



Bilaga A – Omvärldsbevakning

Det pågår flera initiativ inom EU kopplat till öppna federationsprotokoll där Tyskland och Frankrike ligger i framkant. Utöver detta har ett flertal rättsakter beslutats på senare år som samtliga pekar på interoperabilitet, öppen källkod och öppna standarder.

Nedan följer en summering av identifierade områden som är relevant för rapporten

Sammanfattning

Förordningar inom EU påverkar och kommer påverka hur vi agerar strategiskt. Tyskland och Frankrike arbetar aktivt med frågor som öppna protokoll.

"En reform för datadelning" (SOU 2023:96) visar tydligt på att det finns ett driv och en vilja inom offentlig sektor att förbättra förmågor inom interoperabilitet. En lag kan komma att träda i kraft under 2026.

Det finns stor efterfrågan från kommuner, myndigheter och universitet på en gemensam väg framåt kopplat till möjlighet att kunna samarbeta mer effektivt och sömlöst.

Identitet, säkerhet, öppenhet och interoperabilitet måste vara grundpelare i en framtida lösning. Öppna protokoll ses som en förutsättning för att uppnå digital suveränitet och minska leverantörsberoende.

Flera aktörer efterlyser nationell samordning, tydliga principer och testmiljöer.

För att åstadkomma verklig förändring behöver offentlig sektor inom EU agera gemensamt, driva teknikutvecklingen själva och inte enbart invänta leverantörers initiativ eller politiska beslut

EU:s förordningar – ökade krav på interoperabilitet och öppenhet

Europeiska unionen har under de senaste åren antagit flera tunga rättsakter som påverkar hur digital infrastruktur ska byggas och styras – särskilt inom offentlig sektor. Dessa regelverk stärker argumenten för att använda öppna, interoperabla och kontrollerbara tekniska lösningar, som exempelvis öppna federationsprotokoll.



Interoperabilitetsakten (Interoperable Europe Act) 1

Denna förordning antogs i april 2024 och är ett viktigt steg för att harmonisera digitala offentliga tjänster inom EU. Den kräver att offentliga digitala system ska kunna samverka över nationsgränser – både tekniskt och organisatoriskt. Aktens syfte är att minska dubbelarbete, spara kostnader och förbättra kvaliteten på offentliga tjänster inom hela unionen.

Offentlig sektor förväntas välja lösningar som stödjer öppen federation, för att säkra interoperabilitet mellan länder och myndigheter. Tillämpning av öppen källkod och standarder är ett krav som lyfts både av EU:s Interoperable Europe Act. Akten vill främja interoperabilitet men aspekter som chattfederation nämns inte uttryckligen i Interoperable Europe Act.

Data Governance Act (DGA)²

DGA syftar till att underlätta delning av data mellan offentliga och privata aktörer, på ett säkert och tillförlitligt sätt. Den ger riktlinjer för hur data ska göras tillgänglig, samtidigt som skyddet för känsliga uppgifter bevaras.

Offentliga kommunikationstjänster måste kunna hantera datadelning enligt dessa principer – något som gynnas av standardiserade och öppna protokoll.

Förordningen om digitala tjänster (DSA)³

Förordningen om digitala tjänster (DSA), Regulation(EU)2022/2065, är en annan central del av EU:s digitala regelverk. Dess syfte är att skapa en säkrare och mer transparent onlinemiljö genom att fastställa skyldigheter för leverantörer av digitala tjänster som fungerar som mellanhänder, vilket inkluderar värdtjänster och onlineplattformar. Många meddelandetjänster kan falla under dessa kategorier, särskilt om de erbjuder funktioner utöver ren peer-to-peer-kommunikation.

Digital Markets Act (DMA)⁴

EU:s DMA, särskilt Artikel 7, inför ett mandat för utsedda "grindvakter" (gatekeepers) – stora digitala plattformar som Meta (med WhatsApp och Messenger) – att göra sina

¹ Interoperable Europe Act | Interoperable Europe Portal

² European Data Governance Act | Shaping Europe's digital future

³ The EU's Digital Services Act

⁴ European Data Governance Act | Shaping Europe's digital future



meddelandetjänster interoperabla med tredjepartstjänster. Detta regelverk syftar till att öka konkurrensen och valfriheten på den digitala marknaden.

DMA stärker behovet av federerade kommunikationslösningar, eftersom de bidrar till att bryta inlåsning och skapa konkurrens.

AI Act⁵

AI-förordningen är den första i sitt slag i världen och ställer krav på öppenhet, spårbarhet och kontroll i användningen av AI-system. För högrisktillämpningar krävs dokumentation, mänsklig övervakning och säkerhet.

Om AI används i samband med meddelandeplattformar, till exempel för automatiserad svarshantering eller analys, måste infrastrukturen vara transparent och kontrollerbar – vilket talar för lösningar där offentlig sektor själva styr tekniken.

NIS2-direktivet (Network and Information Systems Directive 2)

Detta direktiv syftar till att stärka cybersäkerheten inom EU genom att fastställa en hög gemensam säkerhetsnivå för nätverks- och informationssystem i viktiga och betydande sektorer. Direktivet nämner specifikt "användning av kryptografi och, där det är lämpligt, kryptering som en riskhanteringsåtgärd. Detta uppmuntrar direkt användningen av E2EE-lösningar för säker kommunikation inom dessa sektorer. NIS2-direktivet anger också att end-to-end-kryptering bör användas för att skydda offentliga elektroniska kommunikationsnät och tjänster.⁶

Cyber Resilience Act(CRA)⁷

Denna akt fokuserar på cybersäkerhetskrav för produkter med digitala element. Den betonar behovet av att produkter levereras utan kända exploaterbara sårbarheter och med säkra standardkonfigurationer, inklusive användning av kryptering.

Digital suveränitet – genomsyrar flera rättsakter

Digital suveränitet handlar i grunden om förmågan att utöva kontroll över den egna digitala miljön – inklusive infrastruktur, data och de regler som styr dem. Digital resiliens

⁵ AI Act | Shaping Europe's digital future

⁶ NIS2 Directive: new rules on cybersecurity of network and information systems, 2025, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

⁷ Cyber Resilience Act | Shaping Europe's digital future



avser förmågan hos system, organisationer och samhället i stort att motstå, anpassa sig till och återhämta sig från digitala störningar, såsom cyberattacker eller tekniska haverier.

En markant acceleration i antal lagstiftningar har observerats under de senaste åren, driven av teknisk utveckling, ökande hotbilder och en politisk vilja att stärka EU:s så kallade "strategiska autonomi". Centrala rättsakter som NIS2-direktivet, Digital Services Act (DSA), Digital Markets Act (DMA), Dataakten (Data Act), Data Governance Act (DGA) och förslaget till Cyber Resilience Act (CRA) har antingen nyligen trätt i kraft, är under implementering eller har presenterats inom en relativt kort tidsperiod. Denna snabba framväxt av ny lagstiftning skapar ett komplext och dynamiskt regulatoriskt landskap som kan vara utmanande för verksamheter att överblicka och anpassa sig till.

EU kommissionen tagit fram ett ramverk för att stödja medlemsländerna i att utvärdera leverantörlösningar och dess förutsättningar att erbjuda digitalt suveräna egenskaper. Detta stöd skapar också en tydlig definition om vilka egenskaper en tjänst ska ha för att kunna kallas digitalt suverän.⁸

EU:s rättsliga ramverk, med förordningen om digitala marknader (DMA) i spetsen, håller på att omforma spelplanen för digitala kommunikationstjänster. Även om ingen EU-rättsakt uttryckligen föreskriver användning av specifika öppna chattprotokoll, pekar den samlade effekten av lagstiftningen tydligt i en riktning som förespråkar öppenhet, interoperabilitet och användarkontroll. DMA:s krav på interoperabilitet för meddelandetjänster från grindvakter är den mest direkta drivkraften, men dess implementering måste ske i harmoni med de grundläggande dataskyddsprinciperna i GDPR och ePrivacy-direktivet, samt EU:s övergripande policy att främja öppna standarder.

