

Rapport

Gemensamt federations-protokoll för chatt i offentlig sektor

ES2025-20





Innehåll

1. Sammanfattning	4
2. Avgränsning.....	6
3. Bakgrund.....	7
3.1 Historik.....	8
3.1.1 Epost – där allt började.....	8
3.1.2 Chatt – teknisk utveckling.....	10
3.2 Nuläge.....	12
4. Omvärld	14
4.1.1 Alternativa lösningar till publika centrala molntjänster	15
4.1.2 Internationella exempel på tillämpning av öppna protokoll.....	16
5. Önskat nyläge	18
5.1 Principer för framtiden	19
5.2 Ekonomisk påverkan.....	20
5.3 Juridik och informationssäkerhet	22
6. Beslut	24
7. Slutord	25



1. Sammanfattning

Att omfamna öppna protokoll för federerad kommunikation är inte enbart en teknisk uppgradering. Det representerar en kulturell och strategisk positionsförflyttning för offentlig sektor – en rörelse mot större självbestämmande, förbättrad samarbetsförmåga och en mer långsiktigt hållbar och ansvarsfull digitalisering. Kommande svenska lagstiftning kan fungera som en katalysator för denna förflyttning.

Medarbetare på våra myndigheter är på väg in i en kanalförflyttning och nya arbetssätt där användare går ifrån traditionell epost och snabbchatt till en mer sammanhållen användarupplevelse med beständig chatt, fildelning, videorum, röstmeddelande, digitala whiteboard, AI, och liknande förmågor. Denna förflyttning gör att användare också förväntar sig att samarbetsförmågor i externa samarbeten motsvarar dem som finns inom den egna myndigheten.

Dagens kommunikationslandskap är splittrat, med många olika verktyg och plattformar. Samverkan över myndighetsgränser försvåras, och beroendet av ett fåtal globala leverantörer växer. Det innebär risker för digital suveränitet, rättslig osäkerhet, minskad kontroll över känslig information och myndigheters rådighet över våra förutsättningar att samarbeta.

Offentlig sektor står inför ett viktigt vägval: att fortsätta på en bana av fragmentering och leverantörsberoenden, eller att enas kring en öppen, interoperabel och demokratifrämjande kommunikationsinfrastruktur – ett gemensamt ”språk”, där myndigheter kan välja fritt mellan både leveransform och leverantör efter sina unika verksamhetsbehov.

Valet av kommunikationsprotokoll är en fråga av stor strategisk betydelse för svensk offentlig sektor. Det handlar om mer än bara teknik; det handlar om att skapa förutsättningar för en effektiv, säker, resilient och ekonomiskt hållbar digital förvaltning som kan möta medborgarnas och samhällets nuvarande och framtida behov. För att kommunikationsinfrastrukturen ska upprätthålla grundläggande egenskaper behöver en gemensam modell för principer etableras.

De rättsliga och strategiska kraven växer inom EU. Regelverk som NIS2, Data Act, Digital Markets Act och Interoperable Europe Act ställer krav på öppenhet, säkerhet och interoperabilitet – både inom och mellan medlemsländer. Svenskt totalförsvaret, kris och



beredskap ställer även detta krav på hur vi formar myndigheters förutsättningar att samarbeta i hela hotskalan.

Nya lagförslag som "En reform för datadelning" (SOU 2023:96)¹ stärker det faktum att offentlig sektor ligger efter vad gäller interoperabilitet och datadelning, eSam arbetsgruppen ser tydliga synergier med ett gemensamt öppet protokoll för chattfederation.

Öppna API:er, publika kodbaserna och standardiserade protokoll gör det möjligt för organisationer att själva utveckla och anpassa digital infrastruktur. Det kan förbättra innovationsförmågan, korta ner utvecklingstider och minska beroendet av enskilda leverantörer, eftersom mer kompetens finns inom offentlig sektor.

För att detta ska bli verklighet krävs dock en medveten satsning på kunskapsdelning och utveckling. Att dra nytta av IT som en resurs förutsätter att offentlig sektor kontinuerligt lär sig, avsätter tid för stegvis utveckling och testning, bygger gemensamma arkiv för kod och kunskap samt uppmuntrar samarbete över organisationsgränser. Erfarenheter från bland annat brittiska Government Digital Service² och de baltiska digitaliseringsprogrammen visar att en långsiktig utveckling av kompetens – inte bara en övergång till ny teknik – är viktig för att gemensamma, distribuerade lösningar ska fungera väl över tid.

Om myndigheter inte tar ägarskap på sin förmåga att samarbeta mellan myndighetsgränserna finns risk att offentlig sektor i praktiken standardiserar sina förutsättningar på att kunna samarbeta kring ett fåtal kommersiella leverantörer. Vi har redan sett detta hända tidigare – med Microsoft Skype for Business som ett tydligt exempel. Detta resulterar i en omfattande inlåsnings-effekt, när en kritisk massa myndigheter väljer samma lösning för att kunna samarbeta med varandra blir det svårt att byta lösning - vem vågar ta första klivet från en lösning och riskera tappa samarbetsmöjligheter? En annan effekt blir att myndigheter anpassar sig efter leverantören – inte tvärtom. Eller att myndigheter väljer samma lösning som ”alla andra” vilket kan leda till minskad konkurrens, minskad innovation och färre lösningar som är anpassade efter offentlig sektors faktiska behov.

Svenska myndigheter behöver kontroll och rådighet över sina förutsättningar att samarbeta med varandra. Detta belyser de remissinstanser som arbetsgruppen varit i kontakt med:

"En federerad, öppen lösning stärker demokratin och skapar robusthet." – RISE

¹ <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2023/12/sou-202396/>

² [Government Digital Service - GOV.UK](https://www.gov.uk/government/organisations/government-digital-service)



"Rapporten är välskriven – vi stödjer det långsiktiga vägvalet."– Sunet

"Viktigt med tydlighet kring tekniska standarder och styrning."– Internetstiftelsen

"En decentraliserad chattinfrastruktur, baserad på öppna standarder och federerade lösningar, kan vara ett sätt att minska beroendet av enskilda leverantörer och centrala molntjänster" - MSB

"Detta initiativ har tydliga synergier med nytt lagförslag inom interoperabilitet- och datadelningsområdet" - Regeringskansliet

Rapporten utgör ett underlag för vidare beslut om hur myndigheter inom eSam kan agera givet att de väljer olika kommunikationslösningar samtidigt som myndigheter har behov av att samarbeta över myndighetsgränserna. Arbetsgruppen tar inte ställning till specifika leverantörlösningar, eftersom myndigheters val av produkt eller tjänst inte är i fokus i detta sammanhang. Baserat på detta är inte den minsta gemensamma nämnaren produkt/tjänst utan istället ett gemensamt protokoll för myndighetsövergripande samarbete. Frågan som behandlas är hur strategiska förutsättningar kan säkerställas för att möjliggöra ett leverantörsoberoende, effektivt och robust samarbete inom offentlig sektor.

