Teknisk referens-arkitektur

Att leverera sekretessbelagd information som SaaS

itsl solutions

Projekttitel: Riktlinjer och plattform för säker SaaS inom offentlig sektor.
Rapport: 2025–05–01, MSB 2024–15281

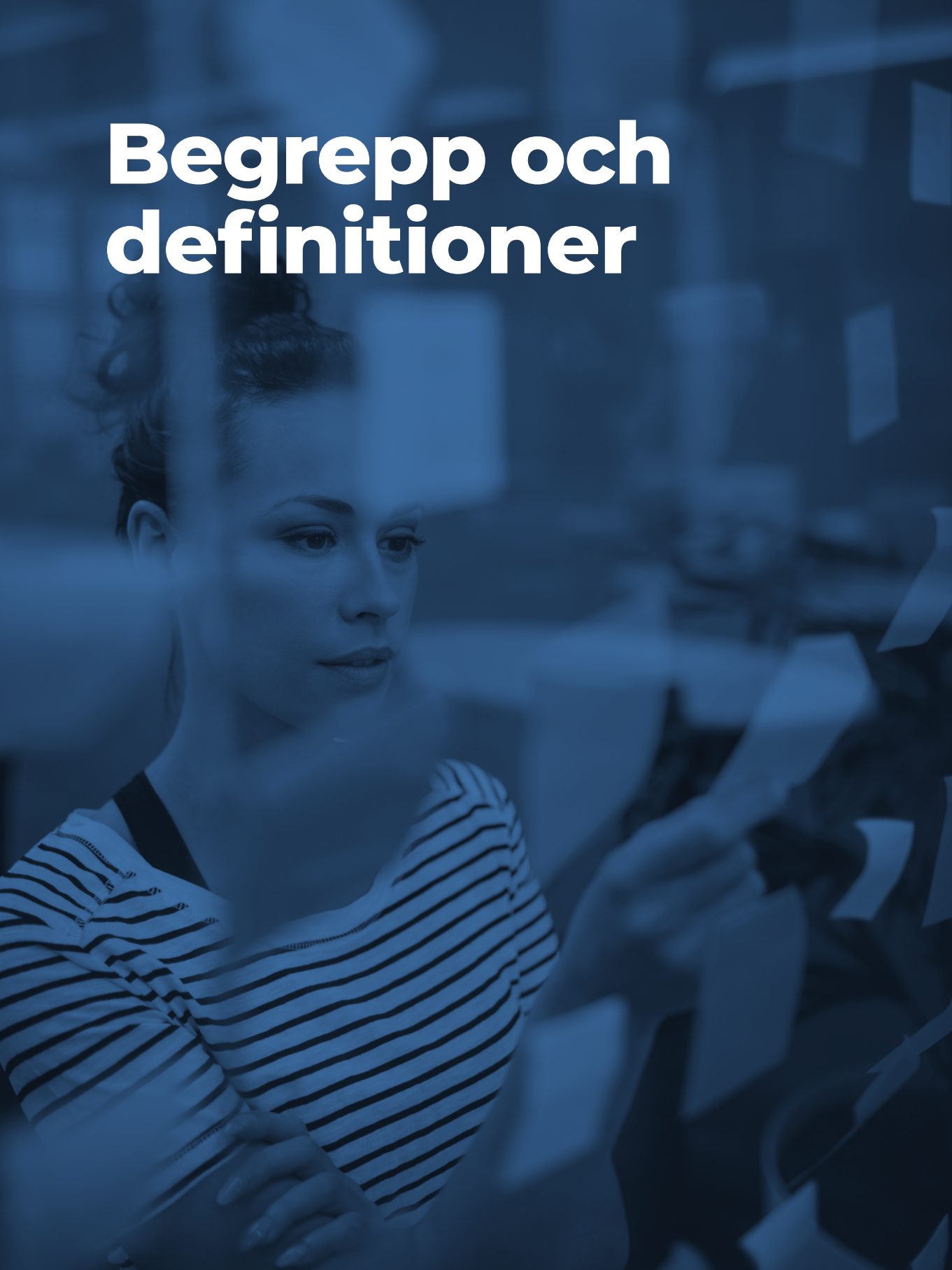
Teknisk referens-arkitektur

Att leverera sekretessbelagd information som SaaS

itsl solutions

Innehåll

Begrepp och definitioner



1. Begrepp och definitioner

OSL:
Offentlighets- och sekretesslagen.

GDPR:
General data protection regulation, dataskyddsförordningen.

SDK:
Säker digital kommunikation.

ZERO-KNOWLEDGE:
Upplägg där tjänsteleverantören hanterar kundens data utan att själv kunna läsa eller dekryptera den. All information krypteras och förblir endast åtkomlig för dataägaren (kunden) – inte för leverantören.

KMS (Key Management System):
Nyckelhanteringssystem som används för att skapa, distribuera, lagra och administrera kryptografiska nycklar på ett säkert sätt.

HOYK (Hold your own key):
Säkerhetsmodell där kunden själv behåller exklusiv kontroll över sina krypteringsnycklar istället för att överlåta dem till en molnleverantör.

OAUTH CLIENT/CLAIM:
Applikation eller tjänst som vill få åtkomst till skyddade resurser på uppdrag av en användare (resursägaren).

CLAIM (i identitets och säkerhetssammanhang):
Information om en entitet (ofta en användare) som intygas av en betrodd part. En claim består av ett namn/nyckel och ett värde – t. ex. *“email”: “”* – och bäddar in en egenskap eller attribut hos användaren.

(GET)ENDPOINT (i API sammanhang):
Specifik URL eller adress där en klient kan nå en viss tjänst eller resurs. Endpoints utgör gränssnittet mot ett API – de tar emot inkommande begäranden och svarar med data eller resultat.

DLP-CONTROLLER:
Implementerar organisationens policyer för att hindra att känslig information läcker ut – till exempel genom att skanna filer, e-post eller nätverkstrafik efter sekretessbelagda uppgifter och vidta åtgärder om policybrott upptäcks.

TEE-HÅRDVARA/DRIFT:
Trusted Execution Environment (TEE) syftar på en teknik där särskild hårdvara i en processor skapar en isolerad säker miljö (även kallad enklav) för att köra kod och hantera data konfidentiellt.

BODY (i API-sammanhang):
Huvudinnehållet i en HTTP-begäran eller -respons, det vill säga själva data-delen av meddelandet (som kommer efter header-sektionen).

PAYLOAD (I API sammanhang):
Avser den faktiska data som överförs i en kommunikation, exklusive de omgivande protokollfälten.

RANDFALL:
Betecknar ett extremfall eller specialfall som ligger i utkanten av de normala förutsättningarna för ett system. Det handlar om scenarier som är ovanliga eller gränsar till systemets gränsvärden, och som därför kan ge upphov till oväntat beteende.

NYCKELLAGER (inom kryptografi):
Lagringsstruktur eller modul där man kan spara flera krypteringsnycklar på ett organiserat och utökningsbart sätt.

SERVERPARK:
En större samling servrar – i princip detsamma som en *serverfarm* eller ett datacenter. En serverpark kan bestå av många rackmonterade servrar i en eller flera datahallar, komplett med kraftförsörjning, kylning och nätverksinfrastruktur, som tillsammans levererar beräkningskraft och lagring för en organisation.

Inledning

2. Inledning

Offentlig sektor i Sverige står inför en stor utmaning när det gäller att säkerställa korrekt hantering av sekretessbelagda uppgifter i SaaS-tjänster. I dagsläget saknas tydliga tekniska riktlinjer för hur sekretessbelagd information ska hanteras i molnlösningar. En viss osäkerhet gällande tillämpningsområdet råder hos både leverantörer och upphandlande myndigheter, vilket resulterat i en inkonsekvent tillämpning av offentlighets- och sekretesslagen. [1]

I ett försök att bemöta ovanstående problematik har offentlig sektor tagit fram en digital infrastruktur i form av en federerad tillitsmodell, *Säker digital kommunikation* (SDK). Syftet med SDK är att offentliga aktörer i form av deltagare i infrastrukturen ska kunna överföra sekretessbelagd och känslig information digitalt sinsemellan. Utgångspunkten är att SDK i praktiken, under offentliga regelverk, ska tillhandahållas dels av offentliga aktörerna själva, dels av privata aktörer. [2]

Denna rapport riktar sig främst till dig med it-rättslig eller teknisk kompetens.

2.1. Bakgrund och syfte

ITSL Solutions AB (ITSL) har ansökt om projektmedel hos Myndigheten för samhällsskydd och beredskap för att utreda möjligheterna till att hantera sekretessbelagd information i SaaS-tjänster i allmänhet och SDK i synnerhet. I projektgruppen har ett flertal resurser deltagit. Den som hållit samman arbetet är Fredrik Jonasson, verkställande direktör ITSL Solutions AB. Därutöver har följande experter deltagit i olika omfattning. Johan Karlsson, systemarkitekt och en av grundarna och tidigare huvudutvecklare till Goobit Group AB, Magnus Hübner, systemutvecklare och grundaren till TDialog AB som sedermera upprättat delar av SDK-lösningen som förvärvats av Compodium AB, Ronnie Johansson, verkställande direktör Compilor AB, Johan Ström, IT-rättsjurist, tidigare verkställande direktör IT-Säkerhetsbolaget AB samt sekretessexpert inför Myndigheten för Digital förvaltnings (Digg) delrapportering av SDK, Erik Einarsson senior driftstekniker Iver AB, Erik Edlund senior systemutvecklare Engcon AB och Petter Ulander grundare till upphandlingsföretaget AdviceU AB som sedermera uppköpts av Sweco AB, idag oberoende upphandlingskonsult hos Level 5 AB.

Projektgruppen har haft följande övergripande målsättningar.

- **Ta fram en teknisk referensarkitektur** för hantering av sekretessbelagd information hos svenska SaaS-leverantörer.
- **Identifiera och dokumentera säkerhetskrav** baserat på bland annat offentlighets- och sekretesslagen (OSL) och dataskyddsförordningen (GDPR).
- **Ta fram en detaljerad checklista** inför upphandling av SaaS-tjänster som hanterar sekretessbelagd information.
- **Sprida resultaten** via öppna forum, presentationer för intresserade myndigheter och vid deltagande på konferenser och mässor.

En underförstådd målsättning är att referensarkitekturen, utöver juridiskt accepterad, ska vara realistisk utifrån ett kostnadsperspektiv.

2.2. Risken med kostnadsdrivna val och SaaS

Projektgruppen har identifierat risker till följd av motsättningar mellan å ena sidan mindre offentliga aktörers ekonomiskt ansträngda situation, privata bolagens vinstintressen som utmynnat i billigare tekniska lösningar, å andra sidan en striktare, och kanske mer korrekt, tillämpning av den svenska informationslagstiftningen (såsom OSL, patientdatalagen, NIS m.fl.) och GDPR. Identifierade risker finner stöd bland annat genom att ett flertal upphandlingar granskats, hos främst kommuner, och där det framgår att OSL inte kravställts med en konkret och konsekvent lagtillämpning. [3] Påståendet får därutöver stöd i Digg:s analyser beträffande mindre kommuners tillgång till it-rättslig kompetens i regeringsuppdragen I2020/0241/DF, I2021/00288. [4] Andra omständigheter som talar i samma riktning är det flertalet statliga myndigheter som valt att tillhandahålla egna tekniska lösningar för sekretessdata.

Projektgruppen noterar en avsaknad gällande myndighetsinterna rättsliga ställningstaganden i frågor om sekretess i SaaS-tjänster och sekretess vid utkontraktering av IT. [5] Projektgruppen har noterat att konsekvensen av passivare it-rättsligt stöd i frågan ett flertal gånger utmynnat i en förskjutning till IT-avdelningar och IT-experter att istället genomföra komplicerade juridiska tolkningar av sekretessfrågan. [6] Eller att privata jurister redogör för ett rättsläge som offentliga aktörer inte står bakom. [7]

Konsekvensen av ovanstående utmynnar i den situation vi befinner oss i idag. Där statliga myndigheter tillhandahåller stora delar av sin it-miljö själva och där mindre kommuner tvingas upphandla tekniska lösningar utan it-juridiskt stöd. Detta har därtill föranlett staten, SKR och Inera att inom ramen för SDK utveckla en egen, heltäckande lösning för samtliga offentliga aktörer, sedan den privata marknaden under nära ett decennium visat sig oförmögen att tillgodose det offentligas behov. [8]

2.2.1. Risker med SDK

SDK baseras på ett tillitsramverk. Samtliga deltagare (dvs. offentliga aktörer) ansvarar själva för att utveckla eller upphandla de tekniska komponenter som krävs för infrastrukturen. Ett av syftena med SDK är att tillhandahålla ett säkert verktyg som offentliga aktörer kan anförtro sig till vid överföring av sekretessbelagd information. I princip ska sekretessinformation som förundersökningsmaterial, journaluppgifter, orosanmälningar, elevhälsa m.m. kunna överföras i SDK. Privata leverantörer får anses utgöra en grundläggande förutsättning till att SDK ska kunna nå ut till samtliga potentiella deltagare (dvs. merparten av Sveriges kommuner). Digg medger molntjänstlösningar i SDK. Samtidigt uppställer Digg inga krav som motverkar nyss nämnda (1.2 och mer i kap. 2) problembeskrivning inför godkännandet av privata SDK-leverantörer. Istället hänskjuts frågan till varje enskild upphandlande myndighet att kravställa korrekt inför upphandling av SDK. Det föreligger en uppenbar risk att SDK utmynnar i samma resultat som var orsakerna till att infrastrukturen togs fram från första början. [9]

Idag förekommer frekvent att upphandlingar genomförs av SDK-tjänster som inte säkerställer juridisk efterlevnad och som stora delar av Sveriges offentliga aktörer inte kan stå bakom dvs. infrastrukturen tillhandahålls, i enlighet med Digg:s regelverk, av ett flertal privata leverantörer som har full åtkomst till all sekretessinformation, från samtliga av deras kunder. Avsändande myndighet kommer inte ha någon möjlighet att identifiera vilka deltagare i infrastrukturen som upphandlat i enlighet med författningsregleringarna eller vilka som upphandlat utifrån samma tekniska upplägg som var en av grundproblemorsakerna till varför SDK togs fram. [10] Det är utanför projektgruppens vetskap om någon acceptansutredning genomförts hos Digg utifrån detta hänseende, dvs. om Domstolsverket, Åklagarmyndigheten, Polismyndigheten, Socialstyrelsen, Försäkringskassan, Skatteverket, Kronofogdemyndigheten, Skolverket och Kriminalvården m. fl., accepterar en sådan lösning, där myndigheterna inte kan kontrollera var deras sekretessdata hamnar vid överföring inom SDK. En uppenbar risk föreligger att statliga myndigheterna tillämpar en lika restriktiv hållning till informationshanteringen i SDK som det som föranleder bedömningarna till on-prem-lösningar idag, dvs. inte använder tekniska lösningar där leverantören får åtkomst till data eller inte tillåter att myndigheterna laddar upp sekretessdata i mottagarens privata molnlösningar. [11] Om konsekvenserna av nyssnämnda risk inträffar, är det mer sannolikt än inte att tillitsramverket raseras och därigenom även SDK.

