lyda under lag och andra författningar, se 1 § tredje stycket regeringsformen och 5 § första stycket förvaltningslagen. Det som myndigheterna har stöd i rättsordningen att göra utgör myndighetens kompetensområde.

  Regleringen av en myndighets kompetensområde sker främst genom myndighetens instruktion och av specialförfattningar som reglerar myndighetens verksamhet. Även mer generella författningar som rör myndigheters verksamhet, exempelvis förvaltningslagen och myndighetsförordningen anger uppgifter som myndigheter har och utgör grund för myndigheters kompetens. Förvaltningsuppgifter kan överlämnas åt kommuner, samt andra juridiska personer och enskilda individer. Förvaltningsuppgifter som innefattar myndighetsutövning får dock endast överlämnas med stöd av lag, se 12 kap. 4 § regeringsformen.

- *Hantering av information för annan myndighets räkning:* En förvaltningsgemensam digital infrastruktur i vilken myndigheter samarbetar genom att använda samma tekniska komponenter kan medföra att myndigheter hanterar information åt varandra. Sådan hantering kan innebära både förvaring och förmedling, det vill säga hantering av mer varaktig karaktär eller tillfällig hantering. Att en myndighet förvarar information för en annan myndighets räkning aktualiserar frågan om information blir allmän handling hos förvarande myndighet eller om exempelvis undantaget enligt 2 kap. 13 § tryckfrihetsförordningen är tillämpligt.

- *Offentlighet och sekretess vid informationsutbyte:* Information hos en myndighet omfattas av bestämmelserna i offentlighets- och sekretesslagen, och det är förbjudet för en myndighet som förvarar uppgifter att röja dessa uppgifter i strid

[15] Checklista för jurister, Rapport från E-delegationen 2014-06-19

med lagens bestämmelser. Av detta följer att en myndighet enbart får lämna ut uppgifter som antingen inte omfattas av sekretess, eller uppgifter som visserligen omfattas av sekretess, men där det finns en sekretessbrytande bestämmelse. Sekretess innebär både ett förbud att lämna ut handlingar och att muntligen röja uppgifter, d.v.s. både handlingssekretess och tystnadsplikt. Sekretess gäller som huvudregel även mellan myndigheter. I offentlighets- och sekretesslagen finns dock ett antal bestämmelser som bryter sekretessen mellan myndigheter, se 10 kap. offentlighets- och sekretesslagen.

- *Personuppgiftsansvar vid informationsutbyte:* Frågan om vem som är personuppgiftsansvarig och vem som är personuppgiftsbiträde vid behandling av personuppgifter i arkitekturen måste vara utredd.
  Personuppgiftsansvarig är enligt artikel 4.7 dataskyddsförordning en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandling av personuppgifter. Det som avgör vem som är personuppgiftsansvarig är själva beslutsfattandet om ändamålen och medlen för behandling.
  Personuppgiftsansvaret kan också pekas ut i nationell rätt, exempelvis i en registerförfattning.

  En eller flera personuppgiftsansvariga kan också gemensamt bestämma ändamålen och medlen för behandling. De är då att beteckna som gemensamt personuppgiftsansvariga, under förutsättning att de följer vissa bestämmelser i artikel 26 dataskyddsförordningen.

  Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, artikel 4.8 dataskyddsförordningen. Ett personuppgiftsbiträde kan t.ex. vara någon anlitas för att exempelvis lagra information som innefattar personuppgifter för en annans räkning. När uppgifter behandlas av ett personuppgiftsbiträde så ska hanteringen regleras genom ett avtal eller en författning, artikel 28.3 dataskyddsförordningen.

- *Överenskommelser och krav på upphandling:* Lagen om offentlig upphandling omfattar anskaffning av tjänster som genomförs av en upphandlande myndighet. En arkitekturlösning som innebär att en myndighet sköter hantering av information för en annan myndighets räkning, skulle därmed i vissa fall kunna ses som en tjänst som borde upphandlas. Av gällande rätt framgår att överenskommelser mellan statliga myndigheter inte omfattas av lagen om offentlig upphandling, men att överenskommelser mellan statliga myndigheter och kommuner mycket väl kan omfattas av kraven på upphandling.

#### *4.2.2.2 Rättsliga styrformer*

- *Samverkan:* Myndigheter kan inom ramen för sitt kompetensområde välja att ta fram lösningar för informationsutbyte i samverkan. En myndighet kan och ska samverka med andra myndigheter. Enligt 8 § förvaltningslagen finns det ett krav på att myndigheter ska samverka med andra inom ramen för den egna verksamheten. Bestämmelsen innebär en generell, men inte obegränsad samverkansskyldighet. En myndighet avgör alltid själv i vilken utsträckning som den egna arbetssituationen medger att resurser avsätts för att bistå den myndighet som begär assistans.
  Bestämmelsen ger inte stöd för samverkansprojekt som faller *utanför* respektive myndighets verksamhetsområde.[16] Det får inte förekomma några nyskapelser i form av särskilda samarbetsorgan, som oberoende av tillämpliga föreskrifter fattar beslut som inte kan härledas till någon av de samverkande myndigheterna.[17]

  Statliga förvaltningsmyndigheter ska enligt 6 § andra stycket myndighetsförordningen verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskild samt för staten som helhet. Myndighetsförordningen ger inte någon rätt för en myndighet att inom samverkan agera utanför sitt kompetensområde. Statliga myndigheter under regeringen ska i sin verksamhet främja utvecklingen av ett säkert och effektivt informationsutbyte, 2 § förordning om statliga myndigheters informationsutbyte. Bestämmelsen medför dock inte någon kompetens att samverka utanför myndigheten allmänna kompetensområde.[18]

- *Tvingande styrning*: Styrningen av en infrastruktur för informationsutbyte kan även ske på tvingande väg genom lag eller andra författningar utifrån fördelningen av normgivningskompetens som regleras i grundlagen. Styrningen avser i detta fall exempelvis skyldigheter och rättigheter avseende anslutning och återanvändning av såväl information som de digitala lösningarna.

#### *4.2.2.3 Rättsliga utgångpunkter för utlämnande av information*

- *Myndigheten ansvar för sin egen information:* En utgångspunkt för utlämnande av information är att varje myndighet ansvarar för sin egen information och för att sådan hantering sker i enlighet med gällande rätt. Det är alltså myndigheten själv som har att se till att myndigheten följer gällande rätt (se vidare 12 kap. 1 § regeringsformen).

---

[16] Prop. 2016/17:180 En modern och rättsäker förvaltning – ny förvaltningslag s. 292 f.

[17] Prop. 2016/17:180 En modern och rättsäker förvaltning – ny förvaltningslag s. 71.

[18] I sammanhanget kan nämnas att i slutbetänkandet av Utredningen om effektiv styrning av nationella digitala tjänster, så föreslogs statliga myndigheter få en rätt att samverka utanför sitt verksamhetsområde när det digitaliseringen av den offentliga förvaltningen. SOU 2017:114 reboot – omstart för den digitala förvaltningen, se s. 56.

- *Rättsligt stöd för att lämna ut information:* En myndighet behöver ha stöd i lag för att lämna ut information. Att en myndighet behöver ta stöd i lag för alla handlingar den vidtar följer av legalitetsprincipen i 1 kap. 1 § tredje stycket regeringsformen samt av 5 § förvaltningslagen som stadgar att en myndighet enbart får vidta handlingar som har stöd i rättsordningen. Legalitetsprincipen ska tolkas som att den innebär att en myndighet i vidsträckt bemärkelse ska ha stöd i rättsordningen för sina åtgärder.[19]

  Som exempel för tvingande rättsliga grunder för utlämnande är myndigheters uppgiftsskyldighet gentemot en annan myndighet, utlämnande av information enligt offentlighetsprincipen, kommunikation enligt förvaltningslagen och utlämnande enligt 6 kap. 4–5 §§ offentlighets- och sekretesslagen. Som exempel på utlämnande på mer frivillig grund är som en service enligt förvaltningslagen, som inte alls preciserar vad som anses vara en service, men på vilken grund en myndighet kan välja att till exempel lägga ut uppgifter på sin hemsida.

  Det saknas gemensamma regler för utlämnande vid nationell informationsförsörjning.

- *Registerförfattningar:* I förekommande fall regleras viss av myndigheters personuppgiftsbehandling av s.k. registerförfattningar, som reglerar bland annat för vilka ändamål som en myndighet får behandla personuppgifter automatiserat.[20] De ändamål som en registerförfattning innehåller medför att myndigheten inte får behandla personuppgifter för något ändamål som är oförenligt med dessa ändamål (finalitetsprincipen, art. 5.1 d dataskyddsförordningen). Det innebär att vid elektroniskt utlämnande av information, om informationen omfattas av registerförfattning, så behöver utlämnande ske i enlighet med de ändamål som stadgas i tillämplig registerförfattning.

- *Informationssäkerhet:* Lagstiftningen på området informationssäkerhet är fragmenterad och består av att antal olika regelverk som behöver tillämpas jämte varandra. Lagstiftningen på informationssäkerhetsområdet kan sägas dels träffa verksamheter som sådana och dels träffa informationen som sådan.[21]

  Dataskyddsförordningen ställer krav på säkerhet vid behandling av personuppgifter. Offentlighets- och sekretesslagen uppställer förbud mot röjande av sekretessbelagda uppgifter, varför allmänna handlingar måste hanteras på ett säkert sätt. Säkerhetsskyddslagen gäller för den som bedriver verksamhet som är

[19] Prop. 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag s. 57–58.
[20] För översikt över svenska registerförfattningar, se SOU 2015:39 Myndighetsdatalag s. 94.
[21] SOU 2018:25 Juridik som stöd för förvaltningens digitalisering s. 315.

av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).

Krav på statliga myndigheters informationssäkerhet finns i förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid beredskap. Därtill har MSB utgivit föreskrifter om statliga myndigheters informationssäkerhet och om statliga myndigheters rapportering av IT-incidenter. Kommuner och landsting träffas inte av sagda förordning och föreskrifter utan har istället lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, vilken saknas specifika bestämmelser om informationssäkerhet. Sedan 2018 gäller även lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, med krav på säkerhet för leverantörer av vissa tjänster.

Uppräkningen av författningar ovan är inte uttömmande. Det saknas lagstiftning som medför ett sammanhållet gemensamt förhållningssätt för samtliga statliga och kommunala myndigheter, något som Digitaliseringsrättsutredningen konstaterade utgör en brist ur digitaliseringsperspektiv.[22]

## 4.3 Förslag till styrform, incitament, roller och ansvar för de förvaltningsgemensamma lösningarna

### 4.3.1 Rättslig styrform för byggblocken

I föregående avsnitt konstateras att det krävs rättsligt stöd för myndigheter att utföra myndighetsuppgifter som avser byggblocken, exempelvis för att kunna tillhandahålla nationella tekniska funktioner. Det konstateras också att gällande rätt behöver utvecklas för att skapa nödvändig normmässig förankring av byggblocken för ansvariga myndigheter (legalitet). I nuvarande avsnitt behandlas alternativ för hur ansvaret för byggblocken kan regleras rättsligt (rättslig styrform). Myndigheternas förslag är att ansvaret för byggblocken ska ingå i det offentliga åtagandet och framgå uttryckligen i författningar med instruktioner för berörda myndigheter.

Val av rättslig styrform är i mångt och mycket en lämplighetsavvägning. Lämpligheten vid val av styrform behöver beakta såväl *demokrati-, rättssäkerhets- och effektivitetsargument.* Bara för att något är möjligt att styra genom samverkan, medför nödvändigtvis inte att det är mest *ändamålsenligt* att använda samverkan som grund.

Något som är viktigt att överväga vid val av styrform av en infrastruktur och dess komponenter är vilket *syfte* den ska uppfylla. Om syftet med infrastrukturen är att uppfylla ett viktigt nationellt intresse, kan det vara nödvändigt att det är en del av det offentliga åtagandet. Det offentliga åtagandet är sådant som lagstiftaren har pekat ut att

[22] SOU 2018:25 Juridik som stöd för förvaltningens digitalisering s. 329.

det tillhör det allmänna att utföra, och förtydligar gränserna för vad som är myndighetsuppgifter, inte enbart i förhållande till enskilda, utan även vad som är förbehållet marknadens aktörer. Om något faller utanför det offentliga åtagandet, kan det typiskt sett utgöra uppgifter som tillfaller marknadens aktörer att utföra.[23]

Vad som är ett offentligt åtagande är i varje enskilt fall ett politiskt ställningstagande och ett politiskt beslut. Ett sådant beslut kan inte delegeras eller decentraliseras till offentliga myndigheter. Några av de skäl som brukar anges för ett offentligt åtagande är effektivare samhällsekonomi, fördelningsmotiv, stabiliseringspolitik och ansvarstagande för det medborgarna inte själva har kunskap om och information nog att sköta själva. Den privata marknaden kan inte uppfylla alla behov som är viktiga för landet och medborgarna. Vissa kollektiva nyttigheter måste i stället garanteras genom offentliga åtaganden.[24]

Det medför att om de intressen och behov som infrastrukturen syftar till att uppfylla är ett viktigt *nationellt intresse*, som är motiverat av ovan anförda typiska skäl, så utgör infrastrukturen ett sådant viktigt nationellt intresse som kan kräva att det är en del av det offentliga åtagandet. Eftersom frågan om vad som utgör en del av det offentliga åtagandet inte kan delegeras till myndigheterna, måste det regleras av riksdagen eller regeringen. Det medför i sig att samverkan är ett olämpligt rättsligt styrmedel för en sådan infrastruktur eller byggblock.

Reboot-utredningen ansåg att det offentliga åtagandet för förvaltningsgemensamma digitala funktioner behöver regleras i författning.[25] Med förvaltningsgemensamma digitala funktioner avsåg utredningen som exempel Mina meddelanden och elektroniska identitetshandlingar. Andra exempel som utredningen menar kan utgöra förvaltningsgemensamma digitala funktioner är system för att kunna hantera behörigheter och digitala underskrifter, system för säker kommunikation mellan myndigheter och standarder för förmedling av information mellan myndigheter och företag och standarder för öppna data.[26] Kännetecknande för förvaltningsgemensamma digitala tjänster är att de är gemensamma digitala lösningar som är av infrastrukturkaraktär och som är en avgörande förutsättning för offentlig e-tjänsteutveckling i sin helhet.[27] Utredningen ansåg dock att det för var och en av de förvaltningsgemensamma digitala funktionerna fanns behov av att närmare analysera och precisera omfattningen av det offentliga åtagandet i förhållande till de privata aktörernas roll.

Samverkan som en rättslig styrform kan dock tjäna som ett komplement vid utveckling och förvaltning av ett byggblock. Om en myndighet saknar rättslig kompetens för samverkan kan det åtgärdas exempelvis genom att regeringen utfärdar en förordning att

[23] SOU 2017:114 reboot – omstart för den digitala förvaltningen s. 104.
[24] SOU 2017:114 reboot – omstart för den digitala förvaltningen s. 103.
[25] SOU 2017:114 reboot – omstart för den digitala förvaltningen s. 101.
[26] SOU 2017:114 reboot – omstart för den digitala förvaltningen s. 107 f.
[27] SOU 2017:114 reboot – omstart för den digitala förvaltningen s. 106 f.

samverka på ett visst sätt, eller genom att myndighetens kompetensområde sträcks ut genom en ändring av myndighetens instruktion.

Rent praktiskt kan det vara fördelaktigt att olika byggblock i en infrastruktur regleras på olika nivåer, så att respektive fördelar och nackdelar med de rättsliga styrmedlen tillvaratas, och så att så väl demokrati-, rättssäkerhets- och effektivitetsaspekter beaktas. Exempelvis kan det framgå av lag eller förordning en skyldighet för en myndighet att delta i en viss infrastruktur, medan frågor om de tekniska ramverken för tjänster i infrastrukturen kan beslutas med andra styrformer, exempelvis genom samverkan eller genom en myndighets verkställighetsföreskrift. Ett exempel på tänkbar styrning finns inom företagsområdet redan idag är förordning (2018:1264) om digitalt inhämtande av uppgifter från företag. Förordningen ska bidra till att företagarnas uppgiftslämnande till myndigheter minskar. Denna typ av styrning skulle kunna användas för hela eller delar av den offentliga förvaltningen, antingen för infrastrukturen som helhet eller för individuella byggblock/domäner.

Mot bakgrund av resonemanget ovan föreslår myndigheterna att byggblocken i den konceptuella arkitekturen ska ingå i det offentliga åtagandet kring den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte (rättslig styrmodell). Det innebär att det som utgångspunkt ska ingå i relevanta statliga myndigheters myndighetsansvar att utveckla och förvalta identifierade samt eventuellt kommande byggblock.

### 4.3.2 Incitament för ökad framdrift

Mot bakgrund av de analyser och förslag som lämnats ovan i denna rapport, kan det förenklat konstateras att det krävs en förflyttning från ett identifierat nuläge till ett nyläge som skissats genom den konceptuella arkitekturen. Nuläget består av fragmenterade digitala lösningar och bristande incitament för nationell samordning av dessa. Nyläget består av konkreta nationella byggblock med utpekade ansvariga aktörer. I nyläget används byggblocken i hela den offentliga förvaltningen vid digitalt informationsutbyte, vilket ger en nyttorealisering av genomförda investeringar. Denna förflyttningsresa behöver en effektiv och långsiktig styrform som skapar incitament för och stimulerar utvecklingen.

Initialt kan incitament skapas genom *samordnad myndighetsstyrning* genom regeringsuppdrag. Detta bör ske i kombination med nationella satsningar på prioriterade användningsområden som har potential att starta en självgående anslutning till byggblocken.

Incitament föreslås skapas också genom *etablering av myndighetssamverkan* kring byggblocken.

För att skapa incitament för användning av byggblocken som föreslås i denna rapport, rekommenderar myndigheterna att det ställs *krav på pågående nationella satsningar* att använda byggblocken i de digitala lösningarna inom dessa satsningar. Ett sådant krav

bedöms säkerställa nyttorealisering samtidigt som det skulle driva utvecklingen av byggblocken utifrån behoven i värdekedjorna och gällande tidsplaner för dessa.

Exempel på nationella satsningar där byggblocken behövs är regeringens beslut från 2016 om digitalisering inom ett antal prioriterade utvecklingsområden i offentlig sektor.[28] Inom ramen för detta gav regeringen digitaliseringsuppdrag till Lantmäteriet, Jordbruksverket, Naturvårdsverket och Tillväxtverket inom fyra värdekedjorna: samhällsbyggnadsprocessen, livsmedelskedjan, miljöinformation och förenklat företagande.[29]

Sådana krav kan uppställas vid utformning av de regeringsuppdrag som säkerställer framdriften i utvecklingen. På sikt behövs det dock en långsiktigt hållbar styrning som stimulerar användningen av byggblocken. Enligt omvärldsanalysen är tidig översyn av lagstiftning en viktig framgångsfaktor. Myndigheterna rekommenderar därför att regeringen tillsätter ett rättsligt beredningsorgan enligt förslaget från Digitaliseringsrättsutredningen, se SOU 2018:25 s. 446. Lantmäteriet har i sin slutrapport om smartare samhällsbyggnadsprocess skissat på en metod och idé till ett arbetssätt i etapper kopplat till ett sådant beredningsorgan vilket också behöver beaktas.[30]

### 4.3.3 Ansvar för byggblocken

Ett byggblock består av flera aspekter som syftar till att standardisera en viss företeelse på nationell nivå. Det kan vara en teknisk komponent, ett slags administrativt nationellt ramverk för byggblocket, exempelvis avseende specifikationer för information eller en teknisk beskrivning. Det är de olika aspekterna som syftar till att standardisera något i byggblocket, som behöver inordnas i den svenska förvaltningsmodellen som ett förvaltningsansvar.

Myndigheterna bedömer att det ansvaret för byggblocken kan delas in utifrån följande aspekter.

*Juridisk*: Ansvaret rör i denna del mandat att samordna tekniska, semantiska och organisatoriska aspekter av byggblocket, utan att det uppstår onödiga överlapp i ansvar med andra myndigheter.

*Teknisk*: Ansvaret rör i denna del den tekniska komponenten av byggblocket och kan avse hela den tekniska infrastrukturen eller en konkret digital tjänst.