Just dessa frågor står i centrum för EU:s digitaliseringsstrategi, både gällande och kommande regleringar. Att inte göra ett aktivt val skulle alltså inte bara vara passivt agerande – det skulle också innebära ett aktivt steg bort från den väg som prioriteras inom det europeiska samarbetet kring digitalisering.

2. Avgränsning

Detta material är framtaget på uppdrag av styrgruppen inom ramen för arbetsgruppen Digitala samarbetsplattformar (dSam) eSam.

Arbetsgruppen består av expertkompetenser från olika myndigheter. Bedömningar beskrivna i rapporten ska dock inte ses som formellt beslutade eller ett officiellt ställningstagande inom respektive myndighet. Detta är en del i den rekommenderade tidslinje som presenteras i rapporten.

Denna rapport utgör ett beslutsunderlag för vidare diskussion inom eSam. Den innehåller inte någon formell rekommendation. Eventuella förslag till fortsatt inriktning hanteras separat i ett missiv.



3. Bakgrund

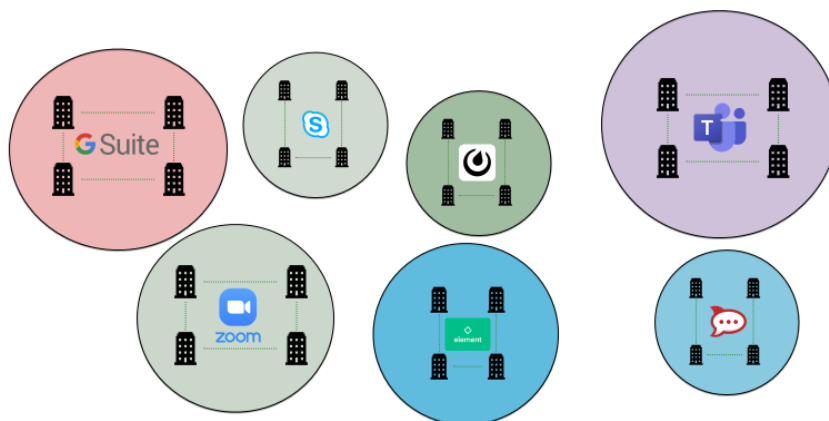
eSams medlemmar ser ett stort behov av att använda gruppchattlösningar som en del av ett modernt arbetssätt. E-post har blivit ett förlegat kommunikationsverktyg och saknar många av de funktioner som moderna samarbetslösningar erbjuder. Myndigheter som inför moderna chattlösningar vittnar om att användare tydligt minskar sitt nyttjande av e-post. Det finns idag ingen beslutad standard för hur chattlösningar inom offentlig sektor ska sammankopplas. Istället har många myndigheter använt Microsoft Skype for Business, vilket fört med sig risker som inlåsning, oönskade beroenden och försämrade förmåga att digitalisera sina verksamheter.

Då Microsoft Skype for Business inte längre kan ses som en modern samarbetslösning står myndigheter inför att utvärdera och implementera andra digitala lösningar för samarbete. Myndigheter, regioner och kommuner vittnar om att detta blivit lättare i och med det arbete som gjorts inom eSam genom projektet Digital Samarbetsplattform (dSam del 1 och del 2).

Varje myndighet gör sin egen bedömning utifrån verksamhetens behov, rättsliga bedömningar, säkerhetsaspekter och försörjningsstrategi. Detta medför att myndigheter landar i olika lösningar vilket i sig är positivt, de får lösningar anpassade efter sina verksamhetsbehov, konkurrensen ökar på marknaden, vilket i sin tur leder till minskad leverantörsinlåsning och fler alternativ anpassade för offentlig sektor.

Samtidigt innebär olika lösningar också ett antal utmaningar. Om leverantörer väljer att fortsätta använda proprietär teknik för att möjliggöra externt samarbete blir det svårare att koppla samman andra leverantörers system. Myndigheter som valt samma lösning har förutsättningar att samarbeta, men mellan olika lösningar saknas ofta tekniska möjligheter för att koppla ihop systemen.

Eftersom myndigheter nu väljer olika chattlösningar ser vi en växande fragmentering och riskerar att på sikt skapa en situation där offentlig sektor tvingas välja en och samma leverantör eller fortsätta med fragmentering och de risker detta medför.



Figur 1 - fragmenteringen ökar

Flera myndigheter har infört eller planerar att införa samarbetslösningar från publika molntjänsteleverantörer. Flera inför begränsningar i funktionalitet eller olika skyddsåtgärder – tekniska eller administrativa – då de bedömer att:

- rättsliga grunden är osäker,
- den digitala kontrollen försvagas, eller
- det inte är lämpligt att dela känsliga uppgifter eller känsliga personuppgifter med leverantören och etablerar därmed kompletterande lösningar för information av högre skyddsvärde

Andra myndigheter värdesätter att erbjuda användarna en helhetsupplevelse och väljer verktyg där de fritt kan välja leveransform och inte berörs av rättsliga frågeställningar eller det osäkra geopolitiska läget. Samtidigt ”tvingas” vissa myndigheter etablera användarkonton åt sina medarbetare i de publika molntjänsterna för att de ska kunna samarbeta effektivt i externa samarbeten.

3.1 Historik

För att skapa en förståelse för vilka nyttoeffekter öppna federationsprotokoll genererar bör myndigheter titta på hur epost utvecklats från början till där vi är idag.

3.1.1 Epost – där allt började

Behovet av decentraliserad och interoperabel kommunikation mellan olika tjänster har, i takt med internets framväxt, drivit på utvecklingen av federationsprotokoll för chatt.



Federationen över standardprotokoll för e-post har sina rötter i internets tidiga utveckling. Under 1970-talet började forskare vid ARPANET, föregångaren till internet, experimentera med e-postsystem. Ray Tomlinson introducerade "@"-symbolen 1971 för att separera användarnamn och värddatorer, vilket blev en grundläggande del av e-postadresser. Vid denna tid utvecklades även Simple Mail Transfer Protocol (SMTP), som gradvis började användas för att överföra e-post mellan olika system och lösningar.

Under 1980-talet togs stora steg mot standardisering av e-post. SMTP formaliserades 1982 i RFC 821 och etablerades som det huvudsakliga protokollet för att skicka e-post. Samtidigt utvecklades protokoll som Post Office Protocol (POP) och senare Internet Message Access Protocol (IMAP) för att möjliggöra hämtning och hantering av e-post från servrar till klienter. Dessa protokoll bidrog till att göra e-post mer tillgängligt och användbart för en bredare grupp användare.