2.3. Avgränsningar

Projektet fokuserar på svenska SaaS (Software as a Service)-leverantörer och lagstiftning som omfattar aktörer i Sverige. Ett särskilt fokus kretsar kring främst *offentlighets- och sekretesslagen* (OSL) och i begränsad omfattning *dataskyddsförordningen* (GDPR).
En utgångspunkt är en analys av molnlösningar som avser hantera sekretessbelagda uppgifter. Projektet tar inte fram en fullskalig produktionslösning, utan avser framföra en referensarkitektur med tillhörande checklistor och rekommendationer. Analysen avser inte beakta sekretess till följd av säkerhetsskydd.

SLUTNOTER, NR 1-11

[1] SOU 2021:1 s. 231 ff, SOU 2018:25 s. 338 f, eSam, ES2023-06 s. 22 ff.

[2] Dnr. I2021/03317, Uppdrag att tillhandahålla infrastruktur för säker digital kommunikation i offentlig sektor, delrapport 30 september 2022, DIGG;s dnr 2021-2909, https://www.digg.se/download/18.129a4fef1939e2e1c1f155c8/1664799324914/Delrapportering%20av%20uppdrag%20att%20tillhandh%C3%A5lla%20infrastruktur%20f%C3%B6r%20s%C3%A4ker%20digital%20kommunikation%20i%20offentlig%20sektor.pdf

SDK bilaga 1 – Rättslig analys
https://www.digg.se/download/18.129a4fef1939e2e1c1f155cb/1664799324960/Delrapportering%20SDK%20%20Bilaga%201.%20R%C3%A4ttslig%20analys.pdf

[3] Med respekt för kommunerna anges inte vilka kommuner som granskats. Det kan dock noteras att genomgående har en bristande förståelse hos kommunerna identifierats gällande grundläggande frågeställningar i förhållande till utkontraktering av sekretessdata och fri åtkomst för privata leverantörer att förfoga över denna. Andra identifierade brister i frågeställningen som varit återkommande är i vilken grad och för vilka fall tystnadspliktsförbindelser kan tillämpas mot privata aktörer.

[4] Slutsatserna i slutrapport DIGG:s dnr. 2021-168 och fallstudie beträffande SDK
https://www.digg.se/download/18.129a4fef1939e2e1c1f23ef0/1647952778352/Analysuppdrag%20kommuner%20och%20regioner%20-%20%20Bilaga%20Fallstudie%20SDK.pdf

[5] SOU:2021:97 s. 163, 181 f. 188 f.

[6] Se exempelvis Skatteverkets ”Inledande utredning avseende Microsoft 365”, dnr. 8-2800157, 2024-02-26, som inte tagits fram hos rättsavdelningen och där det inte går att finna några spår gällande huruvida myndigheternas jurister står bakom utredningen.

[7] SOU 2021:1 s. 260 ff. Försäkringskassans vitbok v. 1.0, 2019-11-18, dnr. 013428-2019

[8] SDK grundades 2016 av SKR till följd av ett tydligt identifierat behov och en avsaknad av lösningar på den privata marknaden.

[9] Dvs. att marknaden (huvudregel statlig sektor) blir så pass osäker beträffande mottagarnas juridiskt bristfälliga lösningar (i huvudsak mindre kommuner), att infrastrukturen inte anses tillräckligt säker eller laglig för statliga myndigheter att använda.

[10] Observera att frågan inte i detta skeende handlar om huruvida OSL förbjuder sådan åtkomst. Avsnittet avser främst belysa en omständighet vi inte tror är tydlig för stora delar av statliga deltagarna.

[11] Åklarmyndighetens aktörsportal, domstolarnas säker e-post, IVO:s SSL-krypterade överföring av digitala handlingar, statens SGSI (Swedish Governtment Secure Intranet) m.fl.

Rättsliga överväganden

3. Rättsliga överväganden

I detta kapitel avses rättsläget för rapportens omfång redogöras. En utgångspunkt har varit ett försök att utröna rättsliga frågeställningar myndigheter står inför vid införskaffande av molntjänstlösningar.

3.1. Utgångspunkter

Några utgångspunkter som legat till grund för utredningen, och de kommande tekniska lösningsförslagen, är följande.

3.1.1. När uppgifter som hålls krypterade mot leverantörer inte anses som röjda[12]

Frågan om, när och i vilken omfattning uppgifter får hanteras vid utkontraktering har under en längre tid varit en omdiskuterad fråga. En utbredd ståndpunkt har sedan tidigare varit att sekretessuppgifter som endast är föremål för teknisk bearbetning eller teknisk lagring inte röjs till en utomstående (myndighet) som särskilt vidtar åtgärder för detta ändamål. I huvudsak kan resonemanget härledas till utgångspunkten att uppgifter som endast varit föremål för teknisk bearbetning eller teknisk lagring inte definierats som vare sig inkommen eller expedierad och således aldrig lämnat en myndighets sekretessfär. [13] Därtill har rättsutvecklingen förtydligat att det i den civilrättsliga ordningen går att organisera ett förhållande så att ett subjekt som annars inte skulle omfattats av straffsanktionerad tystnadsplikt, ändå gör det. [14]

Praxis är oklar beträffande röjandebegreppet. Samma rättskällor har åberopats i decennier av olika aktörer med ibland helt olika bedömningar och slutsatser. Särskilt fokus har varit NJA 1991 s. 103 (frågan om innebörden av uttrycket ”röjt uppgift” i 19 kap. 9 § BrB om straffbarhet till följd av vårdslöshet med hemlig uppgift) och JO 1982/73 s. 238 (om utkontraktering till servicebyråer) i förhållande till JO 2014-09-09, dnr 3032-2011, (om utkontraktering av läkarsekreterare).

Ett prejudikat som inte bör tillmätas någon större betydelse i förhållande till utkontraktering kopplat till röjandebegreppet i samband med nyttjande av molntjänster är NJA 1991 s. 103. Visserligen fördes resonemang om vårdslöshet med hemlig uppgift och vissa resonemang om sannolikhet och besittning. Det går dock inte bortse från att domstolen prövade den straffrättsliga frågan mot enskild i förhållande till den straffsanktionerade tystnadsplikten. Det är svårt att utröna om bedömningen varit densamma om röjandefrågan prövats gentemot en myndighet och att myndigheten beslutat om att förvara sekretesskyddade handlingar i skåp som inte uppfyllt adekvata säkerhetskrav.

I ett försök att finna en enhetlig rättstillämpning går det göra en tolkning av JO:s beslut om läkarsekreterare som att JO främst uppmärksammade det faktum att civilrättsliga avtal, som inte kan likställas en straffsanktionerad tystnadsplikt, inte alltid kan medföra att utkontraktering anses förenlig med sekretessbestämmelserna och att omständigheterna

kan medföra att en sekretessbrytande bestämmelse behövs vid utkontraktering. Detta till skillnad från JO:s beslut om servicebyråer där omständigheterna och därtill det civilrättsliga avtalet beträffande upplägget mellan parterna medförde att sekretessuppgifterna aldrig var att anse som röjda. JO tar inte ställning i något av besluten till frågan om samtliga utlämnanden och även i krypterad form medför att sekretessuppgifter röjs.

I IT-driftsutredningen fördes ett resonemang om att utkontraktering alltid medför att uppgifterna som är föremål för utkontrakteringen röjs, oavsett om utkontraktering skett inom ramen för teknisk bearbetning eller teknisk lagring och oavsett om uppgifterna är krypterade även för mottagande deltagare. [15] Det får anses finnas en logik i IT-driftutredningens strikta bedömning av röjandebegreppet. Det går att ifrågasätta behovet av tystnadspliktsbestämmelser i 11 kap. 4 § a OSL om uppgifter aldrig ansetts lämnat sekretessfären och således blivit röjda (även om resonemanget går emot en hos vissa sedan tidigare inarbetad etablerad praxis beträffande röjandebegreppet). [16] IT-driftsutredningens förslag har mött ett stort motstånd hos remissinstanserna, inte minst beträffande ställningstagandet om att även krypterade uppgifter alltid ska anses som röjda. [17] Något som kan haft betydelse för meningsskiljaktigheterna är myndigheternas olika tolkningar av begreppet teknisk bearbetning eller teknisk lagring. [18] Vissa myndigheter förespråkar en vidare tolkning av begreppet som innebär att den som tar emot information för teknisk bearbetning eller teknisk lagring även har visst utrymme att behandla informationen för egna syften, såsom statistikändamål. Denna tolkning av begreppet medför att det är avsevärt svårare att argumentera för att uppgifter inte röjs för annan aktör eftersom den mottagande aktören hanterar information för egna syften och får ta del av okrypterad information. Dessutom aktualiseras frågorna om sekretessbrytande bestämmelser och sekretessavtalens juridiska tillkortakommanden. Andra myndigheter tillämpar en snävare tolkning av begreppet som innebär att den som tar emot informationen endast får hantera informationen i krypterad form och på den avsändande myndighetens instruktioner. Denna tolkning av begreppet medför att det är lättare att argumentera för att uppgifterna inte röjs.

Om leverantören endast bereds åtkomst till informationen genom brottsliga åtgärder, såsom tekniska intrång, får det anses som att uppgifterna inte anses som röjda. [19] Utifrån ett sådant scenario tillämpas inte OSL. Myndigheter likställer då leverantörens hantering av krypterad data med liknande tillämpning som analog posthantering, överföring via fiberlina eller förvaring av sekretessuppgifter i lokal med privat hyresvärd.

Utifrån samma bakgrund får det anses som att merparten av de myndigheter som tagit ställning till sekretessfrågan gör bedömningen att uppgifterna är röjda i händelse av att data finns tillgänglig gentemot leverantören, leverantören har krypterad data men har själv åtkomst till dekrypteringsnycklar eller andra metoder där leverantören med egna tekniska eller fysiska hjälpmedel kan bereda sig åtkomst till informationen. Med fysiska avses bland annat åtkomst till serverhall och där leverantören med förhållandevis enkla medel kan bereda sig åtkomst till information genom att tillgodose sig hårdvaran. Utifrån scenariot att uppgifterna anses som röjda i förhållande till leverantören behövs en sekretessbrytande bestämmelse.

Utgångspunkten innebär således att så snart en leverantör får åtkomst till myndighetens information direkt eller indirekt (genom att själva förfoga över dekrypteringen) röjs sekretessuppgifter för leverantören. Myndigheten är då skyldig att säkerställa att röjandet är lagligt utifrån OSL.

3.1.2. Teknisk bearbetning och teknisk lagring är svårdefinierad men bör tolkas snävt

Frågan gällande exakt vad som kan anses omfattas i tillämpningen av teknisk bearbetning eller teknisk lagring i en digital infrastruktur är oprövad. En utgångspunkt får anses vara att förhållanden där en leverantör uteslutande hanterar data för annans räkning och inte har egna ändamål för hantering av data samt att åtkomst begränsas tekniskt för leverantören, omfattas förfarandet av juridiska begreppet teknisk bearbetning eller teknisk lagring. Utgångspunkten är även i linje med det resonemang som fördes till begreppsdefinitionen vid införandet av tystnadspliktslagen. [20]

Som exempel på teknisk bearbetning och teknisk lagring kan anges; införa, förvalta, utveckla och så småningom avveckla en it-driftstjänst. Inom ramen för nyssnämnda inbegrips att vidta åtgärder för att säkerställa tillgänglighet, funktionalitet och prestanda. Inom begreppet inryms även förändringar och tillägg i funktionaliteten såsom etablering av tilläggstjänst, integration med andra tjänster, konfiguration, test, utvecklande och tillhandahållande av supporttjänster (obs. att det sistnämnda kan tolkas brett och det finns definitivt delar av begreppet som faller utanför tillämpningen för teknisk bearbetning och teknisk lagring). Inom tillämpningsområdet omfattas säkerhetsåtgärder såsom uppgradering, uppdatering, kopiering, kryptering, pseudonymisering och incidenthantering. Vid avvecklande av tjänsten omfattas adekvata tekniska åtgärder, såsom exportering. [21]

Varje *frihet* upphandlande myndighet ger leverantören medför att affärsupplägget får anses bli mer oförenligt med lagens tillämpningsområde. Vid en hög grad av *frihet* behövs en annan sekretessbrytande bestämmelse, som i praktiken är svår att finna. Som *frihet* kan bland annat nämnas support, handläggning eller statistik i olika omfattning. [22]

Myndigheter och privata aktörer har i remissutlåtanden öppet uttryckt en oro beträffande svårigheterna att tillämpa begreppet i moderna miljöer. Frågan har dock upprepat bemötts från lagstiftaren som att tolkningssvårigheter inte torde föreligga. [23] Till följd av lagstiftarens officiella inställning till begreppet och kortfattande bemötande gentemot remissinstanserna görs tolkningen att, i enlighet med analoga tillämpningen, begreppet bör definieras som snävt. [24]

3.1.3. Vid utkontraktering innebär 10 kap. 2 a § OSL fortfarande att en bedömning måste göras i förhållande till leverantören och molntjänsten

Sekretessbrytande bestämmelsen 10 kap. 2 a § OSL reglerar att uppgifter kan lämnas till enskild, dvs. privat extern leverantör av tjänster inom teknisk bearbetning och teknisk lagring. Utöver definitionen av teknisk bearbetning och teknisk lagring måste en bedömning göras *om det inte med hänsyn till omständigheterna är olämpligt att uppgifterna lämnas ut* (lämplighetsbedömning).