EU:s befintliga och kommande lagstiftningen skapar förutsättningar och incitament där öppna chattprotokoll framstår som en stark och logisk lösning för att möta de mångfacetterade kraven på interoperabilitet, säkerhet, integritet och transparens. Det handlar mindre om ett direkt mandat och mer om att forma en marknad där öppna, standardiserade och användarcentrerade lösningar har en bättre chans att konkurrera och frodas.

Svenskt lagförslag – öka interoperabilitet för offentlig sektor

"En reform för datadelning" (SOU 2023:96)⁹, är ett betänkande av Utredningen om interoperabilitet vid datadelning. Utredningen tillsattes för att analysera befintlig styrning och reglering av interoperabilitet vid datadelning inom den offentliga förvaltningen och

⁸ [09579818-64a6-4dd5-9577-446ab6219113_en](https://www.regeringen.se/09579818-64a6-4dd5-9577-446ab6219113_en)

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



till externa aktörer, samt att föreslå hur denna kan utvecklas. Syftet är att öka den offentliga förvaltningens förmåga att dela data på ett effektivt och säkert sätt, vilket är avgörande för att möta samhällsutmaningar, effektivisera verksamheter och förbättra servicen till medborgare och företag.

Utredningen konstaterar att dagens brister i interoperabilitet försvårar och ibland hindrar datadelning, vilket bromsar digitaliseringen och realiseringen av dess nyttor. Den nuvarande styrningen är fragmenterad, ofta sektorsvis, och saknar en sammanhållen nationell strategi. Detta leder till ineffektivitet, manuell hantering, sämre datakvalitet och att Sverige halkar efter andra jämförbara länder, särskilt de nordiska, som har kommit betydligt längre i att skapa regelverk och system för interoperabilitet.

För att åtgärda dessa brister föreslår utredningen en reform som inkluderar:

- "Lagen om den offentliga förvaltningens interoperabilitet" föreslås samla styrningen för att uppnå interoperabilitet vid datadelning. Lagen ska tillämpas av statliga myndigheter, kommuner, regioner, kommunalförbund och kommunala bolag. Den ska dock inte påverka befintliga regler om rätt att få tillgång till data eller skydd av personuppgifter.
- Att offentlig förvaltnings mest angelägna datadelning ska vara fullt interoperabel senast år 2030. Detta för att tydliggöra ambitionerna och skapa en mätbar målsättning
- Lagen ska innehålla definitioner av centrala begrepp som
 - Data - Information i digitalt format oberoende av medium.
 - Datadelning - Att tillhandahålla data eller ta del av data.
 - Interoperabilitet vid datadelning - Förmågan att tillhandahålla eller ta del av data genom informationssystem som interagerar med varandra.
 - Interoperabilitetslösning - En återanvändbar resurs (rättslig, organisatorisk, semantisk eller teknisk) som syftar till att uppnå interoperabilitet, t.ex. ramverk, standarder, och källkod.
 - Nationell interoperabilitetslösning - En lösning för interoperabilitet som är gemensam för den offentliga förvaltningen.
- Offentlig förvaltning ska använda nationella interoperabilitetslösningar som meddelas genom föreskrifter. Undantag kan göras om det är olämpligt av säkerhetsskäl.
- Myndigheten för digital förvaltning (Digg) får en central roll och ska b.l.a ska ta fram nationella interoperabilitetslösningar i samarbete med offentlig förvaltning, förmedla meddela föreskrifter om nationella interoperabilitetslösningar och agera som ett interoperabilitetsråd. Digg ska även analysera nyttor och kostnader på lösningarna och årligen rapportera till myndigheten om utvecklingen av interoperabilitet. De ska även vara med och normera arbetet enligt EU:s kommande interoperabilitetsförordning och beakta internationellt interoperabilitetsarbete.
- Interoperabilitet inom specifika sektorer eller områden bör styras genom speciallagstiftning för respektive sektor. Behovet av fortsatt utredning för att införa sådan styrning inom fler sektorer poängteras.
- Myndigheten för samhällsskydd och beredskap (MSB) föreslås få i uppdrag att utreda om



adekvata, gemensamma och koordinerade skyddsnivåer eller andra lämpliga säkerhetsåtgärder kan användas vid datadelning inom hela den offentliga förvaltningen och med externa aktörer. Detta för att stärka tilliten och säkerheten vid ökad datadelning.

Utredningen bedömer att förslagen kommer att skapa förutsättningar för en mer effektiv och sammanhållen offentlig förvaltning, bättre service och en ökad förmåga att hantera samhällsutmaningar. Även om det initialt kan innebära kostnader, särskilt för implementering, förväntas nyttorna på sikt överväga dessa. En viktig aspekt är att minska den "interoperabilitetsskuld" som Sverige har byggt upp. Förslagen bedöms inskränka den kommunala självstyrelsen, men detta anses nödvändigt och proportionerligt för att uppnå de eftersträvade målen. Frågan om finansiering för kommuner och regioner behandlas, där det konstateras att en stor del av åtgärderna är kopplade till teknisk utveckling som ändå behöver ske. Ambitionen är att gå ut med proposition under hösten 2025 för att under 2026 kunna stifta ny lag baserat på utredningens betänkande.

Vilka öppna protokoll tillämpas inom EU?

Matrix-protokollet är vanligt förekommande, vi har därför skapat ett eget stycke för att beskriva dess olika tillämpningar.

Utöver Matrix används t.ex. XMPP¹⁰, ett öppet federationsprotokoll för chatt. XMPP stöder federation, vilket möjliggör kommunikation mellan olika XMPP-servrar. Protokollet har en bred användning utöver snabbmeddelanden, inklusive VoIP och IoT.

Ett exempel på användning inom offentlig sektor 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.

Ett annat vanligt förekommande protokoll är SIP/SIMPLE¹¹ (Session Initiation Protocol). Även om protokollet primärt är avsett för VoIP och närvaroinformation, kan det även användas för snabbmeddelanden dock ej för beständig chatt. Det är idag möjligt att federera t.ex Skype for Business mot Cisco Webex och Meeting.

Likt matrix-protokollet ger dessa protokoll möjlighet till att följa EU:s strategiska preferens att välja öppna standarder inom offentlig sektor.

¹⁰ XMPP | The universal messaging standard

¹¹ ietf.org/rfc/rfc3261.txt



XMPP protokollet har funnits länge och har relativt omfattande användning inom vissa områden, beskrivning av specifika storskaliga implementeringar inom den offentliga saks i jämförelse med t.ex. matrix-protokollet. Även om XMPP har bred användning bedöms protokollet som föråldrat och mer komplicerat att tillämpa.

Utöver detta sker arbete inom Internet Engineering Task Force (IETF) att ta fram standard för interoperabilitet mellan chattlösningar. Dels genom framtagande av Message Layer Security¹², ett säkert protokoll för gruppnnyckelöverenskommelse, designat för asynkrona meddelandemiljöer. Det är inte ett komplett chattprotokoll i sig, utan snarare ett säkerhetslager avsett att integreras i andra protokoll, såsom XMPP eller potentiellt MIMI.

Andra IETF initiativet är MIMI¹³ - huvudmålet med More Instant Messaging Interoperability (MIMI) är att skapa en standard för olika att meddelandetjänster ska kunna kommunicera med varandra på ett standardiserat och säkert sätt. I linje med de behov som denna rapport beslyser. MIMI är tänkt att tillämpa MLS för b.la E2EE-krypteringsmekanismer. MIMI kan i dagsläget mer definieras som ett pågående arbete inom en dedikerad IETF-arbetsgrupp. Gruppens mål är att specificera den minimala uppsättning mekanismer som krävs för att göra moderna, E2EE-baserade internetmeddelandetjänster interoperabla. Arbetsgruppens bedömning av arbetet är att det är oklart vilken omfattningen blir, dvs. stödjer den eSams behovsbild, samt att det är svårt att bedöma när/om leverantörer kan tänkas börja tillämpa MIMI.