På 1990-talet expanderade användningen av e-post snabbt och blev en av de mest populära tjänsterna på internet. IMAP och POP3 vidareutvecklades för att ge användare mer flexibilitet i hur de hanterade sin e-post, till exempel genom att låta dem läsa meddelanden direkt på servrar istället för att ladda ner dem lokalt. E-postens växande popularitet ledde dock också till nya utmaningar, bland annat spam och bedrägerier.

Under 2000-talet började säkerhetsfrågor få mer uppmärksamhet. För att bekämpa skräppost och förfalskade avsändare infördes säkerhetsprotokoll som SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) och DMARC, som gjorde det svårare för obehöriga att skicka e-post i andras namn. Vid denna tid undersöktes även federerade lösningar för e-post genom protokoll som XMPP (Extensible Messaging and Presence Protocol), vilket tidigare använts för snabbmeddelanden men nu började ses som en möjlighet för mer decentraliserade e-postsystem.

På 2010-talet växte intresset för integritet och decentralisering av e-post. Med ökad medvetenhet om dataskydd blev det viktigare att ge användare mer kontroll över sina e-postservrar. Initiativ som DANE (DNS-based Authentication of Named Entities) introducerades för att förbättra säkerheten, samtidigt som allt fler tjänster började erbjuda totalsträckskryptering för att skydda användarnas kommunikation.

E-post bygger fortfarande på dessa grundläggande standardprotokoll och är ett av de mest robusta federerade systemen på internet. Tack vare denna öppna struktur/protokoll kan användare på olika tjänster och domäner fortfarande kommunicera med varandra utan att vara bundna till en specifik leverantör. Att gå tillbaka till den fragmentering som e-post hade i början vore helt otänkbara idag.



3.1.2 *Chatt – teknisk utveckling*

Federationsprotokoll för chatt har utvecklats i takt med internets framväxt och behovet av decentraliserad, interoperabel kommunikation mellan olika tjänster. Under 1990-talet började de första nätverken för snabbmeddelanden växa fram, ofta som slutna system där användare var begränsade till en specifik tjänst. Populära plattformar som ICQ, AOL Instant Messenger (AIM), MSN Messenger och Yahoo Messenger dominerade marknaden, men eftersom de saknade kompatibilitet med varandra var användare tvungna att ha flera konton för att kommunicera med olika personer.



Under början av 2000-talet växte intresset för öppna standarder, vilket ledde till utvecklingen av protokoll som XMPP (Extensible Messaging and Presence Protocol). XMPP, ursprungligen känt som Jabber, skapades för att möjliggöra federerad kommunikation mellan olika tjänster och plattformar. Det erbjöd en öppen, decentraliserad modell där olika XMPP-servrar kunde kommunicera med varandra, på liknande sätt som e-post fungerar. Google integrerade XMPP i sin tjänst Google Talk, vilket ökade protokollets popularitet, men många kommersiella aktörer fortsatte att använda slutna system.

Trots XMPP:s framgång stötte federerade chattlösningar på utmaningar under 2010-talet. Många stora aktörer, inklusive Facebook och Google, valde att överge XMPP till förmån för egna, proprietära lösningar som gav dem mer kontroll över ekosystemet och användardata. Samtidigt ökade behovet av säker och krypterad kommunikation, vilket ledde till utvecklingen av protokoll som Signal Protocol, som lade grunden för säkra meddelandetjänster som Signal och WhatsApp.

Under senare år har federerade chattprotokoll fått en form av renässans, särskilt inom öppna och decentraliserade nätverk. IETF har tagit fram en internetstandard för end-to-end-kryptering i grupper i form av MLS-protokollet och har en pågående utredning i form av MIMI-arbetsgruppen för att ”specificera den minimala uppsättning mekanismer som krävs för att göra moderna internetmeddelandetjänster interoperabla”. Matrix-protokollet, som lanserades under 2010-talet, har blivit en populär lösning inom offentlig sektor för federerad kommunikation. Till skillnad från XMPP fokuserar Matrix på synkronisering av meddelanden över flera servrar, vilket gör det mer robust för modern användning. Matrix har anammats av organisationer och myndigheter som vill kontrollera sina egna kommunikationskanaler utan att vara beroende av en enskild leverantör.

Idag fortsätter utvecklingen av federerade chattprotokoll där frågor som säkerhet, integritet och interoperabilitet blir allt viktigare. Medan många stora aktörer fortfarande föredrar slutna system, drivs alternativa lösningar av en stark öppen källkods-community och av organisationer som ser värdet i decentraliserad kommunikation.



3.2 Nuläge

Marknaden för samarbetslösningar domineras av olika former av publika centraliserade molntjänster. Dessa lösningar är ofta användarvänliga och snabba på att leverera nya och innovativa funktioner till sina användare. Gemensamt för dessa molntjänster är att de ofta bygger på proprietär teknik, med få incitament som driver emot interoperabilitet och stöd för att sammankoppla med andra leverantörlösningar. Tredjepartsleverantörer erbjuder olika former av bryggor som sammanlänkar dessa lösningarna, men det löser inte grundproblemet och tappar ofta funktionalitet mellan systemen.

Offentlig sektors samarbetsverktyg präglas idag av ett fragmenterat landskap där olika myndigheter valt olika tekniska lösningar för snabbmeddelanden, videomöten och samarbetsytor. Flera myndigheter är i färd med att lämna Skype for Business, samtidigt som flera ännu inte har beslutat om en långsiktig lösning. En förflyttning mot publika amerikanska molntjänster kan skönjas, inte sällan i form av begränsade implementationer eller med kompletterande lösningar.

eSams utredning pekar på att det endast är en av eSams 41 medlemmar som valt amerikansk publik molntjänst som sin enda kommunikationslösning. Övriga medlemmar som valt amerikanska publika amerikanska molntjänster har valt att begränsa funktionalitet eller införa andra lösningar parallellt – ofta på grund av juridiska utmaningar, informationssäkerhet, och behov av digital suveränitet.

Flera myndigheter befinner sig fortfarande i analysfas och vissa avvaktar utfallet av hur rättsliga och geopolitiska läget påverkar det beslut som EU-kommissionen fattade juli 2023³, gällande adekvat skyddsnivå för överföring av personuppgifter till USA. Några har valt att förlänga livslängden på Skype genom övergång till ”Skype SE”, vilket har minskat det omedelbara behovet att byta.