En utgångspunkt med bestämmelsen är alltså att uppgifterna är röjda gentemot leverantören och att bestämmelsen utgör en sekretessbrytande bestämmelse för när det kan anses vara lagligt att röja uppgifterna. Inom ramen för sekretessbrytande bestämmelsen inbegrips leverantörers åtkomst till data för samtliga arbetsuppgifter som är nödvändiga för att tillhandahålla teknisk bearbetning och teknisk lagring, det kan som exempel vara åtkomst till användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar m.m. [25]

I lämplighetsbedömningen ska annan lagstiftning beaktas, som exempel GDPR.[26] GDPR medför inga generella hinder mot utkontraktering, eller ingående av personuppgiftsbiträdesförhållanden, artikel 28 GDPR. Till skillnad mot sekretessregleringen presumerar GDPR att utkontraktering, utifrån reglerade förutsättningar, kan genomföras, jämfört med OSL som snarare presumerar att röjanden till exempelvis externa leverantörer är otillåtna så länge inte sekretessbrytande bestämmelse föreligger eller menprövning genomförts. Nu aktuell reglering i OSL medför i det närmaste en uppluckring av personuppgiftsbiträdesförhållanden, där möjligheter finns att i enlighet med GDPR:s bestämmelser om biträden, överlämna sekretessuppgifter för myndighetens räkning. Regleringen i OSL får tolkas som att om det föreligger hinder för att utkontraktera utifrån GDPR, torde det även föreligga hinder att röja sekretess till biträdet som varit föremål för prövningen enligt GDPR. Alltså, om myndigheten i egenskap av personuppgiftsansvarig anser att personuppgiftsbiträdet inte är pålitligt enligt GDPR, föreligger även hinder att röja sekretessdata till denna.

Utöver tillämpningen av GDPR vid lämplighetsbedömningen ska samtliga omständigheter beaktas, såsom vem som i det specifika fallet utgör uppgiftslämnande myndighet, vem som i det specifika fallet är uppgiftsmottagare, vilka uppgifter som lämnas ut, avtalsförhållandet mellan uppdragsgivande myndigheten och uppgiftsmottagaren eller det allmänna säkerhetsläget, nationellt som internationellt. [27] Utifrån ovanstående går det inte att göra annan bedömning än att exempelvis en socialtjänst, eller teknisk förvaltning i en kommun som avser lämna ut uppgifter till leverantör avseende socialtjänstärenden eller uppgifter om vital infrastruktur, står inför en mer restriktiv bedömning än jfr. en kulturförvaltning. Detsamma gäller en mindre myndighet som till vardags inte hanterar sekretessuppgifter, jfr. en brottsbekämpande myndighet där sekretess förekommer i större omfattning. I avtalsrelationen mellan myndigheter i Sverige och några av världens största molntjänstleverantörer, tillika världens största bolag får, samtliga myndigheter,

inbegripet Regeringskansliet, anses ingå en ofördelaktig partsrelation sett till bland annat det reella inflytandet i avtalsrelationen. Detta utgör en försvårande omständighet i lämplighetsbedömningen vid utkontraktering. Situationen försvåras ytterligare till följd av mer ansträngda internationella relationer.

Utöver ovanstående ska även andra omständigheter vägas in lämplighetsbedömningen. Som exempel vilken typ av uppgifter som leverantören får åtkomst till, vilka intressen som ligger till grund för sekretessen (myndighetens egna jfr. en skyldighet att skydda enskildas sekretess), uppgifternas omfattning, åtgärder som vidtas hos leverantören för att skydda uppgifterna, om leverantörens anställda omfattas av en lag- eller avtalsreglerad tystnadsplikt, avtalsvillkor som riskerar frånta den utlämnande myndigheten kontrollen över uppgifterna, var uppgifterna kommer hanteras geografiskt och om uppgifter kommer samlokaliseras med uppgiftsmängder som tillhör andra kunder samt vilka risker detta medför. [28] Det är tydligt att nu aktuell sekretessbrytande bestämmelse inte upprättades för att möjliggöra massiv utkontraktering av myndigheters sekretess till amerikanska molntjänstleverantörer.

En utgångspunkt i detta projekt har varit att merparten av de myndigheter som ö.h.t. genomför juridiska bedömningar, anser att sekretessbrytande bestämmelsen inte utgör en omfattande möjlighet att lämna ut sekretessuppgifter till privata molntjänstleverantörer. En annan utgångspunkt är att de kommuner som idag överför en stor mängd sekretessuppgifter till privata leverantörer har gjort detta på annan grund än genom juridiska bedömningar. [29]

3.1.4. Dataskyddsförordningen anses utgöra ett hinder för användning av molntjänster

I det följande avses översiktligt tydliggöra i vilken grad GDPR kan anses utgöra ett hinder beträffande nyttjande av molntjänster. Utifrån vår erfarenhet har det återkommande noterats att svårigheter föreligger för den personuppgiftsansvarige att dels tekniskt granska molntjänstleverantörer i förhållande till GDPR, dels reglera och styra molntjänstleverantören med instruktionen tillhörande personuppgiftsbiträdeavtalet, enligt artikel 28 GDPR. Utöver kraven som uppställs i GDPR inför anlitande av ett personuppgiftsbiträde kan det även föreligga nationell lagstiftning som ålägger myndigheten att vidta ytterligare åtgärder, såsom lämplighetsbedömningen i 10 kap. 2 a § OSL eller lämplighetsbedömningen för brottsbekämpande och rättskipande myndigheter i 3 kap. 16 § brottsdatalagen. En utgångspunkt är att merparten av myndigheterna anser det som generellt svårt att säkerställa korrekta behandlingar utifrån rådande författningar vid införskaffande av molntjänster i allmänhet och i avtalsrelationen mot amerikanska molntjänster i synnerhet. Orsaken kan dels anses vara en begränsad insyn i tekniska lösningar, dels bero på ojämlika partsförhållande och därav obefintliga möjligheter att påverka avtalets innehålls, dels bero på en avsaknad av it-rättslig eller teknisk kompetens.

Den fråga kopplad till GDPR som kanske varit mest aktuell är frågan om överföringar till tredjeland. I ett försök att följa med diskussionerna kan argumenten främst sammanfattas till två motsättningar [1] överföringar är lagliga eller inte till följd av rådande adekvansbeslut, [2] överföringar sker till tredjeland eller inte till följd av Bindl-målet.

En utgångspunkt råder fortsatt, enligt artikel 44 GDPR, att överföringar till tredjeland är förbjudna om inte undantagen i artikel 45–50 GDPR kan tillämpas. Några mer förekommande undantag som tillämpas (enskilt eller i kombination) är adekvansbeslutet EU-U.S Data Privacy Framework som har sitt stöd i artikel 45 GDPR och standardavtalsklausuler som har sitt stöd i artikel 46.2 c GDPR. Adekvansbeslutet är tillämpligt vilket medför att nyttjande av molntjänster som överför uppgifter till USA är lagliga, enligt GDPR. Något som fortsatt skapar oro bland myndigheter är enligt vår uppfattning utfallet av tidigare adekvansbeslut (Schrems I C-362/14 och Schrems II C-311/18). Osäkerheten är inte obefogad då det inte är uppenbart vad den juridiska skillnaden är (om det ens är någon skillnad) mot föregående adekvansbeslut. Det är rimligt att myndigheter som värnar om regelefterlevnad intar en restriktiv hållning i sin relation till amerikanska molntjänstleverantörer, särskilt i ljuset av den inlåsning som avtalsrelationen kan medföra.

Andra frågeställningar som uppstått i närtid är hur bedömningen ska göras beträffande när en överföring till tredjeland ö.h.t. sker. I det så kallade Bindl-målet (T-354/22) [30] framgick att en överföring till tredjeland inte anses föreligga endast då det föreligger en risk att en överföring kan ske (*punkten 135 i domen: the mere risk of access to personal data by a third country cannot amount to a transfer of data*). En betydande faktor för att överföringar inte kunde anses presumeras var att standardavtalsklausuler tillämpades. För det första innebär domen inte att samtliga överföringar till amerikanska molntjänster som har serverhall på Irland är tillåtna, överföringar i form av åtkomst eller direkt transportering, är fortfarande att betrakta som en överföring. För det andra kan noteras att sökanden fick till viss del rätt beträffande viss överföring till tredjeland. För det tredje kan noteras att överprövning i högsta instans är sannolik. Det råder delade meningar om vilka konsekvenser domen medför. Kvarvarande frågeställningar kan sammanfattas i följande två [1] vad som innebär en risk i detta hänseende, [2] i vilken omfattning standardavtalsklausuler är tillämpliga.

Målet klargör att risk inte är tillräckligt för att en tredjelandsöverföring skett, det framgår dock inte hur en risk i detta hänseende definieras. Å ena sidan går det göra tolkningen att det föreligger en betydande bevisbörda för den som hävdar en tredjelandsöverföring och att denna måste bevisa att en överföring de facto skett. Om detta är utfallet av Bindl-målet kommer det föreligga oerhörda svårigheter för enskilda att hävda sin rätt mot internationella molntjänstleverantörer även när en tredjelandsöverföring är *allmänt känd* och de facto sker. Utfallet skulle medföra dels en hög teknisk kompetens, dels insyn i tekniska arkitekturen hos ett icke-offentligt internationellt bolag. En sådan slutsats av underinstansmålet Bindl är enligt vår uppfattning alldeles för långsgående. Å andra sidan går det göra tolkningen att det som prövats beträffande tredjelandsöverföring endast var den snäva frågan om påståendet att tredjelandsöverföring anses föreligga endast till följd av åberopande av amerikanska myndigheters legala åtkomst genom amerikansk lagstiftning (CloudAct och FISA 720). Utfallet av den nyssnämnda tolkningen får klart

mindre betydelse för den rådande tillämpningen av tredjelandsöverföringar. Mer talar för denna tolkning då målet, i det avseende GDPR-relaterade frågor ö.h.t. prövats, främst kretsat kring detta påstående, dvs. en åberopad överföring endast till följd av att åberopa en utländsk lagstiftning.

Frågan om möjligheter att tillämpa standardavtalsklausuler är återkommande. Det råder inget tvivel om att avtalsmekanismens giltighet, utöver artikel 46 GDPR har det tydliggjorts både i Schrems II och i Bindl att standardavtalsklausuler är giltiga. Frågan får snarare hanteras inom ramen för när standardavtalsklausuler är möjliga att använda. Till följd av Schrems II, den 18 juni 2021, upprättade EDBP rekommendationer (01/2020). Rekommendationerna ska tillämpas tillsammans med standardavtalsklausulerna. [31]

Sammanfattningsvis rekommenderar EDBP tillämpning av standardavtalsklausuler och att sex steg ska beaktas.

1. Kartlägga överföringarna av personuppgifter.
2. Verifiera att någon av undantagsbestämmelserna i GDPR för överföringar till tredje land är tillämpliga.
3. Bedöm om det finns något i det specifika tredje landets lagstiftning eller praxis som kan påverka effektiviteten hos skyddsåtgärderna i den undantagsbestämmelsen i GDPR som tillämpas för den specifika överföringen.
4. Identifiera och vidta kompletterande åtgärder som är nödvändiga för att höja skyddsnivån till motsvarande nivå i GDPR. Steg 4 är endast nödvändig om bedömningen i steg 3 visar att lagstiftningen påverkar effektiviteten av de undantag som tillämpas. I bilaga 2 till rekommendationerna har kommissionen exemplifierande förteckning över kompletterande åtgärder.
5. Vidta formella förfarandeåtgärder som kan krävas i enlighet med de specifikationer som framgår av rekommendationen.
6. Omvärdera den skyddsnivå som har uppnåtts med jämna mellanrum.

Något som återkommande aktualiseras i diskussionen om tredjelandsöverföringar är punkten 3 och 4. Beträffande punkt 3 kan nämnas att EDPB understryker, i sin rekommendation, att det inte är möjligt att uppnå en likvärdig skyddsnivå om den som tar emot personuppgifterna är förhindrad att följa de villkor som följer av det aktuella undantaget i GDPR på grund av mottagarlandets lagstiftning eller praxis. Därutöver kan noteras att utfallet av Schrems II i kombination med punkt 3 EDPB:s rekommendationer, medför att överföringar till exempelvis USA eller andra länder där motsvarande lagstiftning, CLOUD Act eller FISA 720, är tillämplig inte kan tillämpa undantagsbestämmelserna i GDPR utan kompletterande åtgärder.

Om en bedömning och analys avseende mottagarlandets lagstiftning och praxis visar sig problematisk, har den personuppgiftsansvarige tre alternativ enligt EDPB:s rekommendationer.

1. Överföringen får inte genomföras (överföringen stoppas).
2. Vidta ytterligare lämpliga skyddsåtgärder för att uppnå likvärdig skyddsnivå (punkten 4 bland annat).
3. Överföringen kan genomföras om det efter en rättsutredning kan konstateras att den aktuella problematiska lagstiftningen i tredje land inte kommer bli aktuell för den aktuella överföringen. Vilket aldrig är fallet med överföringar till USA.

Beträffande punkt 4 kan nämnas att inga andra skyddsåtgärder än tekniska är tillämpliga som kompletterande åtgärder för att möjliggöra en överföring till tredje land om nationell lagstiftning och praxis undergräver undantagsbestämmelserna i GDPR. [32]

Lämpliga tekniska åtgärder enligt EDPB:s rekommendationer består i huvudsak av följande.