*Semantisk*: Ansvaret rör i denna del den administrativa komponenten av byggblocket och avser specifikationer för hur information och tjänster ska beskrivas så att informationen ska kunna utbytas helt maskinellt.

[28] Budgetproposition prop. 2016/17:1, utgiftsområde 22, avsnitt 4.4.2.

[29] Se bland annat budgetproposition prop. 2016/17:1, utgiftsområde 18, avsnitt 3.5.7, samt regeringsuppdrag att verka för digitalt först - för en smartare samhällsbyggnadsprocess, N2016/01419/EF.

[30] Lantmäteriet, Nationellt tillgängliggörande av geodata i samhällsbyggnadsprocessen 2019-04-19 – slutrapport i uppdraget att verka för en smartare samhällsbyggnadsprocess, Lantmäteriets dnr 519-2018/2889, bilaga 1.

*Organisatorisk*: Ansvaret rör i denna del den administrativa komponenten av byggblocket som säkerställer enkel (obligatorisk eller frivillig) anslutning till byggblocket exempelvis genom att en viss myndighet får mandat att besluta om anslutning istället för att beslut ska fattas av varje informationsproducerande myndighet som ingår i en samverkan kring byggblocket. Det kan också handla om att effektivisera avtalshantering som krävs enligt lagstiftning, till exempel personuppgiftsbiträdesavtal, genom att den samordnande myndigheten ges föreskriftsrätt inom området.

Varje byggblock har minst någon del av de semantiska och organisatoriska aspekterna.

Att ansvara för krav kring ett byggblock kan dock kräva särskild kunskap avseende till exempel informationens egenskaper, användarnas behov eller ett sakområde som bland annat dataskydd och säkerhet.

Myndigheters rättsliga kompetens (och därmed också specialkunskap) är idag indelad utifrån sakområden som definieras av varje myndighets instruktion. Detta talar för att de olika aspekterna, teknisk, semantisk och organisatorisk, ska i lämpliga fall kunna fördelas på myndigheter som har sådan relevant kompetens.

Mot bakgrund av detta resonemang, bedömer myndigheterna att det behövs följande typer av ansvar för byggblocken.

- Ansvar för att byggblocken finns och konceptuellt ”sitter ihop” i en arkitektur. Detta inbegriper exempelvis att ta fram och förvalta ett nationellt ramverk för grunddata[31], metadatahantering av information samt tjänster.
- Ansvar att realisera lösningar av byggblock – centralt eller lokalt.
- Ansvar att skapa semantisk ordning och reda – centralt och sektors-/domänspecifik. Se vidare förslag om grunddatadomäner.[32]

Myndigheterna bedömer att ansvaret bör fördelas mellan DIGG och domänansvariga (informationsdomäner) myndigheter, initialt Bolagsverket, Lantmäteriet och Skatteverket inom respektive informationsdomän. Närmare beskrivning av denna ansvarsfördelning behöver tas fram i samband med en fördjupning kring varje byggblock, se kapitel 5 om åtgärder.

### 4.3.4 Övriga ansvarsområden

Ett byggblock är till för att användas av andra aktörer, och kan vara beroende av ett samarbete med olika aktörer för att fungera. Det innebär att det förutom ansvar för själva byggblocket också finns ansvarsområden för de aktörer som bidrar till eller använder byggblocket.

[31] Uppdrag om säker och effektiv tillgång till grunddata – Bolagsverket, DIGG, Lantmäteriet och Skatteverket Dnr 2018-31 s.50

[32] Uppdrag om säker och effektiv tillgång till grunddata – Bolagsverket, DIGG, Lantmäteriet och Skatteverket Dnr 2018-31 s.51

Myndigheterna har identifierat följande ansvarsområden, vilka dock behöver fortsatt utredning för att kunna utformas som konkreta förslag.

- Ansvar som datavärd: Offentliga aktörer har idag olika förutsättningar för att använda digitaliseringens möjligheter. Även om det införs en tydlig ordning med ansvar för byggblock, kan det finnas en tröskel för myndigheter att använda dessa. Något som skulle kunna underlätta användning av byggblocken är ett slags serviceansvar gentemot såväl statliga som kommunala myndigheter. Ett så kallat datavärdskap syftar till att underlätta tillgängliggörande av information genom API. En datavärd agerar i sådana fall för en annan (statlig eller kommunal) myndighets räkning.

- Ansvar som informationsproducent: De ramverk kring byggblocken som tas fram av berörda myndigheter kommer att ställa krav på informationsproducerande aktörer, det vill säga i de fall informationen som hanteras i ett byggblock tas fram av eller uppstår hos av andra aktörer än den myndighet som ansvarar för byggblocket. Ett ansvar som diskuteras är "informationsansvar" för informationsproducenter, utifrån ett digitaliseringsperspektiv. Ett sådant ansvar skulle tydliggöra exempelvis vilka skyldigheter en aktör har kopplat till ett byggblock. I ett första steg kan dock detta ansvar utvecklas inom ramen för en producentsamverkan.

- Ansvar för användare av byggblocken: Syftet med byggblocken är att skapa nytta hos de aktörer (användare) som behöver säker och effektiv åtkomst till information i digital form. Det innebär att om användarna inte ser anledning att nyttja byggblocken, kommer målet om effektivare och säkrare informationsutbyte inte att kunna uppnås. För att stärka incitament för användning skulle användaransvaret kunna utvecklas mot bakgrund av den så kallade "the once only principle" (TOOP), se EU-kommissionens eGovernment Action Plan. Flera europeiska länder har börjat inkorporera TOOP i sin lagstiftning. I Belgien, Estland och Nederländerna finns redan tvingande lagstiftning på plats.[33] En sådan utveckling bör också kunna diskuteras kopplat till den rättsliga styrningen av byggblocken i Sverige.

[33] EU-wide digital Once-Only principle for citizens and businesses – policy options and their impact, EU 2014

# 5 Förslag till åtgärder

**Förslag:** Myndigheterna föreslår att regeringen:

- Säkerställer en styrform som motsvarar de nationella program som skapats i analyserade länder, för att över tid kunna besluta om aktiviteter för utveckling och realisering av en förvaltningsgemensam digital infrastruktur för informationsutbyte inom och med offentlig sektor.
- Beslutar om regeringsuppdrag och nödvändiga medel för de nedan beskrivna kortsiktiga förslagen, vilka kan ses som en förstudie till nästa punkt och ska resultera i en färdplan för utveckling av den förvaltningsgemensamma infrastrukturen, vilken koordineras av DIGG.
- Över tid, i samråd med DIGG, beslutar om regeringsuppdrag och nödvändiga medel och andra förutsättningar för utveckling av byggblocken, för de myndigheter som förväntas ha ett nationellt förvaltningsansvar av respektive byggblock, samt initiativ som främjar nationell implementering av dessa.
- Inrättar ett rättsligt beredningsorgan för att säkerställa att nödvändigt långsiktigt rättsligt stöd för byggblocken och informationsutbytet tas fram.

I ett första steg (2019–2020) föreslås att regeringsuppdragen avser följande:

1. En färdplan (DIGG, Bolagsverket, Försäkringskassan, Lantmäteriet, Skatteverket, E-hälsomyndigheten och Domstolsverket)
2. API-hantering (DIGG, Bolagsverket, Lantmäteriet, Skatteverket, Naturvårdsverket och E-hälsomyndigheten)
3. Identitet (DIGG i samverkan med SKL, Försäkringskassan och E-hälsomyndigheten)
4. Mina ombud (Bolagsverket och Skatteverket)

## 5.1 Utgångspunkter och utmaningar

Enligt uppdraget ska myndigheterna, för de lösningar som bedöms vara lämpliga, lämna förslag på åtgärder som möjliggör ett långsiktigt och utökat användande av dessa inom den offentliga sektorn.

En utmaning för utvecklingen som leder till effektivt och säkert informationsutbyte är att balansera

- standardisering, likriktning, styrning mot
- flexibilitet, innovation och frivillighet.

Fortsatta åtgärder och vägval behöver ske mot bakgrund av en proportionalitetsbedömning utifrån dessa motstående behov. Fördjupade säkerhetsanalyser krävs för samtliga åtgärder kopplade till byggblock.

En viktig utgångspunkt i valet av åtgärder har varit att befintliga arkitekturer och lösningar ska utvecklas och inte nödvändigtvis skall bytas ut mot nya lösningar. Det innebär att utgångspunkten för den fortsatta utvecklingen föreslås gå mot en vidareutvecklad förvaltningsgemensam digital infrastruktur för informationsutbyte, men som tillåter myndigheter att behålla sina lösningar samtidigt som ett modernare användargränssnitt kan införas.

Lagstiftning, styrning och finansiering bedöms vara avgörande framgångsfaktorer för utvecklingen. Det praktiska genomförandet bör som utgångspunkt läggas på myndigheter med högre digital mognadsgrad och kapacitet. Förutom juridiska styrmedel krävs också andra incitament för ökad framdrift i utvecklingen.

En ytterligare utgångspunkt vid val av teknisk lösning är principer för återanvändning av redan befintliga lösningar som bör appliceras:

- Finns en redan användbar lösning som ägs av det offentliga som kan återanvändas och täcka gemensamma behov?
- Finns det en lösning som ägs av det offentliga som kan återanvändas och vidareutvecklas till en gemensam lösning?
- Finns det en lösning som tillhandahålls i EU eller omvärlden som kan återanvändas och vidareutvecklas till en lösning för Sverige?
- Finns det en kommersiell standardlösning som går att köpa in och nyttja för samtliga aktörer?
- Utveckla en ny gemensam lösning för användning inom det offentliga.

## 5.2 Åtgärder

Myndigheterna föreslår att regeringen vidtar följande åtgärder:

- Säkerställer en styrform som motsvarar de nationella program som skapats i analyserade länder, för att över tid kunna besluta om aktiviteter för utveckling *och realisering* av en förvaltningsgemensam digital infrastruktur för informationsutbyte inom och med offentlig sektor.
- Beslutar om regeringsuppdrag och nödvändiga medel för de nedan beskrivna kortsiktiga förslagen, vilka kan ses som en förstudie till nästa punkt och ska resultera i en färdplan för *utveckling* av den förvaltningsgemensamma infrastrukturen, vilken koordineras av DIGG.
- Över tid, i samråd med DIGG, beslutar om regeringsuppdrag och nödvändiga medel och andra förutsättningar för utveckling av byggblocken, för de myndigheter som förväntas ha ett nationellt förvaltningsansvar av respektive byggblock, samt initiativ som främjar nationell implementering av dessa.
- Inrättar ett rättsligt beredningsorgan för att säkerställa att nödvändigt långsiktigt rättsligt stöd för byggblocken tas fram.

Som underlag till relevanta regeringsuppdrag vill myndigheterna lyfta följande inspel:

- *Koordinering.* DIGG föreslås bereda, planera och koordinera insatser och uppdrag tillsammans med myndigheter som berörs av utvecklingen av relevanta byggblock, samt framtagande av riktlinjer och standarder för dessa.

- *Färdplan.* DIGG föreslås tillsammans med Bolagsverket, Lantmäteriet, Försäkringskassan, Skatteverket, Domstolsverket och E-hälsomyndigheten ges i uppdrag att ta fram en färdplan för utvecklingen. Färdplanen ska beskriva:
    - Detaljering av infrastrukturella byggblock och arkitektur för den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte.
    - Styr-, samverkans-, ansvars- och förvaltningsmodell
    - Kostnadsberäkning
    - Finansieringslösning
    - Samlad förenklad avtalsmodell

  Uppdraget föreslås starta under hösten 2019 och pågår till slutet av september 2020 med delrapportering i januari 2020. DIGG föreslås ersättas med 1,5 miljoner kronor för att leda arbetet. Övriga myndigheter föreslås ersättas med 500 000 kronor vardera. (Totalt 6 miljoner kronor.)

- *API-hantering.* DIGG föreslås att i samverkan med Bolagsverket, Lantmäteriet, Skatteverket, Naturvårdsverket och E-hälsomyndigheten ges i uppdrag att genomföra förberedelser och realisering av byggblocket API-hantering. Detta omfattar bland annat följande:
    - Ta fram förslag på standardisering av beskrivningar av juridiska regler, verksamhetsregler samt teknik
    - Förvaltningsmodell av ovan nämnda beskrivningar
    - Etablera förmågan att kunna söka efter en tjänst
    - Etablera förmågan att kunna adressera en tjänst
    - Färdplan för fortsatt utvecklingsarbete av byggblocket (som redovisas i ovanstående uppdrag)
    - Etablera utvecklingsstöd för utvecklare
    - Ta fram en standardiserad process för API livscykelhantering
    - I samverkan med styrningsuppdraget hantera frågor kopplat till centrala (gemensamma) komponenter

  Uppdraget föreslås starta under hösten 2019 och avslutas i slutet september 2020. DIGG ersätts med 2 miljoner kronor för att leda arbetet. Övriga deltagande myndigheter ersätts med 750 000 kronor vardera. Detta ger en total kostnad för uppdraget på 5,75 miljoner kronor. I DIGGs uppdraget ingår att samordna uppdraget API-hantering med uppdraget fördjupad styrning.

- *Identitet.* DIGG föreslås att i samverkan med SKL, Försäkringskassan och E-hälsomyndigheten få i uppdrag att utreda nationella identifieringslösningar som stödjer den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte. Arbetet omfattar bland annat följande:

- Nationell lösning gällande e-legitimationer i tjänsten, som medför att det går att använda e-legitimation i tjänsten över olika verksamhetsområden.
- Belysa möjligheterna att tillämpa identifieringslösningen även för organisationer och enheter.
- En nationell lösning för e-underskrifter som även skall omfatta privata utförare.

Uppdraget avses starta under hösten 2019 och avslutas i slutet av januari 2020. DIGG föreslås ersättas med 1,5 miljoner kronor, Försäkringskassan med 0,5 miljoner kronor och E-hälsomyndigheten med 0,5 miljoner kronor för uppdraget.

- *Mina ombud* – Bolagsverket och Skatteverket föreslås få nedanstående uppdrag. Baserat på utfallet av det arbete som genomförs 2020 kan de kommande uppdragen behöva justeras innehållsmässigt.

  - *Nationell behörighet - pilot inom företagsområdet,* (Bolagsverket)
    Tidsperiod: 2020-01 -- 2020-12
    Kostnad: 7 mkr
    Samverkansparter: DIGG, Skatteverket
    Mål: Att utveckla en första version av en nationell behörighetslösning där en fysisk person får möjlighet att företräda ett företag (registrerat hos Bolagsverket) i en digital tjänst. Detta inkluderar även en tjänst för att underlätta konsumenternas användning av firmateckningen.

  - *Nationell behörighet - breddning/ vidareutveckling inom företagsområdet,* (Bolagsverket)
    Tidsperiod: 2021-01 -- 2021-12
    Kostnad: 7 mkr
    Samverkansparter: DIGG, Skatteverket och andra offentliga aktörer.
    Mål: Att etablera lösningen och skala upp användningen baserat på fångade behov samt till att omfatta fler tjänster där fysiska personer behöver företräda företag. Utreda förutsättningar att företräda andra juridiska personer än företag/fysiska personer, se föreslaget uppdrag 2022.

  - *Nationell behörighet - företräda fysisk person* (Skatteverket)
    Tidsperiod: 2021-01--2021-12
    Kostnad: 7 mkr
    Samverkansparter: DIGG, Bolagsverket
    Mål: Att bredda användningen av den föreslagna lösningen till situationer där fysiska personer behöver företräda andra fysiska personer.

- *Nationell behörighet - breddning/ vidareutveckling mot fler juridiska personer, (*Bolagsverket)
  Tidsperiod: 2022-01 -- 2022-12
  Kostnad: 3 mkr
  Samverkansparter: DIGG, Skatteverket och andra organisationsnummertilldelande myndigheter
  Mål: Vidareutveckla den framtagna lösningen till att omfatta typer av juridiska personer som är registrerade hos andra organisationsnummertilldelande myndigheter än Bolagsverket.

# 6 Konsekvenser

**Sammanfattning**:

Det finns idag en utbredd problembild med informationsutbytet inom och med offentlig sektor vilket leder till en rad olika negativa konsekvenser. De förslag som myndigheterna har lagt fram syftar till att åtgärda dessa problem. Konsekvenserna av lagda förslag innebär stärkt styrning och samordning genom skapandet av förvaltningsgemensamma byggblock.

Förslagen kommer ha olika konsekvenser beroende hur man väljer att hantera gemensamma kostnader och finansiering av förvaltningsgemensamma byggblock. Konsekvenserna är dock små i förhållande till de potentiella nyttor och positiva samhällsekonomiska effekter som ett ökat tillgängliggörande av offentlig data kan leda till.

## 6.1 Övergripande konsekvenser

Syftet med förslaget avseende förvaltningsgemensamma byggblock är att stärka styrningen och samordningen av den offentliga sektorn avseende säkert och effektivt informationsutbyte. Förslaget innebär att staten ska ansvara för att byggblocken finns och används. Vilka alternativa lösningar finns och vad blir effekterna om förslaget inte genomförs?

Alternativet till förslaget är att utvecklingen och förvaltningen av byggblocken drivs av marknadsaktörer inom digitaliseringsområdet. Redan idag erbjuder företag digitala lösningar, där företaget åtar sig att hålla och tillgängliggöra aktörers information. Men staten har ett övergripande ansvar för samhällets grundläggande informations-infrastruktur.[34] Staten har även ansvar för utveckling av grundläggande principer för hur offentlig information ska tillhandahållas till samhället. Myndigheterna bedömer därför att alternativet att utvecklingen drivs av marknadsaktörer inte är aktuellt utifrån målbilden om ett effektivt och säkert informationsutbyte.

Om förslaget inte genomförs, bedöms att fragmenteringen och dubbelarbetet inom offentlig förvaltningen avseende digitala lösningar kommer att öka och motverka målet om effektivare och säkrare informationsutbyte.

## 6.2 Kostnader och finansiering

Inom uppdraget har tre alternativ för finansiering av utveckling och förvaltning av nödvändiga lösningar diskuterats, som alla är neutrala på statens budget,

1. frivillig finansiering av en eller flera myndigheter
2. finansiering genom avgifter vid användning eller

[34] SOU 2003:111 s. 216, 221 och 318 samt prop. 1995/96 :125 s. 19.

3. genom en omfördelning av anslag.

Ett ytterligare alternativ skulle kunna vara en kombination av några av dessa. Frivillig finansiering genom myndighetssamverkan har prövats till exempel i utvecklingen av verksamt.se och Mina meddelanden. Även om det fungerat initialt i dessa fall så medför sådan finansiering en stor osäkerhet. Överenskommelserna är ofta kortsiktiga och finansieringen behöver årligen säkras för nästkommande år. Detta innebär att det är svårt att hantera den långsiktiga utvecklingen av komponenterna och det medför också stor osäkerhet för nyttjarna. Incitament för att skapa återanvändbara komponenter saknas. Är det värt att investera i denna komponent? Hur länge kommer den finnas, kommer det införas avgifter framgent? Även om en frivillig finansiering kombineras med ett uppdrag till tillhandahållaren, vilket kommer behövas i de flesta fall, kommer osäkerheten vara stor.

Finansiering via avgifter vid användning (transaktionsbaserade avgifter) riskerar att motverka nyttandet av de gemensamma komponenterna, särskilt om avgifterna är transaktionsbaserade. Det kommer medföra att kostnaden blir svår att budgetera för nyttjarna. Kostnadsökningen för nyttjaren av en gemensam komponent torde normalt inte stå i proportion till tillhandahållarens kostnadsökning då marginalkostnaden normalt är väldigt låg för tillhandahållandet (den ökar i stället stegvis när olika kapacitetströsklar nås).

Ska det dessutom vara självkostnadspris kommer tidiga nyttjare att drabbas osedvanligt hårt. För att inte styckkostnaden för de först anslutna myndigheterna ska bli orimligt hög kommer det åtminstone under en övergångsperiod vara nödvändigt med kompletterande finansiering även om man väljer avgiftsmodellen.