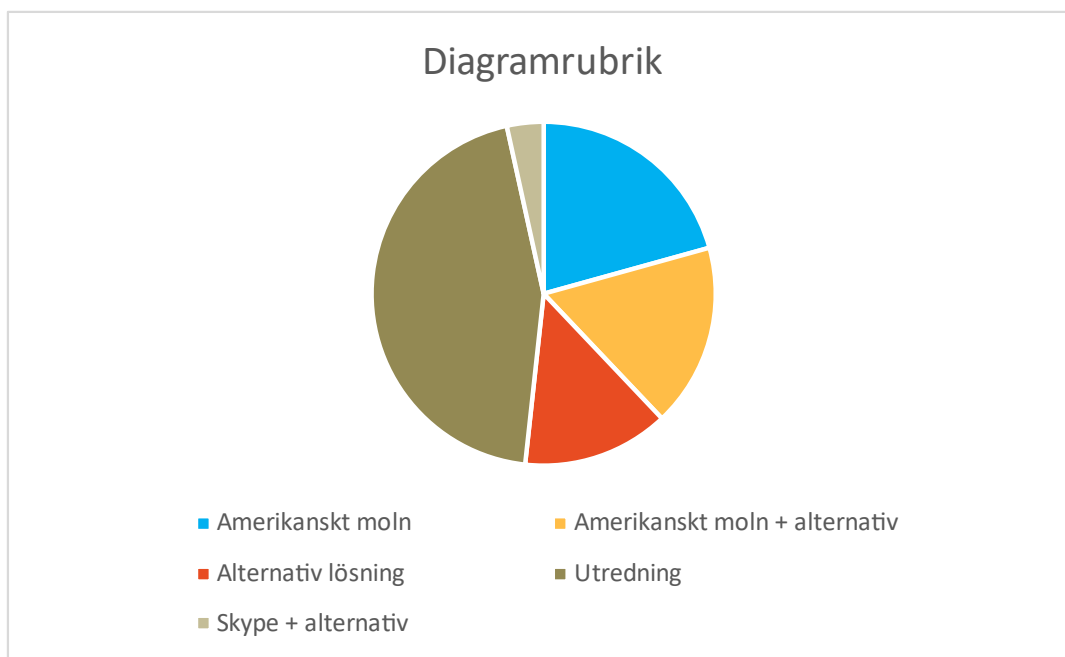
En fundamental skillnad mellan publika centrala lösningar och Skype for Business är hur tjänsterna levereras och exponeras. Medan Skype kan driftas i myndigheters egna datacenter eller via privata leverantörer, är publika molntjänster centraliserade – utan möjlighet till lokal kontroll eller att möjlighet att välja hur tjänsten exponeras mot internet.

Myndigheternas val illustreras i figur 2, kartläggningen är genomförd av eSam april 2025 inom ramen för projektet digital samarbetsplattform (dSam). Den sammanfattar ett

³ [Beslut om adekvat skydd för säkra uppgiftsflöden mellan EU och USA](#)



nuläge hos myndigheter, både inom eSam och andra myndigheter. Notera att många befinner sig i övergångs- eller hybridläge, snarare än i ett slutligt val av lösning.



Figur 2. Översikt över myndigheters val och strategi för samarbetsverktyg (april 2025).

Figuren visar att flera myndigheter redan idag använder olika tekniker och lösningar. Denna fragmentering understryker behovet av att utgå från gemensamma protokoll snarare än gemensamma produkter

Det finns en stor efterfrågan på bättre digital samverkan inom offentlig sektor, men det saknas idag en gemensam kommunikationsinfrastruktur som möjliggör säker, standardiserad och interoperabel kommunikation mellan myndigheter, vilket riskerar att minska offentlig sektors effektivitet, samordning och resiliens. Aktörer som Sunet, Sambruk, Internetstiftelsen och RISE har i andra sammanhang lyft behov av nationell samordning, teknisk vägledning och juridisk tydlighet. Centrala aspekter som lyfts är stark identitetshantering, säkerhet (E2EE), öppenhet och interoperabilitet.

Dessa frågor lyftes även tidigare av eSam inom ramen för projektet Digital samarbetsplattform 2021–2022. Vägledande principer⁴ som laglighet, lämplighet, federation och standardisering förordades som grundpelare i en strategisk förflyttning inom detta område.

⁴ [Digital samarbetsplattform - det finns lämpliga och lagliga alternativ för offentlig sektor - eSamverka](#)



Intresset för öppna standarder för samarbetslösningar har ökat i intresse senaste åren, inte minst inom EU⁵, i länder som Tyskland⁶ och Frankrike⁷. Det osäkra geo- och säkerhetspolitiska läget har på nytt satt frågor som rådighet och digital suveränitet på agendan inom en rad olika organisationer inom EU, både inom offentlig som privat sektor. Det är inte längre en "GDPR-fråga", utan myndigheter väger in fler perspektiv i sina strategiska val. Behovet av nationell samordning i Sverige har också lyfts av DIGG, de skriver i rapporten "*Ett samhälle i förändring (2024)*"⁸ att –

"Den sannolikt enskilt viktigaste trendbrytande åtgärden inom det digitaliseringspolitiska området är ökad samordning, något som kan åstadkommas genom ett större inslag av rätt sorts styrning."

Leverantörer med befintliga produkter och lösningar som börjat tillämpa och analysera öppna protokoll vittnar dels om en farhåga att vara "sist på bollen" jämfört med andra leverantörer som tillämpat öppna protokoll från start. De ser också en komplexitet och ökade kostnader för att anpassa sin produkt att fungera med öppna protokoll.

4. Omvärld

På politisk nivå inom EU hanteras frågan om interoperabilitet genom olika former av förordningar eller akter. EU har under de senaste åren intensifierat sina ansträngningar att reglera den digitala sfären, med ett tydligt fokus på att främja konkurrens, skydda grundläggande rättigheter och säkerställa en rättvis inre marknad. Flera centrala rättsakter, framför allt förordningen om digitala marknader (DMA), förordningen om digitala tjänster (DSA), den allmänna dataskyddsförordningen (GDPR) och ePrivacy-direktivet formar tillsammans en komplex men allt tydligare ram som direkt och indirekt påverkar val av chattprotokoll.

Kärnan i EU:s strategi, särskilt genom DMA, är kravet på interoperabilitet för stora meddelandetjänster för konsumenter som utsetts till "grindvakter" (t.ex. WhatsApp och Messenger). Detta tvingar tidigare slutna ekosystem att öppna sig, vilket skapar ett potentiellt utrymme för öppna protokoll att erbjuda standardiserade och transparenta lösningar. Även om DMA inte uttryckligen föreskriver användning av specifika öppna protokoll, pekar dess krav på rättvis, rimlig och icke-diskriminerande (FRAND) tillgång

⁵ [Open source software strategy - European Commission](#)

⁶ [About us | openDesk](#)

⁷ [La Suite numérique](#)

⁸ [Ett samhälle i förändring – underlag till regeringens strategiska prioriteringar | Digg](#)



och bevarandet av säkerhet, inklusive totalsträckskryptering (E2EE), i riktning mot lösningar som är robusta och väldefinierade.