Tillämpning av öppna Matrix-protokollet inom EU

Diskussionen och tolkningen av digital suveränitet har intensifierats senaste åren. Flera europeiska aktörer har uttryckt oro för möjligheten att USA, genom CLOUD Act eller politiska beslut, skulle kunna beordra avlyssning eller avstängning av molntjänster i Europa. I rapporteringen från de länder som väljer alternativa lösningar framhålls att öppen källkod och europeiskt kontrollerade plattformar ett mer långsiktigt hållbart alternativ.

Flera europeiska länder har redan tagit konkreta steg mot att etablera nationella kommunikationsplattformar baserade på öppna protokoll, där Matrix är vanligt förekommande federationsprotokoll.

¹² RFC 9420 - The Messaging Layer Security (MLS) Protocol

¹³ More Instant Messaging Interoperability (mimi)



Frankrike – Tchapp¹⁴

Frankrike var tidigt ute att införa en nationell chattlösning baserad på Matrix. Lösningen heter **Tchap** och används för intern kommunikation mellan offentliga tjänstemän.

- Projektet drivs av DINUM – statens digitala direktorat.
- Tchapp är särskilt utvecklat med fokus på säkerhet, användarvänlighet och digital självständighet.
- Tjänsten levereras till hundratusentals användare inom franska offentliga sektorn och man har nyligen beslutat att Tchapp ska användas inom hela offentliga administrationen¹⁵
- Systemet innehåller funktioner som krypterade samtal, gruppchattar och mobilappar – och är kopplat till franska identitetstjänster.
- Lösningen är idag i huvudsak centraliserad men DINUM arbetar mot att öka decentraliseringen i lösningen

Frankrike ser federerad kommunikation med öppna protokoll som ett sätt att minska beroendet av amerikanska molntjänster och att återta kontrollen över statlig IT-infrastruktur. DINUM arbetar för att skapa en helhetslösning kallad *La Suite*¹⁶, där lösningar för informationshantering och möten håller på att utvecklas. Även Tyskland och Nederländerna bidrar aktivt i tjänsteutvecklingen. Ref - La Suite numérique · GitHub

Luxemburg – Luxchat och Luxchat4Gov¹⁷

Luxemburg har tagit ett helhetsgrepp på digital kommunikation genom två parallella lösningar.

Luxchat riktar sig till privatpersoner och företag. Luxchat4Gov är anpassad för offentlig sektor. Båda lösningarna är byggda på Matrix och erbjuder, krypterad reklamfri kommunikation, nationell drift (för att säkerställa datakontroll och säkerhet) och integration med offentliga tjänster.

Luxemburg har valt Matrix på grund av dess flexibilitet, säkerhet och möjligheten att behålla all data inom landets egna infrastrukturer.

Tyskland – brett nationellt införande

Tyskland har kommit långt i att införa Matrix på bred front inom offentlig sektor. Satsningen omfattar flera sektorer och användningsområden:

¹⁴ Tchapp - la messagerie instantanée des agents de la fonction publique

¹⁵ [Public sector employees required to use French-developed Tchapp app | Interoperable Europe Portal](#)

¹⁶ La Suite numérique

¹⁷ Luxchat – La solution de messageries instantanées du Luxembourg !



- BwMessenger¹⁸ – används av hela det tyska försvarsmakten som ett säkert alternativ till kommersiella appar.
- TI-Messenger¹⁹ – en obligatorisk lösning för sjukvården, beslutad av Gematik. Över 150 000 organisationer berörs, på sikt 80+ miljoner medborgare.
- OpenDesk²⁰ – en ny digitalt suverän arbetsplatsplattform, utvecklad av BMI (Inrikesdepartementet) och ZenDiS.
- Dataport²¹ – statligt ägd it-driftleverantör till åtta regionerna i Tyskland
- Utbildning²² och polisväsende – flera delstater har infört Matrix inom skolor, universitet och polismyndigheter. 2-3 miljoner användare.
- FITKO²³ – tillsammans med inrikesministeriet driver FITKO ett pilotprojekt för att utveckla en federerad, statlig kommunikationsplattform.
- IT Planning Council - Justizpostfach, Zentrales Bürgerpostfach, Elster-Postfach & Co ser över nästa generations kommunikationslösning²⁴

Tysklands strategi bygger på öppen källkod, suverän infrastruktur och standardisering kring ett enda protokoll – Matrix – som olika sektorer kan implementera utifrån sina behov. Till skillnad mot Frankrike tillämpar man en mer decentraliserad federerad modell med flera självständiga instanser.

EU Kommissionen

EU kommissionen planerar öka sin digitala suveränitet under 2026 genom att byta ut externa appar som Signal mot appar som bygger på det öppna protokollet Matrix. Målet är att skapa en säker, statlig kommunikationsplattform där de äger data själva och erbjuder komplement till Microsoft Teams. Behovet är att kunna verifiera alla användare och kommunicera krypterat mellan olika EU-institutioner – utan att personalen behöver använda sina privata telefonnummer samt att kunna köra i helt isolerade miljöer som ägs av EU kommissionen själva, snarare än att förlita sig på amerikanska molntjänster för allt.²⁵

Efter att ha sett andra länder (som Frankrike, Tyskland och Sverige) använda Matrix, startade kommissionen ett "Proof of Concept". De installerade en egen Matrix-server på säkra molnservrar och använde klienten Element X. Planen framåt är att expandera lösningen till hela kommissionen, använda den i högsäkerhets miljöer och koppla samman olika EU-institutioner i ett stängt, säkert nätverk.

¹⁸ Bw Messenger | Sicher. Flexibel. Open Source.

¹⁹ TI-Messenger

²⁰ The office and collaboration suite for public administration | openDesk

²¹ Who we are | Dataport

²² Why Matrix? :: Matrix Documentation

²³ Matrix Conference 2024 | FITKO

²⁴ Matrix replacing MJP, ZBP & Co: Will state mailbox chaos belong to the past? | heise online

²⁵ [Trialing Matrix within the European Commission for resilient and sovereign communications - YouTube](#)



Österrike – ELGA och vårdsektorn²⁶

Österrike planerar att införa Matrix som kommunikationslager i ELGA – landets nationella system för elektroniska patientjournaler. Tanken är att olika vårdgivare ska kunna, skicka och ta emot krypterad patientinformation, kommunicera säkert i realtid mellan olika aktörer inom vård och omsorg samt integrera med andra system via federerad identitet

Initiativet har inspirerats av tyska Gematik och drivs av önskan att förbättra interoperabilitet, federation och säkerheten i patientkommunikation.

NATO – säker kommunikation mellan allierade²⁷

NATO har utvecklat en egen chattapp vid namnet NICE en Matrix-baserad lösning för icke-sekretessbelagd kommunikation för allierade inom NATO. Syftet är att erbjuda en säker, interoperabel och federerad kommunikation (chatt, fildelning etc.) mellan olika NATO-länder och partners.

NICE erbjuder den typ av modern, säker och federerad kommunikationsplattform som NATO och dess medlemmar strävar efter.

Vilka fördelar ser länder med matrix-protokollet?