Central finansiering via anslag är den lösning som har störst möjlighet att stödja digitaliseringen av den offentliga förvaltningen. Framförallt för att de måste kombineras med ett uppdrag till myndigheten och därmed signalerar långsiktighet och stabilitet men det har även andra fördelar.

Fördelar med anslagsfinansierat:

- Följer tanken med öppna data, information ska vara gratis att hämta för de som behöver den.
- Det behöver inte byggas upp en administration för fakturering och fakturahantering, d.v.s. en kundtjänst som kan svara på fakturafrågor och en eventuell anpassning av den tekniska lösningen.
- Det blir ingen risk för en svår årlig avräkning som måste ske för att undvika subventionering mellan myndigheterna.

Finansieringen skulle ske genom en omfördelning av anslagsmedel från de statliga myndigheterna till en gemensam pott för utveckling- och förvaltning av gemensamma förmågor/komponenter/byggblock. En sådan konstruktion är budgetneutral vilket är

utgångspunkten i utformningen av statliga reformer. Det behövs vidare utredning för att avgöra hur de myndigheter som är avgiftsfinansierade ska bidra till finansieringen.

I nästa steg skulle en modell som dessutom utgår från en omföring genom en minskning av de statliga bidragen till kommuner och landsting kunna utredas.

## 6.3 Nyttor

Nytto- och kostnadskalkyler kopplade till respektive förslag och åtgärder har inom ramen för detta uppdrag inte varit möjligt att genomföra sett till tidsbegränsningar. I kommande arbete med att realisera föreslagna åtgärder föreslås att varje deltagande aktör ansvarar för verksamhetens egna nyttoanalyser. Detta för att nyttorna som beräknas ska vara realistiska och att det finns ett eget ansvar för realisering av nyttorna. Dessa beräkningar kan sedan aggregeras och appliceras i en större kontext.

Omvärldsanalysen[35] visar tydligt på att det finns stora samhällsekonomiska effekter och nyttor som uppkommer av ett tillgängliggörande och användande av offentliga data. Det finns även direkta verksamhetsnyttor i form av tidsbesparingar och minskade administrativa kostnader samt effektivitetsaspekter i form av ökad återanvändning av förvaltningsgemensamma byggblock.

Om man ser till verksamhetsnytta specifikt kan man uppskatta att statsförvaltningens verksamhetskostnader[36] och främst IT-kostnader[37] kommer att gå ner genom minskad arbetstid och effektivare användning av resurser som en följd av återanvändning av förvaltningsgemensamma byggblock för informationsutbyte. Inhämtade uppgifter från deltagande myndigheter underbygger att kostnaderna för informationsutbyte belastar olika delar av verksamheten. Främst rör det sig dock om IT-kostnader i form av kostnader för systemutveckling, drift och arkitektur men även andra verksamhetskostnader såsom kostnader för juridik, avtal och verksamhetsutveckling. En övergripande uppskattning är att mellan 60–80% av kostnaderna för informationsutbyte belastar it-kostnader och resterande delar övriga verksamhetskostnader.

Verksamhetsnytta kan uppkomma genom direkta budgetpåverkande nyttor i form av reducerade driftskostnader. Exempelvis billigare/gratis användning av centrala komponenter, reducerade avgifter för porto och papper till följd av elektroniskt informationsutbyte och minskad arbetstid.

[35] Se Bilaga 1, avsnitt 7.4.3.2 Samhällsekonomiska effekter och nyttor

[36] Verksamhetskostnader definieras i denna rapport som den kostnad som består av verksamhetens totala kostnader inklusive avskrivningar. Motsvaras i regel av raden "Verksamhetens kostnader" i myndigheternas resultaträkning.

[37] IT-kostnader definieras i denna rapport som de kostnader som kan härledas till IT-funktioner, men begränsas inte till IT-organisationen. Kostnaderna består av kostnader inklusive avskrivningar för drift, förvaltning och utveckling av IT-system och utrustning.

Även indirekta nyttor i form av effektiviseringsvinster som en följd av ändrade arbetsprocesser samt kvalitativa nyttor som är svåra att kvantifiera i form av bättre tillgänglighet till tjänster, bättre beslutsunderlag och användarnöjdhet kan uppstå.

### 6.3.1 Beräkningsexempel av effekt på verksamhetsnytta

It-kostnaderna[38] för myndigheterna som ingår i uppdraget uppgår till följande belopp:

| **Myndighet** | **IT-kostnad 2017** |
|---|---|
| Skatteverket | 2 081 084 000 kr |
| Försäkringskassan | 2 050 000 000 kr |
| Lantmäteriet | 397 735 000 kr |
| Bolagsverket | 222 188 000 kr |
| E-hälsomyndigheten | 186 707 000 kr |
| Domstolsverket | 259 948 000 kr |
| **Totalt:** | 5 197 662 000 kr |

Om man utifrån olika scenarion räknar med att de föreslagna åtgärderna i detta uppdrag kommer leda till effektiviseringar och minskade it-kostnader uppgående till årliga nyttoeffekter motsvarande 0,5/1/2 procent[39] per år av it-kostnaden leder detta således till stora besparingar. Scenariona bedöms gå från restriktivt till optimistiskt beräknat och det ska tilläggas att det kan finnas svårigheter att direkt realisera och kvantifiera denna typ av effekter på årsbasis.

Minskade IT-kostnader med 0,5 % motsvarar en besparing för myndigheterna på 25 988 310 kr årligen. Minskade IT-kostnader med 1 % motsvarar en besparing för myndigheterna på 51 976 620 kr årligen. Minskade IT-kostnader med 2 % per år motsvarar en besparing på 103 953 240 kr årligen. Detta motsvarar bara den beräknade verksamhetsnyttan sett till minskade IT-kostnader för de medverkande parterna i uppdraget, för övriga aktörer inom offentliga sektor beräknas uppkomma liknande effektiviseringsvinster.

### 6.3.2 Beräkningsexempel av effekt på samhällsnytta

2017 genomförde Ramböll[40] en metaanalys av befintlig litteratur som syftade till att uppskatta potentialen av en nationell digital infrastruktur i Sverige. I metaanalysen har

[38] Myndigheters strategiska it-projekt, it-kostnader och digital mognad, DIGG 2019. Uppgifterna avser IT-kostnad för 2017 förutom för Domstolsverket där siffrorna avser 2016.

[39] Denna uppskattning kan jämföras med att Riksarkivet 2011 uppskattade nyttan med E-arkiv och E-diarium till att minska årliga IT-kostnader med ca 5 procent till följd av minskade kostnader för lagring och systemförvaltning.

[40] Potentialanalys av NDI, Ramböll på uppdrag av Finansdepartementet 20170324

identifierade samhällsekonomiska effekter från de olika undersökta länderna extrapolerats till svenska förhållanden.

Resultatet av metaaanlysen visar sammantaget att en reform kring nationell digital infrastruktur kan förväntas ge mycket positiva nettoeffekter för Sverige.

En satsning på infrastruktur för informationsförsörjning förväntas skapa ett årligt positivt nettovärde för samhället om 1,2 miljarder kronor, där 906 miljoner kronor kan ses som en lägsta uppskattning och 1,3 miljarder kronor som en högsta uppskattning

Nyttorna med reformerna förväntas överstiga kostnaderna efter 3–5 år. En samlad fördelningsanalys indikerar att ca 40 procent av reformens effekter kan förväntas tillfalla offentliga aktörer medans resterande del om 60 procent tillfaller privata aktörer i form av företag och privatpersoner.

## 6.4 Förslagens påverkan på det kommunala självstyret

Myndigheterna bedömer att förslaget om att inrätta förvaltningsgemensamma byggblock i en digital infrastruktur för informationsutbyte inte ändrar på de grundläggande förhållandena om kommuners beslutsrätt enligt gällande rätt. Däremot påverkar förslaget informationshanteringen vid utövandet av denna beslutsrätt. Kommunerna kommer att behöva följa nationella regler för att kunna ansluta sig till och nyttja byggblocken.

En effekt av förslaget bedöms vara att den enskildes möjlighet att utöva inflytande över egen information och egna ärenden ökar. Standardiserad information som är enkel att komma åt och använda är grunden för att kunna utöva ett inflytande.

Förslaget bedöms också ha en positiv effekt på processer som förutsätter ett säkert och effektivt informationsutbyte, till exempel samhällsbyggnadsprocessen, eftersom dessa kommer att kunna automatiseras i högre utsträckning. Automatisering av processer ökar transparensen och likabehandling i ärenden.

Nämnda effekter bedöms övervägande positiva utifrån de intressen som det kommunala självstyret är satt att värna, vilket är till fördel för förslaget.

Påverkan på det kommunala självstyret innebär att styrning måste ske genom lag. Med andra ord, det räcker inte att reglera byggblocken genom förordningar. Att enbart reglera den digitala infrastrukturen för informationsutbyte i förordningar innebär att infrastrukturen inte blir förvaltningsgemensam, det vill säga gemensam för statlig och kommunal verksamhet.

## 6.5 Övriga konsekvenser

### 6.5.1 Påverkan på det offentliga åtagandet

Myndigheterna bedömer att förslaget om byggblock i en förvaltningsgemensam digital infrastruktur för informationsutbyte innebär ett utökat ansvar för staten. Ansvaret avser skapande och förvaltning av föreslagna byggblock. Ansvaret omfattar även framtagande av regelverk och standarder för varje byggblock samt i relevanta fall tekniska komponenter i ett byggblock. Berörda myndigheter vars nuvarande ansvarsområde torde behöva tydliggöras eller utvecklas i ett första steg är DIGG och grunddatamyndigheter som Bolagsverket, Lantmäteriet och Skatteverket. På sikt behöver också andra så kallade stabsmyndigheters ansvar tydliggöras avseende byggblocken, till exempel MSB:s roll.

### 6.5.2 Påverkan på gällande rätt

Att införa nödvändig ny lagstiftning för att stödja det utökade offentliga åtagandet och skapa en förvaltningsgemensam reglering för såväl staten som kommuner, är omfattande och kan vara svårt att åstadkomma inom den närmaste tiden. Myndigheterna bedömer dock att det är en kritisk framgångsfaktor för digitaliseringen och de investeringar som måste göras i utvecklingen av föreslagna byggblock.

Som ett första steg föreslås att myndigheterna gör en fördjupad analys av vilket rättsligt stöd som behövs för respektive byggblock enligt föreslagna åtgärder i kapitel 5. Myndigheterna föreslår även att nödvändig rättsutveckling koordineras av ett rättsligt beredningsorgan, det vill säga en av regeringen inrättad kommitté.

### 6.5.3 Påverkan på konkurrensförhållanden för företagen

De lämnade förslagen bedöms i ett längre perspektiv påverka företagen positivt genom att det kommer att uppstå nya möjligheter att skapa behovsanpassade produkter, baserat på de tjänster som ska vara tillgängliga i den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte. Utifrån företagens perspektiv är det viktigt att tidigt i processen få kännedom om vad det offentliga kommer att leverera, särskilt i fråga om tekniska komponenter. Ur ett kortsiktigt perspektiv kan förslagen innebära negativ påverkan för några företag, då befintliga privata tjänster som ersätts med offentliga lösningar.

### 6.5.4 Överensstämmelse med EU-lagstiftning

Förslaget är förutsättningsskapande för implementering av relevanta EU-direktiv, bland annat Europaparlamentet och Europeiska unionens råd en gemensam förordning om införandet av ”Single digital gateway EU/2018/1724. Förslaget ligger också i linje EU:s mål som driver utvecklingen av EU-lagstiftningen inom området, bland annat EU:s digitala agenda.

# 1 Bilaga 1 – Omvärldsanalys

## 1.1 Nationella lösningar och initiativ

Det finns en rad olika befintliga lösningar för informationsutbyte inom olika sektorer och domäner idag i Sverige, och det pågår flertalet spännande initiativ på området. Inom ramen för denna rapport har det inte funnits möjlighet att ge en heltäckande beskrivning av samtliga utan fokus har istället lagts på lösningar och initiativ som har en bred/förvaltningsgemensam ansats.

### 1.1.1 Spridnings och hämtningssystemet (SHS)

SHS är ett kommunikations- och överföringsprotokoll som syftar till ökad säkerhet i kommunikationen över internet och SGSI. Både asynkront och synkront flöde av information stödjs.[41]

Med protokoll avses i detta sammanhang en överenskommelse mellan två eller flera parter kring regler för hur kommunikation ska gå till mellan datorer, program eller mellan noder i ett nätverk. Dessa regler ser till att kommunikationen är teknisk möjlig genom att alla parter använder sig av samma språk.

SHS togs fram på initiativ av Svenska myndigheter men det är inte bara myndigheter som använder SHS idag utan även inom kommuner och landsting används protokollet.

SHS används idag för att[42]:

- skicka elektroniska dokument
- hämta information från andra myndigheters datasystem
- prenumerera på information från andra myndigheter
- ställa frågor till en annan myndighet, som besvaras en annan dag
- lämna information, som till exempel kvitton

Ingen ny teknik har tagits fram för SHS, utan etablerade standarder med brett leverantörsstöd som exempelvis http/SSL och SOAP används i SHS.

SHS erbjuder en meddelandeorienterad tjänstearkitektur och utgör en grundsten i infrastrukturen att nå en sammanhållen förvaltning och möjlighet att utveckla e-förvaltningens e-tjänster. SHS är inte proprietär utan SHS är öppen för alla att använda.

SHS utgör idag det mest väletablerade och utbredda systemet som hanterar kommunikation mellan myndigheter via internet. SHS används idag som tekniskt protokoll i en rad olika domän och myndighetsspecifika lösningar såsom SSBTEK (sammansatt bastjänst för ekonomiskt bistånd), RIF (rättsväsendet), Lefi Online

[41] SHS Fördjupad analys MSB SOES oktober 2014

[42] Informationsplats SHS Försäkringskassan: https://www.forsakringskassan.se/myndigheter/e-tjanster/shs - läst 2019-06-27

(förmånsinformation) m.fl. Dessa lösningar är skapade för att uppfylla specifika behov inom en viss målgrupp.

SHS 2.0 som fastställdes 2013 använder samma standarder och regelverk för teknisk interoperabilitet som används för att kommunicera via Ineras nationella tjänsteplattformen (baserad på RIV-TA). Detta innebär att kommuner, landsting och myndigheter kan kommunicera tekniskt med varandra.[43]

SHS tillhandahåller en komponent i form av en global SHS-katalog som fungerar som en katalogtjänst där det publiceras information om vilka aktörer som använder SHS samt adresser (beteckningar för kommunikation) till dessa. I katalogen publiceras även information om vilka typer av produkter som kan avropas.

I en analys från Ramböll[44] gjorde SKL bedömningen att SHS fungerar väl för de större nationella myndigheterna med stora datamängder men att mindre aktörer såsom kommuner och regioner ansett att den tekniska lösningen varit för kostsam och dåligt anpassad till behovet av synkron informationsöverföring.

SHS ensamt kan inte anses motsvara en helhetslösning på ett lands behov av informationsförsörjning och saknar en rad komponenter som finns i jämförbara nationella lösningar i omvärlden. SHS är i grunden bara ett tekniskt protokoll (kan jämföras med eDelivery's AS4 protokoll). Det är således inte rättvisande att göra direkta jämförelser mellan SHS och de andra lösningarna inom ramen för denna omvärldsanalys.

Försäkringskassan har en samordnande roll avseende administration och drift av SHS. Officiellt förvaltas SHS idag av ett SHS-råd under ledning av Försäkringskassan som ansvarar för regelverk och specifikationerna. SHS-rådets roll är att leda och överse utvecklingen av SHS-specifikationen och anpassa det till nya trender och teknik.

### 1.1.2 Nationella tjänsteplattformen

Nationella tjänsteplattformen[45] är en teknisk plattform som förenklar, säkrar och effektiviserar informationsutbytet mellan olika it-system inom vård och omsorg. Plattformen är navet mellan system och e-tjänster som behöver kommunicera med varandra, och gör att informationsutbytet kan ske på ett säkert och kostnadseffektivt sätt.

Nationella tjänsteplattformen möjliggör lös koppling genom att fungera som en växel för alla system som vill kommunicera med varandra. Verksamheter kan ansluta sina system till Nationella tjänsteplattformen och på så sätt utbyta information utan att upprätta direkta kopplingar mellan varandra. Ett system som vill kontakta ett annat system gör ett anrop till tjänsteplattformen som dirigerar meddelandet vidare till rätt system.

För att informationsutbytet via Nationella tjänsteplattformen ska fungera måste alla aktörer vara överens om hur kommunikationen ska gå till. Inera ansvarar för utveckling

[43] RIV Anvisningar: http://www.rivta.se/ - läst 2019-06-27
[44] Analys av det estnisk-finska samarbetet kring den digitala infrastrukturen X-road, Ramböll 2016-01-29
[45] Nationella tjänsteplattformen: https://www.inera.se/digitalisering/infrastruktur/nationella-tjansteplattformen-och-tjanstekontrakt/ - läst 2019-06-27

och förvaltning av tekniska specifikationer, så kallade tjänstekontrakt, som beskriver hur det system som vill ställa en fråga ska utforma sitt frågemeddelande, och hur det system som ska svara ska utforma sitt svarsmeddelande. Tjänstekontrakten utformas för specifika funktioner eller verksamhetsprocesser, exempelvis för listning eller tidbokning.

Det finns även regionala tjänsteplattformar i olika regioner t.ex. i Dalarna och Stockholm. En regional tjänsteplattform underlättar integrationen mellan lokala system som ska kommunicera med varandra via tjänstekontrakt som följer RIVTA-standard. Dessutom underlättar en regional tjänsteplattform anslutningsförandet mot Nationella tjänsteplattformen. När en anslutning mellan en regional tjänsteplattform och Nationella tjänsteplattformen väl etablerats, kan denna återanvändas för alla nya anslutningar mot Nationella tjänsteplattformen.[46]

Tjänsteplattformens huvudsyfte är att tillhandahålla en nationell web-service för varje typ av tjänst. Vårdens IT-stöd består sällan av en nationell tjänst för en viss funktion. Ansvaret för verksamhetens operativa IT-stöd är regionalt. Därför finns samma funktion på många ställen. Ibland i form av kopior av samma system, ibland som olika system. Floran av system försvårar för konsumenter av tjänster, så som medborgarportaler. Utan tjänsteplattformen skulle varje tjänstekonsument behöva hålla reda på vilken tjänst som hör till vilken vårdgivare och dessutom förstå olika tekniska dialekter för kommunikation.

Tjänsteplattformen stödjer teknisk och semantiskt interoperabilitet på ett teknikoberoende sätt, och ligger till grund för tjänster som Nationell patientöversikt, Elektronisk remiss och Journalen via nätet.

Över 500 vårdsystem är anslutna och kommunicerar med varandra via tjänsteplattformen och antalet anrop över plattformen ökar och varje månad görs i snitt över 70 miljoner producentanrop.[47]

Inera ansvarar för den nationella tjänsteplattformen och utvecklar och förvaltar nationella digitala tjänster inom e-hälsa och digitalisering på uppdrag av regioner och kommuner. Inera ansvarar även för den gemensamma infrastruktur och IT-arkitektur som ligger till grund för tjänsterna. Inera är ett bolag som ägs av SKL Företag AB, regioner och kommuner.

### 1.1.3 Säker digital kommunikation (SDK-projektet)

Projektet Säker digital kommunikation[48], som förkortas SDK har målet att Sverige ska ha en standardiserad förmåga till säker digital kommunikation mellan offentliga aktörer, inklusive privata utförare av offentligt uppdrag. Det innebär att definiera ett gemensamt sätt att överföra känslig information på ett enhetligt, effektivt, säkert och överenskommet sätt. På sikt ska det även vara möjligt att förmedla information till privatpersoner och

[46] Tjänsteplattformen i conflucence: https://skl-tp.atlassian.net/wiki/spaces/SKLTP/overview - läst 2019-06-27
[47] Antal anrop och svarstider: https://www.inera.se/aktuellt/statistik/tjansteplattformen/ - läst 2019-06-27
[48] SDK Inera: https://www.inera.se/aktuellt/projekt/saker-digital-kommunikation/ - läst 2019-06-27

andra intressenter via befintliga kommunikationskanaler genom att anpassa till samma standarder. Säker digital kommunikation ska också vara möjlig utanför Sveriges gränser.