Andra direktiv som NIS2-direktivet (Network and Information Systems Directive 2), Cyberresiliensakten (CRA) pekar även de på olika sätt på vikten av interoperabilitet och säkra och öppna kommunikationsprotokoll. Se ”*Bilaga_A_Omvärldsbevakning*” för fördjupning.

Ett svenskt lagförslag "En reform för datadelning" (SOU 2023:96)⁹, syftade till att analysera befintlig styrning och reglering av interoperabilitet vid datadelning inom den offentliga förvaltningen. Syftet är att öka förmågan att dela data effektivt och säkert för att kunna effektivisera offentliga verksamheter och service till medborgare och företag. Den lyfter, precis som denna rapport, en form av fragmentering och avsaknaden av en nationell strategi för interoperabilitet. Regeringens ambition är att kunna lämna proposition på lagförslaget till riksdagen under hösten 2025 med förhoppningar om ny lagstiftning under 2026.

Det är viktigt att notera att "öppenhet" i sammanhanget chattprotokoll är mångbottnat. Medan öppen källkod är en viktig aspekt för transparens och gemensam utveckling, är det troligt att EU:s primära intresse ligger i "öppna standarder". Sådana standarder är avgörande för att säkerställa verklig interoperabilitet mellan olika tjänster och för att förhindra inlåsningseffekter hos dominerande leverantörer, vilket är en kärnprincip i EU:s strävan att främja konkurrens. Denna inriktning på standardiserade gränssnitt är sannolikt den främsta drivkraften bakom EU-länders eventuella preferens för "öppna" kommunikationslösningar, även om öppen källkod och öppna standarder ofta går hand i hand.

4.1.1 Alternativa lösningar till publika centrala molntjänster

Utöver de populära publika molntjänsterna från Microsoft, Google, Zoom, Slack m.fl. finns ett antal samarbetslösningar på marknaden, som möjliggör eget val av leveransform, decentralisering och egen datakontroll. Organisationer kan köpa support och även få tillgång till enterprise-specifika funktioner som stöd för flerfaktorautentisering, antivirusintegrationer, hantera storskalig IT-drift, flerkundsstöd, egna appar mm.

Arbetsgruppen har inte fokuserat på omvärldsanalys av färdiga samarbetslösningar, utan på öppna protokoll. Mot bakgrund av detta ska nedanstående lista av leverantörer ses som exempel och inte som en rekommendation eller ”nettolista” av leverantörer.

⁹ <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2023/12/sou-202396/>



Marknaden är betydligt mer mångfacetterad. Nedan listas några exempel på klienter och tjänster som erbjuds på marknaden med olika former av chattförmågor.

Element¹⁰ - Element är en populär klient och erbjuder även hostingtjänster (Element Services) där du kan välja hostingregion (inklusive EU) samt egen IT-drift (on-premise).

Mattermost¹¹ – Beskrivs ofta som ett alternativ till Slack/Teams. Kan installeras på egna servrar (on-premise) eller i valfritt moln (inklusive europeiska leverantörer).

Nextcloud Talk¹² – Ingår som app i ett Nextclouds plattformslösning tillsammans med andra funktioner som dokumenthantering, digital whiteboard, kanban mm. Kan självhostas eller som tjänst hos ett flertal molntjänstleverantörer.

Rocket.Chat¹³ - Erbjuder flexibilitet med självhosting eller via molntjänst från partner inom Sverige samt andra länder inom EU.

AWS Wickr¹⁴ – E2EE baserad chattlösning som erbjuds både som SaaS tjänst men kan även sättas upp för egen IT-drift på Kubernetes.

Andra mer nischade lösningar som SimpleX, Delta chat och Session är också alternativ som väljs av vissa organisationer.

4.1.2 Internationella exempel på tillämpning av öppna protokoll

Utvecklingen inom vissa EU-länder visar en tydlig trend mot öppna standarder och lösningar som minskar beroendet mot enskilda leverantörer. Flera länder har redan implementerat nationella eller sektorsspecifika kommunikationsplattformar baserade på det öppna federationsprotokollet Matrix.

Den franska staten använder en tjänst baserad på Matrix-protokollet, kallad Tcham, för kommunikation mellan offentliga tjänstemän. Tjänsten har idag över 400 000 användare med siktet inställt på stora delar av offentliga förvaltningen i Frankrike. Projektet drivs av Direction interministérielle du Numérique (DINUM) med fokus på säkerhet och digital suveränitet.¹⁵

Europeiska kommissionen planerar under 2026 byta ut externa appar som Signal mot appar som bygger på det öppna protokollet Matrix. Målet är att skapa en säker, statlig kommunikationsplattform där man äger data själva och kan erbjuda komplement till Microsoft Teams.

¹⁰ [Digital samarbetsplattform - det finns lämpliga och lagliga alternativ för offentlig sektor - eSamverka](#)

¹¹ [Mattermost | Collaboration Platform for Mission Critical Work](#)

¹² [Calls, chat and video conferencing with Nextcloud Talk](#)

¹³ [Rocket.Chat | Secure CommsOSTM for Mission-Critical Operations](#)

¹⁴ [AWS Wickr | Secure Enterprise Messaging & Collaboration Platform](#)

¹⁵ [Tchap - la messagerie instantanée des agents de la fonction publique](#)



Luxchat är en meddelandetjänst för allmänheten och företag, medan Luxchat4Gov är avsedd för offentliga sektorn i Luxemburg. Båda tjänsterna är interoperabla och erbjuder säker, krypterad kommunikation utan reklam eller användning av personuppgifter. De levereras som en tjänst i datacenter placerade i Luxemburg. 16

Tyskland har på flera håll en tydlig strategi att tillämpa öppet protokoll (Matrix) inom offentlig sektor. Detta inkluderar bland annat:

- BwMessenger: En version av Element som används av hela den tyska försvarsmakten som ett säkert alternativ till kommersiella meddelandeappar 17
- TI-Messenger: Ett Matrix-baserat system som har gjorts obligatoriskt av Gematik för säker kommunikation inom den tyska hälso- och sjukvårdssektorn, vilket involverar över 150 000 organisationer 18
- openDesk: Förbundsministeriet för inrikesfrågor (BMI) och ZenDiS har valt Matrix och Element som kommunikationslager för den öppna och suveräna arbetsplatsplattformen openDesk 19
- Universitet: Många universitet i Tyskland och Österrike använder Matrix som sin primära kommunikationsplattform
- Skolor: Flera tyska delstater har infört Matrix för säker kommunikation inom online-undervisning
- Polisen (P20 Program): En undergrupp inom polisen har rekommenderat användningen av Matrix som ett enhetligt meddelandeprotokoll
- FITKO (Föderale IT-Kooperation): Tillsammans med det tyska inrikesministeriet har FITKO initierat ett pilotprojekt för att utveckla en modern kommunikationsplattform baserad på Matrix 20

ELGA (Elektronische Gesundheitsakte) är Österrikes nationella elektroniska hälsojournalssystem, utformat för att förbättra informationsutbytet inom hälso- och sjukvården. Det möjliggör för vårdpersonal att snabbt och säkert få tillgång till patienters medicinska data, vilket leder till bättre samordning och vårdkvalitet. ELGA planerar implementera Matrix-protokollet som en bas, likt Gematik, för att utbyta känsliga uppgifter mellan olika partner inklusive medborgare.