1. Personuppgifterna har en stark kryptering innan överföringen och driftleverantören är noggrant kontrollerad.
2. Krypteringsalgoritmen och dess parametrar (krypteringsnyckelns längd, driftläge med mera) uppfyller kraven för den senaste tekniska nivån och kan anses vara skyddade mot en kryptoanalys som utförs av de offentliga myndigheterna i det mottagande landet med beaktande av de resurser och den tekniska kapaciteten (till exempel datorkapacitet för uttömmande attacker) som de har tillgång till.
3. Styrkan i krypteringen har fastställts med beaktande av den specifika tidsperiod under vilken de krypterade personuppgifternas konfidentialitet måste upprätthållas.
4. Krypteringsalgoritmen har genomförts felfritt med hjälp av korrekt underhållen programvara vars överensstämmelse med den valda algoritmens specifikation har verifierats, till exempel genom certifiering.
5. Nycklarna hanteras på ett tillförlitligt sätt (genereras, förvaltas, lagras, i relevanta fall, kopplas till den avsedda mottagarens identitet och upphävs)
6. Nycklarna helt och hållet förvaras under kontroll av personuppgiftsansvarig eller någon annan aktör som anförtrotts denna uppgift och som är verksam inom EES eller i ett tredjeland, ett territorium eller en eller flera angivna sektorer i ett tredjeland, eller vid en internationell organisation för vilken kommissionen i enlighet med artikel 45 i GDPR har fastställt att en adekvat skyddsnivå säkerställts.

EDPB anser att det inte finns några kompletterande tekniska åtgärder att vidta om den personuppgiftsansvarige överför personuppgifter, eller gör dem elektroniskt tillgängliga, till en molntjänstleverantör eller andra personuppgiftsbiträden i ett tredje land där det krävs att data hanteras öppet. Notera att kompletterande teknisk åtgärd [2] kan bli särskilt problematisk för nationer där statliga myndigheter kommit långt inom IT- och teknisk

underrättelsetjänst. Det är med andra ord oklart om det över huvud taget finns någon teknisk åtgärd idag som är tillräcklig för överföringar till länder som USA utifrån EDPB:s rekommendationer.

En utgångpunkt i detta projekt har varit att myndigheter fortsatt sannolikt anser att GDPR utgör ett problem vid införskaffande av molntjänster, att tredjelandsöverföringar fortfarande går att göra gällande (trots marknadsförd serverhall på Irland) och att standardavtalsklausuler är svåra att tillämpa, främst i förhållande till SaaS-leverantörer stationerade i USA.

3.2. Rättslig tillämpning i förhållande till tekniska lösningen

Med utgångspunkt i föregående avsnitt kan SaaS-leverantörer upprätta [två]kategorier av, för myndigheter, lagliga molntjänster. [1] Dels handlar det om molnlösning där sekretessbelagd information hålls krypterad gentemot leverantören och krypteringsnycklarna förvaras hos annan part än den (leverantören) som har åtkomst till den krypterade sekretessinformationen. Tekniska lösningen utgår från att ingen sekretessbelagd information röjs till leverantören. [2] Dels handlar det om en teknisk lösning som i tillräckligt hög grad anpassas utifrån OSL:s lämplighetsbedömning att den får anses accepteras hos myndigheterna. Utifrån scenario [2] anses uppgifterna som röjda och sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL tillämplig.

En förutsättning är utöver OSL-anpassad teknisk lösning att data inte överförs utanför EES. För att undanröja samtliga tvivel beträffande tolkningen om överföring föreslås en helsvensk lösning.

3.2.1. När information inte anses som röjd

I projektet har svårigheter identifierats gällande att hålla information krypterad (utifrån zero-knowledge-principen) [33] gentemot leverantören och samtidigt bibehålla fördelarna med att nyttja molntjänstlösningar. Samtliga försök att bygga en arkitektur utmynnade i hybrid-cloud-lösningar där väsentliga delar av arkitekturen tillslut överfördes till myndigheten on-prem. Något förenklat bestod problemen främst i att när data dekrypteras i molntjänsten kommer den finnas tillgänglig för leverantören.

Slutligen kvarstod endast en teknisk lösning som i vart fall kunde likställas en rättslig tillämpning där sekretessinformation hanteras i molntjänsten. Lösningen baseras på Decrypt on Demand (mer om detta i senare kapitel), dvs. en lösning där myndigheten praktiskt och teknisk bestämmer när informationen ska tillgängliggöras för leverantören. En viss parallell har eftersträvats i förhållande till analog brevöverföring. I ett försök att efterlikna exemplet skulle hanteringen kunna beskrivas enligt följande.

Myndigheten får avisering om att de har ett brev att hämta hos ett postombud. Företrädare för myndigheten hämtar brevet och öppnar det tillsammans med postombudet. I liknelsen skulle leverantören av molntjänsten inte omfattas av tystnadspliktsbestämmelser enligt 2 kap. 14 § postlagen, eller 9 kap. 31 § lagen om elektronisk kommunikation. Å andra sidan

skulle leverantören i liknelsen sakna möjligheter att på förhand öppna brevet, till skillnad mot exempelvis ett postombud eller en brevbärare. Leverantören skulle även omfattas av tystnadspliktsbestämmelserna i lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller teknisk lagring. Myndigheten skulle inte få samma exklusivitet till innehållet i meddelandet som ett analogt brev. Myndigheten skulle dock erhålla en större faktisk kontroll över vilken information som delges samt när denna information delges leverantören. Det går att argumentera för att ordningen skulle säkerställa att avsändande myndighet inte röjer till mellanman i form av leverantör, utan i stället lämnar ut till mottagande myndighet och där den senare väljer att (att inom ramen för sin sekretessprövning) delge en viss privat leverantör.

3.2.2. När 10 kap. 2 a § OSL är tillämplig

Ett mer sannolikt reellt alternativ än nyssnämnda är att myndigheten accepterar att röjande sker men att den sekretessbrytande bestämmelsen i 10 kap 2 a § OSL är tillämplig. Frågor som då beaktats är att säkerställa var och hur informationen lagras och bearbetas, hur leverantören säkerställer att obehöriga får åtkomst till sekretessuppgifter, vilka säkerhetsgarantier en leverantör kan lämna, vilka kontrollmöjligheter myndigheten har säkerställa så att leverantören agerar som denne utlovat. För att omvandla lämplighetsbedömningens juridiska krav till teknisk tillämpning rekommenderas den utlämnande myndigheten överväga teknisk tillämpning i form av *Hold your own key, extern lagring med extern nyckelhantering, decrypt on demand och confidential compute* (mer om detta i följande kapitel).

3.3. Myndigheternas ansvar

En annan fråga som är av betydelse för sekretessfrågan i en gemensam infrastruktur, är när ansvaret övergår till respektive myndighet. I det analoga exemplet råder en betydande skillnad mellan att en myndighet lämnar en papperslåda med sekretesshandlingar utanför dörren till myndighet jfr. att en myndighet lämnar över sekretess till en myndighet och där mottagande myndighet senare själv väljer att förvara sekretesshandlingarna i en papplåda utanför myndigheten). En liknelse mot digitala förhållandet torde vara skillnaden mellan att en myndighet laddar upp sekretessuppgifter i en annan myndighets Google drive jfr. med att en myndighet lämnar över sekretessuppgifter och den mottagande myndigheten därefter väljer att ladda upp filerna i sin Google drive.

Som utgångspunkt och utifrån ett sekretesshänseende ankommer det inte längre avsändande myndighet att säkerställa korrekta sekretessprövningar av mottagande myndighetens utlämnanden. Mottagande myndigheten ansvarar självständigt för sin egen prövning och mottagande myndighetens resurser omfattas av straffsanktionerad tystnadsplikt.

Ovanstående måste beaktas om det ska vara möjligt att upprätta en digital infrastruktur mellan offentliga aktörer. En striktare sekretesstolkning torde även medföra att avsändande myndighet idag via brev förvägrar mottagande myndighet analoga handlingar, då denna

inte vet hur handlingen kommer förvaras hos mottagande myndigheten och i ljuset av att samtliga myndigheter idag omvandlar analog information till elektronisk i någon omfattning.

En avsändande myndighet skulle kunna förvägra en elektronisk försändelse direkt till en myndighet. Grunden till nekande skulle då bestå i att avsändande myndighet kan anta att mottagande myndighet kommer behandla personuppgifterna i strid med GDPR, 21 kap. 7 § OSL. Ett sådant antagande är i och för sig inte otänkbart om det kommit avsändande myndighet för kännedom att mottagande myndighet behandlar personuppgifter i öppna utländska molntjänster. Det torde dock vara för långtgående att utgå från att myndigheterna gör liknande tolkningar vid nyttjande av svenska och nationellt säkerhetsanpassade molntjänstlösningar.

3.3.1. Konsekvensen för SDK

Nuvarande SDK-regelverk som tillhandahålls av Digg saknar reglering som säkerställer exemplet att avsändande myndighet kan utgå från att information inte först hamnar hos en ”leverantör i mitten” likt Google drive exemplet. Nuvarande regelverk tillåter att en deltagare i SDK (exempelvis en kommun) upphandlar en privat molntjänst och där lösningen medför att informationen bearbetas och lagras helt öppet eller med fri åtkomst (leverantörens åtkomst till krypteringsnyckeln) gentemot leverantören. I praktiken blir överföringen mer lik *att avsändande myndighet laddar upp hos mottagande myndighets Google drive* än exemplet *att avsändande myndighet överför (helt krypterat för leverantören) och där leverantören senare väljer att ladda upp i sin Google drive*. Utifrån samtliga molnbaserade SDK-upphandlingar som kommit ut [34] har ingen av upphandlande de myndigheterna säkerställt kryptering utifrån det som borde vara det mest juridiskt accepterade exemplet.

[12] Stora delar av 2.1.1. är inhämtat från Digg:s delrapportering beträffande SDK

[13] Prop. 1975/76:160, s. 137 f.

[14] Prop. 1979/80:2, del A, s. 128 f, Lagkommentar till 2 kap. 1 § OSL från JUNO (Lexino) där bl.a. ett resonemang om förbehåll utifrån 10 kap.14 § OSL finns), lagkommentar 2 kap. 1 § OSL från JUNO (Norstedts juridik), JO 1982/83 s. 238.

[15] SOU 2021:1, s. 281–283.

[16] Observera att denna tolkning gjordes innan sekretessbrytande bestämmelsen infördes i 10 kap 2 a § OSL.

[17] Se bland annat följande remissvar: Arbetsförmedlingen (Af-2021/0008 2776, s.4 ff.), E-Hälsomyndigheten (2021/00541 s.1 f.), Försvarsmakten (FM2021-4977:3, s. 1), Försäkringskassan (FK2021/001872 s.3 f.), Myndighet för digital förvaltning (2021–185 s. 2 och 4).

[18] Vilket påtalatades i flera remissvar enligt ovan men även i Skatteverkets remissvar (8–744868, s. 3 f.). Detta lyftes även av remissinstanserna inför prop. 2019/20:201 men som lagstiftaren aktivt valt att inte besvara och där otydlighet beträffande definitionen tydliggjordes i SOU 2021:97.

[19] Prop. 2022/23:97 s. 6 f.

[20] Prop. 2019/20:201, s. 22 f.

[21] Prop. 2022/23 s. 16 f., lagkommentaren från Juno (E. Lenberg, A Tansjö, U. Geijer, v. 30, 2024-12-11) 10 kap 2 a § OSL.

[22] Se dock avsnitt 2.1.1. om att myndigheter tolkar begreppet olika. Den oöverensstämmande tillämpningen kan dock inte tolkas som att betydande skillnader råder. Det handlar främst om statistikdata som i och för sig kan tolkas ske på myndighetens beställning. Än så länge har ingen, inbegripet lagstiftaren, ansett att exempelvis teknisk support som inte direkt härleds driften ska anses omfattas av begreppet.

[23] Prop. 2022/23:97 s. 11 f., Prop. 2019/20:201, SOU 2021:97

[24] HFD 2019:24, RÅ 1992 ref. 63, RÅ 1996 ref. 19. Det är svårt att applicera resonemangen i en digital infrastruktur, åtgärder som anses behövas för att tillhandahålla en infrastruktur som definitivt omfattar mer än teknisk bearbetning och teknisk lagring (vilket är det vanligaste, särskilt för stora tjänsteleverantörer) får anses utgöra en gråzon, då lagstiftaren ändå hänvisar till tidigare (i detta sammanhang snäva) tolkningarna borde myndigheterna gör detsamma, dvs. endast medge åtgärder som uteslutande är nödvändiga för att tillhandahålla just den tekniska bearbetningen och tekniska lagringen. I realiteten medför en sådan tolkning av säkerhetsåtgärder som vidtas på en infrastruktur som omfattar mer, inte kan anses utgöra teknisk bearbetning och teknisk lagring. I praktiken kommer åtgärder som vidtas hos leverantörer av mer omfattande infrastruktur oftast falla utanför tillämpningsområdet.

[25] Prop. 2022/23:97 s. 17

[26] Lagkommentaren Juno (E. Lenberg, A Tansjö, U. Geijer, v. 30, 2024-12-11) 10 kap 2 a § OSL.

[27] Prop. 2022/23:97 s. 12 f.

[28] Prop. 2022/23:97 s. 17

[29] Försök har tidigare gjort att säkerställa rättsutredningar från kommuner som öppet argumenterat för omfattande utkontraktering av sekretessdata till amerikanska molntjänstleverantörer (exempelvis Uddevalla kommun), ingen nämnvärd rättsutredning har kunnat presenterats.

[30] Viktigt att notera var att detta mål prövades före adekvansbeslutet.

[31] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/schrems-ii-domen-overforingar-till-tredje-land/

[32] Kompletterande skyddsåtgärder kan vara avtalsrättsliga, organisatoriska eller tekniska. I fallet då nationell lagstiftning överordnas avtal och organisatoriska åtgärder, återstår endast tekniska åtgärder.