Gemensamma nyttoeffekter som lyfts från de länder som valt att standardisera på matrix-protokollet är:

- **Öppenhet** - Protokollet är öppet och väldokumenterat.
- **Säkerhet** - Stöd för end-to-end-kryptering i samtliga funktioner, kontroll över metadata och lokal drift.
- **Suveränitet och rådighet**- Möjliggör nationell kontroll över digital infrastruktur.
- **Decentralisering** – möjlighet att välja leveransform, placering och få riskspridning
- **Interoperabilitet** - Stödjer federation – olika organisationer kan kommunicera med varandra utan att använda samma leverantör, tjänst eller klient.
- **Integration** - Möjlighet att ansluta via API, autentisering (SAML, OIDC) och koppla till andra system (ex. Slack, Zoom, Teams, e-post).

Se bilaga ”Bilaga_F_Matrix och EU-tillämpningar_eSammallen” för en fördjupning kring matrix-protokollet

²⁶ Austrian electronic health records (ELGA)

²⁷ NI2CE Messenger – The Innovation Hub for Allied Command Transformation



Sverige – myndigheters behov och förutsättningar

I Sverige växer intresset för federerade lösningar för realtidskommunikation inom offentlig sektor. Samtidigt råder ett fragmenterat nuläge, där många aktörer söker vägledning, teknisk riktning och juridisk trygghet. Nedan följer en sammanfattning av dialoger som skett med centrala aktörer såsom **Sunet**²⁸, **Sambruk**²⁹, **Internetstiftelsen**³⁰, **RISE**³¹ och **MSB**^{32 33}

Sunet, som tillhandahåller nät- och identitetstjänster till högre utbildning och forskning, uttrycker liknande behov. Deras erfarenhet visar att det finns ett växande intresse för federerad kommunikation – men också osäkerhet kring vilka tekniska standarder som är bäst lämpade och hur dessa kan kopplas till svensk identitetshantering (exempelvis SAML, eduGAIN och Skolfederation).

Sunet betonar också vikten av stark identitet i alla federerade lösningar. De lyfter särskilt riskerna med appar som Signal, där identiteten i praktiken bygger på telefonnummer – något som kan vara olämpligt i myndighetssammanhang där entydig identifiering krävs.

Sunet ingår i ett EU-projekt där universitet ska samverka kring hur man kan kommunicera med varandra på ett mer sömlöst sätt. Här nämns matrix-protokollet som en potentiell möjliggörare.

Sunet ska också genomföra en PoC på Element (matrix-baserad klient) som ersättare för Slack som man använder idag inom delar av Sunet:s organisation.

Internetstiftelsen framhåller att Sverige historiskt har gynnats av ett decentraliserat internetklimat och ett brett engagemang i öppna protokoll. Men man varnar för att alltför mycket kontroll i händerna på enskilda plattformslieferantörer kan undergräva digital suveränitet. Därför behöver offentlig sektor ta en mer aktiv roll i att bygga eller kravställa öppna och federerade lösningar.

Under möten har det lyfts att det finns ett behov av nationell samordning för att skapa vägledning – både tekniskt och juridiskt – kring hur federation kan genomföras på ett sätt som uppfyller kraven i GDPR, NIS2 och nationell säkerhetslagstiftning. Det saknas

²⁸ Sunet

²⁹ Sambruk – Kommunal verksamhetsutveckling

³⁰ Internetstiftelsen

³¹ Svensk forskning för hållbar tillväxt | RISE

³² MSB – Myndigheten för samhällsskydd och beredskap

³³ Följande sammanställning bygger på dialoger, remissvar och offentliga källor från aktörer såsom Sunet, Sambruk, Internetstiftelsen, RISE och MSB



idag ett tydligt nationellt ramverk som överbryggat teknik, identitet, juridik och verksamhetsnytta.

Internetstiftelsen ser att identitetsfederation har en nyckelroll för att lyckas med en robust och säker chattfederation. Här kan DIGG ha en central roll i frågan då de planerar att bygga nationell identitets- och auktorisationsarkitektur baserat på OI DF (OpenID Federation). Det skapar potential att utnyttja en gemensam federationsinfrastruktur även för realtidskommunikation – så lösningarna blir kompatibla.

RISE har lyft särskilt att interoperabilitet inte får ske på bekostnad av säkerhet. Deras experter understryker att totalsträckskryptering bör vara en självklar utgångspunkt i all realtidskommunikation och öppna protokoll, särskilt i offentlig sektor. Detta gäller oavsett om kommunikationen är intern, mellan myndigheter eller i framtiden inkluderar medborgarkontakt.

RISE menar att det i vissa fall kan behövas två olika system – ett som är öppet och interoperabelt, och ett annat som används för särskilt känslig kommunikation där säkerheten går först. De lyfter också att det är viktigt att staten väljer protokoll, inte produkter – och att kontroll över metadata och drift är avgörande för att undvika framtida inlåsning.

RISE ser matrix-protokollet som ett intressant alternativ för chattfederation eftersom det är decentraliserat, bygger på öppen källkod, totalsträckskryptering som standard och har stöd för federation. De jämför det positivt med e-postens modell – där varje aktör driver sin egen server men ändå kan kommunicera över gränser.

Man lyfter även att offentlig sektor bör anamma öppna protokoll och lösningar för sociala medier som t.ex. ActivityPub eller AT-protokollet. En av de stora fördelarna med dessa protokoll är att myndigheter får rådighet över sina demokratiska kommunikationskanaler.

Myndigheten för Samhällsskydd och Beredskap (MSB) ser att det finns ett behov av att kunna upprätthålla myndigheternas funktioner även vid störningar i digital infrastruktur, till exempel om delar av landet blir avskurna från centrala tjänster. Man pekar specifikt på följande regelverk från Förordningen om statliga myndigheters beredskap (2022:524) som innehåller ett antal paragrafer som direkt kan kopplas till behovet av säkra, robusta och decentraliserade kommunikationslösningar:



§7: Myndigheter ska identifiera samhällsviktig verksamhet och analysera sårbarheter inför fredstida kriser och höjd beredskap. Det ingår också att arbeta systematiskt för att kunna upprätthålla verksamheten (kontinuitet), samt verka för att andra aktörer inom området gör detsamma.

§10: Myndigheter ska beakta totalförsvarets krav och planera för att verksamheten ska kunna fortsätta även vid höjd beredskap, utifrån tillgång till personal och rådande förhållanden.

§20–21: Beredskapsmyndigheter ska ha god förmåga att motstå hot och risker, förebygga sårbarheter och genomföra sina uppgifter vid fredstida kriser och höjd beredskap.

Mot bakgrund av ovanstående blir det tydligt att krav på funktionalitet under kris och krig ställer särskilda krav på offentlig sektors förmåga att kommunicera med varandra. En decentraliserad chattinfrastruktur, baserad på öppna standarder och federerade lösningar, kan vara ett sätt att minska beroendet av enskilda leverantörer och centrala molntjänster. En sådan lösning kan stärka motståndskraften vid störningar, minska risken för avbrott vid till cyberangrepp samt möjliggöra fortsatt kommunikation även om en del av nätverket slås ut. Detta ligger i linje med det ansvar som myndigheter, särskilt beredskapsmyndigheter, har enligt gällande regelverk.

Sambruk, ett samverkansorgan för kommuner, lyfter att det finns ett stort behov av bättre digital samverkan, särskilt i kommunal verksamhet där samarbete med regioner och statliga myndigheter är vardag. Men tekniska lösningar för säker chatt över organisationsgränser saknas ofta, eller bygger på tillfälliga bryggor snarare än hållbara standardiserade protokoll.

Sambruk belyser att ett öppet protokoll i sig inte hanterar frågor som t.ex. digital suveränitet och rådighet. Om många offentliga aktörer ändå väljer externa driftleverantörer som t.ex. träffas av extraterritoriell lagstiftning kan suveränitet undermineras. På så vis kan federationsnätverket bli sårbart vilket kräver tydliga principer och policys.