Ett annat exempel är ActivityPub, ett öppet, decentraliserat protokoll för sociala nätverk, mest känt som tekniken bakom "Fediverse" (en samling sammankopplade sociala plattformar som Mastodon, PeerTube, Lemmy, m.fl.). Det har på senare tid skett ett

¹⁶ [Luxchat – La solution de messageries instantanées du Luxembourg !](#)

¹⁷ [Bw Messenger | Sicher. Flexibel. Open Source.](#)

¹⁸ [TI-Messenger | gematik](#)

¹⁹ [The office and collaboration suite for public administration | openDesk](#)

²⁰ [FITKO](#)



skifte från plattformen X (tidigare Twitter) till andra alternativ givet de organisatoriska och principiella förändringarna som skett sedan Twitter blev uppköpt. Vissa EU-organ och tjänstemän har börjat utforska och använda plattformar baserade på ActivityPub. Till exempel lanserade Europeiska datatillsynsmannen (EDPS) initiativet EU Voice, som är en egen Mastodon-instans (Mastodon använder ActivityPub), för att ge EU-institutioner en närvaro i Fediverse.

Andra protokoll som XMPP och SIP är vanligt förekommande öppna protokoll inom offentlig sektor, där det sistnämnda främst är avsett för röst och video samt närvarohantering. Ett exempel på XMPPs nyttjande är Cisco Webex, en chattlösning som använder XMPP för chatt med stöd för federering. Det finns ett antal publika XMPP-servrar i EU-länder som Tyskland, Nederländerna, Frankrike, Österrike, Tjeckien, Polen, Lettland och Finland.

Parallellt med detta pågår det arbete inom Internet Engineering Task Force (IETF) kring två olika former av protokoll, Message Layer Security (MLS) och More Instant Messaging Interoperability (MIMI). Dessa två i kombination har potential att bli standardprotokoll för interoperabilitet för chattlösningar, det är dock för tidigt att bedöma givet att MIMI-arbetsgruppen ännu inte har presenterat ett förslag. Arbetet har kantats av intressekonflikter och komplexa frågor, vilket i sig är en naturlig del i processen till att komma fram till en gemensam öppen standard.

5. Önskat nyläge

Det finns flera möjliga strategier för hur offentlig sektor kan organisera sin kommunikationsinfrastruktur framåt. SWOT-analysen i Bilaga C beskriver sex vägval i detalj.

De mest framträdande alternativen är:

- Att fortsätta som idag, med olika verktyg och utan gemensam samordning.
- Att införa en central brygglösning som kopplar ihop befintliga system tillfälligt.
- Att införa ett gemensamt federerat och öppet protokoll, med decentraliserad drift och standardiserad interoperabilitet.

Bland de övriga alternativen finns även att införa en central statlig chattlösning, bilda sektorsvisa kluster kring nuvarande verktyg. Att samtliga myndigheter enas om en gemensam kommersiell tjänst/produkt bedöms inte som realistiskt alternativ då myndigheter gör olika bedömningar och styrs av olika krav och behov. De presenterade



vägvalen har olika grad av komplexitet, inlåsningseffekt, kostnad och anpassningsförmåga.

Arbetsgruppens bedömning är att vägvalet för en öppen federerad lösning ger en långsiktig hållbarhet, möjlighet till innovation och kontroll i linje med EU:s strategiska mål. Bedömningen är dock att vi kan behöva interimslösningar på kort sikt för att nå önskat nyläge samt att myndigheter ska kunna göra egna bedömningar gällande lösningar för t.ex. internt samarbete.

5.1 Principer för framtiden

Inom ramen för arbetet har arbetsgruppen tagit fram ett förslag på principer för öppet federationsprotokoll för chatt. Principerna ska inte ses som en komplett kravlista utan mer som exempel på hur arbete med att harmonisera valet av chattlösningar kan fungera framöver.

Grunden för principerna är att de ska stödja interoperabilitet, inte vara knutna till en leverantör, ha full insyn och stödja myndigheters krav på robusthet och kris- och beredskapsplanering inom totalförsvaret och svensk suveränitet.

Att ett protokoll är "öppet" i detta sammanhang innebär mer än bara tillgång till källkoden. European Committee for Interoperable Systems (ECIS) har formulerat principer för öppna standarder som belyser detta. Dessa principer inkluderar:

- En samarbetsinriktad och demokratisk utvecklings- och förvaltningsprocess.
- En transparent utvecklings- och förvaltningsprocess öppen för alla intresserade parter.
- Godkännande genom en vederbörlig process med konsensus bland deltagarna.
- Att korrekta implementationer av standarden måste vara interoperabla.
- Att de är plattformsoberoende, leverantörsneutrala och användbara av ett obegränsat antal konkurrerande implementationer.
- Att de är öppna publicerade, inklusive specifikationer och dokumentation.
- Att de är tillgängliga royaltyfritt eller till minimal kostnad, med de enda licensieringsrestriktionerna som ömsesidighet och defensiv avstängning.

Denna principbaserade syn skulle resultera i att myndigheter undviker att forma sin samverkan kring enskilda lösningar, och istället samlas kring en teknisk och organisatorisk grund som möjliggör valfrihet och konkurrensfördelar.



Den "öppna" aspekten av ett protokoll är inte enbart en teknisk detalj; den utgör en fundamental garant för långsiktig tillgänglighet, anpassningsbarhet och kontroll, vilket är av särskild vikt för offentlig sektor. När ett protokoll är proprietärt innebär det att en enskild kommersiell aktör äger och kontrollerar dess specifikation och framtida utveckling. Detta ger leverantören en betydande maktposition att diktera villkor, prissättning och teknisk inriktning, vilket kan leda till ett starkt beroende för de organisationer som använder protokollet.