[33] Dvs. att hålla data krypterad på klientsidan med utgångspunkt att tjänsten ska kunna lagra, överföra men leverantören ska inte kunna läsa. Leverantören ska även saknas åtkomst till krypteringsnycklar.

[34] Dagens datum 2025-05-01, endast kommuner beträffande SaaS.

Teknisk kravinsamling

4. Teknisk kravinsamling

I den juridiska redogörelsen framkommer att en extern molntjänstleverantör kan hantera sekretessbelagd information utan att bryta mot OSL. Det kan dels handla om situationer då uppgifterna aldrig ens är att betrakta som röjda, dels utgöra situationer där uppgifterna är att anse som röjda men att leverantören endast står för teknisk bearbetning eller teknisk lagring och har vidtagit adekvata åtgärder som medför att röjandet är tillåtet. En god utgångspunkt för båda situationerna är att myndigheten säkerställer att leverantören inte på egen hand får tillgång till den information som omfattas av sekretess. Detta kan exempelvis ske genom att införa robusta krypteringslösningar, kontrollera nyckelhanteringen samt säkerställa att eventuella bearbetningar av data sker under förhållanden som innebär att leverantören inte behandlar data i läsbart format.

Utifrån nyssnämnda förutsättningar har projektet identifierat fyra tekniska koncept; Hold Your Own Key (HYOK), Confidential Compute, Extern lagring med extern nyckelhantering och Decrypt on Demand. Beroende på hur tekniken används torde samtliga koncept kunna underlätta vid en lämplighetsbedömning om huruvida sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL är tillämplig. Utifrån vissa tekniska upplägg är det inte otänkbart att få till en lösning där myndigheter kan komma att bedöma att ingen sekretess ö.h.t. röjs för leverantören.

I det följande avses varje koncept presenteras mer utförligt och med fokus hur tekniken fungerar och vilka krav tekniken ställer.

4.1. Hold Your Own Key (HYOK)

Hold Your Own Key (HYOK, fritt översatt "behåll din egen nyckel") är en metod för kryptering där en organisation själv behåller fullständig kontroll över sina krypteringsnycklar. Nycklarna lämnar aldrig kundens egen miljö eller säkerhetsdomän, till skillnad från standardlösningar där molnleverantören hanterar eller har tillgång till nycklarna. All känslig information krypteras **innan** den skickas till molntjänsten och förblir krypterad under hela sin livscykel i molnet. **Dekryptering sker först när data åter är under kundens kontroll**, till exempel lokalt hos myndigheten. På detta vis kan **varken molnleverantören eller någon utomstående** dekryptera eller läsa innehållet, eftersom de saknar åtkomst till nycklarna. [35] HYOK-tekniken adresserar därmed behovet av maximal datasekretess – även om informationen lagras hos en extern leverantör kan endast kunden själv låsa upp den. Detta är särskilt betydelsefullt för organisationer med strikta säkerhetskrav, såsom offentliga myndigheter eller annan författningsreglerad verksamhet, där man kräver **absolut kontroll** över vem som får åtkomst till informationen.

4.1.1 Skillnaden mellan HYOK och BYOK

HYOK ska inte blandas ihop med det mer vanliga konceptet *Bring Your Own Key* (BYOK, "ta med din egen nyckel") som många molnleverantörer erbjuder idag. BYOK innebär att kunden själv genererar sin krypteringsnyckel och **sedan** tillhandahåller en kopia **av** nyckeln till molntjänsten för att använda i dekryptering av data. Det ger visserligen ökad kontroll jämfört med leverantörsgenererade nycklar, men nyckelmaterialet lagras fortfarande hos leverantören (t. ex. i molntjänstens nyckelvalv eller HSM). Leverantören – eller dess system – kan därmed i praktiken komma åt nyckeln eller använda den för att dekryptera data vid behov (exempelvis för att kunna indexera och söka i krypterat material. [36] I en HYOK-modell överlämnas aldrig nyckeln till leverantören. All kryptering och dekryptering sker istället under kundens egen kontroll, vilket eliminerar risken att leverantören får tillgång till klartextdata utanför kundens kontroll. Sammanfattningsvis anses BYOK vara mer smidigt att använda i molntjänster men erbjuder en väsentligen lägre säkerhetsnivå, medan HYOK ger maximal säkerhet men en **mer** krävande implementation och en mindre praktisk drift.

4.1.2 Fördelar med HYOK

- **Full nyckelkontroll och högre säkerhet:** Kunden behåller exklusiv kontroll över nycklarna, och molnleverantören har ingen teknisk möjlighet att dekryptera informationen. Detta minimerar risken för obehörig åtkomst till data och skyddar även mot att uppgifter utlämnas till tredje part utan kundens. [37]
- **Dataintegritet och isolering:** Eftersom data förblir krypterat i molnet kan eventuella intrång hos leverantören **inte exponera känslig information i klartext**. Kundens data är isolerad och förblir oanvändbar för angripare eller obehöriga även om de kommer över lagringsmediet.
- **Regulatorisk efterlevnad och suveränitet:** HYOK underlättar uppfyllandet av **strikta säkerhetsregler** och lagkrav, eftersom organisationen kan demonstrera full kontroll över sina krypteringsnycklar. Detta är särskilt värdefullt i sektorer med krav på datasuveränitet och sekretess (t. ex. offentlig sektor), där man måste säkerställa att ingen utomstående part kan få tillgång till skyddade uppgifter.
- **Flexibilitet i kryptografiska val:** Eftersom nyckelhanteringen ligger hos kunden kan organisationen själv bestämma över kryptografiska algoritmer, nyckellängder och andra säkerhetsparametrar som bäst möter behoven. Kunden är inte bunden till en specifik leverantörs nyckelhanteringssystem, vilket ger ökad kontroll beträffande hur data skyddas.

4.1.3 Utmaningar med HYOK

- **Hög komplexitet och extra infrastruktur:** Att införa HYOK är tekniskt mer **komplicerat**. Det kräver ofta att kunden sätter upp egen **säker nyckelinfrastruktur**, till exempel lokala hårdvarubaserade nyckelresurser som HSM:er (Hardware Security Modules).

Denna extra hantering medför både ökad administrativ overhead och nya potentiella sårbarheter (t. ex. risk för felkonfiguration eller fysisk åtkomst till egen hårdvara)

- **Kostnads- och resurskrävande:** En HYOK-lösning med egna HSM:er och tillhörande nyckelhantering kan vara **kostsam** att implementera och underhålla. Utgifter för specialiserad hårdvara, drift av nyckeltjänster och kompetensbehov tillkommer, vilket innebär att totalkostnaden ofta blir högre än för mer standardiserade lösningar.
- **Ansvar för nyckelsäkerhet:** All säkerhet vilar på att kunden skyddar sina nycklar. Om krypteringsnyckeln skulle komma bort, förstöras eller på annat sätt bli otillgänglig finns ingen möjlighet att återskapa data – information som krypterats under HYOK blir då **permanent oläslig**. (Detta är samma risk som vid BYOK, men i en HYOK-modell finns ingen leverantör som kan erbjuda backup eller återställning av nyckeln åt kunden.)
- **Begränsad molnfunktionalitet och prestanda:** En nackdel med att molnleverantören inte kan dekryptera data är att vissa **inbyggda funktioner i molntjänster** går förlorade eller försämras. Till exempel kan man ofta **inte använda sökning, indexering eller molnbaserat samarbete** på krypterat innehåll när HYOK används. [38] Dessutom kan prestandan påverkas, eftersom all kryptering/dekryptering måste ske på klientsidan eller i kundens miljö, vilket kan ge fördröjningar och ökad komplexitet i användningen.

4.1.4 Påverkan på Säker digital kommunikation

- **Strikt spårbarhet:** Inkomna SDK-meddelanden dekrypteras inte förrän en specifik fysisk användare har begärt det. Varje gång nyckelhanteringstjänsten bryter en SDK meddelandekryptering loggar nyckelhanteringstjänsten denna operation på sådant sätt att tidpunkt, initierande fysisk användare och vilket meddelande som dekrypterats tydligt framgår, och på sådant sätt att meddelandetjänsteleverantören inte kan påverka denna logg. Nackdelen med detta sätt är att meddelandetjänsten kan initiera dekryptering utan att en användare faktiskt begärt det, fördelen är att en sådan överträdelse tydligt går att verifiera i loggarna utan påverkansmöjlighet för meddelandetjänstleverantören.

4.2. Confidential Compute

4.2.1. Vad är Confidential Compute?

Confidential Compute är ett samlingsnamn för tekniker som gör det möjligt att skydda data även medan den bearbetas i processorn (“data-in-use”). I stället för att dekryptera informationen i systemets vanliga minne skapas en Trusted Execution Environment (TEE) – ofta kallad enklav – där både kod och data är isolerade och krypterade i hårdvara. Endast den skyddade processen själv kan läsa klartext; allt annat – hypervisor, operativsystem, administratörer och angripare med root-åtkomst – ser enbart krypterad information. (Azure confidential computing Overview - Learn Microsoft, Trusted execution environment)

I praktiken bygger dagens konfidentiella miljöer på specialiserade CPU-funktioner, t. ex.:

Leverantör	Teknik	Kort beskrivning
Intel	**TDX** (Trust Domain Extensions)	Isolerar hela virtuella maskiner i "Trust Domains" där minnet krypteras och valideras vid varje access.
AMD	**SEV-SNP** (Secure Encrypted Virtualization – Secure Nested Paging)	Krypterar gästens minne med en unik nyckel per VM och verifierar sidtabeller för att förhindra manipulation.
Arm	**CCA** (Confidential Compute Architecture)	Tillhandahåller hårdvaruenklaver i server-CPU:er med attestation av körande mjukvara.

Processen att skapa en enklav omfattar **attestation** – kryptografisk bevisning av att rätt kod körs – vilket gör det möjligt för externa parter att kontrollera förtroendet innan känslig data laddas in.

4.2.2. Hur fungerar Confidential compute?

- **Enklav-teknologi:** Applikationen körs i en isolerad minnesregion som skapas och skyddas direkt av CPU:n. Ingen annan process – inte ens hypervisorn – kan läsa innehållet.
- **Hårdvarustöd:** Funktionen kräver processorer som exponerar TEE-instruktionsuppsättningar (Intel TDX, AMD SEV-SNP, Arm CCA m.fl.).
- **Fjärrattestation:** Innan data skickas till enklaven verifierar avsändaren nyckelhashen av den exakta mjukvarubinär som körs. Detta ger bevis för att miljön är oförändrad och inte kompromitterad.

4.2.3. Varför är Confidential Compute viktigt?

- **Fullständig kryptering genom hela livscykeln:** Data förblir krypterad i vila, under transport **och under beräkning**, vilket drastiskt minskar angreppsytan för minnesdumpning eller sidkanalsattacker
- **Tydlig sekretessgräns:** Driftpersonal hos molnleverantören får aldrig tillgång till klartext, vilket klargör att leverantören enbart utför *teknisk hantering* av krypterad payload. Därmed stärks den juridiska argumentationen att ingen obehörig åtkomst sker.
- **Regelefterlevnad och datasuveränitet:** Tekniken har framförts som ett sätt att möta europeiska regelverk (GDPR, Data Act, DORA) där *data-in-use-skydd* anses central för laglig internationell behandling av känsliga uppgifter.

- **Samarbete över domäner:** Flera parter kan dela och analysera sekretessbelagd data i gemensamma moln¬miljöer utan att avslöja rådata för varandra (“privacy-preserving analytics”).

4.2.4. Alternativ: Fysiskt kontrollerad serverkapacitet med kundägd kryptering

I scenarier där TEE-stöd saknas eller där högsta möjliga kontroll krävs kan motsvarande skyddsnivå uppnås genom egen fysisk kontroll av servrarna kombinerad med **Hold Your Own Key (HYOK):**

	Fördel	Nackdel
Egen eller dedikerad hårdvara (colocation)	Total isolering – leverantören saknar både fysisk och logisk åtkomst när diskar och minne krypteras med nycklar som endast myndigheten besitter.	Hög investerings- och driftkostnad; begränsad elasticitet jämfört med moln.

Denna modell är väl beprövad men är mindre skalbar och ger inte samma flexibilitet som moderna molntjänster med Confidential Compute, där man kan kombinera molnets kapacitet med en TEE-baserad sekretessgaranti.

4.3. Extern lagring med Hold your own key

Genom att separera kundens data från själva programvaran skapas en säkerhetsarkitektur som stärker både systemets verifierbarhet och skyddet av känslig information.

4.3.1. Separering av kunddata från mjukvarukonfiguration

För att uppnå högsta säkerhet och integritet måste kunddata hållas åtskild från applikationens konfiguration och mjukvara. Om flera datatyper samlagras på en och samma disk – exempelvis att programfiler, konfigurationsfiler och kundens data blandas – undermineras systemets verifierbarhet. Anledningen är att det då blir omöjligt att kryptografiskt verifiera att rätt programversion körs, eftersom diskens innehåll ständigt förändras av kundspecifika data. Utan en konsekvent och oföränderlig programavbild går det inte att ta fram en referenshash eller signatur för mjukvaran, vilket i sin tur omöjliggör tillförlitlig maskinidentifiering (det går inte kryptografiskt bekräfta att en given maskin kör oförändrad, godkänd kod). Ur säkerhetssynpunkt innebär detta en oacceptabel osäkerhet – systemägare kan inte lita på att plattformen är oförändrad och fri från manipulering när kunddata och kod ligger sammanblandade. Sammanfattningsvis är strikt separering en grundförutsättning för att uppnå både hög säkerhet och verifierbarhet i miljön.