Projektet genomförs med Inera som projektägare tillsammans med Sveriges kommuner och landsting, SKL, Kommentus och i samverkan med regioner, kommuner och statliga myndigheter.

Säker digital kommunikation baseras på eDelivery. Att utgå ifrån eDelivery i framtagandet av lösningen för Säker digital kommunikation innebär att projektet använder EU:s specifikationer för eDelivery för att sätta upp komponenter som accesspunkter, metadatatjänst, adressregister och koppling till eDelivery-komponenter på nationell nivå respektive inom EU. Projektet kompletterar med delar som saknas i eDelivery idag men som behövs för Säker digital kommunikation, exempelvis en SDK adressbok som ska möjliggöra att utöver som i eDelivery adressera mellan organisationer, även kommer kunna adressera mellan funktioner inom organisationer. Projektet tar också fram en meddelandespecifikation för hur det säkra meddelandet ska se ut.

Drivkrafterna i att använda eDelivery för Säker digital kommunikation är att återanvända etablerade standarder för säkra meddelanden, att undvika stuprörslösningar och att möjliggöra kommunikation även utanför Sveriges gränser. I Sverige ansvarar Myndigheten för digital förvaltning, DIGG, för eDelivery.

2018 genomfördes en så kallad proof of concept för att verifiera konceptet för Säker digital kommunikation inklusive ansatsen att bygga på EU-ramverket eDelivery för säker meddelandehantering. Resultatet innebar att de standarder och de specifikationer som Säker digital kommunikation bygger på, fungerar för att skicka, ta emot, få notifiering och kvittens av säkra meddelanden och bilagor, mellan olika fiktiva aktörer.

### 1.1.4 Swedish government secure intranet (SGSI)

SGSI[49] är en avgiftsfinansierad kommunikationstjänst för säker kommunikation mellan organisationer i Sverige och i Europa. SGSI har en egen infrastruktur som är skild från Internet och påverkas därför inte av störningar på Internet, som till exempel överbelastningsattacker. Mellan anslutna organisationer sker trafiken i så kallade VPN-tunnlar som krypteras.

Med SGSI kan man få åtkomst till andra anslutna myndigheters databaser, skicka skyddad e-post och använda förbindelsen till skyddade videokonferenser. Med SGSI är det även möjligt för svenska myndigheter att komma åt sektorspecifika EU-tjänster eller att utbyta information med andra EU-medlemsstater eftersom det är kopplat till det skyddade nätet TESTA.[50]

Anslutna organisationer använder SGSI som en infrastruktur för utbyte av känslig information. Därmed minskar risker relaterat till att skicka känslig information. Anslutna

[49] SGSI MSB: https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyhetsarkiv/Nyhetsarkiv-2017/Sa-fungerar-SGSI-natet2/ läst 2019-06-27

[50] Isa2: https://ec.europa.eu/isa2/solutions/testa_en - läst 2019-06-27

organisationer bestämmer själva vad som ska kommuniceras över SGSI och med vem. För att det ska vara möjligt att kommunicera över SGSI måste avsändare och mottagare komma överens om att en förbindelse ska öppnas, och vilken typ av kommunikation den ska användas till.

Endast en myndighet som är ackrediterad för SGSI kan ansluta sig. Detta i syfte att skapa tillit och förtroende till hur myndigheten hanterar informationssäkerhetsfrågor och då främst säkerheten i SGSI. Detta sker genom att myndigheten öppet redovisar sitt informationssäkerhetsarbete i stort, samt mer i detalj om säkerheten kring anslutningen till SGSI.[51]

## 1.2 Europeiska unionens initiativ och lösningar

### 1.2.1 EUs målsättning och strategier

Europa 2020 – EU:s gemensamma strategi för tillväxt och sysselsättning – och den Digitala agendan för samma period pekar tydligt ut ”Digital Single Market”[52] (DSM) som ett huvudmål. Detta mål speglar verkliga behov av ökad digital rörlighet över europeiska gränser. För att uppnå detta mål är ett effektivt informationsutbyte en avgörande förutsättning. Utan ett komplett, säkert och effektivt utbyte av grundläggande data finns ingen garanti av aktualitet och kvalitet i informationsutbytet mellan medlemsstaterna.¨

För att genomföra etableringen av DSM finns dels det övergripande ramprogrammet för forskning och utveckling Horizon 2020, dels de underliggande programmen Interoperability Solutions for European Public Administrations (ISA²) och Connecting Europe Facility (CEF).

Genomförandeplaner som EU: s ”e-government action plan” samt överenskommelser mellan medlemsstaterna, som “The Tallinn Declaration”[53], förstärker målet ytterligare genom att lyfta fram viktiga aktiviteter som gränsöverskridande och stabila EID-system (eIDAS) och gränsöverskridande informationsutbyte enligt ”The Once Only Principle”[54]. Aktivitetsplanens 20 aktiviteter syftar till att göra offentliga förvaltningar och offentliga institutioner inom EU öppna, effektiva och inkluderande genom att tillhandahålla gränsöverskridande och användarvänliga digitala offentliga tjänster till alla medborgare och företag i EU.

I kommunikationen av planen pekar EU-kommissionen på att det är upp till medlemsstaterna att själva välja teknisk plattform och systemstöd samt även decentraliserad eller central infrastruktur. Detta under förutsättning att överenskomna principer följs.

Alla aktiviteter i e-government action plan samt de sju principerna är intressanta för regeringsuppdraget om ett säkert och effektivt elektroniskt informationsutbyte inom den

[51] Faktablad SGSI MSB 180817
[52] Digital Single Market: https://ec.europa.eu/digital-single-market/en
[53] Ministerial Declaration on eGovernment – the Tallin Declaration october 2017
[54] The Once Only Principle: http://www.toop.eu/

offentliga sektorn. Vi bör dock särskilt fokusera på principen ”Interoperability by default” i den del av uppdraget som gäller ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn. Principen förklaras i aktivitetsplanen med texten ”Offentliga förvaltningar bör organiseras på ett sådant så att de fungerar sömlöst på hela den inre marknaden och utan några vattentäta skott, baserat på den fria rörligheten för uppgifter och digitala tjänster i europeiska unionen”.

Skrivningen innebär ett troligt mål att samordna och knyta ihop medlemsstaternas infrastrukturer för informationsutbyte. Som tidigare konstaterat förutsätter en sådan sammankoppling en heltäckande svensk infrastruktur. I annat fall där exempelvis skilda domäner ansluter separat till en EU-infrastruktur uppstår multipla kostnader.

De aktiviteter i e-government action plan som är mest aktuella ur uppdragets perspektiv är främst aktivitet 18 ”Analysera möjligheten att tillämpa principen om endast en gång i gränsöverskridande sammanhang”. Även de något mer tydliga och pågående aktiviteterna 7 ”Lägga fram ett förslag om en gemensam digital ingång” samt 9 ”I samarbete med medlemsstaterna uppnå obligatorisk sammankoppling av alla medlemsstaternas företagsregister” kommer vid ett genomförande att ha en stark påverkan på svensk infrastruktur.

### 1.2.2 Interoperability solutions and common frameworks for European Public Administrations (ISA²)

ISA²-programmet[55] ska stödja medlemsländerna att tillhandahålla digitala interoperabilitetstjänster. Stödet omfattar bland annat metoder för samverkan, standardisering, semantik, arkitektur och delning av data. Målet är att bidra till att europeiska offentliga förvaltningar på ett smidigt sätt kan kommunicera elektroniskt med varandra samt med medborgare och företag.

ISA² har i samarbete med medlemsländerna tagit fram arkitekturramverket European Interoperability Framework (EIF). Ramverket ger specifik vägledning om hur man utvecklar och inför interoperabla digitala offentliga tjänster. Programmet bistår också införanden av interoperabla tjänster med referensarkitekturen European Interoperability Reference Architecture (EIRA).

### 1.2.3 Connecting Europe Facility (CEF)

Connecting Europe Facility (CEF)[56] är ett viktigt EU-finansieringsinstrument för att underlätta gränsöverskridande samverkan bland annat mellan offentliga förvaltningar, företag och medborgare genom att distribuera digital serviceinfrastruktur (DSI). De projekt som finansieras och stöds förväntas bidra till skapandet av ett europeiskt ekosystem för driftskompatibla och sammankopplade digitala tjänster som upprätthåller den digitala inre marknaden.

[55] ISA2: https://ec.europa.eu/isa2/home_en - läst 2019-06-27
[56] CEF Telecom: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom - läst 2019-06-27

CEF Byggblock är en uppsättning tjänster (inklusive programvara, dokumentation, utbildning och stöd) som tillhandahålls av Europeiska kommissionen och stöds av medlemsstaterna. Syftet med byggblocken är att stödja utvecklingen av DSM genom att tillhandahålla återanvändningsbara funktioner och stöd för gränsöverskridande digitala tjänster. De byggblock som EU-kommissionens fokuserar på nu är eID, eSignature, eDelivery, eTranslation och eInvoicing.

Byggblocken med tillhörande stöd och support är fritt att använda för alla europeiska projekt relaterade till digitala offentliga tjänster. Varje byggblock består av

- en tjänsteplattform som erbjuder tekniska specifikationer och standarder som ska följas,
- ett lager av exempelprogramvara avsedd för återanvändning för att underlätta genomförandet av tekniska specifikationer och standarder,
- ett lager av tjänster t ex programvara, testmöjligheter, helpdesk – beroende på byggsten.

Det finns möjlighet för medlemsstater att få finansiering från EU i genomförande av projekt som använder byggblocken.

### 1.2.4 eDelivery

eDelivery[57] består av återanvändningsbara specifikationer, mjukvara och tjänster som formar en digital service infrastruktur inom en rad olika domäner.

Huvudsyftet med eDelivery är att säkerställa att offentliga aktörer kan utbyta data och dokument över EUs gränser på ett säkert, interoperabelt, tillförlitligt sätt. eDelivery kan även möjliggöra utbyte med företag och medborgare.

eDelivery är baserat på en distribuerad modell som innebär att deltagarna blir en nod i ett nätverk genom att använda standardiserade protokoll och säkerhetsrutiner. eDelivery möjliggör kommunikation direkt mellan deltagare utan behov att sätta upp bilaterala kanaler.

eDelivery innehåller en rad olika komponenter och verktyg såsom transportprotokoll, adresseringsfunktion, kuvertering och certifikatshantering som kan användas och anpassas/utvecklas utifrån ett specifikt behov. Lösningen är således anpassningsbar och det är även möjligt att lägga till och komplettera med egna komponenter och specifikationer.

eDelivery är framtagen för att stödja en så kallad fyrahörnsmodell men kan också användas i andra konstellationer. eDelivery tillämpar tekniska specifikationer och kan användas i alla typer av domäner för att säkerställa säker och tillförlitlig överföring av strukturerad, ostrukturerad och binära data och dokument. Överföringen behöver inte ske över EUs gränser utan kan även ske inom en sektor eller inhemsk domän.

[57] eDelivery: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery - läst 2019-06-27

eDelivery används redan idag inom flera olika domäner och storskaliga projekt på EU-nivå. Bland annat i systemet för sammankoppling av företagsregister, e-juridik portalen, PEPPOL m.fl. EU-kommissionen är tydlig i strategin att använda byggblocken för digital service infrastruktur för att uppnå en inre digital marknad inom EU. Man finansierar bland annat teknisk utveckling, support och administration av centrala komponenter och det finns även möjlighet till bidrag för implementation.

Användningen av eDelivery är idag i huvudsak domänspecifik även om lösningen rent tekniskt inte är begränsad till det ändamålet. Huvudsyftet med dagens implementationer är att underlätta interoperabilitet över landsgränserna och säkra ett utbyte mellan länder inom olika sektorer och domäner.

### 1.2.5 Single digital gateway (SDGR)

I oktober 2018 antog Europaparlamentet och Europeiska unionens råd en gemensam förordning om införandet av ”Single digital gateway (EU) 2018/1724. Förordningen syftar huvudsakligen till att ge medborgarna och företag inom EU tillgång till information, förfaranden och problemlösningstjänster.

Förordningen är publicerad och genomförandeakterna är under framtagande. Dessa kommer att ha en genomförandetid på 3-5 år. Ett genomförande kommer att innebära en anpassning till en Europeisk toppdomän där information och e-tjänster ska vara sök- och användningsbara för alla EU-medborgare. Förordningen kommer att gälla för de flesta områden inom offentlig sektor. SDGR innebär vidare att visst data, bland annat grunddata ska kunna sökas och hämtas på samma gränsöverskridande sätt.

### 1.2.6 The Once Only Principle (TOOP)

EU-projektet TOOP är ett delprojekt inom ramen för Horisont och är en av 20 prioriterade insatser i EU-kommissionens eGovernment Action Plan för perioden 2016–2020. TOOP utgår från principen om att en uppgift enbart ska behöva lämnas en gång och till en myndighet/instans. Projektet inriktas mot gränsöverskridande digitalt informationsutbyte av företagsinformation mellan myndigheter inom EU. Det övergripande syftet är att visa genomförbarheten av ”The Once Only Principle” genom att ta fram ett förslag till en federerad europeisk infrastruktur för digitalt informationsutbyte. Förslaget ska vara baserat på pilotutveckling inom flera områden, alla med fokus på utbyte av företagsinformation. Trots detta fokus ska resultatet vara möjligt att vidareutveckla för hantering av digitalt informationsutbyte även inom andra områden.

Projektet ska efter en förlängning på nio månader göra sin slutleverans i mars 2020. Ett av skälen till förlängningen är tilläggsuppdraget att TOOP ska vara det tekniska system som förmedlar information enligt Single Digital Gateway Regulation.

Flera europeiska länder har börjat inkorporera TOOP i lagstiftning och regelverk. I Belgien, Estland och Nederländerna finns redan tvingande lagstiftning på plats.[58]

[58] EU-wide digital Once-Only principle for citizens and businesses – policy options and their impact, EU 2014

## 1.3 Internationella lösningar

### 1.3.1 Estland – X-road (X-tee)

X-road[59] är ett centralt förvaltat distribuerat mellanlager för informationsutbyte. X-road möjliggör säker överföring och utbyte av data mellan informationssystem över internet. X-road fungerar som ett mellanlager och minskar komplexiteten för medlemmar att kommunicera mellan parter på ett säkert sätt.

De grundläggande komponenterna i X-road består av två centrala komponenter. Central server som är ett register över X-road medlemmar och deras säkerhetsservrar. Säkerhetsservern är ingången till nätverket och krävs både för att producera och konsumera tjänster via X-road. Servrarna förmedlar förfrågningar mellan informationssystem.

Utöver dessa bygger lösningen på en rad olika tillitstjänster såsom certifiering, validering och loggning för meddelanden och överföringar. Dessa kan vara tillhandahållna av tredjepart eller tillhandahållas centralt.

X-road tekniken används idag av Estland (kallas i landet X-tee), Finland (suomi.fi-informationsled) och ett tiotal andra länder såsom Färöarna, Kirgizistan m.fl. Även Island står i takt med att implementera lösningen.

X-tee beskrivs som ett fullt ut distribuerat och säker plattform för informationsutbyte[60]. Plattformen var initialt bara tillgängligt för den offentliga sektorn men har senare inkluderat även privata aktörer för ökad effektivitet och bekvämlighet. Vidare brukar man kalla lösningen för ryggraden av den Estniska statsapparaten eftersom en absolut majoritet av deras register och databaser görs tillgängliga genom plattformen. X-tee's logik och arkitektur innebär att det saknas central lagring av information. Istället hämtas och skickas all data mellan aktörer vid behov.[61]

Det är ingen unik teknik som ligger bakom X-tee, systemet är byggt på internationell standard och protokoll och sedan 2016[62] är dess källkod öppen och tillgänglig för vem som helst att använda.

I Estland strävar man efter att varje typ av data, till exempel medborgarnas adresser, bara ska finnas lagrade på ett ställe – och att alla andra har tillgång till informationen via X-tee, utan att behöva spara ner egna kopior. Estland har också lagstiftning som innebär att en myndighet inte ska fråga medborgaren eller företaget om uppgifter som redan finns hos någon annan myndighet, i stället ska de använda X-tee för att få dessa uppgifter.

[59] X-road e-Estonia: https://e-estonia.com/solutions/interoperability-services/x-road/ - läst 2019-06-27
[60] Introduktion till X-tee: https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html - läst 2019-06-27
[61] Rapport om X-road – Ramböll 2016-01-29
[62] Öppen källkod: https://github.com/ria-ee/X-Road - 2019-06-27

Användningen av X-tee i Estland är mycket utbredd, under 2018 hanterades nästan 1 miljard förfrågningar genom X-tee[63].

Koordinering och implementation av Estlands digitaliseringspolitik sker genom Estonian Information System Authority (RIA). Myndighetens uppdrag är att samordna och koordinera utvecklingen och förvaltningen av informationssystem så att Estniska medborgare får bästa tänkbara service. RIA ansvarar för all offentlig infrastruktur som relaterar till informationsteknologi såsom X-tee, den statliga e-portalen[64] m.m. Myndigheten lyder under Estlands Ministry of Economic Affairs and Communication som ansvarar för utvecklingen av landets informationspolitik. Inom ministeriet finns även en avdelning som heter Government CIO Office som spelar en viktig roll i informationspolitiken i landet. Denna avdelning ansvarar för statens IT-budget, koordinering av IT, standardisering m.m. Avdelningen är uppdelad i sex olika team (Legal, Financing, ICT Skills, Cybersecurity Policy, Govtech, International Affairs).

Estland har tillsammans med Finland inrättat ”Nordic institute for interoperability solutions (NIIS)” som är ett gemensamt nätverk och en plattform för samverkan för utveckling av X-road teknologin. NIIS ansvarar för och reviderar X-road’s källkod, principer för licenser och distribution, utveckling och support m.m.

### 1.3.2 Finland – eSuomi.fi-informationsled

Suomi.fi-informationsled[65] är ett standardiserat, enhetligt, koordinerat, interoperabelt och datasäkert informationslager som möjliggör utbyte av data och tillgång till informationskällor på ett enkelt och kostnadseffektivt sätt.

Suomi.fi-informationsled är Finlands implementation av X-road tekniken i landet. Till skillnad från Estland är X-road inte den enda teknologin som används i landet, utan man har även kvar vissa sektor/domän-specifika lösningar. Suomi.fi-informationsled i helhet innehåller också andra komponenter, t.ex. katalog över tjänsterna och några komponenter relaterade till monitorering av tjänsterna.

Befintliga tjänster som ansluts till informationsledet möjliggör att utnyttja alla integrerade informationskällor och tjänstekomponenter vilket leder till kostnadseffektivitet och effektivare utveckling genom återanvändning.

Suomi.fi-informationsled använder i alla kärnkomponenterna samma kodbas som används i X-tee i Estland. Alla skillnader mellan Suomi.fi-informationsled och X-tee handlar om lokal konfiguration

Finlands API-katalog[66] är en katalog över API:er som finns i deras nationella informationsutbyteslager. Syftet med katalogen är att hjälpa producenter och

[63] X-tee factsheet: https://www.x-tee.ee/factsheets/EE/#eng – läst 2019-06-27
[64] Eesti.ee gateway: https://www.eesti.ee/en/ - läst 2019-06-27
[65] eSuomi.fi informationsled: https://esuomi.fi/suomi-fi-tjanster/suomi-fi-informationsled/?lang=sv – läst 2019-06-27
[66] Finlands API-katalog: https://liityntakatalogi.suomi.fi/sv/ - läst 2019-06-27

konsumenter att utveckla effektivare elektroniska tjänster och främja återanvändning av uppgifterna. Som tjänsteleverantör kan man välja att endast utnyttja API-katalogen.

Organisationer inom den offentliga sektorn är skyldiga eller har rätt att använda informationsledet enligt finsk lagstiftning. Organisationer inom den privata sektorn har enligt samma lagstiftning rätt att använda informationsledet för att föra över information.

Att ansluta sig till och använda tjänsten är gratis för alla, inklusive den privata sektorn. Varje aktör betalar sina egna implementationskostnader, men finansministeriet kan i vissa fall bevilja finansiering för offentliga organisationer.