Att införa ett öppet chattprotokoll är komplext och kräver djupt tekniskt kunnande av leverantörer. En federation kräver säker certifikathantering och att man sköter tillitskedjorna – vem som egentligen litar på vem. Utöver detta ser Sambruk behov av en gemensam styrgrupp som ger möjlighet styra arbetet och styra utvecklingen av offentlig sektors federation på sett ansvarsfullt sätt.

Sambruk ser en risk att en ny form av centralisad inläsning skapas om endast ett fåtal aktörer sätter upp federationslösningar.



Ämnesråd inom digitalisering, data och digital förvaltning på **Regeringskansliet** anser att eSam:s arbete med gemensamt protokoll för chattfederation har tydliga synergier med ”En reform för datadelning” (SOU 2023:96)” och skulle kunna vara en fråga att hantera tidigt om lagförslaget går igenom. Ursprunglig ambition var att lagen skulle träda i kraft redan 1 januari 2025 men på grund av prioriterade frågor (b.la. kriget i Ukraina, Nato-processen och USA-vale) har tidsplanen justerats.

Norden – hur våra grannländer?

Arbetsgruppen har sökt kontakt med våra nordiska grannar för att förstå hur de arbetar med denna fråga men ännu inte hittat rätt kontaktytor. Därmed rekommenderar vi i ev. fortsatt arbetet att knyta kontakt med våra grannländer. Det enda exempel som vi snappat upp hittills är ett SMS-liknande krypterat meddelandesystem (Meshtastic³⁴), baserat på öppen källkod som, som Århus kommun pilotar. Syftet med systemet är att säkerställa kommunikation i svåra förhållanden, likt det strömavbrott som påverkade Iberiska halvön (Spanien och Portugal) april 2025.

Denna bilaga har uppdaterats utifrån synpunkter från RISE, Sambruk, DIGG, MSB, Sunet och Internetstiftelsen under remissrundan våren 2025.

³⁴ Meshtastic



Bilaga B: Teknisk jämförelse av protokoll

Sammanfattning

Det finns ingen universellt "bästa" protokoll för alla ändamål, utan snarare olika protokoll som är optimerade för olika ändamål och behovsbilder.

XMPP-protokollet är historiskt starkt men kräver mer tillägg och konfiguration för full funktionalitet, utvecklingstakten bedöms även som låg. Tillämpningen är begränsad inom EU.

Signal erbjuder stark säkerhet men saknar federation och öppen integration samt begränsat stöd för identitetshantering. Riktat mot privatpersoner.

WebRTC, SIP och andra protokoll lämpar sig bättre för röst/video och kompletterande funktioner – inte för helhetslösningar inom federerad chatt.

ActivityPub har stor potential för offentlig sektor när det gäller sociala medier givet dess stöd för decentraliserad kommunikation. Protokollet har dock inte de förmågor som krävs för chattfederation och realtidskommunikation.

MLS och MIMI har potential att tillsammans bli en gemensam standard för chattfederation. Utvecklingen av framförallt MIMI är dock i tidigt stadiet och arbetet bedöms vara komplex och tidskrävande process där flera kommersiella aktörer behöver hitta en gemensam grund, innan protokollet har möjlighet att bli en formell RFC standard.

Matrix-protokollet sticker ut som det mest kompletta alternativet för federerad, säker, realtidskommunikation och chatt – särskilt för offentlig sektor. Protokollet ger även god integration med befintlig infrastruktur via t.ex. bryggor mot e-post, Slack, Teams och andra plattformar. Denna bedömning stärks genom att flera EU länder börjat investera och bygga lösningar baserat på matrix-protokollet.

Skillnader mellan öppna och proprietära protokoll

Ett kommunikationsprotokoll kan beskrivas som en uppsättning regler och specifikationer som definierar hur data ska formateras, sändas, tas emot och tolkas mellan olika datorsystem. Protokollen kan antingen vara öppna eller proprietära ("stängda"), en distinktion som har betydelse för deras användning och de effekter de medför.



Öppna Standarder/Protokoll

En standard beskrivs ofta som en gemensam och överenskommen lösning på ett återkommande problem eller behov. En öppen standard, och därmed ett öppet protokoll, kännetecknas av att dess specifikation är offentligt och fritt tillgänglig för alla att studera, implementera och använda. Eventuella immaterialrätter kopplade till standarden licensieras vanligtvis på rättvisa, rimliga och icke-diskriminerande (FRAND¹) villkor, och helst helt utan royaltyavgifter. Utvecklingen och underhållet av öppna standarder sker ofta genom en transparent process där alla intressenter har möjlighet att delta och påverka. Centrala egenskaper hos öppna protokoll inkluderar främjandet av interoperabilitet, återanvändbarhet och att det inte föreligger några godtyckliga begränsningar för deras användning. De möjliggör kompatibilitet mellan produkter och tjänster från olika tillverkare, vilket i sin tur stimulerar fri konkurrens på marknaden.

Proprietära Standarder/Protokoll

Proprietära standarder och protokoll, i motsats till de öppna, är tekniska specifikationer som kontrolleras av en enskild leverantör eller organisation. Specifikationerna är ofta inte offentligt tillgängliga, utan kan vara skyddade som affärshemligheter eller endast erbjudas under restriktiva licensvillkor. I många fall är de utformade så att de inte lätt kan implementeras av oberoende utvecklare utanför den kontrollerande entitetens ekosystem. Dokumentationen kan vara otillräcklig, eller i vissa fall avsiktligt utformad för att försvåra oberoende implementation och därmed skydda leverantörens marknadsposition. Egenskaper som ofta förknippas med proprietära protokoll är begränsad interoperabilitet med system utanför leverantörens kontrollsfär och en inneboende risk för leverantörsinlåsning.

Marknaden för öppna chattprotokoll

I en digital värld där kommunikation utgör en central del av både privatliv och verksamhet, spelar valet av underliggande protokoll en viktig roll. Öppna protokoll för chattkommunikation erbjuder ett standardiserat sätt att kommunicera, vilket möjliggör interoperabilitet mellan olika applikationer och tjänster. Nedan följer en beskrivning och analys av de vanligaste förekommande öppna protokollen på marknaden

XMPP (Extensible Messaging and Presence Protocol)

Extensible Messaging and Presence Protocol (XMPP) är mer känt från sina rötter i Jabber. Även om det inte alltid hamnar i rampljuset på samma sätt som vissa nyare protokoll, pågår en kontinuerlig utveckling driven av XMPP Standards Foundation (XSF) och en aktiv community. Protokollet har en decentraliserade arkitektur, vilket

¹ [FRAND-patent – Wikipedia](#)



innebär att det inte är beroende av en central server utan kan distribueras över flera servrar som kommunicerar med varandra. XMPP stödjer en rad chattfunktioner, inklusive textmeddelanden, närvaroinformation, gruppchatt, filöverföring. Stöd för röst- och videosamtal hanteras genom tillägg, grundläggande stöd saknas i XMPP.

Utvecklingstakten för XMPP kan beskrivas som stabil snarare än revolutionerande. Protokollets kärna är väletablerad (specificerad i RFC 6120 och RFC 6121), och mycket av utvecklingen sker genom XMPP Extension Protocols (XEPs). Dessa XEPs tillåter att protokollet utökas och anpassas för nya funktioner och användningsområden utan att bryta kompatibiliteten med grundläggande implementeringar. Processen för att standardisera XEPs innefattar olika stadier från experimentell till slutgiltig, vilket kan ta tid men också bidrar till en robust och genomtänkt utveckling. Utmaningarna ligger ibland i den volontärsdrivna naturen och att säkerställa att implementeringar brett anammar nya tillägg.