4.3.2. Lösningsdesign: statisk programdel och extern kunddata

Den föreslagna lösningen baseras på att applikationen delas upp i två distinkta delar för att hantera ovanstående problem:

- **Statisk programdel** (kodbas utan kundspecifik information):
  Denna del består av mjukvarans körbara kod och standardkonfiguration som inte innehåller någon kunddata. Den statiska delen paketeras typiskt som en oföränderlig diskavbild (eng. *image*) eller firmware-liknande enhet. Eftersom innehållet är statiskt och gemensamt för alla installationer kan denna programavbild enkelt hashas och signeras som referensversion. Ingen kundunik konfiguration skrivs här, vilket gör att dess innehåll förblir konstant över tid.
- **Extern data- och konfigurationsdel (kundens data på extern lagring):**
  All kunddata och all kundspecifik konfiguration lagras separat, utanför den statiska programavbilden. Denna del kan till exempel utgöras av en krypterad databasmapp, ett separat datadiskvolym eller annat lagringsutrymme som laddas in vid uppstart av systemet. Kritisk är att denna lagringsenhet endast innehåller kundens informationsinnehåll (databaser, filer, inställningar specifika för kunden) och ingen körbar programkod. Vid systemstart kopplas den externa lagringen till applikationen, men fram till dess är den logiskt skild från programvaran.

Genom denna uppdelning uppnås en tydlig gräns mellan å ena sidan oföränderlig kod och å andra sidan föränderliga data. Applikationen kan i drift fungera exakt som tidigare, men under ytan har arkitekturen omformats så att all persistent kundinformation ligger externt. Detta medför att uppgraderingar eller patchning av mjukvaran kan ske oberoende av kunddata, och mer väsentligt: den statiska programdelen kan behandlas som en *betrodd referens* utan att kundens konfidentiella data riskerar att kompromitteras i processen.

4.3.3. Arkitektur och säkerhetsmodell

Den beskrivna uppdelningen möjliggör en appliance-liknande säkerhetsmodell. Precis som när en fysisk säkerhetsappliance levereras med ett fast programvarubibliotek som verifieras via en hash-summa eller digital signatur, kan den statiska programavbilden kontrolleras kryptografiskt. Varje gång systemet startar går det jämföra diskavbildens hashvärde mot en känd referens. På så sätt valideras att rätt kod (och rätt version) körs och att ingen obehörig förändring skett. Sådan verifiering skapar en tillförlitlig grund för maskinidentifiering och systemtillit – det går att säkerställa att den instans som kör applikationen är autentisk och oförändrad eftersom dess programvara matchar referensen.

Det är viktigt att understryka att denna arkitektur förutsätter *Hold Your Own Key* (HYOK) för hantering av kunddata. I praktiken betyder det att kundens data i den externa lagringsdelen hålls krypterad och endast görs tillgänglig efter explicit autentisering och nyckelinjektion av kunden. När den statiska programdelen startar har den inledningsvis inte tillgång till någon kunddata – den kan enbart läsa in kundinformationen om och när kunden (eller dennes nyckelhanteringssystem) tillhandahåller rätt dekrypteringsnyckel efter uppstart.

Detta designmönster garanterar att om någon skulle få åtkomst till eller kopiera den statiska programavbilden, så förblir kundens information oåtkomlig utan nyckeln. Samtidigt kan diskavbilden fritt distribueras eller kontrolleras (t. ex. via hash) utan risk för läckage av känsligdata, eftersom ingen kundinformation förvaras på det stället, innan nyckeln injicerats.

Hela säkerhetsmodellen sätts ur spel om data blandas på samma disk. Om kunddata förvarats okrypterad tillsammans med programfilerna föreligger omständigheter att antingen systemet skulle behöva starta med data olåst (vilket strider mot HYOK och exponerar informationen), eller så skulle programavbilden inte kunna valideras separat (eftersom dess hash då ständigt ändras när datan ändras). I båda situationer går den avgörande tillit och kontroll som modellen säkerställer, förlorad. Av denna anledning är konceptet med extern lagring under HYOK centralt, inte minst för offentliga aktörer och myndigheter som behöver kunna styrka datasuveränitet och sekretess.

Genom HYOK behåller organisationen full kontroll över krypteringsnycklarna och därmed sin data, vilket garanterar att ingen utomstående – varken molnleverantör eller obehörig part – kan ta del av informationen. [39] Myndigheter kan därmed uppfylla strikta regulatoriska krav och bevisa att deras data förblir under inhemsk kontroll och är åtkomlig endast för behöriga, till följd av att kunden själv kontrollerar nyckeln. [40] Detta arkitekturella grepp, i kombination med möjligheten att kryptografiskt attestera programvarans integritet, ger en lösning där både kod och data kan säkras fullt ut – en nödvändighet för miljöer med höga krav på säkerhet och efterlevnad.

4.4. Decrypt on Demand

4.4.1. Vad innebär Decrypt on Demand?

Decrypt on Demand betyder att meddelanden eller filer är krypterade i och med att den mottagande parten (eller i tillämpliga fall avsändaren) aktivt måste initiera en dekrypteringsprocess för att kunna läsa innehållet. Fram till att dekrypteringen är initierad är informationen i ett helt oåtkomligt skick, inklusive för leverantören.

- **Användarinitierad dekryptering:** I praktiken innebär det att mottagaren klickar på “Öppna” eller motsvarande, varpå systemet använder en hemlig nyckel (som mottagaren kontrollerar) för att dekryptera informationen (se avsnittet om HYOK för mer information om nyckelhanteringen).
- **Tydlig spårbarhet:** Varje dekrypteringshändelse loggas med information om vad som dekrypterats och vem som initierat dekrypteringen, vilket tydliggör ansvarsfördelningen.

4.4.2. Varför är Decrypt on Demand viktigt?

- **Juridisk tydlighet:** Skapar en distinkt gräns för när krypteringen bryts och en uppgift faktiskt är "röjd" (se analogin med ett oöppnat brev). Oavsett myndighetens bedömning av röjande svarar lösningen mot avvägningarna i lämplighetsbedömningen för när sekretessbrytande bestämmelse kan tillämpas.
- **Reducerad risk:** Även om någon obehörig får tag på en krypterad fil, kan den inte läsas utan rätt nyckel.
- **Kontroll för slutanvändaren:** Användaren bestämmer exakt när innehållet ska vara läsbart, vilket minimerar fönstret för potentiell dataläcka.

4.4.3. Tekniska krav för Decrypt on Demand

- **Tydlig interaktionsdesign:** Användare måste förstå när data är krypterad och när de aktivt dekrypterar.
- **Omfattande loggning:** Varje dekrypteringstillfälle ska loggas, åtminstone inkluderande vem som initierat dekryptering, när det skedde och vad som dekrypterats (förslagsvis genom en hash/kondensat av den krypterade informationen).

[35] regeringen.se

[36] forsakringskassan.se – Vitbok, bilaga 7
https://www.forsakringskassan.se/download/18.7b234aa517b3a0b7f3734e/1629891143456/vitbok.pdf

[37] forsakringskassan.se – Vitbok. bilaga 7
https://www.forsakringskassan.se/download/18.7b234aa517b3a0b7f3734e/1629891143456/vitbok.pdf

[38] forsakringskassan.se

[39] complior.se

[40] complior.se

Säker digital kommunikation, Meddelande-klient och meddelande-tjänst

5. Säker digital kommunikation, Meddelandeklient och meddelande-tjänst

Ovanstående rättsliga frågeställningar och redogjorda tekniska lösningar kan med fördel utmynna i en förändring i Digg:s regelverk kopplat till SDK. Detta med syfte att minimera riskerna för att tilliten för infrastrukturen ska rubbas.

I ovan tekniska beskrivning beaktas inte separerad meddelandeklient och meddelandetjänst. Sådant tekniskt upplägg inverkar framförallt på HYOK och Decrypt on Demand. Därför beskrivs i det följande projektets sammanfattande rekommendationer för meddelandeklientens och meddelandetjänstens roller med dessa utökade säkerhetskrav, samt ett förslag på utbyggnad av API:et.

Decrypt on Demand och HYOK har inverkan på relationen meddelandetjänst-meddelandeklient, liksom det API som finns mellan dessa, eftersom vi behöver specificera var meddelandedekryptering sker och vem/vilka systemkomponenter som har möjlighet att initiera dekryptering. Som nämns i avsnittet om HYOK har varken meddelandetjänst eller meddelandeklient tillgång till den privata O2O-nyckeln för dekryptering av meddelanden, men det är relevant att säkerställa ansvarsfördelningen vad gäller dekrypteringen och lagringen av den dekrypterade informationen.

Observera att rollfördelningen som uttrycks nedan är designrekommendationer snarare än krav för meddelandeklient respektive meddelandetjänst. Eftersom de flesta lösningar som används idag består av meddelandetjänst och meddelandeklient tillsammans skulle eventuella sådana krav ha liten praktisk betydelse, i alla fall i dagsläget.

Eftersom det primära syftet med föreslagen ändring är att öka tilliten hos avsändande organisation handlar de utökade kraven om mottagande av meddelanden (snarare än om att skicka meddelanden). Nedan beskrivs alltså bara meddelandetjänstens och meddelandeklientens roll vid mottagande av meddelanden, och de API-förändringar som skissen gäller läsning av inkommande meddelanden. Decrypt-on-demand innehåller inga förändringar vad gäller roller och API:er beträffande att skicka meddelanden.

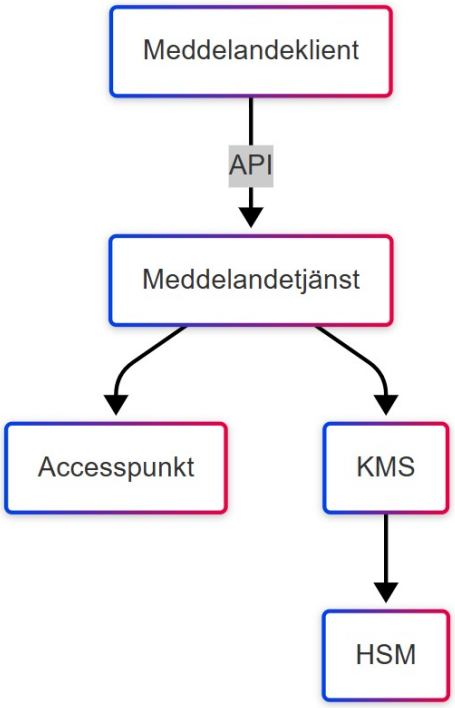
5.1. Meddelandeklientens roll

Meddelandeklientens roll för inkommande meddelanden är att hantera dessa meddelanden efter att de dekrypterats. Meddelandeklienten rekommenderas inte kunna initiera dekryptering.

5.2. Meddelandetjänstens roll

Meddelandetjänstens roll är att lagra inkommande krypterade meddelanden och att initiera dekryptering på meddelandeklientens begäran. Det rekommenderas att meddelandetjänsten inte sparar den dekrypterade informationen. Detta för att den känsliga informationen inte ska finnas på flera ställen.

Relationen mellan meddelandetjänst, meddelandeklient och dekrypteringsinfrastrukturen åskådliggörs i figur 1 nedan.



Figur 1.
Relation mellan meddelandetjänst, meddelandeklient och dekrypteringsinfrastrukturen.

5.3. API-förändringar

Tyngdpunkten i rapporten, beträffande SDK, ligger på de krav om säkerhet och krav om flöde som, av projektet, bedömts nödvändiga för att bibehålla tillit för SDK hos våra mer säkerhetsmedvetna myndigheter. Eftersom projektet föreslår förändringar/förtydliganden i relation mellan meddelandeklient och meddelandetjänst lämnas förslag på hur ändringarna kan se ut i praktiken. Notera att syftet från projektets sida inte är att det behöver se ut just på detta sätt. Syftet är snarare att ändringarna tar höjd för principen om *Decrypt on Demand*.

Nedan följer förslag som skulle uppfylla kraven på *Decrypt on Demand*.

Ett exempel på något som kan behöva förfinas är i vilken utsträckning man ändrar i befintliga API:er. Projektet föreslår att man för API 2.0 lägger till endpoint *encrypted-messages* med två metoder, samtidigt som man tar bort två befintliga metoder från *messages*.

5.4. 1.0 och 2.0

I detta dokument definieras API version 1.0 som den version som finns och används av SDK:s aktörer idag, medan 2.0 är API:et inklusive de API-förändringar som föreslås här.

5.5. Autentisering/auktorisation

Eftersom autentisering/auktorisation av meddelandeklient till meddelandetjänst inte regleras i API-specifikationen i SDK förutom en rekommendation att *OAuth Client Credentials flow* [41] utökas denna med ett krav på att meddelandeklienten i auktorisatonsprocessen tilldelas ett *claim* som reglerar huruvida API 1.0 eller API 2.0 ska användas. Exakt hur det görs kommer vara upp till meddelandeklient och meddelandetjänst, eftersom autentisering och auktorisation i sig inte regleras.
En sådan *claim* är nödvändig för säkerheten i helhetslösningen, eftersom det gör att en meddelandeklient inte på eget bevåg kan “nedgradera” säkerheten från ”den högre nivån” till ”den lägre” dvs. ändra lösningen så att *Decrypt on Demand* inte längre tillämpas.

5.6. Tillagda endpoints i API 2.0

Tillägg: PUT /v1/sdk/encrypted-messages

Ny endpoint som tar ett krypterat meddelande i sin helhet och returnerar ett dekrypterat. Denna endpoint ska alltså i sin tur anropa KMS för att utföra själva dekrypteringen (vilket i sin tur leder till spårbar loggning av dekrypteringen).

Rekommendationen är att det dekrypterade meddelandet inte sparas i meddelandetjänsten.

Parametrar i anropets *body*:

- *user*: Den fysiska användare som initierar anropet (skickas till loggning i KMS).
- *encrypted-message*: Det meddelande som ska dekrypteras.
- *message-id*: Meddelande-ID för meddelandet som ska dekrypteras.

Meddelandetjänst verifierar att krypterade *payloaden* är korrekt, dvs motsvarar krypterad *payload* för meddelandet med det meddelande-ID och auktoriserar meddelandeklienten för just den *endpoint*. I den mån det finns auktorisation kopplad till fysisk användare i detta steg görs även detta. Därefter anropas KMS för dekryptering, se avsnitt om HYOK.