Öppna protokoll, med sina fritt tillgängliga specifikationer och transparenta utvecklingsprocesser, begränsar denna exklusiva kontroll från en enskild aktör. För offentlig sektor, som har ett uttalat långsiktigt ansvar och ett behov av stabilitet, förutsägbarhet och ansvarsfull användning av skattemedel, innebär detta att risken för plötsliga och ofördelaktiga licensändringar, upphörande av support för äldre versioner, eller påtvingade och kostsamma uppgraderingar minskar avsevärt. Valet av ett öppet protokoll kan därmed ses som en strategisk riskminimeringsåtgärd och en aktiv investering i att säkra och upprätthålla digital autonomi.

De föreslagna principerna bygger på en balans mellan teknisk neutralitet och operativ rådighet. De ska stödja att lösningar kan utformas med hänsyn till både verksamhetsbehov, juridik och säkerhet. Genom att utgå från ett gemensamt protokoll kan offentlig sektor behålla valfrihet mellan klienter, driftformer och leverantörer – utan att ge avkall på interoperabilitet.

Ett gemensamt öppet chattprotokoll innebär däremot inte per automatik digital suveränitet och ökad rådighet. När offentliga aktörer väljer externa driftleverantörer för myndighetsgemensamt samarbete där t.ex. ägarförhållande/drift sker i tredjeland eller beroende till lagstiftning utanför EU kan kontrollen undermineras.²¹

Arbetsgruppens framtagna exempel på principer för öppet federationsprotokoll för chatt, exemplifieras i *bilaga E, Principer för federerad kommunikation*

5.2 Ekonomisk påverkan

Det är nära till hands att tänka att det vore mest ekonomiskt fördelaktigt om myndigheter investerar i samma lösning och maximerar sitt nyttjande av redan genomförda investeringar. Arbetsgruppens bedömning är dock att standardisera

²¹ Det är viktigt att skilja på t.ex. Matrix-protokoll och klienter som t.ex. Element. Rapportens rekommendationer utgår från protokollets egenskaper – inte från specifika implementationer eller leverantörer.



myndigheters förutsättningar att samarbete på ett fåtal proprietära lösningar riskerar ge negativa ekonomiska effekter på lång sikt för offentlig sektor.

För att offentlig sektor framgångsrikt ska kunna dra nytta av de ekonomiska och strategiska fördelar som öppna protokoll för chattfederation erbjuder, krävs ett antal medvetna strategiska överväganden och ett proaktivt agerande. Det handlar inte enbart om ett tekniskt val, utan om en inriktning som påverkar upphandling, kompetens, samverkan och policyutveckling.

- Prioritera öppna standarder och protokoll
- Investera i kompetensuppbyggnad kring öppna teknologier och federerade system
- Främja och delta i nationella och internationella samarbeten kring utveckling och standardisering
- Genomför noggranna TCO-analyser som inkluderar långsiktiga strategiska kostnader och vinster
- Utveckla tydliga riktlinjer och policyer för användning av federerade chatttjänster

En framgångsrik övergång till och ett effektivt nyttjande av öppna federationsprotokoll inom offentlig sektor kräver mer än bara lämpliga tekniska val. Det förutsätter en tydlig strategisk viljeinriktning från ledningsnivå, en beredskap till organisatorisk anpassning och ett aktivt, långsiktigt engagemang i det ekosystem som omger öppen teknologi. Att enbart "välja" ett öppet protokoll är inte tillräckligt om organisationen inte är rustad för att hantera och dra full nytta av de möjligheter som följer.

Proprietära federationsprotokoll levereras ofta som en del av en helhetslösning med omfattande support från en enskild leverantör, vilket kan framstå som enklare och mindre resurskrävande på kort sikt. Öppna protokoll kan, å andra sidan, kräva mer intern kunskap och engagemang för implementation, anpassning, integration och styrning. Därför måste en satsning på öppna protokoll ses som en strategisk investering i den egna organisationens digitala kapacitet och mognad. Detta kräver förankring i ledning, resurstilldelning för kompetensutveckling och en vilja att förändra etablerade arbetssätt och upphandlingsmodeller.

Chattbaserad federation för dock med sig komplexitet i form av drift och säkring av federationsnätverket så som tillitskedjor – vem som litar på vem och hur skadlig kod förhindras spridas mellan myndigheter behöver hanteras med tydliga modeller.



Utöver de direkta ekonomiska aspekterna medför öppna protokoll för chattfederation en rad nyttoeffekter. Förbättrad interoperabilitet är central för att möjliggöra en verkligt sammanhållen offentlig sektor där information kan flöda och samarbete kan ske smidigt över organisationsgränser. Öppenheten fungerar som en katalysator för innovation och anpassningsbarhet, vilket ger offentlig sektor möjlighet att utveckla och skräddarsy lösningar som är optimerade för dess unika behov. Transparensen och granskningsmöjlighet i öppna system stärker informationssäkerheten och bygger förtroende, samtidigt som den decentraliserade och federerade egenskapen bidrar till ökad resiliens och driftskontinuitet. Kanske viktigast av allt är att valet av öppna protokoll för samarbete är ett konkret steg mot att säkra digital suveränitet, vilket ger offentlig sektor ökad kontroll över sin kritiska kommunikationsinfrastruktur och minskar beroendet av enskilda, ofta externa, aktörer.

Dessa fördelar är dock inte utan motkrav. Att realisera den fulla ekonomiska potentialen i öppna federerade lösningar kräver en målmedveten strategi och en annan typ av investering än den som krävs för proprietära lösningar. Istället för att primärt betala licensavgifter, måste organisationen investera andra lösningar – antingen genom att bygga egen teknisk förmåga för egen drift eller genom att köpa managerade tjänster och supportavtal.

5.3 Juridik och informationssäkerhet

Federation av chattbaserade lösningar mellan svenska myndigheter är en komplex process som involverar flera viktiga juridiska aspekter. Uppgifter av olika karaktär och informationsklass kommer delas mellan myndigheter.

När personuppgifter behandlas i den federerade chattlösningen måste det tydligt fastställas vilken myndighet som är personuppgiftsansvarig för respektive behandling. All behandling av personuppgifter måste ha en laglig grund enligt GDPR. Personuppgifter får endast samlas in för specifika, uttryckligt angivna och berättigade ändamål och får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Detta är särskilt viktigt vid federering där information kan delas mellan olika myndigheter med olika uppdrag. Endast de personuppgifter som är nödvändiga för ändamålet får behandlas. Personuppgifter får inte lagras längre än nödvändigt. Rutiner för gallring och radering är viktiga och att lämpliga tekniska och organisatoriska åtgärder måste vidtas för att skydda personuppgifterna. Detta inkluderar kryptering, åtkomstkontroller och loggning.



Om behandlingen sannolikt leder till en hög risk för enskildas fri- och rättigheter måste en konsekvensbedömning genomföras av respektive myndighet.