WebRTC (Web Real-Time Communication)

WebRTC (Web Real-Time Communication) är en teknik som möjliggör realtidskommunikation, såsom röstsamtal, videosamtal och dataöverföring, direkt mellan webbläsare och enheter i ett peer-to-peer-nätverk. Målet med WebRTC är att tillhandahålla dessa funktioner utan krav på plugins eller tredjeparts-mjukvara, vilket revolutionerat möjligheterna för webbaserade kommunikationstillämpningar. I grunden är WebRTC en uppsättning standarder, protokoll och JavaScript API:er som gör det möjligt för webbläsare att utbyta mediaflöden och data direkt med varandra. Istället för att all kommunikation går via en central server (klient-server-modell), strävar WebRTC efter att upprätta direkta förbindelser mellan användarnas enheter. Detta minskar fördröjning och förbättrar prestandan för realtidsapplikationer.

WebRTC har uppnått en hög grad av mognad och är idag en etablerad och allmänt implementerad standard. Utvecklingen har drivits gemensamt av World Wide Web Consortium (W3C), som ansvarar för API:erna i webbläsaren, och Internet Engineering Task Force (IETF), som specificerar underliggande protokoll och säkerhetsaspekter.

SIP/SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions)

Session Initiation Protocol (SIP) är ett signaleringsprotokoll som används i stor utsträckning för att upprätta, modifiera och avsluta realtids-sessioner som röst- och videosamtal över IP-nätverk. Protokollet är en central komponent i moderna kommunikationssystem, särskilt inom IP-telefoni (VoIP). SIP är ett relativt moget protokoll, standardiserat av Internet Engineering Task Force (IETF). Utvecklingstakten



för kärnspecifikationerna är inte lika snabb som för vissa nyare, mer agila protokoll. Dock sker en kontinuerlig utveckling genom publiceringen av Request for Comments (RFC) som antingen förfinar befintlig funktionalitet eller introducerar tillägg för att möta nya krav och användningsområden. Utvecklingen drivs av behovet att förbättra säkerhet, interoperabilitet och stödja nya kommunikationstjänster. Arbetet sker inom olika IETF-arbetsgrupper och bidrag från leverantörer och utvecklare som implementerar SIP i sina produkter och tjänster.

Funktioner som multimediasessioner, inklusive röst- och videosamtal samt snabbmeddelanden genom tillägget SIMPLE stöds. Protokollet har inte inbyggt stöd beständig chatt eller totalsträckskryptering.

WebSocket

WebSocket är ett kommunikationsprotokoll som möjliggör dubbelriktad (full-duplex) och ihållande kommunikation över en enda TCP-anslutning. Till skillnad från den traditionella HTTP-modellen, där klienten initierar varje begäran och servern svarar, tillåter WebSocket både klienten och servern att skicka data till varandra när som helst efter att anslutningen har upprättats. Detta gör WebSocket idealiskt för realtidsapplikationer som kräver låg fördröjning och frekventa datauppdateringar

WebSocket är ett moget och brett implementerat protokoll som har varit en officiell webbstandard under lång tid. WebSocket-protokollet standardiserades av IETF (Internet Engineering Task Force) i RFC 6455 år 2011. W3C (World Wide Web Consortium) har specificerat WebSocket API:et, vilket definierar hur webbläsare kan interagera med WebSocket-anslutningar via JavaScript. Dessa standarder är stabila och har genomgått omfattande granskning.

IRC (Internet Relay Chat)

IRC är ett textbaserat applikationsskiktsprotokoll och ett av de äldsta textbaserade chattprotokollen som utvecklades sent 1980-tal för realtidskommunikation i form av chatt. Det möjliggör kommunikation i grupper (kanaler) samt privatmeddelanden mellan enskilda användare. IRC var en av de tidigaste formerna av realtidsinternetkommunikation som blev allmänt populär och ligger till grund för många koncept som återfinns i dagens meddelandetjänster.

IRC är ett moget protokoll i den meningen att dess kärnspecifikationer är funnits länge och väletablerade. Däremot har dess status och användning förändrats markant över tid i takt med framväxten av nyare kommunikationstekniker.



MQTT (Message Queuing Telemetry Transport)

MQTT (Message Queuing Telemetry Transport) är ett lättviktigt meddelandeprotokoll som designats för maskin-till-maskin (M2M) kommunikation och används brett inom Internet of Things (IoT). Protokollet bygger på en "publicera-prenumerera"(pub-sub)-modell, vilket skiljer sig från den traditionella klient-server-modellen där klienten direkt begär data från en server. Denna modell gör MQTT mycket effektivt för miljöer med begränsad bandbredd, hög fördröjning eller opålitliga nätverk, samt scenarier med ett stort antal anslutna enheter.

MQTT är ett moget, stabilt och brett antaget protokoll, särskilt framstående inom IoT-världen tack vare sin lättviktiga design och effektiva "publicera-prenumerera"-modell. Dess standardisering och det rika ekosystemet av implementationer gör det till ett pålitligt val för realtidsdataöverföring i många olika tillämpningar.

AMQP (Advanced Message Queuing Protocol)

AMQP (Advanced Message Queuing Protocol) är ett öppet standardiserat applikationsskiktprotokoll för meddelandehantering. Det är designat för att möjliggöra robust och tillförlitlig meddelandeutväxling mellan applikationer och system, oavsett plattform eller programmeringsspråk. AMQP är särskilt lämpat för meddelandesystem på enterprise-nivå, systemintegration och scenarier där tillförlitlighet och avancerad routning är viktig.

AMQP är ett moget och robust protokoll, väl etablerat för avancerad meddelandehantering i företags- och integrationsscenarier där tillförlitlighet, flexibel routning och garanterad leverans är av yttersta vikt. Dess standardisering och det breda stödet i form av broker- och klientimplementationer bidrar till dess pålitlighet och fortsatta relevans.

RCS (Rich Communication Services)

RCS (Rich Communication Services) är ett kommunikationsprotokoll som syftar till att ersätta och modernisera de åldrande SMS- och MMS-standarderna för mobilmeddelanden. Målet är att erbjuda en mer interaktiv och appliknande meddelandeupplevelse direkt i mobilens inbyggda meddelandeapplikation, utan att kräva nedladdning av separata "over-the-top" (OTT) appar som WhatsApp eller Messenger.

Till skillnad från SMS/MMS som primärt använder det kretskopplade nätverket, bygger RCS på IP Multimedia Subsystem (IMS) och använder paketbaserade data (mobildata eller Wi-Fi) för meddelandeöverföring. När en RCS-anslutning inte är möjlig (t.ex. på



grund av bristande täckning eller inkompatibel mottagare), kan meddelandet falla tillbaka till att skickas som ett vanligt SMS eller MMS.

Som protokoll och ekosystem är RCS fortfarande i en utvecklings- och mognadsfas jämfört med äldre protokoll som SMS eller nyare men mer nischade protokoll som MQTT. Även om kärnstandarderna finns, pågår fortfarande arbete med att säkerställa full global interoperabilitet, en konsekvent användarupplevelse över olika plattformar och operatörer, samt att hantera utmaningar relaterade till roaming, integritet och affärsmodeller för operatörerna. Google och Apple arbetar med att möjliggöra interoperabilitet med RCS mellan sina meddelandetsjänster. Standardprotokollet saknar idag end-to-end-kryptering.

MLS

MLS (Message Layer Security) är ett relativt nytt protokoll som designats specifikt för att tillhandahålla effektiv och säker end-to-end-kryptering för gruppmeddelanden i stor skala. Målet är att lösa de utmaningar som uppstår med nyckelhantering och säkerhet i stora gruppkonversationer, problem som blir mer komplexa ju fler deltagare som finns och ju oftare medlemmar läggs till eller tas bort.