Tillägg: GET /v1/sdk/encrypted-messages[filter]

En kopia av API 1.0 /v1/sdk/messages[filter], men med filter *createDateTimeStart/ creationDateTimeStop* som enda tillåtna filter, eftersom dessa är de enda sökkriterier som kan evalueras utan att bryta meddelandenas kryptering. Notera att *endpoint* måste returerna meddelanden med obruten kryptering. Denna begränsade meddelandesökning försämrar möjligheten till sökvyer för meddelanden som ännu inte har öppnats, men en förutsättning för *Decrypt on Demand* är att meddelanden inte dekrypteras innan de ska visas för användaren, och det medför att sådana sökvyer inte kan aktualiseras för olästa meddelanden. Efterfrågas sökvyer över meddelanden kan dessa tillgodoses inom meddelandeklienten med redan öppnade meddelanden.

5.7. Borttagna endpoints i API 2.0

Utgår: GET /v1/sdk/messages[filter]

Returnerar okrypterat data, och sökfiltren (förutom *CreationDate*) kräver åtkomst till okrypterat data för att kunna realiseras. Det bör betraktas som en rekommendation snarare än ett krav att meddelandetjänsten inte sparar dekrypterade meddelanden. Om en organisation inte följer rekommendationen och sparar redan dektrypterade meddelanden så kan organisationen tänka sig att ha kvar dessa filter och då visa redan dekrypterade meddelanden, men det får anses vara ett *randfall*. Annars bör denna *endpoint* returnera *"501 not implemented"* i API 2.0

Utgår: GET /v1/sdk/messages/{id}

Projektet bedömer att det behövs en *endpoint* som explicit dekrypterar (PUT /v1/sdk/ encrypted-messages) för att säkerställa *Decrypt on Demand*, snarare än en *GET-endpoint* som bara returnerar okrypterat data. Därför utgår denna enligt projektets förslag.

5.8. Att uppdatera från 1.0 till 2.0

Följande information bör betraktas som rekommendationer snarare än förslag till nya krav.

I nuläget finns ett API mellan meddelandeklient och meddelandetjänst som används av ett antal organisationer. Nedan finns därför en lista med aktiviteter för att gå från en 1.0-tjänst till en 2.0-tjänst, samt för den offentliga organisationen att säkerställa att SaaS-meddelandetjänsten använder *Decrypt on Demand* och *HYOK*.

Federationsoperatör

- Utöka den befintliga verifieringstjänsten för befintligt API för att även omfatta det nya.

Meddelandetjänstleverantör

- Implementera API enligt skiss ovan (API behöver specificeras tydligare av Digg eller annan aktör).

Meddelandeklientleverantör

- Testa och verifiera att meddelandeklienten kan utföra sina uppgifter med de nya *endpoints* som beskrivs ovan.
- Om meddelandeklienten förlitar sig på sökningar bland meddelanden som ännu inte öppnats behövs nytt UX.

Medlemsorganisation

- Säkerställ att leverantör av meddelandetjänst och samtliga leverantörer av meddelandeklient är medvetna om förändringarna i API 2.0.
- Säkerställ att meddelandetjänst har stöd för API 2.0 och att stödet aktiveras.
- Säkerställ att auktoriseringen av meddelandeklient tvingar in samtliga klienter att använda 2.0.
- Testa och verifiera att önskad funktionalitet finns.

5.9. Adapter för Decrypt on Demand

För en organisation som önskar implementera *Decrypt on Demand*, men är tvingad att stödja API 1.0 (exempelvis på grund av gammal meddelandeklient) redovisas en gångbar ”mellanväg”. Det går att utveckla en adapter, en översättare mellan API 2.0 och API 1.0. Det innebär att meddelandeklienten fortsätter att kommunicera med API 1.0 och adaptern översätter anropen till API 2.0 och skickar vidare till meddelandetjänsten. Eftersom skillnaden mellan API 1.0 och API 2.0 är att meddelandena dekrypteras i förväg i API 1.0 så måste adaptern som dekrypterar meddelandena vara on-prem, liksom datalagret som sparar meddelandena (oavsett om meddelandena sparas krypterat eller dekreterat, eftersom meddelandekryptering är bruten oavsett). Att skapa en sådan, förhållandevis liten, adapter med datalager on-prem skulle kunna utgöra en lösning för att nå följsamhet mot *Decrypt on Demand* även om man har kvar meddelandeklienter som tillämpar API 1.0.

5.10. Fördelarna med SDK 2.0

SDK 2.0 ger en tydligt förstärkt sekretesskedja. En ny *endpoint* **PUT /encrypted-messages** innebär att varje dekryptering alltid initieras av klienten och samtidigt loggas i myndighetens eget KMS. Meddelandetjänsten lagrar därmed enbart krypterad *payload* och behöver aldrig hantera klartext, vilket eliminerar ett viktigt angreppsfönster.

Samtidigt skapar lösningen en klar roll- och ansvarsfördelning: klienten ansvarar för samtliga läsbara data, medan meddelandetjänsten enbart hanterar lagring och nyckelanrop mot KMS. Ingen systemkomponent kan ”tjuvläsa” informationen utan att det omedelbart syns i revisionsloggarna.

För de organisationer som ännu kör **API 1.0** finns en framåtkompatibel väg – en on-prem-adapter kan översätta anropen till 2.0 och därmed uppfylla *Decrypt on Demand* utan att klienterna behöver uppgraderas omedelbart. Ett särskilt *OAuth-claim* markerar dessutom om en klient arbetar mot version 1.0 eller 2.0, vilket hindrar avsiktliga eller oavsiktliga ”nedgraderingar” till ett mindre säkert arbetsflöde.

Det nya APIet exponerar tydliga händelser som ***”message* decrypted”**. Dessa kan användas för att automatisera exempelvis e-arkivering, ärende¬start eller DLP-controller – allt utan att störa krypterings¬modellen.

Tillsammans med *HYOK*, *Confidential Compute*, lagring med extern nyckelhantering och *Decrypt on Demand* skapar SDK 2.0 ett flerlagers skydd: data är krypterad i vila, under transport och under körning; varje åtkomst är spårbar i realtid; myndigheten behåller molnets skalbarhet utan att förlora kontrollen på nycklar eller kontroll över leverantörens åtkomster av information i klartext; och leverantören utför endast teknisk bearbetning eller lagring av krypterad information, något som underlättar bedömningen enligt 10 kap. 2 a § OSL. Sammanfattningsvis blir SDK 2.0 den samlande mekanismen som gör de fyra säkerhetskoncepten praktiskt användbara och ger offentliga aktörer ett robust, framtidssäkert ramverk för säker digital kommunikation i molnet.

[41] https://www.digg.se/saker-digital-kommunikation/sdk-for-leverantorer-av-meddelandesystem/tekniska-beskrivningar/apier-for-sdk/sdk-api-mt-mk/rekommendation-api-mt-mk

Ekonomiska avvägningar

6. Ekonomiska avvägningar

Även om tekniska lösningar som *HYOK, Confidential Compute*, lagring med extern nyckelhantering samt *Decrypt on Demand* kan stärka säkerheten och underlätta regelefterlevnad, uppstår sannolikt frågor hos kunden gällande ekonomiska avvägningar. Det kan antas att mindre kommuner eller mindre statliga myndigheter måste ta ställning till hur de kan motivera kostnader för infrastruktur, mjukvarulicenser och nödvändig kompetens.

Nedan följer en översikt av centrala kostnadsdrivare och förslag på hur dessa kan hanteras:

6.1. Kostnadsdrivare för respektive teknik

6.1.1. Hold Your Own Key (HYOK)

- **Nyckelhanteringsinfrastruktur:** *Hardware Security Modules* (HSM:er) eller motsvarande säkra nyckellager kan vara dyra både i inköp och underhåll.
- **Kompetenskrav:** Kräver personal eller konsulter med specialistkunskap inom krypteringsarkitektur och incidenthantering.
- **Skalbarhet:** Kan vara enklare för större aktörer men relativt kostsamt för mindre organisationer som behöver investera i robust infrastruktur ändå.

6.1.2. Confidential Compute

- **Specialiserad hårdvara:** Kräver CPU-stöd (t.ex. Intel SGX, AMD SEV). Detta kan innebära uppgradering av befintlig serverpark eller att välja specifika molnleverantörer som erbjuder "*confidential compute*"-kluster.
- **Licens- och mjukvarukostnader:** Programvara måste vara anpassad för att dra nytta av *enklaver*. Licensmodeller kan skifta och ibland innebära en ökad kostnad.
- **Implementationstid och utbildning:** För att fullt ut nyttja tekniken behöver systemdesign, applikationer och processer anpassas, vilket kan kräva omfattande resurser.

6.1.3. Lagring med extern nyckelhantering

- **Molnlagringskostnader:** Priset för själva lagringen (pris per GB) samt eventuella avgifter för bandbredd, API-anrop och dataåterhämtning (*egress*).
- **Externa KMS-tjänster:** Använder man en extern *Key Management Service* kan det tillkomma separata avgifter för nyckeloperationer, beroende på volym.
- **Integration och övervakning:** System för Identity and Access Management (IAM), loggning och nyckelrevision behöver sättas upp och övervakas kontinuerligt.

6.1.4. Decrypt on Demand

- **Utvecklings- och licenskostnader:** Implementering av logik som möjliggör "*on-demand*"-kryptering/dekryptering kan kräva anpassade programvarulösningar eller integrationer med e-tjänster.
- **Brukarperspektiv:** Varje användare behöver kunna initiera kryptering och dekryptering. Det kan medföra viss supportbörda, utbildningsinsatser och extra tester.
- **Drift och loggning:** Ytterligare loggningskapacitet krävs för att spåra samtliga dekrypteringshändelser, vilket i sin tur kan öka kostnader för datalagring och analys.

Samman-fattning

7. Sammanfattning

Den juridiska analysen tydliggör att OSL och GDPR tillåter en viss form av extern hantering av sekretessbelagd information – förutsatt att leverantören inte får allt för omfattande åtkomster och friheter, något som kan aktualiseras är leverantörens möjligheter att komma åt innehållet i klartext.

De fyra tekniska koncept som lyfts fram (*HYOK, Confidential Compute*, objektbaserad lagring med extern nyckelhantering och *Decrypt on Demand*) representerar olika verktyg för att uppnå detta mål. Varje lösning angriper rättsliga problemet från varierande vinklar:

- **HYOK** säkerställer att nycklarna aldrig lämnar kundens kontroll.
- **Confidential Compute** krypterar data även under aktiv bearbetning, skyddad mot driftspersonal.
- **Lagring med extern nyckelhantering** skapar en kombination av enkel, skalbar objektlagring och fullständig kundkontroll över kryptering.
- **Decrypt on Demand** ger en tydlig juridisk gräns för när uppgifter anses "röjda".

Vid en korrekt teknisk tillämpning kan dessa tekniska lösningar drastiskt minska risken att leverantören får reell åtkomst till känsliga uppgifter, samt stärka regelefterlevnaden gentemot OSL, GDPR och annan informationslagstiftning. Samtidigt bevarar man flexibiliteten och kostnadseffektiviteten i att nyttja molnlösningar för verksamhetskritisk data inom offentlig sektor.

Projektet har identifierat **fyra kompletterande säkerhetskoncept** som, vid korrekt tillämpning, gör det möjligt för en myndighet att använda externa molntjänster utan att leverantören får reell åtkomst till sekretessbelagda uppgifter. Samtidigt har projektet analyserat **hur Säker Digital Kommunikation (SDK)** behöver uppdateras för att dra nytta av dessa tekniker på ett konsekvent och realistiskt sätt.

Byggblock	Kärnidé	Huvudnytta	Nytt krav på SDK 2.0
Hold Your Own Key (HYOK)	Nycklarna lämnar aldrig kundens domän; kryptering/ dekryptering sker i kundens HSM/ KMS.	Absolut kontroll över krypteringsnycklar, ingen klartext hos leverantören.	SDK måste kunna kalla ett externt KMS vid behov av dekryptering.
Confidential Compute	Data skyddas i CPU-enklaver (TEE) även under körning.	Klartext är osynlig för driftpersonal och angripare med root-privilegier.	SDK-komponenter som processar data i moln-VM:er bör kunna köras i TEE-aktiverade instanser.
Lagring med extern nyckelhantering	Objekt (filer) lagras i skalbara buckets; nycklar hålls i kundägd KMS.	Molnlagringens elasticitet utan att molnet kan dekryptera data.	SDK bör lagra bilagor i objektlagring men hämta dekrypterings-nycklar via HYOK-gränssnitt.
Decrypt on Demand	Inkommande meddelanden öppnas först när mottagaren aktivt begär det.	Tydlig gräns för **när** information klassas som ”röjd”, minimal attackyta.	SDK behöver ett API där klienten explict begär dekryptering och får audit-logg som kvitto.

SDK 2.0 föreslår en strikt rolluppdelning där meddelandeklienten endast ser klartext efter att den själv begärt dekryptering, medan meddelandetjänsten lagrar och transporterar data uteslutande i krypterad form. Detta förverkligas via *Decrypt on Demand* och *HYOK-stödd* nyckelhantering som loggar varje dekrypteringshändelse i kundens KMS.
Ett nytt API 2.0 (med de två *endpoints* **PUT/GET encrypted-messages**) ersätter äldre anrop som returnerar okrypterat innehåll; ett *OAuth-claim* förhindrar nedgradering till API 1.0 och en on-prem-adapter erbjuder bakåtkompatibilitet för äldre klienter. Tillsammans med *Confidential Compute* och extern objektlagring skapas ett ”flerlagrigt” skydd som eliminerar klartext hos leverantören, ger full spårbarhet och minska risken för juridisk motsättningar utifrån 10 kap 2 a § OSL.

Kostnadsanalysen visar att den största utgiften omfattar *HSM-infrastruktur* för *HYOK* och *TEE-hårdvara* för *Confidential Compute*, följt av integration med extern *KMS* och detaljlogg för *Decrypt on Demand*.