Uppgifterna som erbjuds via informationsledet är antingen avtalsenliga mellan dem som utnyttjar och erbjuder dem eller fritt användbara av alla som anslutit sig.

I Finland är det Befolkningsregistercentralen som ansvarar för drift och förvaltning av den nationella servicearkitekturen för e-tjänster och styrningen sker från det finska Finansministeriet.

### 1.3.3 Danmark – Datafordeler

Datafordeler[67] (datafördelaren) i Danmark ger säker och enkel tillgång till grundläggande data från offentliga register till myndigheter, företag och medborgare. Datafördelarens syfte är att tillgängliggöra grunddata och facilitera överföringen genom en gemensam datamodell[68]. Lösningen är den digitala infrastrukturen för distribution av grunddata i Danmark och har gradvis ersatt en rad olika tidigare distribuerade lösningar.

Datafördelaren säkerställer att myndigheter och organisationer har enkel och säker tillgång till grunddata i ett och samma system, istället för olika utspridda system och gränssnitt.

Datafördelaren är avgränsad till och skapad för informationsutbyte gällande grunddata men kan även användas för att distribuera annan relevant data. Lösningen förmedlar information både inom offentlig och privat sektor.

Datafördelaren togs fram inom ramen för Danmarks grunddataprogram ”Gode grunddata till alle” som är ett nationellt program för att standardisera och tillgängliggöra de basregister som finns i landet. Programmet startade 2012 och har succesivt moderniserat grunddata inom en rad olika delprogram.

Det är Styrelsen for Dataforsyning och Effektivisering (SFDE) som är operativt ansvarig för Datafördelaren. SFDE ingår i det danska ministeriet Energi-, Forsynings- og Klimatministeriet.

[67] Om datafordeleren: https://datafordeler.dk/vejledning/om-datafordeeren/ - läst 2019-06-27
[68] Datamodell: https://datafordeler.dk/vejledning/datamodel/ - läst 2019-06-27

### 1.3.4 Singapore – APEX

Government Technology Agency of Singapore (GovTech) ansvarar för och utvecklar Singapore's API exchange (APEX)[69]. APEX är en centraliserad platform för informationsutbyte för offentliga aktörer för att utbyta data på ett effektivt och säkert sätt genom att använda sig av API:er. Plattformen möjliggör central monitorering och säkerhetshantering för API:erna. APEX är Singapores svar och verktyg för att koppla ihop olika typer av system som används av olika myndigheter och ministerium som i många avseenden har olika befintliga domän- och sektorsspecifika lösningar.

APEX grundar sig i en self-service modell där den anropande myndigheten kan hämta olika typer av data och information direkt från andra myndigheter med hjälp av i förhand konfigurerade kontroller av rättigheter och tillgång. API:erna som publiceras på APEX kan antingen vara öppna för allmänheten eller privata (för internt bruk av offentlig sektor).

API:erna är återanvändbara för integration med andra tjänster och applikationer alternativt för statistik. Detta möjliggör att man kan återanvända befintlig infrastruktur och besparar kostnader då myndigheter inte behöver bygga nya tjänster från början, detta innebär även förkortad tid för utveckling av nya tjänster.

Genom att använda APEX kan offentliga aktörer hantera och utvärdera/följa deras API:er och konsumtionen av data i realtid och får en överblick av användningen av deras tillgängliggjorda information.

APEX har idag ett hundratal anslutna API:er och fler läggs till löpande. GovTech använder APEX bland annat för deras "MyInfo"-tjänst som är en plattform där användare bara behöver uppge sina personliga uppgifter en gång till staten, istället för att göra det vid varje transaktionstillfälle.

APEX är en del av en gemensam nationell digital infrastruktur som kallas "Singapore Government Technology Stack (SGTS)"[70], som består av ett antal tekniska byggblock som bistår med gemensamma mjukvarutjänster och delade infrastrukturtjänster som myndigheter och andra offentliga aktörer kan återanvända för att bygga och testa nya tjänster och applikationer på ett effektivt och snabbt sätt. Huvudsyftet är att skapa en gemensam plattform för back-end services så att myndigheterna kan fokusera på innehåll och tjänster mot slutkonsument utan att behöva bygga infrastruktur, lagring och informationsutbytessystem från början.

SGTS består ett antal olika standardiserade lager, ett grundläggande infrastrukturlager bestående av container-baserade hosting och molnlösningar. Ett applikationslager (mellanlager) som består av en samling hjälpmedel eller komponenter som hjälper utvecklare. Här finns komponenter som APEX, platform-as-a-service (NECTAR) och

[69] Apex och Nectar: https://www.tech.gov.sg/media/technews/getting-to-know-nectar-and-apex - läst 2019-06-27
[70] Singapore Tech Stack: https://www.tech.gov.sg/products-and-services/singapore-government-tech-stack/ - läst 2019-06-27

gemensamma säkerhets och analyskomponenter. I mikrotjänstlagret hanteras olika återanvändbara förvaltningsgemensamma tjänster såsom betalningar, autentisering och identifikationslösningar. Det översta lagret består av front-end tjänster för digital service mot slutkonsumenterna.

GovTech är en myndighet (statutory board) som ingår i ”Smart Nation and Digital Government Group” (SNDGG) vilket lyder direkt under premiärministerns avdelning (Prime Minister’s Office, PMO). PMO består av flertalet myndigheter och råd som stödjer och ger råd i strategiskt viktiga frågor. GovTech arbetar tillsammans med offentliga aktörer för att utveckla och leverera säkra digitala tjänster och applikationer till individer och företag i Singapore. GovTech ansvarar för infrastrukturen och lösningar som behövs för att realisera landets strategier.

### 1.3.5 Belgien – Federal Service Bus

Belgien beskrivs som en föregångare när det kommer till informationsutbyte mellan myndigheter och deras federala plattform Federal Service Bus (FSB) och den regionala lösningen Maximum Data Sharing Between Agencies (MAGDA) lyfts fram som goda exempel.[71] Magda plattformen blev även 2017 tilldelad pris för bästa IT-lösning för offentlig sektor i en tävling anordnad av EU-kommissionen.[72]

Belgien har inte en och samma lösning för informationsförsörjning och överföring i landet utan snarare ett nätverk bestående av flera olika ”service integrators” inom olika sektorer som man arbetar med att koppla ihop med varandra. Det finns två regionala service integratorer, en för Flandern och en för Vallonien, det finns en federal service integrator och så finns det en för välfärdssektorn och en för e-hälsosektorn. Dessa integratorer knyter samman och möjliggör tillgång till olika datakällor inom nätverket.

Landet har identifierat och definierat vad man kallar auktoritära data[73] och källor vilket motsvarar datakällor där grunddata förvaras. Denna data skickas sedan vidare inom deras ekosystem genom ett gemensamt informationslager uppbyggt på service integratorerna med hjälp av webbaserade tjänster.

I Belgien kallar man sina ministerium för Federal Public Services (FPS) och varje FPS har en eller flera ansvariga ministrar. Det är FPS Policy and Support som ansvarar för federal IT, budget, organisation, stöd m.m. Inom denna organisation har man en avdelning som heter ”Directorate General Digital Transformation”[74] (tidigare FEDICT, numera BOSA) som har ansvaret för och stöder regeringen i digitaliseringen av landet. BOSA (Digital transformation office) ansvarar för den nationella infrastrukturen och utvecklar komponenter såsom den gemensamma lösningen för informationsutbyte (federal service

[71] Access to base registries report 2016 – EU-komissionen
[72] Sharing and reuse awards contest 2017: https://ec.europa.eu/isa2/awards_en - läst 2019-06-27
[73] Informationsutbyte Belgien: https://dt.bosa.be/en/gegevensuitwisseling - läst 2019-06-27
[74] DG DT: https://dt.bosa.be/en - läst 2019-06-27

bus, FSB). Man ansvarar för implementation och utvecklingen av regeringens politik och är den drivande kraften i landet.

### 1.3.6 Nederländerna – Digikoppeling

Digikoppeling[75] är en uppsättning standarder för elektronisk informationsutbyte mellan offentliga aktörer. Digikoppeling möjliggör utbyte av data mellan offentliga aktörer och anslutning till andra byggstenar inom den Nederländska digitala infrastrukturen. Digikoppeling reglerar inte innehållet i överföringen utan endast logistiken.

För att kunna utbyta data mellan IT-system måste organisationer göra överenskommelser om format, transportsätt och förpackningen. Digikoppeling är en specifikation av två internationella standarder för elektronisk överföring, WUS och ebMS2. De olika standarderna används för att uppfylla olika typer av behov och lösningsmönster.

Logius ansvarar för förvaltning, utveckling och främjande av nationella digitala infrastruktur-komponenter i Nederländerna. Logius är en avdelning inom ministeriet Ministry of the Interior and Kingdom Relations.

### 1.3.7 Norge – Alltinn

Altinn[76] är en förvaltningsgemensam lösning och gränssnitt för att ta fram och underhålla blanketter och processer tillsammans med en lösning för rapportering och informationsutbyte främst mellan privat sektor och myndigheter. Företag och individer kan rapportera sin information genom Altinn antingen genom en internet portal alternativt genom sitt egna interna informationssystem eller mjukvarulösningar. Altinn fungerar som Norges point of single contact[77]. Altinn är som namnet också indikerar således en helhetslösning och plattform för digitala tjänster snarare än en lösning för informationsutbyte.

Altinn har en rad olika typer av funktionalitet, bland annat kan lösningen användas för att skicka dokument eller stora mängder data mellan offentliga aktörer och privat sektor. Information från aktörernas register kan skickas till en eller flera mottagare. Informationen skickas antingen från maskin till maskin eller via inkorgen/meddelandetjänsten. Altinn agerar endast som mellanhand och kontrollerar inte innehållet i sändningen utan garanterar leverans och spårbarhet. Altinn tillhandahåller en gemensam teknisk infrastruktur som säkerställer säker transport mellan aktörerna. Altinn har en egen förvaltningsorganisation som hanterar underhåll, drift och backup av den tekniska lösningen.

Altinn möjliggör också att användare kan få tillgång till information som offentliga aktörer har sparat i sina system. Detta möjliggör användare att enkelt komma åt sin egna

[75] Digikoppeling: https://www.logius.nl/diensten/digikoppeling - läst 2019-06-27
[76] Vad är Altinn: https://www.altinn.no/om-altinn/hva-er-altinn/ - läst 2019-06-27
[77] Points of singe contact EUGO: https://ec.europa.eu/growth/single-market/services/services-directive/in-practice/contact_en - läst 2019-06-27

data och hämta den direkt från registret. Detta kan användas för att hämta kundinformation, tillstånd, licenser m.m.

Altinn erbjuder också en tjänst för samtycke som gör det möjligt att få tillgång till data om personer eller organisationer som offentlig sektor har sedan tidigare, exempelvis taxeringsuppgifter. Samtyckestjänsten används när en offentlig aktör inte har laglig rätt att utan medgivande ta del och erhålla informationen. Användaren kan se vad de delar och med vem, samt hur länge och vad informationen kommer användas till. Tjänsten förenklar datainsamlingen från användare och gör att data som tidigare hämtas in kan användas i flera syften efter att samtycke erhållits. Detta gör det också möjligt för privata aktörer att använda offentliga data på ett säkert och effektivt sätt.

Altinn har även en tjänst för behörighet som är en produkt som styr vem som kan använda en digital tjänst. Användarna loggar in via den norska ID-porten[78]vilket är Norges förvaltningsgemensamma portal för inloggning till offentliga tjänster på internet. Via ID-porten får de sedan tillgång till tjänsten. Om en person ska använda en tjänst på uppdrag av ett företag görs en slagning mot Norges centrala samordningsregister för juridiska personer för att bekräfta att personen har mandat att agera för företagets räkning.

Det här är en produkt som låter dig styra vem som kan använda en digital tjänst. Användarna loggar in via ID-porten och skickas sedan vidare till tjänsten. Om en person ska använda en tjänst på uppdrag av ett företag görs ett uttalande mot det centrala enhetsregistret[79] för juridiska personer för att bekräfta att personen har en roll för företagets räkning.

Altinn tillhandahålls och förvaltas av Brønnøysundregistrene som har i uppdrag att utveckla och driva digitala tjänster och register. Brønnøysundregistrene är en myndighet som lyder under det norska Naerings og fiskeridepartementet.

## 1.4 Omvärldsanalys utifrån särskilda aspekter

### 1.4.1 Tekniska förutsättningar

Övergripande ur ett tekniskt perspektiv är det inte särskilt stor skillnad mellan de olika lösningarna som vi studerat närmare i omvärlden och de lösningar vi redan idag har i Sverige. Lösningarna bygger oftast på liknande topologier i form av tre eller fyra hörnsmodeller. De baseras ofta på samma typ av teknik eller standard, XML, SOAP eller REST är de vanligast förekommande. Både SHS och Tjänsteplattformen (SHS) har flera likheter med X-road och eDelivery då samtliga grundar sig i distribuerade arkitekturer utan central mellanlagring, transport via internet och autentisering genom certifikat.

[78] ID-porten: https://eid.difi.no/nb/id-porten - läst 2019-06-27

[79] Enhetsregistret: https://data.norge.no/data/registerenheten-i-br%C3%B8nn%C3%B8ysund/enhetsregisteret - läst 2019-06-27

Flera länder har publicerat källkoden för sina lösningar under öppna licenser. Det råder generellt stor transpararens kring de tekniska lösningarna framförallt i syfte att främja utveckling och användning.

Det som skiljer lösningarna åt är oftast vilken typ av centrala komponenter som man har skapat och styrning kring användningen av lösningen. Centrala komponenter i lösningarna återfinns ofta i form av adressering/adressregister, certifikatshantering, transportprotokoll samt olika typer av säkerhets och tillitstjänster.

Om man jämför med den privata sektorn och motsvarande lösningar för informationsförsörjning är det tydligt att flera av de olika ländernas lösningar baseras på ett till synes utdaterat tänk och teknik.

Det är vanligt att man har flera olika tekniska lösningar i de analyserade länderna, ofta har man kvar sektor/domänspecifika lösningar eller regionspecifika lösningar trots att man infört en gemensam digital infrastruktur för informationsförsörjning. Oftast består den gemensamma digitala infrastrukturen av standarder, regelverk och gemensamma centrala återanvändningsbara komponenter snarare än en gemensam teknisk plattform eller lösning för alla behov.

Länder som exempelvis Finland, Belgien och Singapore har kvar region, sektor och/eller domänsspecifika lösningar som sedan knyts samman genom nationella standarder eller förvaltningsgemensamma lösningar och komponenter. Danmark har avgränsat sin gemensamma lösning för informationsutbyte till att bara tillgängliggöra grunddata.

Primära syftet med en förvaltningsgemensam lösning i länderna är således sektors/domänöverskridande utbyte samt att tillgängliggöra viktiga datakällor på ett standardiserat sätt. De flesta ländernas lösning tar höjd för integration och utbyte även med den privata sektorn och medborgare.

Exempel Belgien – regionala lösningar som samverkar

Belgien har inte en och samma lösning för informationsförsörjning och överföring i landet utan snarare ett nätverk bestående av flera olika ”service integrators” inom olika sektorer som man arbetar med att koppla ihop med varandra.

Det finns två regionala service integratorer, en för Flandern och en för Vallonien, det finns en federal service integrator och så finns det en för välfärdssektorn och en för e-hälsosektorn. Dessa integratorer knyter samman och möjliggör tillgång till olika datakällor inom nätverket. Alla integratorer använder samma typer av standarder och regelverk för att säkerställa interoperabilitet sinesemellan.

#### 1.4.1.1 API-hantering

Flera länder lyfter upp framväxten och att det håller på sker en övergång från traditionella lösningar till API-lösningar baserade på REST/JSON. Singapore använder en helt API-baserad lösning som grund för sitt informationsutbyte. Finland har en API-katalog som

komplement till sitt informationsled och kommande versioner av X-road[80] kommer ha stöd för REST vilket kommer möjliggöra att producera och konsumera REST-API över X-road. Även Nederländerna lyfter upp framväxten av API-baserade lösningar som en utmaning och stor möjlighet framöver. Utvecklingen belyses också i ett citat[81] av Estlands Government CIO Sim Sikkut på följande vis:

*"...we have to change how we procure and architect things. For example, we have to be much more micro-service and API-based as opposed to [deploying] monolith systems."*

API:er och API Gateways är inte längre ny teknik eller särskilt innovativa lösningar, utan snarare praxis inom den privata sektorn. Innovationen och nyttan kommer från att göra dessa teknologier mer tillgängliga och öka deras användning inom offentlig sektor.

Gartner lyfter i en rapport[82] på ämnet upp begreppet "Full Life Cycle API Management" med följande definition:

" *Full life cycle API management involves the planning, design, implementation, testing, publication, operation, consumption, versioning and retirement of APIs. It includes a developer's portal to target, market to and govern an ecosystem of developers to use APIs, as well as API gateways for runtime management, security and gathering of usage data."*

Rapporten beskriver hur en teknologi går igenom olika faser och hur teknologier förväntas mogna och leverera värde inom offentlig sektor.

De slutsatser som kan dras utifrån rapporten är att "Full lifecycle API management" är en teknologi som är på väg att mogna och som har stor potential att leverera värde inom den offentliga förvaltningen.

I en annan rapport[83] från Gartner belyses utmaningar, rekommendationer och offentliga förvaltningars införande av den offentliga förvaltningens införande av API:er.

Gartner pekar i rapporten ut följande nyckelutmaningar:

- *The versatility of APIs can be a disadvantage, causing confusion when trying to communicate API strategies to government executives. The potential of APIs, along with the challenges associated with using them, is not well-understood.*
- *APIs are key to empowering ecosystem partners and promoting service innovation. But ad hoc API initiatives without focus can result in a scattered array of APIs that are not linked to government or community outcomes.*
- *Maintaining funding or support for an API program can be difficult if the value the program produces cannot be translated to business outcomes and measured.*

Gartner pekar även ut följande rekommendationer:

[80] X-road rest support: https://www.niis.org/blog/2019/3/25/two-steps-from-the-x-road-rest-support - läst 2019-06-27
[81] Intervju i IDG: https://www.idgconnect.com/idgconnect/news/1023053/creating-digital-society-learn-estonia - läst 2019-06-27
[82] Gartner – Hype Cycle for Digital Government Technology, 2018
[83] Gartner – Government APIs Are About Delivering Outcomes, Not Technology

- *Instill a business outcome focus into your API program by using key business leaders as API product managers. Add API product manager responsibilities to the current roles of key business-focused champions that are passionate about alternate service delivery channels and business models.*
- *Focus on API programs that represent value to internal and external stakeholders by co-creating a multifaceted strategy that supports the development, delivery and curation of API products.*
- *Deliver APIs that have clear, measurable benefits, or that are considered strategic investments, by establishing critical evaluation criteria for potential API products as part of your API framework. These criteria should categorize and prioritize API development, but should not be so restrictive that they stifle transparency or innovation.*

Rapporten rekommenderar en resultatfokuserad strategi för att identifiera den bästa metoden för API-program inom den offentliga förvaltningen.

Rapporten beskriver även en status för hur API:er används inom den offentliga förvaltningen.

- *Many government organizations are largely ignoring APIs, not positioning them within their business or technology strategies.*
    - *in these organizations, APIs are integration tools and only used for point-to-point solutions to unlock data in legacy systems or on an ad hoc basis.*
- *Others are tacking them onto open data programs by wrapping static government datasets as APIs.*
- *Other government organizations and central information and communication technology (ICT) bodies have established API standards, guidelines, reference architectures and supporting governance models*
- *More API-centric government ICT departments are working to establish an "API first" culture, creating APIs for all government services, building internal and external development communities, and implementing full life cycle management*

#### 1.4.1.2 Interoperabilitet och kompatibilitet

Interoperabilitet mellan de olika analyserade lösningarna förekommer endast i ett fåtal fall. Med interoperabilitet menas här system som har förmåga att fungera tillsammans och kunna kommunicera med varandra. Exempelvis kan detta ske genom att lösningarna använder samma typ av tekniska protokoll.