MLS är formellt definierad i RFC 9420 och 9750(arkitektur), publicerad i juli 2023 som en föreslagen standard. Dess primära syfte är att tillhandahålla ett högeffektivt och säkert protokoll för gruppnyckelöverenskommelse, designat för asynkrona meddelandemiljöer. Det är inte ett komplett chattprotokoll i sig, utan snarare ett säkerhetslager avsett att integreras i andra protokoll, såsom XMPP, Matrix eller potentiellt MIMI. MLS fokuserar på att tillhandahålla ett säkert och effektivt kryptografiskt lager för gruppkommunikation. Protokollet används i olika omfattning i chattlösningar från Wire, Google, AWS(Wickr) och Matrix.

Som standard betraktas MLS-protokollet som stabilt efter att ha genomgått IETF:s granskningsprocess. Däremot är ekosystemet kring MLS, inklusive en bred uppsättning av färdiga lösningar, fortfarande under uppbyggnad. Utmaningar kvarstår med att uppnå bred tillämpning, säkerställa interoperabilitet mellan olika MLS-implementationer i praktiken och hantera integrationen av MLS i komplexa befintliga meddelandesystem. Säkerhetsegenskaperna har granskats formellt av olika instanser, men som med alla nya kryptografiska protokoll krävs tid och bred användning för att identifiera eventuella oväntade sårbarheter.

More instant Messaging Interoperability (MIMI)



MIMI (More Instant Messaging Interoperability) är inte ett enskilt protokoll på samma sätt som t.ex WebRTC, WebSocket, Matrix, MQTT, AMQP eller MLS. Istället är MIMI ett initiativ och en arbetsgrupp inom IETF (Internet Engineering Task Force) vars mål är att specificera en ram och relaterade protokoll för att möjliggöra säker och interoperabel meddelandehantering mellan olika meddelandetjänster och plattformar. Det primära syftet är att bryta ner de ”silos” som finns idag, där användare på olika chattplattformar inte kan kommunicera med varandra.

MIMI är ett standardiseringsinitiativ inom IETF som är tänkt att hantera den komplexa utmaningen med interoperabilitet mellan meddelandetjänster med fokus på säkerhet. Ramverket och dess relaterade specifikationer är under utveckling och har ännu inte uppnått fullständig standardstatus. Implementering och bred adoption är dock en bit bort i framtiden. MIMI är därför i ett tidigt skede av sin mognadscykel jämfört med mer etablerade internetprotokoll. Dess framgång kommer att bero på slutförandet av standarderna och på att ett tillräckligt antal meddelandeleverantörer väljer att implementera och samarbeta baserat på MIMI-ramverket.

ActivityPub

ActivityPub är ett decentraliserat socialt nätverksprotokoll som möjliggör för olika sociala plattformar och applikationer att kommunicera med varandra i ett federerat nätverk, ofta kallat "Fediverse". Till skillnad från traditionella centraliserade sociala nätverk (som drivs av ett enda företag), möjliggör ActivityPub att användare på en plattform (en "instans" eller server) kan interagera med användare på en annan plattform som också stöder protokollet. Målet är att skapa ett öppet och sammanlänkat socialt webb-ekosystem där användare har mer kontroll över sina data och sin online-upplevelse.

ActivityPub är ett öppet, decentraliserat socialt nätverksprotokoll som standardiserades av World Wide Web Consortium (W3C) 2018. Det utgör ryggraden i det så kallade "Fediverse" (en federation av olika, interoperabla sociala nätverk).

ActivityPub ett moget och standardiserat protokoll som framgångsrikt driver Fediverse som ett decentraliserat alternativ till traditionella sociala nätverk. Själva specifikationen är stabil och brett implementerad, men ekosystemet som helhet är fortfarande under utveckling när det gäller att lösa utmaningar relaterade till storskalig drift, moderering och användarupplevelse. Dess mognad ligger i att vara en etablerad och fungerande standard med en växande bas av implementationer och användare

Matrix



Matrix är ett öppet standardiserat protokoll för säker, decentraliserad realtidskommunikation. Det skiljer sig från mer traditionella protokoll genom sin federerade arkitektur, där olika servrar kan utbyta meddelanden med varandra, vilket ger användarna större kontroll över sin data och valfrihet av klient och server

Utvecklingstakten för Matrix-protokollet är hög och dynamisk. Projektet drivs aktivt av Matrix.org Foundation och en engagerad global community av utvecklare. Utvecklingen sker öppet med fokus på snabb iteration och implementering av nya funktioner och förbättringar. Detta inkluderar ständigt arbete med att förbättra prestanda, skalbarhet, användarupplevelse och säkerhet. Konceptet "Matrix 2.0" visar på ett driv mot att införa betydande förbättringar, såsom snabbare synkronisering ("Sliding Sync"), modernare autentiseringsmekanismer (Native OIDC) och inbyggt stöd för end-to-end-krypterade gruppsamtal (MatrixRTC).

Matrix erbjuder end-to-end-kryptering som standard för privata konversationer och stöder bryggor till många andra populära kommunikationsprotokoll och tjänster.

Matrix arbetar aktivt med att integrera MLS i Matrix-protokollet, inklusive utveckling av "Decentralized MLS" (DMLS) för att anpassa MLS till federerade och decentraliserade miljöer.

SimpleX Chat Protocol

SimpleX Chat Protocol är ett modernt, decentraliserat meddelandeprotokoll som medvetet använder sig av konceptet med enkelriktade meddelandeköer (simplex) för att uppnå en hög grad av integritet och anonymitet för sina användare. Till skillnad från de flesta andra meddelandetjänster som bygger på användaridentifierare (som telefonnummer, e-postadresser eller användarnamn), länkar SimpleX inte användare till permanenta identiteter

Utvecklingstakten för SimpleX Chat Protocol och dess tillhörande applikationer är relativt hög och drivs av SimpleX-projektet. Eftersom det är ett nyare protokoll sker aktiv utveckling för att lägga till funktioner, förbättra prestanda och stärka säkerheten baserat på feedback från communityn och nya insikter inom integritetsbevarande kommunikation. Utvecklingen är öppen och följer en tydlig färdplan.

På grund av dess centraliserade arkitektur och att det saknas formell standardisering bedöms protokollet som svårt att skala till myndighetsgemensam federation i dagsläget.



Tabellen nedan sammanfattar de tekniska huvudegenskaperna hos respektive protokoll baserat på kriterier som federation, kryptering, mediastöd, skalbarhet och mognadsgrad.

Tabell 1: Tekniska egenskaper och jämförelse av utvalda kommunikationsprotokoll

Protokoll	Stöd för federation	Stöd för E2EE	Mediastöd	Bryggning	Skalbarhet	Mognad
XMPP	Ja	Via tillägg	Text, Filer (Jingle/HTTP), VoIP (Jingle)	Ja	Hög	Mogen (IETF RFCs, XSF XEPs). Låg utvecklings-takt
Matrix	Ja	Inbyggt	Text, Filer, Bilder, Ljud, Video, VoIP	Ja, omfattande	Hög	Mognande (Matrix.org Spec, ingen IETF RFC)
Signal	Nej	Inbyggt	Text, Filer, Bilder, Ljud, Video, Samtal	Nej	Hög (Centraliserad infrastruktur)	Mogen (Protokoll väletablerat, App populär)
WebRTC	Nej	Inbyggt	Realtids Ljud/Video, Godtycklig Data (Data Channels)	Ja	Hög (P2P), Begränsad av signalering/TURN	Mogen (W3C Rec, IETF RFCs)
IRC	Ja	Via tillägg	Primärt Text, Filer (DCC - osäkert/föråldrat)	Ja	Medel (Begränsad av netsplits, äldre design, beror på IRCd)	Mogen (men åldrande, IETF RFCs)
RCS	Ja (Operatörskontrollerad)	Implementationspecifik	Text, Filer, Högupplöst media, Rich Cards (ersätter SMS/MMS)	Begränsad	Hög (Beroende på operatörens IMS-infra.)	Mognande (GSMA Universal Profile, ökande tillämp.)
MLS	N/A	Ja	N/A	Ja	Ja	Mognande (standard RFC 9420)