När blir ett chattmeddelande en allmän handling, det är inte alltid självklart - generellt sett när det har kommit in till myndigheten eller upprättats där och är förvarat hos myndigheten. Hur hanteras chattmeddelanden som är av mer tillfällig karaktär och inte nödvändigtvis ska bevaras som allmänna handlingar? Här krävs tydliga myndighetsgemensamma riktlinjer.

Beroende på myndigheters bedömning kan information som utbyts via chattlösningen utgöra allmänna handlingar. Detta innebär att de kan begäras ut av allmänheten. Myndigheterna måste ha rutiner för att hantera sådana begäranden, inklusive att kunna söka och sammanställa information från chattloggar. Innan en handling lämnas ut måste en sekretessprövning göras för att bedöma om någon information omfattas av sekretess enligt OSL. Detta kan vara komplicerat när information delas mellan myndigheter med olika sekretessbestämmelser.

Även om informationen är sekretessbelagd kan den i vissa fall lämnas ut till andra myndigheter om det finns lagstöd för det (s.k. sekretessbrytande bestämmelser). Detta måste bedömas i varje enskilt fall.

Myndigheter har även skyldigheter gällande registrering och diarieföring av allmänna handlingar samt när den eventuellt kan gallras (raderas). Detta måste ske i enlighet med gällande gallringsföreskrifter. Informationen måste kunna bevaras och vara läsbar över tid, även om tekniken förändras. Detta måste beaktas för information som skapas och delas i chattlösningen.

Om information mellanlagras (t.ex. på servrar hos en tjänsteleverantör eller i en gemensam infrastruktur), måste myndigheter säkerställa att lagringen uppfyller alla relevanta krav (säkerhetsskydd, GDPR, OSL). Var serverna fysiskt befinner sig kan ha betydelse, särskilt om de är utanför EU/EES (vilket kan medföra ytterligare krav enligt GDPR).

Myndigheter behöver kartlägga vem som har åtkomst till den mellanlagrade informationen och under vilka förutsättningar.

Det är en komplex juridisk och teknisk utmaning att ha federation mellan chattbaserade lösningar. En noggrann genomlysning av alla dessa aspekter, och involvering av juridisk expertis inom respektive område, är nödvändig för att säkerställa en laglig och säker implementering. Det är viktigt att se detta som en helhet där de olika lagstiftningarna samverkar och ställer krav på processer, teknik och organisation.



Dessa juridiska frågeställningar behöver utredas oavsett vilket vägval myndigheter väljer för att samarbeta mellan chattbaserade lösningar.

6. Beslut

Baserat på genomförd analys föreslår arbetsgruppen att styrgruppen beslutar att arbetet med ett öppet federationsprotokoll ska fortsätta under hösten 2025 samt att myndigheter tilldelar ekonomiska resurser och kompetens för fortsatt förankring och utveckling.

Det handlar bland annat om att utse en samordnande aktör med ansvar för styrning, stöd och uppföljning. Identifierade synergier med lagförslag gällande "En reform för datadelning" (SOU 2023:96)²² behöver analyseras och ageras på. Utöver detta behöver myndigheter verka för att integrera arbetet med övriga digitaliseringsinitiativ i Sverige och EU.

Mot denna bakgrund föreslår arbetsgruppen att eSam etablerar ett samarbete för att på sikt etablera ett gemensamt, öppet federationsprotokoll för beständig chatt och meddelandetjänster inom offentlig sektor. Lösningen bör bygga på öppna standarder, vara leverantörsberoende, och stödja decentraliserad drift.

Fördelarna med detta vägval är:

- Bättre samverkan mellan myndigheter, regioner och kommuner
- Bättre förutsättningar att erbjuda säkra medborgartjänster
- Bättre kontroll över data, drift, säkerhet och möjligheten att samarbeta i hela hotskalan
- Minskad inlåsning till enskilda leverantörer
- Investeringen som ger ringar på vattnet i kringliggande områden
- Möjlighet till innovation och europeiskt ledarskap

Arbetsgruppen rekommenderar att styrgruppen beslutar följande nästa steg:

- Prioriterar fortsatt arbete med federerad chatt som strategiskt mål för eSam
- Säkerställer finansiering och kapacitet från hösten 2025
- Beslutar om ansvarsfördelning och styrmodell
- Förankrar de principer som föreslås i Bilaga E

²² <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2023/12/sou-202396/>



- Det fortsatta arbetet ska omfatta etablering av ett styr- och governance-ramverk, inklusive modell för gemensamma federationen
- Involvera DIGG:s arbete inom behörighets- och identitetshantering etablera att nyttja synergier mellan identitet- och chattfederationslösningar
- Använder tidslinjen i Bilaga D som färdplan för genomförande

7. Slutord

Flera europeiska länder har redan börjat införa federerade chattlösningar baserade på öppna protokoll som Matrix. Sverige riskerar att halka efter – både vad gäller teknisk utveckling och möjligheten till samarbete inom och utanför landets gränser.

Det positiva är att det finns en realistisk väg framåt – men det kräver långsiktighet, beslutsamhet, resurser och en gemensam riktning.

Att omfamna öppna protokoll för federerad kommunikation är inte enbart en teknisk uppgradering. Det representerar en kulturell och strategisk positionsförflyttning för offentlig sektor – en rörelse mot större självbestämmande, förbättrad samarbetsförmåga och en mer långsiktigt hållbar och ansvarsfull digitalisering. Kommande svenska lagstiftning kan fungera som en katalysator för denna förflyttning.

Vägen framåt kräver medvetna beslut, investeringar i kompetens och ett aktivt engagemang, men de potentiella vinsterna i form av en mer effektiv, säker, innovativ och suverän digital kommunikation gör det till en strategiskt viktig och ekonomiskt fördelaktig färdriktning för svensk offentlig sektor i den digitala tidsåldern. Detta är en resa som i grunden stärker offentlig sektors egen digitala mognad och dess förmåga att navigera i ett alltmer komplext digitalt landskap, vilket är avgörande för framtidens välfärd och samhällsservice.

eSamverkansprogrammets syfte är att genom frivillig samverkan mellan myndigheter, underlätta och driva på medlemmarnas digitala transformation.

Tillsammans bidrar vi med hållbara och rättssäkra lösningar till nytta för såväl medlemmar som samhälle.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Arbetsmiljöverket, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Finansinspektionen, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kemikalieinspektionen, Kronofogdemyndigheten, Kustbevakningen, Lantmäteriet, Livsmedelsverket, Läkemedelsverket, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Riksantikvarieämbetet, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statens veterinärmedicinska anstalt, Statistiska centralbyrån, Statskontoret, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket, Universitets- och högskolerådet samt Utbetalningsmyndigheten. (Jan 2026.)