*SHS 2.0 är interoperabelt med Tjänsteplattformen.*[84]

Inera har tagit fram ett regelverk för interoperabilitet som har använts inom svensk e-hälsa sedan 2009. Regelverket omfattar styrande principer och detaljerade anvisningar för hur system och tekniska lösningar ska utformas för att skapa förutsättningar för samverkan mellan regioner och kommuner. Det omfattar även mallar för hur system som utvecklas enligt den tekniska referensarkitekturen ska dokumenteras och granskas.

[84] Inera om interoperabilitet: https://www.inera.se/digitalisering/interoperabilitet/teknisk-interoperabilitet/ - läst 2019-06-27

Regelverket bygger på ett antal standarder, specifikationer och rekommendationer från erkända standardiseringsorgan.

Samma uppsättning standarder och regelverk för teknisk interoperabilitet finns i myndigheternas specifikationer som kallas Spridnings- och Hämtningssystem (SHS 2.0). Det betyder att kommuner, regioner och myndigheter kan kommunicera tekniskt med varandra om systemen hos båda parter följer dessa regelverk.

*X-tee är interoperabelt med soumi.fi informationsled.*

Befolkningsregistercentralen i Finland och den estniska datasystemmyndigheten Riigi Infosüsteemi Amet (RIA) avtalade i september 2016 om federering mellan sina informationsleder, dvs. om att införa förtroende mellan Finlands och Estlands informationsleder. Avtalet möjliggör teknisk förmedling av information från en tjänst som kopplats till Suomi.fi-informationsleden till den estniska informationsleden och vice versa.

Enligt avtalet ska organisationer som utbyter information ingå inbördes avtal om detta. När informationslederna har samordnats i produktionsmiljön blir det bland annat möjligt att utbyta befolkningsregisterdata mellan länderna.

*Internationella lösningars kompatibilitet till befintliga Svenska*

Även om det finns i många avseenden tekniska likheter mellan nationella lösningar och de analyserade när det kommer till val av programmeringsspråk, lösningsmönster och komponenter är de inte direkt kompatibla med varandra. Det skulle kräva ett omfattande arbete med att bygga om anslutningar och finnas behov av tjänsteväxlar och bryggor för att möjliggöra interoperabilitet.

### 1.4.2 Styrning, organisation och finansiering

#### 1.4.2.1 Styrning och organisation

Flera länder har kommit mycket längre än Sverige gällande hanteringen av grunddata och informationsutbyte. Det finns i regel formulerade nationella strategier och en utpekad aktör eller organisatorisk modell för hantering och förvaltning av gemensam infrastruktur. Oftast är den utpekade aktören en central myndighet eller avdelning inom ett departement med ansvar för digitalisering. Dessa aktörer har i flera av fallen betydande kapacitet, kompetens och mandat inom området.

I både Norge och Finland har man från politiskt håll gått ut med övergripande strategier inom digitalisering som är exempel på tydlig målstyrning. ”Lösningar för Finland”[85] och Norges ”En digital offentlig sektor” [86] beskriver en önskad målbild för 2025 där förvaltningsgemensamma lösningar och infrastruktur spelar en viktig roll.

[85] Lösningar för Finland – Strategiskt program för statsminster Juha Sipiläs regering 2015-05-29
[86] En digital offentlig sektor – Digitaliseringsstrategi for offentlig sector 2019-2025, 2019-06-11

När det kommer till metoder för styrning skiljer det sig åt mellan länderna, flera har valt styrning genom lagstiftning, medan andra använder sig av politiska direktiv och avtalslösningar inom och mellan olika sektorer. I avsaknad av lagstiftning behövs starka alternativa incitament som i praktiken leder till obligatorisk användning av gemensamt framtagen infrastruktur. Erfarenheter från Finland visar särskilt på vikten av att politiken är tydlig och pekar ut vägen och att ett nära samarbete sker mellan genomförande aktörer.

Även vikten av samverkan lyfts upp som en framgångsfaktor ibland annat Finland och Belgien, där gemensam utveckling av flera tekniska lösningar ger snabbare nyttohemtagningar samt säkerställer interoperabilitet mellan lösningarna.

När det kommer till koordineringsfrågor finns det även exempel på andra typer av samverkansmodeller i form av gemensamma råd, kommittéer eller nätverk som bedömts som framgångsrika i flera länder exempelvis SKATE (Styrning og koordinering av tenester i e-förvaltning) i Norge och Coordination commitee of service integrators i Belgien.

När det kommer till styrning på Europeiskt nivå så är målsättningen för EU att etablera Digital Single Market (DSM) vilket innebär i praktiken att styrningen mot digitalisering utgår från behovet av ordning och reda på grunddata och gränsöverskridande utbyte mellan myndigheter och mellan medlemsländer.

### Exempel Finland – styrande lagstiftning

Finland har när det gäller digitalisering av samhället haft ett stort fokus på centralisering, både vad gäller offentlig sektors organisering men även i form av lagstiftning. Finland har aktivt arbetat med ramlagstiftningar för samhällets digitalisering. Ett exempel på detta är lagen (24.1.2003/13) om elektronisk kommunikation i myndigheters verksamhet som beslutades redan 2003 och sedan dess kontinuerligt uppdaterats. Lagen är brett tillämpbar på myndigheter och definierar sådant som elektroniska dokument, att beslutshandlingar får signeras (undertecknas) elektroniskt[87] och att elektroniska dokument som huvudregel uppfyller krav på skriftlig form. Lagen ålägger också myndigheter flera skyldigheter. De är bl.a., om de har kapaciteten, skyldiga att upprätta system för att motta, sända och behandla elektroniska dokument.

För styrningen av informationsförvaltningen[88] inom offentlig förvaltning finns en särskild lag[89] som tydliggör att Finansministeriet ska ta hand om den allmänna styrningen av informationsförvaltningen inom den offentliga förvaltningens myndigheter. Detta innebär bl.a. planering av den övergripande IT-arkitekturen. I lagen finns också bestämmelser om att myndigheter ska sträva efter att ordna sin verksamhet så att de använder vissa utpekade

[87] I Enligt med Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

[88] Definieras i 3 § Lag om styrning av informationsförvaltningen inom den offentliga förvaltningen (10.6.2011/634) enligt följande: *informationsförvaltningen inom den offentliga förvaltningen en stödfunktion som tryggar skötseln av offentliga förvaltningsuppgifter med hjälp av informations- och kommunikationstekniska metoder och förfaranden.*

[89] Lag om styrning av informationsförvaltningen inom den offentliga förvaltningen (10.6.2011/634).

registeruppgifter[90] för sina verksamhetsbehov. Dessa uppgifter är sådana som skulle kunna kallas grunddata, såsom uppgifter ur befolkningsdatasystemet och föreningsregister. Någon författningsreglerad definition av grunddata finns dock inte i Finland.[91]

Ovanstående har enligt de finska representanter som utredningen talat med underlättat för implementation och användande av den finländska plattformen för elektroniskt informationsutbyte då det sedan tidigare funnits en vana av att använda sig av samma tjänster och det finns en tydlighet i styrningen.[92]

### Exempel Danmark – statlig styrning

Det finns exempel på detaljerade krav i lagstiftningen avseende standarder och liknande, exempelvis avseende elektroniska fakturor till staten[93], men dessa är begränsade till antalet. I november 2017 publicerades ett strategidokument som redogör för hur it ska användas i staten[94]. I dokumentet lyfter man bland annat fram behovet av sammanhängande it i staten, ökad datadelning, tätare samarbete om grundläggande it-drift, gemensamma lösningar och utveckling. Det framgår att offentliga aktörer ska säkra det egna området ur it-hänseende, men också se till att man kan ingå i processer andra myndigheter samt dela data med dem.[95] Vidare framgår att man vill se fler gemensamma lösningar och samlad it-drift, samt fler standardiserade processer.[96] Ambitionen är alltså tydlig, däremot framgår inte om detta är tänkt att uppnås via lagstiftning eller på annat sätt. Eftersom att det i dagsläget finns begränsat med lagstiftning om myndigheternas it och informationsutbyte är det troligt att anta att detta är tänkt på att uppnås på andra sätt än genom lagstiftning.

När det gäller Danmarks lösning för informationsutbyte, Datafordeler så har man en styrning uppdelad i en övergripande samordnings och utvecklingsorganisation som bland annat ansvarar för kontakt och relationer med andra områden där det finns beroenden för grunddata. Den andra delen består av en genomförandeorganisation som har det operativa ansvaret för drift, förvaltning och förändringar).

#### 1.4.2.2 Finansiering

Flera av de analyserade länderna har genomfört storskaliga satsningar för att skapa en gemensam infrastruktur flertalet länder har valt att bedriva dessa satsningar inom ramen för nationella program. Det finns även exempel på motsatsen där man börjat i mindre begränsad skala (exempelvis bara kopplat till grunddata) och där den gemensamma infrastrukturen fått växa fram i takt med den tekniska utvecklingen och den offentliga sektors krav och behov.

Många länder lyfter upp vikten av central finansiering och att de tekniska lösningarna i alla fall initialt bör tillhandahållas avgiftsfritt för att underlätta och motivera

[90] Se 10 § samma lag.
[91] Se dock s. 45 RP 59/2016 rd där en beskrivning av basregister och basregisteruppgifter finns.
[92] Se även s. 11 Programmet för genomförande av en nationell servicearkitektur (KaPA) 2014–2017 Slutrapport, Finansministeriet, Helsingfors 2018.
[93] Bekendtgørelse om information i og transport af OIOUBL elektronisk regning til brug for elektronisk afregning med offentlige myndigheder.
[94] IT-styrning i Danmark: https://digst.dk/strategier/strategi-for-it-styring-i-staten/ - läst 2019-06-27
[95] Et solidt it-fundament – Strategi för it-styrning i staten 2017-11-21, s. 19
[96] Aas s. 20.

implementation och för att nå upp till en kritisk massa av användning. En central finansieringsmodell av implementering, drift och förvaltning bedöms vara en viktig framgångsfaktor.

Det finns även exempel från de analyserade länderna där man använder sig av avgiftsfinansiering. Generellt kan man säga att finansieringsmodellerna varierar och att man oftast saknar en generell mall eller principer för hur finansieringen av den digitala infrastrukturen ska gå till.

### Exempel Danmark – finansiering av grunddataprogrammet

I Danmark finansierade man grunddataprogrammet genom generella anslagsminskningar hos aktörer i den offentliga sektorn, men att man i gengäld lät organisationer som anslöt sig behålla nyttoeffekter i form av besparingar utan att det påverkar deras kommande anslag. Denna lösning kan fungera som ett ytterligare incitament för att implementera och ansluta sig.

Danmark saknar generella principer för hur den digitala infrastrukturen ska finansieras och man har idag flera olika typer av finansieringsmodeller beroende på sammanhang. Primärt använder man sig av antingen avgiftsfinansiering där varje nyttjande aktör betalar en avgift vid de tillfällen då tjänsterna utnyttjas eller anslagsfinansiering för förvaltning av tjänster eller tillgängliggörande av data.[97]

### Exempel Singapore – centrala finansieringsmodeller

Singapore lyfte att man initialt bör ha en central finansieringsmodell baserad på anslag för att uppnå en kritisk massa av användning. Därefter kan man se över och övergå till andra typer av finansiering, exempelvis avgifter. Det är lätt att investeringskostnaden annars blir ett hinder mot att skapa nya och effektiva lösningar.

### Exempel Norge – principer för finansiering av förvaltningsgemensamma digitala funktioner

Den Norska regeringen har tagit fram ett antal principer för finansiering[98]:

**1.** Finansieringsmodellerna ska vara enkla och förutsägbara, och innebära så lite administration som möjligt.

**2.** Fasta kostnader för utveckling och förvaltning ska täckas genom anslagsfinansiering till den förvaltande myndigheten.

**3.** Den förvaltande myndigheten ska vara transparent med sina kostnader så att det framgår vad som används till förvaltning och vad som används till utveckling.

**4.** Den förvaltande myndigheten ska inte ta ut avgifter för att ge tillgång till grunddata från register som ingår i den digitala infrastrukturen.

[97] Modeller för fördelning av nyttor och kostnader för digital infrastruktur – Statskontoret Dnr 2018/40-5
[98] Ibid – källa från Regjeringen (Norge), Hva er felleskomponenter?

**5.** För de förvaltningsgemensamma digitala funktioner som inte är register ska den förvaltande myndigheten ta betalt av de nyttjande myndigheterna för sina omkostnader, det vill säga för rörliga kostnader som uppstår när funktionen används. De nyttjande myndigheterna betalar en proportionell andel av den förvaltande myndighetens omkostnader.

**6.** Betalning mellan myndigheter ska som huvudregel ske genom avgift.

**7.** En eller flera nyttjande myndigheter kan tillsammans beställa en anpassad funktionalitet från den förvaltande myndigheten, men måste då finansiera utvecklingen av funktionen. Detta kan ske under förutsättning att utvecklingen är kompatibel med den förvaltande myndighetens kapacitet och övriga åtaganden.

### 1.4.3 Kostnader, nyttor och ekonomiska effekter

#### 1.4.3.1 Kostnader

Kostnaderna för implementationen i de olika länderna varierar något och har varit svår att urskilja, ofta är investeringarna kopplade till ett nationellt program som har en större ansats än bara grunddata och informationsutbyte, oftast med fokus på hela den digitala infrastrukturen inom landet. Kostnaderna för den tekniska lösningen är oftast försumbar i sammanhanget och merparten av kostnaderna i exempelvis Finland istället allokerade till implementation (i form av bidrag), anpassning och utveckling av centrala komponenter.

Det går inte att bortse från att satsningarna i flertalet fall varit kostnadsintensiva initialt, framförallt p.g.a. höga implementerings och anpassningskostnader. Kostnaderna kan dock ställas i relation till andra infrastrukturella satsningar (som exempelvis vägar) och förfaller då snarare som väldigt billiga, det är således en fråga om perspektiv.

#### Exempel Danmark – kostnader för grunddataprogrammet

Danmarks totalkostnad för deras Grunddataprogram beräknas uppgå till omkring 673 miljoner DKK[99]. Programmet har blivit försenat och utvidgats vilket innebär att man inte hållit den ursprungliga tidsplanen. Trots förseningarna finns det fortfarande ett stort stöd för programmet, och det är viktigt att betona att man nått ett stort antal milstolpar och mål.[100]

#### Exempel Finland – kostnader för KaPa-programmet

Vid inledningen av Finlands KaPa-program hade man 120 miljoner EUR i anslag[101]. Den totala slutgiltiga kostnaden i Finland landade på ca 70 miljoner EUR, kvarstående medel har sedan dess använts för vidareutveckling av Suomi.fi-tjänsterna och främjande av användning. Programmet har ansetts vara en framgång och man blev färdig i tid och under planerad budget, detta attribuerar

[99] Ändrad finansering: https://en.digst.dk/news/news-archive/2018/march/new-timetable-for-the-basic-data-programme-approved-by-the-finance-committee-of-the-danish-parliament/ - läst 2019-06-27

[100] Ändrad tidsplan: https://digst.dk/nyheder/nyhedsarkiv/2017/november/grunddataregistre-paa-ejendomsomraadet-udskydes-til-2019/ - läst 2019-06-27

[101] Programmet för genomförande av en nationell servicearkitektur (KaPA) 2014-2017 Slutrapport

man till en agil utvecklingsmodell kombinerat med motiverad och kompetent bemanning inom både styrning och genomförande.[102]

### Exempel Norge – kostnader för Altinn 2

Norges satsning på Altinn 2 uppskattas totalt till 939 miljoner NOK.[103] I satsningen ingår flertalet olika tjänster och komponenter som inte är direkt hänförliga till informationsutbyte.

#### 1.4.3.2 Samhällsekonomiska effekter och nyttor

Den främsta drivkraften för reformer och initiativ i de analyserade länderna har ursprungligen oftast handlat om ekonomiska incitament i form av en vilja att effektivisera och minska kostnader för den offentliga sektorn. Detta ger sig i uttryck bland annat genom att initiativen och projekten ofta initierats och i vissa fall drivs av respektive lands finansdepartement eller avdelningar och myndigheter med kopplingar dit.

Beräkningar från flera av de analyserade länderna visar på att det finns stora positiva samhällsekonomiska effekter framförallt kopplat till ett tillgängliggörande och avgiftsfritt användande av grunddata och ett effektivt informationsutbyte. Nyttorna realiseras främst i form av besparingar när det kommer till minskning av administrativ börda, minskade IT-kostnader, tidsvinster och indirekta effekter såsom högre kvalité samt säkrad tillgång.

Beräkningarna indikerar också att den största delen av den samhällsekonomiska effekten (samhällsnyttan) uppkommer i den privata sektorn.

Samhällsnytta definieras som summan av verksamhetsnytta och extern nytta[104]


### Exempel Norge – kostnads och nyttoberäkningar

I Norge har man gjort flertalet kostnads och nyttoberäkningar hänförligt till nationell digital infrastruktur. 2015 gjordes en beräkning[105] av samhällsekonomisk effekter (kostnads- och nyttoanalyser) kopplat till olika alternativ för förvaltningsgemensamma koncept för informationsförvaltning av DNV Global på uppdrag av Bronnoysundregistrene. Analysen utgick från tre olika scenarion, ett nollalternativ där man utgick ifrån dagens situation och beslut som redan är tagna. Alternativ 1 där man föreslår förvaltningsgemensamma standarder och beskrivningar för informationsförvaltningen. Alternativ 2 där man föreslår förvaltningsgemensamma standarder och beskrivningar samt gemensamma tjänster och teknisk infrastruktur för informationsförvaltning.

[102] Kapa-programmets utfall lägre än budget: https://vm.fi/en/article/-/asset_publisher/kapa-ohjelman-palvelut-ovat-valmistuneet-aikataulussa-ja-alle-budjetin - läst 2019-06-27
[103] Revidert nyttekostnadsanalyse Norge 2010 E.Fossum & E.Pedersen
[104] Figur från Modeller för fördelning av nyttor och kostnader för digital infrastruktur Dnr 2018/40-5
[105] Gevinstpotensialet I et felles konsept for informasjonsforvaltning i offentlig sektor. DNV GL 2015-02-27

Jämfört med nollalternativet bidrar de olika alternativen till en samordning av informationsförvaltningen tvärs över offentlig sektor. Alternativ två är en utökning av det första alternativet där man utöver att sätta en förvaltningsgemensam standard också tillgängliggör och använder informationen i gemensamma web-portaler och tjänster. Alternativ 2 bidrar till att visa vem i offentlig sektor som har vilken data samt inbegriper katalogtjänst som beskriver begrepp och informationsmodeller.

Över en analysperiod på 15 år beräknar man utifrån effektiviseringsvinster och besparingar att potentialen för alternativ 1 uppgår till ca 13 miljarder NOK och att motsvarande potential för alternativ 2 uppgår till 30 miljarder NOK. Beräkningarna utgår ifrån effektiviseringar från reducerad arbetstid samt reducerad/effektivare användning av resurser till följd av en förvaltningsgemensam informationsförvaltning.

Man påtalar i rapporten att det är viktigt att inte bara se till kostnadsbesparingar när det kommer till satsningar på förvaltningsgemensamma lösningar för informationsförvaltning utan att det också finns vinster med exempelvis minskad rapporteringsbörda för företag och möjlighet till att skapa nya tjänster. Man tar också upp vissa farhågor som kan hindra att nyttorna kan räknas hem, bland annat lyfter man upp koordineringsproblem inom offentlig sektor samt att resultatet är avhängt att de största aktörerna tar alternativen i bruk och att användningen av lösningarna främjas.

### Exempel Danmark – nyttoberäkningar

2010 genomförde Erhverstyrelsen (tidigare Danish Enterprise and Construction Authority) en studie kring värdet av det danska adressregistret som 2002 blev gratis att använda. Deras beräkningar visar på finansiella nyttor hänförligt till tillgängliggörandet på 471 miljoner danska kronor för perioden 2005-2009. Kostnaderna beräknades motsvara omkring 2 miljoner euro under samma period. För 2010 beräknade man att effekterna skulle motsvara besparingar på 14 miljoner euro varav 30 % var hänförligt till offentlig sektor och resterande 70 % hänförligt till nyttor i den privata sektorn.[106]

Beräkningarna utgick från en metod där man beräknande det ekonomiska värdet av att tillgängliggöra adresser gratis för alla utifrån vad man betalade för motsvarande uppgifter innan. Utöver dessa har man även listat ett antal andra nyttor och ekonomiska effekter som man inte beräknat i monetära termer. Detta är nyttor som realiseras längre ner i värdekedjan och består av en rad indirekta effekter såsom minskad användning av egna databaser, högre tillit till att akuttjänster får tillgång till samma och korrekt data, enklare process vid rättning av felaktigheter då man bara behöver ändra hos en källa, minskade kostnader för att uppdatera databaser och ökad kvalité på data i ett gemensamt standardiserat format.