Mindre myndigheter kan mildra investeringen genom delad *HSM*-tjänst, successiv migrering till *TEE-kluster* och gemensam kompetens-pool. De samlade drift- och utvecklingskostnaderna måste ställas mot minskade risker för sanktioner och förtroendeskada; kalkylen pekar på att de föreslagna åtgärderna är samhällsekonomiskt försvarbara när sekretessbelagd information ska hanteras som SaaS.

Rekommenda-tioner och fortsatt arbete

8. Rekommendationer och fortsatt arbete

Projektets utredning har visat att det sannolikt är både **juridiskt möjligt** och **tekniskt genomförbart** att leverera sekretessbelagd information som SaaS – förutsatt att lösningen vilar på fyra nyckelprinciper: *HYOK, Confidential Compute,* extern lagring med kundstyrd *KMS* och *Decrypt on Demand*. Samtidigt har utredningen identifierat väsentliga luckor i dagens regelverk för *Säker digital kommunikation* (SDK) och betydande kompetens- och kostnadsutmaningar hos flertalet myndigheter.

Syftet med detta kapitel är att **översätta rapportens slutsatser till konkreta nästa förslag till åtgärder** – både för Digg som ramverkshållare, leverantörer och upphandlande organisationer. Rekommendationerna är indelade i fyra fokusområden:

1. **Regelverkslyft för SDK** – hur Digg bör modernisera API-specifikation, certifieringskrav och tillsyn så att de fyra säkerhetskoncepten kan användas i praktiken.
2. **Produkt- och utvecklingskrav** – hur systemleverantörer bör implementera *Decrypt on Demand, HYOK-stöd* och *TEE-drift* för att nå ”zero-knowledge”.
3. **Upphandlingsstöd och kompetens** – hur offentliga köpare kan använda den medföljande checklistan för att ställa rätt krav och dela kostnader.
4. **Revision och incidenthantering** – hur hela federationen behöver bygga gemensamma processer för log¬granskning, nyckel¬spärr och CPU-sårbarheter.

Nedan följer de konkreta rekommendationerna inom respektive område.

Se över brister i SDK och tillsätt utredning för att arbeta vidare med rapportens förslag

Digg bör adressera de utmaningar som finns idag för att leverera SDK som en SaaS. Projketet rekommenderar att de koncept som presenteras i rapporten tillgodoses och att API uppdateras för att möjliggöra att informationen kan skickas krypterat i alla led.

Uppmuntra systemleverantörer att implementera *”Decrypt on Demand”* generellt vid all kommunikation med sekretessinformation

Metoden tydliggör vem som bär ansvaret vid varje dekryptering och ger en skarp gräns för när data anses ”röjd”. Rekommendera samtliga parter att implementera enhetliga rutiner för hur dekryptering initieras och loggas. Konceptet tydliggör när det juridiska ansvaret för en uppgift flyttas mellan organisationer vilket borde medföra enklare diskussioner framgent beträffande ansvarsförhållandet mellan organisationerna. Samtliga leverantörer som tillverkar system som utlämnar information mellan varandra bör utreda om denna funktionalitet kan implementeras i sina system för att tydliggöra informationshanteringen.

Uppmuntra organisationer som upphandlar system som hanterar sekretess att använda checklistan (i denna rapport) med krav för en leverantör att uppnå *”Zero-knowledge”*

Checklistan som finns i Bilaga A är tänkt att vara till hjälp för organisationer som vill upphandla system som följer de principer som projektet redovisar i denna rapport. Checklistan kan med fördel tillämpas i befintlig kravställning i t. ex. Addas *DIS* för *Säker digital kommunikation* eller som ett generellt stöd vid inköp av molntjänstleverantörer som hanterar sekretessinformation.. Checklistan är utformad så att aktörer inte ska diskvalificeras men att myndigheten samtidigt ska främja en god och säker datahantering med eftersträvan att *”Zero-Knowledge”* uppnås där leverantören inte har tillgång till kundens information.

Tydlig revisions- och incidenthantering

Federationens ramverk bör tydliggöra hur incidenter rapporteras, hur nycklar spärras vid misstänkt kompromettering och hur loggar snabbt kan revideras. Då *Confidential Compute* utgör en utgångspunkt, är det viktigt att även denna komponent omfattas av rutiner för t. ex. CPU-buggar eller sårbarheter i *”enclaves”*.

I en federerad miljö som SDK, där man ställer höga krav på sekretess, är det ännu viktigare att eliminera risken för att leverantören eller andra obehöriga får tillgång till klartextdata. *Decrypt on Demand* förtydligar när handlingar överlämnas utifrån ett juridiskt hänseende mellan organisationer, *Confidential Compute* bör ses som en obligatorisk komponent för att säkerställa att data förblir skyddad även vid drift eller avancerad bearbetning.

Bilagor

Bilaga A – Checklista upphandling

Nedan följer en sammanhållen checklista för upphandling som bygger på de tekniska och juridiska resonemang som presenterats i rapporten. Checklistan är framtagen för att säkerställa att SaaS-tjänster som används inom ramen för SDK-federationen uppfyller de krav på säkerhet och sekretess som OSL och GDPR ställer. Samtidigt möjliggör den en modulär ansats, i enlighet med de rekommendationer som diskuterats i tidigare kapitel:

- **Ska-krav** anger den miniminivå som varje leverantör måste uppfylla för att ingå i en SDK-federation på ett juridiskt säkert sätt.
- **Bör-krav** är starkt rekommenderade för att skapa en högre nivå av informationssäkerhet och transparens, men kan prioriteras olika beroende på verksamhetens storlek, risknivå och budget. För bör-krav anges även en viktning (hög/medel) för att tydliggöra dess betydelse i förhållande till andra rekommendationer.

Varje krav har en motivering som knyter an till de juridiska kraven (OSL, PDL, GDPR) och/eller SDK-federationens behov av tillit och spårbarhet. Tillsammans ger checklistan ett tydligt ramverk för hur upphandlande myndigheter och kommuner kan ställa krav på leverantörer kring nyckelhantering, kryptering, loggning, revision och datahantering inom EU/EES. På så sätt blir det enklare att uppnå en gemensam säkerhetsnivå och samtidigt ge utrymme för successiv upptrappning (till exempel genom att lägga till Confidential Compute eller Decrypt on Demand) när verksamhetens behov växer eller riskbilden förändras.

Nedan följer kravlistan i detalj. Varje krav innehåller:

- **Kravtext** och **kravtyp** (Ska eller Bör)
- En **beskrivning** av vad kravet innebär i praktiken
- En **motivering** som förklarar varför kravet är relevant
- Vid **Bör-krav** anges även ett förslag till **viktning** (hög eller medel) för att hjälpa upphandlande myndighet att prioritera rätt.

Nyckelhantering och Hold Your Own Key (HYOK)

Krav 1.1

- **Kravtext:** *Leverantören* ska möjliggöra en arkitektur där *upphandlande organisation* behåller full kontroll över huvudnycklar (Hold Your Own Key).
- **Typ: Ska**
- **Beskrivning:** SaaS-tjänsten ska erbjuda en lösning där kundens (myndighetens/kommunens) nycklar **inte** hanteras av leverantören. Detta kan inkludera integrering mot en extern KMS (Key Management Service) eller myndighetens egen HSM. Beskrivning hur detta sker ska medfölja kravställningen.
- **Motivering:** Säkerställer att leverantören inte får "tillgång i sak", vilket underlättar efterlevnad av OSL:s sekretessbrytande undantag. Det är viktigt att säkerställa att leverantören förklarar hur detta sker i upphandlingen så att ska kravet inte slentrianmässigt fylls i.

Krav 1.2

- **Kravtext:** *Leverantören* bör tillhandahålla dokumentation från KMS-/HSM-leverantör som säkerställer att nycklarna aldrig lämnar dessa.
- **Typ: Bör**
- **Viktning: Medel**
- **Beskrivning:** Tydlig spårbarhet i leverantörens plattform/loggsystem för att påvisa att inga nycklar hanteras utanför kundens eget KMS/HSM.
- **Motivering:** Underlättar revision och efterlevnadskontroll, skapar förtroende i SDK-federationen.

Krav 1.3

- **Kravtext:** Leverantören ska stödja lagring av objekt med möjlig integration mot extern KMS.
- **Typ: Ska**
- **Beskrivning:** Myndigheten ska kunna lagra data som objekt (exempelvis "buckets" eller "containers") och använda en extern nyckelserver/HSM för att kryptera varje objekt. Detta ger kunden full kontroll över nyckelhanteringen (HYOK).
- **Motivering:** Möjliggör en standardiserad och skalbar lagring, samtidigt som kundens nycklar hanteras separat (HYOK).

Kryptering och Confidential Compute

Krav 2.1

- **Kravtext:** Data ska vara krypterad *i vila och under transport* med branschstandarder (t. ex. TLS 1.2+ för transport, AES-256 för lagring).
- **Typ: Ska**
- **Beskrivning:** Leverantören ska implementera kryptering av data på disk (i vila) och kryptering av data under överföring. Minimikrav är TLS 1.2+ och AES-256 eller motsvarande säkra algoritmer.
- **Motivering:** Grundläggande skyddsnivå enligt OSL, PDL, GDPR och gängse informationssäkerhetsstandarder.

Krav 2.2

- **Kravtext:** *Leverantören bör erbjuda stöd för Confidential Compute (t. ex. Intel TGX, AMD SEV) eller fysisk kontrollerad serverkapacitet med kundägd kryptering, så att leverantören inte får meningsbärande åtkomst till data i minnet.*
- **Typ: Ska**
- **Viktning: Mede**l
- **Beskrivning:** För att ytterligare höja säkerheten vid känslig databehandling ska leverantören antingen kunna tillhandahålla en “secure enclave”-arkitektur (Confidential Compute) eller en fysisk driftmiljö där myndigheten äger servrarna och förhindrar leverantörsåtkomst med egen kryptering.
- **Motivering:** Skyddar mot avancerade hot (t. ex. minnesdumpning, insiderattacker) och förhindrar leverantören från att se klartextdata, vilket är särskilt viktigt för kritiska personuppgifter eller sekretessklassad information.

Lagring (objektsbaserad lagring och extern nyckelhantering)

Krav 3.1

- **Kravtext:** Leverantören bör erbjuda *finkorniga åtkomsträttigheter* (IAM, bucket policies) samt loggning av samtliga åtkomstförsök.
- **Typ: Bör**
- **Viktning: Hög**
- **Beskrivning:** Möjlighet att definiera vem (användare, tjänstekonto) som får vilka rättigheter (läsa, skriva, radera) till vilka funktionsbrevlådor samt detaljerad loggning av alla accessförsök.
- **Motivering:** Kritisk för att uppfylla spårbarhetskrav, identifiera obehöriga försök och följa upp händelser i en eventuell incidentutredning.

Decrypt on Demand

Krav 4.1

- **Kravtext:** Tjänsten bör stödja *Decrypt on Demand*, där data förblir krypterad tills mottagaren aktivt avkrypterar data som kan innehålla sekretess.
- **Typ: Bör**
- **Viktning: Hög** (särskilt i en federerad miljö)
- **Beskrivning:** Möjlighet att konfigurera arbetsflöden så att meddelanden, filer eller dokument endast dekrypteras när en auktoriserad mottagare explicit begär det.
- **Motivering:** Skapar tydlig ansvarsgräns för när uppgifter “röjs” och stärker den gemensamma tilliten i SDK-federationen.

Krav 4.2

- **Kravtext:** Vid Decrypt on Demand ska systemet tydligt logga avkrypteringshändelser (tid, användare, fil/objekt-ID).
- **Typ: Bör**
- **Beskrivning:** Varje dekryptering måste spåras i loggar, helst i realtid eller nästintill, och vara åtkomlig för revisionsändamål.
- **Motivering:** Underlättar incidenthantering och juridiska bedömningar, då man kan visa exakt när en handling öppnats.

Loggning och revision

Krav 5.1

- **Kravtext:** Leverantören ska tillhandahålla *centraliserad och detaljrik loggning* av all relevant system- och åtkomstaktivitet.
- **Typ: Ska**
- **Beskrivning:** Systemet behöver producera loggar på applikations-, system- och nätverksnivå, med tidsstämpel, användar-ID, IP-adress etc. Loggarna ska kunna samlas i en central lösning för analys.
- **Motivering:** Möjliggör spårbarhet och audit, krävs för OSL-efterlevnad och uppföljning enligt GDPR (t. ex. art. 5, 24, 32).

Krav 5.2

- **Kravtext:** Leverantören bör erbjuda *revisionstjänster* eller möjlighet för kund att utföra penetrationstester och regelbundna revisioner.
- **Typ: Bör**
- **Viktning: Medel**
- **Beskrivning:** Möjlighet att genomföra externa revisioner eller granskningar (ex. ISO 27001-liknande) för att säkerställa att leverantörens miljö uppfyller avtalade säkerhetskrav.
- **Motivering:** Bygger förtroende och tillit i SDK-federationen; identifierar potentiella brister innan de leder till incidenter.

Placering och jurisdiktion

Krav 6.1

- **Kravtext:** All data som hanteras i SaaS-tjänsten ska lagras och bearbetas inom *EU/EES*, helst i Sverige, för att uppfylla lämplighetskravet i OSL.
- **Typ: Ska**
- **Beskrivning:** Leverantören behöver garantera att inga servrar eller underleverantörer använder datacenter i tredjeland, såvida inte explicit avtal träffats och extra åtgärder vidtagits.
- **Motivering:** Adresserar rättsliga osäkerheter och integritetsskydd enligt OSL, PDL och GDPR (kapitel V).

Krav 6.2

- **Kravtext:** Leverantören bör erbjuda *tydlig data residency-funktion* som bekräftar att data enbart finns i önskad region.
- **Typ: Bör**
- **Viktning: Medel**
- **Beskrivning:** Kund ska kunna välja specifik region för lagring/bearbetning och leverantören ska ge bevis för var data är placerad.
- **Motivering:** Förenklar compliance-rapporter och skapar transparens gentemot SDK-federationens övriga medlemmar.

Bilaga B – Detaljerad arkitektur-illustration

itsl solutions

Elevate IT. Ignite Possibility.