2012 gjorde man beräkningar att från 2020, med grunddata-strategin helt implementerad skulle de ekonomiska effekterna för samhället skulle uppgå till 800 miljoner danska kronor årligen varav 500 miljoner för den privata sektorn.[107]

[106] Danish Enterprise and Construction Authority, The value of Danish address data 2010.
[107] Good basic data for everyone – a driver for growth and efficiency

## Exempel Estland – ekonomiska effekter

De största ekonomiska effekterna av X-tee beskrivs vara besparing av tid och pengar för medborgare, offentlig sektor och företag. Som exempel tar det endast omkring 18 minuter att starta ett företag i Estland[108], 98 % av alla företag startas online, 95 % av alla skattedeklarationer lämnas in online samt tar i snitt omkring 3 minuter att fylla i[109]. Det har gjorts beräkningar på effekterna av Estlands digitala signaturer som visar på att tidsbesparingen per person uppgår till 5 dagar per år[110].

Det finns inte officiella nyttokalkyler eller beräkningar på samhällsekonomisk nytta gjorda av den Estniska staten att tillgå gällande effekterna av X-road. 2016 gjorde Världsbanken en rapport[111] ”Digital Dividends” och i bakgrundsmaterialet till denna finns en studie[112] där man försökt kvantifiera delar av de ekonomiska effekterna av X-road.

I denna studie har man beräknat tidsbesparing kopplat till medborgare och offentlig sektor interaktioner. Interaktioner som vanligen skulle ha gjorts fysiskt men som möjliggjorts digitalt genom X-tee. Konservativt räknat har man uppskattat tidsvinningen till 15 minuter per interaktion och utifrån den tesen uppskattat den totala besparingen fram till 2014 till 2,8 miljoner timmar. För att beskriva det på ett annat sätt kan man beskriva att produktiviteten för X-tee plattformen motsvarar 3,225 personer som jobbar 24/7 i ett helt år. Dessa beräkningar är av karaktären svåra att bedöma tillförlitligheten i eftersom det rör sig om uppskattningar. Den ekonomiska nyttan är inte direkt hänförlig till plattformen utan snarare till och beroende av tjänsterna som möjliggörs.

Estland gör liknande beräkningar löpande och uppskattar att 5 % av förfrågningarna som görs via X-tee är initierade av en fysisk person. Och om man antar att endast dessa förfrågningar besparar 15 minuter kontra om det hade gjorts per brev så besparades det under bara under 2017 in 1,264 arbetsår i tidsvinster[113].

## Exempel Belgien – administrativa besparingar

Belgien har en myndighet (Dienst Administratieve Vereenvoudiging, DAV) som ansvarar för att mäta administrativ förenkling och följa upp användningen av e-tjänster. DAV följer upp e-government initiativ genom att mäta ekonomiskt utfall i form av minskning av administrativ börda för ett antal e-tjänster. Man mäter minskning i administrativ börda ur medborgarnas, företag och myndigheters perspektiv. Administrativ börda kan exempelvis bestå av tidsvinster eller minskade avgifter och transfereringar.

För 2017[114] beräknar DAV att de 16 e-tjänster (Tax-on-web, MyEnterprise, eBirth m.fl.) som man följer ha sparat in 7 017 477 euro. Den största delen av den minskade administrativa bördan anses hänförlig till vinster hos medborgarna i landet (59 %).

[108] Eestonia: https://estonia.ee/enter/ - läst 2019-06-27
[109] Eestona e-tax: https://e-estonia.com/solutions/business-and-finance/e-tax - läst 2019-06-27
[110] Eestonia e-identity: https://e-estonia.com/solutions/e-identity/ - läst 2019-06-27
[111] World Development Report 2016: Digital Dividends
[112] Estonian e-Governance Ecosystem: Foundation, Applications, Outcomes 2016 – Kristjan Vassil University of Tartu
[113] X-tee factsheet: https://www.x-tee.ee/factsheets/EE/#eng – läst 2019-06-27
[114] 2017 Les Autorites, Catalyseurs de La Simplification, Evaluation des charges administratives federales.

Ackumulerat för dessa tjänster sedan de driftsattes har inbesparingen beräknats till 100 847 174 euro i minskad administrativ börda. Tjänsterna har varit i drift i olika antal år, startpunkt för mätningarna var 2008.

Den ekonomiska effekten beräknas således inte direkt hänförlig till deras lösning för informationsutbyte (FSB) utan snarare hänförligt till de tjänster som möjliggörs genom tillgång till data från olika autentiska källor.

### 1.4.4 Rättsliga förutsättningar

#### 1.4.4.1 Rättsliga ramverk för grunddata

I de flesta länder saknas ett övergripande rättsligt ramverk för hantering av grunddata och man har istället registerlagstiftning hänförligt till de olika datakällorna. Vissa länder har valt att peka ut ett antal källor som grunddata i lagstiftning medan andra har löst det genom avtal och överenskommelser kring användningen stöttat av tydlig politisk styrning.

När det kommer till att definiera grunddata så skiljer sig länderna åt, flera länder har inte lagstiftat om eller definierat grunddata medan det i andra finns specifik lagstiftning. I många länder används dock begreppet eller varianter därav även om det inte återfinns i lagstiftning. Ofta används det då i en vidare mening och syftar till att peka ut autentiska eller unika källor av data som är av stor vikt för samhället.

#### Exempel Danmark – avtal istället för lagstiftning

Sedan ett antal år tillbaka pågår Grunddataprogrammet, som syftar till att lyfta kvaliteten på grunddata, göra den sammanhängande och tillgänglig både för myndigheter, privata verksamheter och borgare. Programmet rör vissa kategorier data (exempelvis persondata(CPR), verksamhetsdata och geo data), som finns i diverse register. Programmet är ett politiskt initiativ och grundar sig på ett avtal[115] mellan regeringen, Kommunernes Landsforening och Danske Regioner. I avtalet beskrivs syftet, olika kategorier data som omfattas och organisationen för styrning. Avtalet innehåller också en punkt om att det ska etableras en gemensamoffentlig intrastrukturkomponent (Datafordeler) för gemensam distribution av grunddata. Av ett av tillhörande delavtal[116] framgår att all grunddata distribueras via datafördelaren.

Begreppet grunddata används inte i dansk lagstiftning och är således inte definierat där. Däremot används begreppet alltså i ovan nämnda avtal. De register som sitter på den data det är fråga om är däremot reglerade i lag, exempelvis CPR[117] och CVR[118].

#### Exempel Belgien – auktorativa data

I Belgien har man i lagstiftning pekat ut auktoritativa data och auktoritativa källor för grunddata.[119] Det auktoritativa data som finns hos den auktoritativa källan är per definition unik

[115] Aftale om gode grunddata til alle: https://digst.dk/media/12881/grunddata-aftaletekst.pdf
[116] Delaftale 7: Fælles distributionsløsning til grunddata (datafordeler) 2012-05-10
[117] Lov om Det Centrale Personregister (LBK nr 646 af 02/06/2017)
[118] Lov om Det Centrale Virksomhedsregister (LBK nr 653 af 15/06/2006)
[119] Law establishing and organising a federal services integrator, 15 August 2012, Art. 2

och det är den data som organisationer ska hämta[120] när de behöver använda data om t.ex. en person, organisation får inte fråga personen om data som redan finns.

### Exempel Norge - grunddata

Begreppet grunddata (grunndata) finns inte i norska lagar eller föreskrifter. Däremot används begreppet flitigt av exempelvis myndigheter när de refererar till vissa kategorier data. Begreppet förekommer även i lagkommentarer. Det förefaller emellertid som om det inte finns en entydig definition. Den typ av data som kallas grunddata är sådan data som finns i olika offentliga register, exempelvis Enhetsregisteret som innehåller information om juridiska personer, såsom bolagsnamn, adress osv. Ett annat exempel är Det sentrale folkeregisteret, som motsvarar det svenska folkbokföringsregistret. I lagstiftningen som reglerar dessa register finns också bestämmelser om att uppgifter från dem kan lämnas ut.

#### 1.4.4.2 En uppgift, en gång

Det är flera av de analyserade länderna som har implementerat lagstiftning som applicerar och i vissa fall direkt refererar till ”Once-Only” principerna. [121]

### Exempel Norge – en uppgift en gång

Det är i Norge krav på statliga offentliga verksamheter att utgå från digitalt som första val och att uppgifter bara ska behöva hämtas en gång. Data kan hämtas från en annan verksamhet om det finns rättslig grund för det (jfr § 7 offentliglova[122]). När statliga offentliga verksamheter tar fram nya tjänster, eller uppdaterar existerande tjänster, ska de se till att maskinläsbar data från tjänsterna kan delas och användas av andra.

### Exempel Estland – once-only principer i lagstiftning

I Estnisk lagstiftning finns hänvisningar och referens till Once-only principerna I artikel 43 i Public information act[123] som innebär att etableringen av separata databaser för insamlingen av samma data är förbjuden. Effekten av skrivelsen blir att uppmuntra offentliga aktörer att använda sig av data som redan finns inhämtad istället för att skapa kopior och dubbletter.

### Exempel Nederländerna – tvingande användning av basregister

Nederländerna har formulerat krav för användning kopplat till deras basregister (grunddata) som inkluderar tvång att använda denna data för olika typer av offentliga tjänster. Nederländerna har separat lagstiftning för 12 av sina basregister.

#### *1.4.4.3 Rättsliga ramverk för informationsutbyte*

De flesta av de analyserade länderna saknar ett övergripande eller generella rättsligt ramverk för informationsutbyte. Däremot finns det flera exempel på lagstiftning som reglerar förvaltningsgemensamma tjänster som ligger till grund för digitalisering.

[120] Only-Once Act, 5 May 2014, Art. 2.
[121] EU-wide digital Once-Only principle for citizens and businesses – policy options and their impact, EU 2014
[122] Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
[123] Estonian Public Information Act: https://www.riigiteataja.ee/en/eli/514112013001/consolide - läst 2019-06-27

## Exempel Finland – KaPa lagstiftning

Ett land som urskiljer sig från övriga är Finland som har lagen (30.12.2013/1226) om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (KaPa-lagen) där det regleras att de flesta statliga myndigheter i huvudsak är skyldiga att använda gemensamma informations- och kommunikationstjänster. Finansministeriet har enligt 4 § i lagen till uppgift att styra anordningen av tjänsterna, säkerställa deras kvalitet och interoperabilitet med den övergripande IT-arkitekturen. En aktör som på grund av särskilda behov nödvändigtvis måste använda andra tjänster måste få tillstånd till det. Det slutliga beslutsmandet ligger hos statsrådet[124].

För den specifika regleringen av det elektroniska informationsutbytet har den s.k. KaPa-lagen[125] tagits fram. Lagens syfte är att förbättra tillgången och kvaliteten på offentliga tjänster, att förbättra tjänsternas informationssäkerhet och interoperabilitet samt styrningen av tjänsterna och att främja effektiviteten och produktiviteten inom den offentliga förvaltningens verksamhet och tillämpas på offentlig förvaltning. I lagen pekas Finansministeriet ut som ansvarig för den allmänna styrningen av stödtjänsterna. Definitioner av stödtjänster klarläggs och lagen föreskriver också vilka stödtjänster, bl.a. ett servicedatalager och en servicevy, som ska finnas samt att vissa myndigheter är serviceproducenter för vissa stödtjänster. Lagstiftningen beslutar om visst ansvar på generell nivå, som behandling av personuppgifter i tjänsteproduktionen, men om vissa uppgifter och behörigheter föreskrivs det separat per myndighet.[126] Någon särskild teknisk lösning pekas inte ut i varken lag eller förordning och Finland använder flera plattformar varav X-road är en av dem.

I KaPa-lagen har den finska lagstiftaren föreskrivit om hur användandet av stödtjänsterna. Lagstiftningen ålägger de flesta organisationer inom offentlig förvaltning, även kommunala organisationer då de sköter lagstadgade uppgifter, att använda sig av stödtjänsterna. Övriga organisationer inom offentlig förvaltning har då de sköter lagstadgade uppgifter rätt att använda alla stödtjänster. Privata aktörer har rätt, en rätt som kan bero på om aktören t.ex. har ett avtal med en myndighet att sköta en offentlig uppgift, att använda vissa av stödtjänsterna.

## Exempel Estland – rättsliga regleringar för informationsutbyte

Även i Estland finns det rättsliga regleringar kring informationsutbyte. Detta regleras i lagen om offentlig information[127] som föreskriver villkoren, förfarandet och metoderna för tillgång till och återanvändning av offentlig information. I lagen finns bestämmelser gällande datautbyte mellan databaser som tillhör det statliga informationssystemet. Estland har också en förordning[128] gällande informationssystem för informationsutbyteslager som fastställer kraven för datautbyteslager, dess användning och hantering av informationssystem.

## Exempel Norge – föreskrifter om användning i offentlig sektor

I Norge finns det krav på att använda vissa gemensamma lösningar, exempelvis ID-porten som möjliggör digital inloggning och autentisering. Som utgångspunkt ska offentliga verksamheter använda Altinns infrastruktur och tjänsteplattform för produktion av relevanta tjänster. Vissa bestämmelser om användning av standarder finns i föreskriften om IT-standarder i offentlig förvaltning.[129] Det rör sig bland annat om obligatoriska standarder för textdokument på offentliga

[124] Statsrådet är i Finland statens regeringsorgan.
[125] Lagen (29.6.2016/571) om förvaltningens gemensamma stödtjänster för e-tjänster.
[126] S.4 proposition RP 59/2016 rd.
[127] Lagen (RT I 2000, 92, 597) om offentlig information.
[128] Information Systems Data Exchange Layer (27.09.2016, 4)
[129] Forskrift om IT-standarder i offentlig forvaltning 2013-03-15-285

webbsidor, multimediainnehåll på sådana sidor och teckenuppsättning vid informationsutbyte mellan offentliga verksamheter och med enskilda och näringslivet.

### Exempel Danmark – obligatorisk anslutning

I Danmark finns inte ett rättsliga övergripande eller generellt ramverk för informationsutbyte mellan myndigheter. Däremot finns det flera exempel på lagstiftning som reglerar vissa övergripande (tvär-sektoriella) tjänster som ligger till grund för digitalisering. Tjänsterna kan anses vara grundläggande infrastrukturkomponenter. Dessutom finns det ett flertal exempel på där det i lag har införts obligatorisk anslutning för medborgare eller obligatorisk användning av vissa tjänster.

Exempel på grundläggande komponenter som är reglerade i lag är Digital Post, en tjänst som möjliggör kommunikation mellan det offentliga (statliga myndigheter, kommuner etc.) och medborgare och företag.[130] Tjänsten kan jämföras med Mina meddelande i Sverige. Det är obligatoriskt för medborgare att ansluta sig till tjänsten[131] för att kunna ta emot post. Däremot är det enligt den aktuella lagen inte obligatoriskt för offentliga aktörer, såsom myndigheter att skicka ut posten digitalt

Ytterligare ett exempel på en grundläggande komponent som regleras i lag är NemID[132], som är den e-id- och underskriftslösning och som tillhandahålls av staten och är den officiella inloggningstjänsten för offentliga tjänster.[133] Tjänsten gör det möjligt för medborgare och medarbetare vid juridiska enheter att identifiera sig och skriva under digitalt, både i tjänster som erbjuds av det offentliga och av privata företag. I lagen om utställande av NemID reglas flera saker, bland annat användarnas rättsliga ställning. Mycket regleras dock i avtalet mellan Nets DanID, som tillhandahåller lösningen och användaren. Det framgår exempelvis av avtalet att information hämtas från det danska personregistret (CPR).[134] Det finns i vissa fall lagkrav på att använda medarbetarfunktionen i NemID, exempelvis när statistik ska inrapporteras till Danmarks Statistik.

Gemensamt för dessa tjänster är att tillhandahålls centralt och att offentliga aktörer (och privata aktörer) kan ansluta sig till dem och använda dem.

## 1.4.5 Säkerhets-, sekretess- och integritetsaspekter

### 1.4.5.1 Säkerhetsfunktioner och byggblock

När det kommer till säkerhetsaspekter för lösningar för informationsutbyte så finns det en rad olika krav och behov.

Offentlig förvaltning behöver säkerställa att infrastrukturen och byggblock är designade ur ett säkerhetsperspektiv. Tjänsterna får inte vara sårbara mot attacker som kan avbryta och störa drift samt orsaka förlust av konfidentialitet eller integritet av information.

[130] Lov om Offentlig Digital Post.
[131] 3 § Lov om Offentlig Digital Post.
[132] Lov om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder.
[133] E-id Danmark: https://en.digst.dk/digitisation/eid/ - läst 2019-06-27
[134] Regler för användning av NemId: https://digst.dk/it-loesninger/nemid/lovgivning/regler-for-brug-af-nemid/ - läst 2019-06-27

Säkerhetsgruppen har identifierat en rad olika viktiga komponenter/byggblock som är avgörande för ett säkert och effektivt informationsutbyte men det ska påtalas att det inte är en komplett analys utan detta arbete behöver bedrivas vidare i det fortsatta arbetet.

Två av de prioriterade byggblocken är identitet och autentisering vilket innebär att både producent och konsument behöver vara verifierade och identifierade. I de analyserade länderna är detta inte en del av den tekniska lösningen för informationsutbyte utan oftast en fristående central komponent som av flera anses vara en grundläggande förutsättning.

Merparten av de analyserade länderna har nationella lösningar för identifiering och signering som tillhandahålls av staten. Bland annat Norge (ID-porten), Singapore (Singpass), Estland (Digi-ID) och Danmark (NemID). Flertalet av de analyserade länderna har även e-legitimationer som är godkända för de högsta säkerhetsnivåerna. Många av de analyserade ländernas lösning för autentisering innefattar också juridiska personer och roller.

I princip samtliga lösningar i de analyserade länderna har funktionalitet för spårbarhet i form av loggning av meddelanden och signering av meddelanden. Omfattningen av loggningen varierar beroende på olika förutsättningar i de olika länderna. Vissa lösningar loggar hela meddelandet (inklusive payloaden) medan andra bara loggar metadata över transaktionen. Ofta beror detta på lokala rättsliga förutsättningar och krav snarare än tekniska begränsningar.

### Exempel X-road - säkerhetsaspekter

För X-road finns det en rad olika designval av arkitekturen som stärker säkerheten. X-road är decentraliserat, utbytet sker direkt mellan producent och konsumenter. Det finns inga mellanhänder och väl efter att en säker anslutning har etablerats är tillgängligheten upp till aktörerna och nätverket mellan dem.

X-road ändrar inte ägarskapet av data, dataägaren (producenten) kontrollerar vem som har åtkomst och tillgång till sina tjänster och data.

Alla meddelanden som skickas genom X-road loggas och kan användas som digital bevisning.

Säkerhetsservern som är en central komponent laddar ner och behåller en cache-kopia över global konfiguration och validitet över certifikat vilket innebär att lösningen kan fungera (under en tidsbegränsad period) även om de centrala komponenterna inte kan nås.

X-roads distribuerade arkitektur gör att plattformen är skalbar och kraftfull mot cyberrelaterade attacker. Man skapar ett tillitsnätverk där meddelanden alltid utbyts mellan två betrodda parter vars identitet verifieras genom certifikat. Även om dessa faktorer är starka fördelar innebär det också i vissa fall en svaghet då nya parter som vill koppla upp sig och certifieras behöver gå igenom registrering och verifikation innan de blir certifierade.[135]

[135] Säkerhetsserver X-road: https://www.niis.org/blog/2018/10/15/standalone-security-server - läst 2019-06-27

### Exempel Danmark - sekretessbedömningar

Alla sekretessbedömningar görs hos de enskilda myndigheterna, de görs alltså inte hos Datafördelaren. Sekretessbelagd information ska inte tillgängliggöras via Datafördelaren. Om sekretessbelagd information behöver tillhandahållas t.ex. till en annan myndighet digitalt, så vidarebefordrar Datafördelaren frågan till myndigheten som har informationen och låter dem lösa det på andra sätt än via Datafördelaren.

Datafördelaren har tre olika behörighetsnivåer för användare som konsumerar informationen, Öppen, Känd användare och Individuell identifiering. Öppen information är helt öppen, ingen information behövs om användaren. Data som går att få tillgång till som Öppen är t.ex. adress. Som känd användare behöver du identifiera dig. Syftet är att Datafördelaren och Grunddatamyndigheterna vill veta mer om användarna så att de kan göra förbättringar för att exempelvis göra datat mer användbart. Individuell identifiering behövs när det finns några som helst begränsningar i hur datat kan lämnas ut, exempelvis om informationen omfattas av sekretess. Då sker inte tillhandahållande via Datafördelaren, utan informationsutbytet hanteras då istället direkt mellan källan till datat och användaren.

### Exempel eDelivery – designval för säkerhet

Designvalen i eDelivery är också gjorda ur ett säkerhetsperspektiv och garanterar att data och dokument inte otillbörligen kan modiferas, att data är krypterat under transport samt att man vet att ursprung och destinationen av data och dokument är tillförlitliga.

#### 1.4.5.2 Dataskyddsförordningen

Dataskyddsförordningen (GDPR) började tillämpas den 25 maj 2018 och är den generella regleringen av personuppgiftsbehandling inom EU. En EU-förordning är bindande och tillämpas direkt i varje medlemsstat av enskilda, myndigheter och organisationer. Eftersom dataskyddsförordningen är en förordning, och inte ett direktiv, har medlemsstaterna begränsade möjligheter att ha nationella bestämmelser om dataskydd. Myndigheter är personuppgiftsansvariga för all behandling av personuppgifter som sker i myndighetens verksamhet. När en myndighet behandlar personuppgifter måste de följa dataskyddsförordningen och den kompletterande dataskyddslagen tillsammans med sina egna särskilda registerförfattningar.

Kraven i dataskyddsförordningen är sammankopplad med myndighets säkerhetsansvar på flera plan. Det är viktigt att information klassas för att klargöra vilket skyddsvärde den har oavsett om den påverkas av dataskyddsförordningen eller inte. Som en helhet måste inbyggd säkerhet (eller integritet) omhändertas vilket påverkar ett systems hela livscykel, från förstudie och kravställning via design (formgivning) och utveckling till användning samt avveckling. Det påverkar beställare och kravställare som är ansvariga för personuppgiftsbehandlingen likväl som leverantören av de produkter och tjänster som används. Begrepp som personuppgiftsansvar, ändamålsbegränsning, informationsägarskap, rättslig grund, de registrerades rättigheter, uppgiftsminimering, behörighetsadministration, arkivering och spårbarhet måste omhändertas inom ramen för dataskyddsförordningens regelverk.

Det går inte att underskatta behovet av att dataskyddet för den personliga integriteten säkerställs i regeringsuppdragen om säker och effektiv tillgång till grunddata samt säker och effektivt informationsutbyte inom den offentliga sektorn. Om en myndighet inte känner sig trygg i att delge information utifrån sitt personuppgiftsansvar kan konsekvensen bli att en nationell samsyn inte nås. Det innebär att det nationella systemet inte blir en robust helhet vilket påverkar EU:s mål att den fria rörligheten för uppgifter och digitala och det gränsöverskridande informationsutbytet.

Ur ett juridiskt perspektiv är slutsatsen att det ska ske inom gällande rätt men utmaningen blir att, i alla steg, hitta processer, metoder och säkerhetsåtgärder som tillgodoser alla behov. Ett annat dilemma är att viss information som delges kan anses lagligt ur ett juridiskt perspektiv men ur en säkerhetssynpunkt kanske det inte är lämpligt att informationen ingår.

Utifrån omvärldsbevakningen är det tydligt att ett svenskt informationsutbyte nationellt och gränsöverskridande ska vara säkert vilket medför att Sverige i ett första steg behöver skapa en säker nationell miljö som samtidigt är effektiv, för att i nästa steg kunna tillgodose det krav som ställs för att denna information ska kunna vara gränsöverskridande.

# 2 Bilaga 2 - Fördjupning prioriterade byggblock

Nedan ges en mer detaljerad beskrivning av de prioriterade byggblock som kortfattat beskrivs i kapitel 4.

### 2.1.1 Mina ombud

#### *2.1.1.1 Beskrivning av byggblocket*

Det finns ett behov av en nationell, gemensam, infrastruktur för hantering av ombud i digitala tjänster. I vissa fall beskrivs detta också som fullmakt eller företrädare. Behovet omfattar såväl fysiska som juridiska personer.

Exempel på tillämpningar är att hantera behörigheter för att:

- Logga in på mina sidor företag (och ta del av företagets information)
- Agera för ett företags räkning.
- Agera för en fysisk persons räkning.
- Företräda andra juridiska personer, till exempel kommuner och myndigheter.

#### *2.1.1.2 Utmaningar*

Sverige saknar en nationell lösning för hantering av ombud i digitala tjänster.

- Ombud i e-tjänster hanteras i vissa fall med pappersfullmakter vilket skapar administration och är oöverskådligt.
- Det finns behov av att företräda både juridiska personer, fysiska personer och andra typer av organisationer i digitala tjänster.
- Det finns ett behov att kunna visa upp vilka behörigheter/fullmakter t.ex. ett företag har delat ut samt vilka fullmakter man tilldelats som fysisk person.

#### *2.1.1.3 Argumentation (Motivation view)*

Byggblocket är förutsättningsskapande och används för att kontrollera vem som får företräda vem i digitala tjänster (auktorisering). Det är en nyckel för pågående och kommande digitalisering hos kommuner, myndigheter och privata aktörer. Byggblocket gör det även möjligt att förenkla för företagare så att dessa kan ta hjälp från anställda eller externa ombud.

#### *2.1.1.4 Organisation*

Det finns behov av att företräda fysiska och juridiska personer samt andra typer av organisationer.  Vidare finns ett behov av att tjänsten får bred/nationell förankring. Bedömningen är därför att ett införande bör ske i samverkan mellan Bolagsverket,

Skatteverket och DIGG. Sannolikt är det lämpligt att börja med möjligheten att företräda företag och därefter skala upp stegvis.

#### *2.1.1.5 Juridik*

Bolagsverket har gjort en första rättsutredning för en konceptuell lösning. Den pekar på att ingen myndighet har rätt att lagra fullmakter för någon annans räkning och det tekniska koncept som tagits fram tar hänsyn till detta, se teknik.

Vidare finns det sannolikt behov av två typer av ombud. En för att ta del av information och en annan för att agera för någon annans räkning.

Det behöver genomföras en fördjupad juridisk utredning.

#### *2.1.1.6 Teknik*

Bolagsverket har tagit fram en konceptuell arkitektur som bygger på en sammansatt bastjänst som förmedlar information om ombud från olika källor. Konceptet ger även möjlighet att presentera alla ombud en person fått eller som ett företag delat ut på en central plats. Det ger även möjlighet att specificera ombud via API som ett steg i en process eller e-tjänst. I konceptet ingår även ett stöd för att förenkla användningen firmateckningen för konsumenten.

#### *2.1.1.7 Beroenden*

Byggblocket har beroenden till flera andra byggblock som t.ex. Identitet, Auktorisation och Tillitsregelverk.

### 2.1.2 API-hantering

#### *2.1.2.1 Beskrivning av byggblocket*

API hantering handlar om funktionalitet för att hantera API:er genom dess hela livscykel från design, utveckling och test till publicering, drift, förvaltning och avveckling. API:er i det digitala ekosystemet som används för externt informationsutbyte handlar om att tillgängliggöra väl definierade gränssnitt med ofta stora krav på dess kvalitetsegenskaper (icke funktionella krav). Dessa gränssnitt kan vara helt öppna eller öppna och säkra. Byggblocket adresserar inte vilken information som utbyts utan den funktionalitet som behövs för att tekniskt utbyta information. Att etablera API-hantering är redan en resa som påbörjats eller planeras av flera offentliga förvaltningar. Hanteringen kommer till stor del vara av ett distribuerat ansvar men med vissa gemensamma delar. Myndigheternas bedömning är att fortsatt arbete behöver genomföras för att analysera vilka delar som bedöms ge ett värde att hantera och organisera gemensamt.

Det finns strategiska beslut inom API-hantering avseende vilka delar som kan eller bör realiseras som gemensamma och vilka delar som kan eller bör realiseras som aktörsspecifika. Byggblocket skall hantera och stödja:

- Utvecklarportal/tjänstekatalog

- API-Gateway
- Livscykelhantering
- Design och utveckling
- API säkerhet
- Publicering
- Exekvering
- Analys och monitorering

#### *2.1.2.2 Fördjupad beskrivning av delen utvecklarportal/tjänstekatalog*

Utvecklarportal hanterar ett standardiserat sätt att beskriva och dokumentera gränssnitt och kontrakt som exponeras publikt för konsumering inom det digitala ekosystemet. Beskrivningar innehåller exempelvis användning, gränssnitt och underliggande datamodeller.

Kan även innehålla andra typer av beskrivningar som exempelvis exempelkod för anrop, regler för anslutning, begränsningar, kostnader, tillgänglighet, förväntad prestanda samt förutsättningar och stöd för utvecklare att genomföra tester mot gränssnitten.

*Utmaningar*

Hur hittar potentiella konsumenter de publika tjänsternas gränssnitt, hur är dessa dokumenterade, vilket stöd finns för att utveckla lösningar som konsumerar dessa tjänster samt gällande regelverk för anslutning.

Olikheterna i hantering och beskrivningar för att ansluta och konsumera ett publikt gränssnitt inom det digitala ekosystemet är en av de utmaningarna som påverkar hur snabbt, effektivt och med vilken kvalité nya lösningar kan tas fram.

Avtalsmodeller för anslutning och användande av APIer är ett annat område som begränsar möjlighet till säkert och effektivt informationsutbyte.

*Argumentation (Motivation view)*

Utvecklarportal är en mycket viktig del för att bygga ett gemensamt digitalt ekosystem. Det är producenternas ansikte utåt i det digitala ekosystemet. Ett myndighetsgemensamt sätt att beskriva och publicera gränssnitt samt för konsumenten att hitta dessa beskrivningar är ett av de första stegen i processen att accelerera utbytet av information.

*Organisation*

Behovet är brett och innefattar att ta ytterligare steg i etableringen av en nationell struktur för informationsutbyte - ekosystem. Här i ingår bl.a. att analysera vilka delar av hanteringen som är gemensamma och därefter etablera en förvaltningsorganisation med fokus på att ta fram och förvalta gemensamma standarder med tillhörande tekniskt stöd.

*Semantik*

Gemensamma standarder för beskrivning av de publika tjänsternas informationsmodeller, tekniska beskrivningar samt verksamhetsregler för anslutning och användning.

*Teknik*

Vilket tekniskt stöd som behövs för att etablera tjänstekatalog/utvecklarportal behöver analyseras inom kommande uppdrag.

### 2.1.3 Identitet

Det är av stor vikt att organisationer, personer och enheter har en entydig global identitet vid informationsutbyte. Framför allt är detta viktigt för att kunna spåra händelser över flera system och i vissa fall i flera led. Det finns dock ganska skilda behov för hantering av dessa identiteter mellan olika entiteter:

- *Personer*: för kommunikation mellan personer och andra entiteter är personnumret (och samordningsnummer) den naturliga identiteten i Sverige idag. Även om många inte gillar spridningen av personnummer har det ändå blivit en de facto standard som används av de flesta e-legitimationsleverantörer idag.
- *Organisationer*: även organisationer har en naturlig identitet med organisationsnummer i Sverige. För personer inom en organisation blir det dock mer komplicerat. Dessa har som regel unika identiteter men de kan se väldigt olika ut och därmed vara svårhanterade. Dessutom vill man inte som regel exponera dessa utanför den egna organisationen på grund av säkerhetsskäl. För kommunikation mellan organisationer bör därför federationer skapas där den interna identiteten översätts till en global identitet på ett, för federationen, standardiserat format. Denna globala identitet kommuniceras sedan via aktuell identitetstoken inom federationen.
- *Enheter*: denna kategori består av fysiska enheter. Dessa brukar som regel kunna identifieras med t ex MAC-adresser. Mer sofistikerade mekanismer kan användas men kräver då oftast stöd i hårdvara för detta (t ex TPM) om en signifikant ökning av säkerheten önskas.

#### *2.1.3.1 Utmaningar*

Asylsökande i Sverige saknar personnummer och samordningsnummer. Detta i sin tur gör att utfärdande av e-legitimationer till denna grupp ej är möjlig, vilket skapar ett digitalt utanförskap. Utan personnummer eller samordningsnummer får bl.a. skola, vård, arbetsförmedling problem att hantera denna kategori. Denna kategori är ett exempel där identifiering inte fungerar idag.

#### *2.1.3.2 Argumentation (Motivation view)*

En unik och konsistent identitet är grunden för att en entitet ska kunna använda digitala tjänster där skyddsbehovet av informationen inte tillåter anonym access.

#### *2.1.3.3 Teknik*

Skapandet av unika konsistenta identiteter är i grunden inte ett teknikproblem utan är har mer karaktären av ett standardiserings- och processproblem.

#### *2.1.3.4 Organisation*

DIGG har i dag ansvar för svensk e-legitimation, men det saknas ett uttalat ansvar för ett övergripande arbete kring identitet som sträcker sig från hårdvara till människor och organisationer.

Det behövs alltså en standardisering och regelverk för hur dessa identiteter skapas och underhålls över tid så att det går att uppnå spårbarhet och möjliggöra ett rättsligt ansvar där så är nödvändigt i de olika kommunikationsmönstren.

### 2.1.4 Auktorisation

#### *2.1.4.1 Beskrivning av byggblocket*

För access till olika informationsresurser behöver i många fall en auktorisation ske. Detta kan ske på ett flertal olika sätt beroende på kommunikationsmönster, resurstyp och skyddsbehov.

Nedan beskrivs några olika typer av kommunikationsmönster och den effekt de kan ha på auktorisationsmekanismerna:

- *Privatperson till organisation*: privatpersoner som anropar en e-tjänst gör detta som regel för att hantera information som rör dem själva eller en person/organisation de har någon form av relation till. I dessa fall är det vanligt att resurshanteraren kan formulera hur access får ske utifrån ett antal regler som upprättas antingen ur ett affärsperspektiv eller på annat sätt, t ex lagrum. Oaktat vilket är det resurshanteraren som genomför auktorisation för användaren och beviljar eller nekar access till resursen, dvs administrationen av auktorisationen är centraliserad hos resurshanteraren (t.ex. en tjänsteleverantör).
- *Organisation till organisation*: för detta kommunikationsmönster förväntas en federation vara den vanligaste lösningen. Detta möjliggör att den autentiseringen som sker via federationen kompletteras med auktorisation (den token som används för att förmedla identitet bekläs med på förhand överenskomna attribut). På så sätt kan administrationen av åtkomsträttigheter administreras av den organisation som nyttjar tjänsten och därmed kan administrationen av auktorisationen ske distribuerat. Detta medför att administrationen kan bli mer skalbar. Detta förutsätter att det finns en tillit mellan organisationerna.
- *Ombud*: den behovsanalys som genomförts indikerar ett behov av att hantera ombud. Detta kan implementeras i båda fallen ovan och innebär i korthet att en entitet kan agera för en annan entitet.

#### *2.1.4.2 Utmaningar*

Ett ökande antal bedrägerier som begås med hjälp av förfalskade identitetshandlingar där en målvakt används för att agera som en entitet som sedan säljs vidare för diverse missbruk.

Organisationer kommer att ingå i stora federationer. Med ett stort antal deltagare i federationer ökar även riskerna med dessa då antalet attackvektorer ökar.

#### *2.1.4.3 Argumentation (Motivation view)*

Utan auktorisation kan endast information utan skyddsbehov delas. Detta skulle begränsa samhällsnyttan med infrastrukturen drastiskt.

#### *2.1.4.4 Teknik*

Tekniken för att implementera de ovan beskrivna scenarierna är väl etablerad idag. De federationslösningar som vi ser bör baseras på den numera väl etablerade SAML 2.0 standarden. Teknikval för den centraliserade auktorisationen kan i stor utsträckning väljas av berörd organisation. Den distribuerade modellen är mer komplex och kräver samarbete, standarder och gemensamma regelverk för att kunna appliceras effektivt i större skala.

### 2.1.5 Tillitsregelverk

#### *2.1.5.1 Beskrivning av byggblocket*

Det finns ingen teknisk lösning för att uppnå tillit utan det behövs en kombination av teknik, processer/arbetssätt och kultur som är gemensam och accepterad av de ingående aktörerna.

Det är ofta lämpligt att skapa flera nivåer av tillit då ett specifikt informationsutbyte inte innebär ett risktagande som motiverar en viss resursallokering.

En uppsättning av tekniska åtgärder, processer och gemensamma kulturella värderingar samlar vi i denna rapport under benämningen tillitsregelverk.

Tillit är något som berör hela systemet och teknik, processer/arbetssätt och kultur kan konkretiseras i fyra delar; tekniska lösningar, samverkanstyper, processer och modeller. Detta är ett stort och omfattande område så nedan ges endast exempel på olika typer av lösningar:

- *Tekniska lösningar*: Olika stark autentisering (t ex lösenord kontra smarta kort) medför att olika nivåer av tillit till vem en given entitet är skapas och i vissa fall kan det vara motiverat att inte ha någon tillit alls.
- *Samverkanssätt*: Ett ingånget avtal mellan två parter ger mer tillit än exempelvis en spontan informationsaccess vid ett enskilt tillfälle.
- *Processer*: Att följa exempelvis ISO27001[136] bör resultera i högre tillit än att följa en icke-etablerad process (eller ingen alls). Processer förutsätter även att det finns mekanismer som kontrollerar att de ingående aktörerna faktiskt följer processerna.

[136] ISO/IEC 27001:2013 Information technology - Securety techniques - Information securety management systems - Resquriments

- Modeller: Förmågan att kommunicera olika nivåer hos tekniska lösningar, samverkanssätt, processer och arbetssätt förutsätter att det finns gemensamma modeller för att beskriva dessa på ett entydigt och accepterat sätt. En fundamental modell är en informationsklassningsmodell som beskriver skyddsbehovet hos olika informationsmängder.

#### *2.1.5.2 Utmaningar*

Tillitsregelverk kan vara omfattande och måste ha acceptans hos de ingående parterna. Tillitsregelverk behöver även kunna utvecklas och förvaltas över tid allt eftersom behoven förändras. Här kan ekosystemets konstruktion vara bidragande till lösning.

#### *2.1.5.3 Argumentation (Motivation view)*

En förutsättning för att kunna skapa ett säkert och effektivt informationsutbyte är att samtliga ingående aktörer känner tillit till de övriga aktörerna och den infrastruktur som används, till en sådan nivå att de kan acceptera den risk som informationsutbytet innebär för dem själva.

#### *2.1.5.4 Organisation*

I samtliga byggblocksbeskrivningar ovan är det uppenbart att det behövs samverkan och koordinering. Den grundläggande strukturen för denna koordinering ligger i Tillitsregelverket som i sin tur påverkar alla de andra byggblocken. Samordning och styrning kommer även behovs kompletteras inom de övriga byggblocken.

Myndigheten för samhällsskydd och beredskap (MSB) har redan idag ett samordningsansvar för informationssäkerhet och publicerar allt från föreskrifter till vägledningar. MSB ses som den naturliga aktören att hantera Tillitsregelverket som sätter ramarna för övrig koordinering.  DIGG är den naturliga aktören att samordna de mer tekniskt orienterade delarna i infrastrukturen (t ex standarder för identiteter och attribut för auktorisation).

Arbetsinsatsen för MSB och DIGG ska inte underskattas och därmed måste det förutsättas att det måste till resursförstärkningar för båda myndigheterna om de ska kunna hantera detta på ett tillfredsställande sätt.