MIMI	Ja (draft)	Ja, via MLS	För tidigt att avgöra	För tidigt att avgöra	För tidigt att avgöra	Låg mognad (IETF status Internet-Drafts). Inte ett protokoll
Activity-Pub	Ja	Nej (Pågående arbete via tillägg/FEPs)	Text, Länkar, Mediaobjekt (AS2), Binärdata (beroende på impl.)	Möjlig	Medel/Hög (Beroende på serverimpl., fan-out/inbox-belastning)	Mogen (W3C Rec)
MQTT	Nej	Via applikationslager	Godtycklig binärdata (Payload), optimerat för små meddelanden (IoT)	Ja	Mycket Hög (Beroende på mäklarimpl. och klustring, designad för miljoner)	Mogen (OASIS Standard, ISO/IEC)
SIP	Ja	Endast signalering	Ljud/Video (via RTP), Annat via SDP-förhandling	Ja	Mycket Hög (Carrier-grade implementationer finns)	Mogen (IETF RFCs, VoIP-ryggrad)
SimpleX	Nej	Inbyggt	Text, Filer (XFTP), Bilder, Ljud, Video, Samtal (WebRTC-signalering)	Nej	Okänd/Experimentell	Tidig (Ingen formell standard)

Brygglösningar

Två huvudsakliga strategier tillämpas för att uppnå interoperabilitet: att bygga bryggor mellan existerande, ofta proprietära, plattformar och att tillämpa öppna federationsprotokoll.



Befintliga brygglösningar skapar förutsättningar att sammankoppla öppna chattlösningar med proprietära chattlösningar som Slack, Microsoft Teams och Zoom. Ett exempel är m.io.

Utmaningen med interoperabilitet inom chattlandskapet är komplex, och det finns ingen universallösning som passar alla. Valet mellan att använda bryggor för att koppla samman befintliga slutna system och att använda öppna federationsprotokoll kräver avvägning mellan omedelbar bekvämlighet och långsiktig kontroll, öppenhet och säkerhet.

Brygglösningar baserade på öppen källkod, som Matterbridge och Matrix-bryggor, erbjuder ett sätt att ansluta till de dominerande plattformar där användarna redan finns. Deras styrka ligger i att möjliggöra kommunikation över ekosystemgränser utan att kräva att alla byter plattform. Denna bekvämlighet kommer dock till priset av betydande nackdelar som kompatibilitet och API-beroenden, inte bibehållen end-to-end-kryptering, tappade funktioner och ett fortsatt beroende av de underliggande slutna plattformarna samt eventuella bryggleverantörer.

En form av hybridstrategi kan bli aktuell för offentlig sektor, där ett federerat protokoll utgör kärnan och bryggor används selektivt för nödvändiga externa anslutningar.

Denna bilaga har uppdaterats utifrån synpunkter från RISE, Sambruk, DIGG, MSB, Sunet och Internetstiftelsen under remissrundan våren 2025.



Bilaga C – SWOT över möjliga vägval

Sammanfattning

Sammantaget visar SWOT-analysen att vägvalen innebär olika avvägningar mellan snabbhet, kontroll, kostnad och långsiktig hållbarhet.

Vägval 1 och 6 erbjuder tillfällig bekvämlighet men innebär stora risker för långsiktig fragmentering och beroende. Vägval 2 och 5 kan fungera som övergångslösningar, men saknar stabilitet och samordnad riktning.

Vägval 3 och 4 bygger båda vidare på öppenhet och interoperabilitet, men vägval 3 är det enda alternativ som i nuläget bedöms möta samtliga kända krav på öppenhet, EU-kompatibilitet, säkerhet och möjlighet till självständig vidareutveckling.

Baserat på analysen framstår vägval 3 – en federerad öppen lösning – som det mest långsiktigt hållbara alternativet. Vägval 3 och 4 kan kombineras.

För att lyckas krävs ett tydligt ramverk för styrning, resurser samt förvaltning av förtroende och certifikat ("trust") – särskilt om federationen ska bli en långsiktig, samhällsbärande lösning.

SWOT

Detta SWOT-underlag visar sex möjliga vägval för hur offentlig sektor kan organisera sin digitala chattkommunikation. Syftet är att belysa styrkor, svagheter, möjligheter och risker för varje alternativ. Analysen är inte ett facit, utan ett verktyg för diskussion och prioritering.

Tidslinjen i Bilaga D bygger på vägval 3 (federerad öppen lösning), men analysen här hjälper till att förstå konsekvenserna om andra strategier skulle föreslås, komplettera eller ersätta det huvudsakliga spåret.



Tänk också på att vägvalen inte är ömsesidigt uteslutande – vissa kan fungera som steg eller parallella lösningar i en övergångsfas.

Vad vi menar med de sex (6) förslagen

1. **Fortsätta som idag** innebär att många myndigheter tills vidare bibehåller verktyget Skype för sin chatt-kommunikation. De flesta myndigheter har etablerat en federation mellan sina respektive Skype-miljöer. Denna bibehålls tills dess att Skype försvinner som produkt. Myndigheter som redan valt eller väljer någon annan lösning än Skype kommer antingen att hamna utanför den tidigare ”gemenskapen” eller tvingas behålla Skype parallellt som lösning för att samverka med andra.
2. **Central brygglösningar** innebär att någon part tar ansvar för att ge myndigheter möjligheten att ansluta sina chatt-verktyg till en nationell integrationshub. Så länge dessa myndigheters chatt-verktyg uppfyller specifikationen kommer de att kunna anslutas. Brygglösningen kommer, om den ska fungera tvingas stödja en mängd olika protokoll och produkter.
3. **Federerad öppen lösning** innebär att eSam ställer krav på sina medlemmar (och andra samarbetspartner) att chatt-verktyg man använder följer standarden för detta öppna protokoll. Kravet bör även förankras på departement och hos myndigheter utanför eSam. Varje myndighet som uppfyller kraven kan därefter på ett enklare sätt bli interoperabel med annan part som också uppfyller aktuell standard. Varje myndighet vet vilken väg som leder till federation och kan skapa förutsättningar genom att följa standard.
4. **Etablera en central chattlösning** innebär att en part får uppdraget att tillgängliggöra ”en svensk myndighetschatt” som blir den enda kanal genom vilken myndigheter och dess medarbetare kan/ska kommunicera med varandra. Exempel finns från Frankrike (Tchap¹). Detta spårval skulle kunna vara en interimslösning i väntan på att vägval 3 etableras.
5. **Bilda kluster för samarbeten** innebär att myndigheter i grupp om två, tre eller flera skapar sina egna federerade chatt-kluster där dessa myndigheter kan kommunicera. Typisk skulle detta kunna ske mellan myndigheter som valt eller väljer samma produkter för intern chatt och där tröskeln för federation är lägre.
6. **Myndigheter väljer samma proprietära lösning** vilket innebär att myndigheter lägger frågan om rådighet åt sidan och samtliga väljer att låta t.ex. ett amerikanskt molntjänstföretag, hantera all kommunikation via deras plattformar. Detta sker på bekostnad av kontroll och anpassning.

¹Tchap — Tchap



SWOT: Vägval för myndighetskommunikation

Tabell 1- En jämförelse av sex strategiska alternativ utifrån styrkor, svagheter, möjligheter och risker

Vägval	Styrkor	Svagheter	Möjligheter	Risker
1. Fortsätta som idag	<ul style="list-style-type: none"> - Låg tröskel - Befintlig funktionalitet - Plattformer redan etablerade 	<ul style="list-style-type: none"> - Ökad fragmentering - Minskande interoperabilitet ö.t. - Inlåsnig till leverantör(er) 	<ul style="list-style-type: none"> - Tillfällig bekvämlighet för vissa användare - Köpa sig tid till att etablera en strategi 	<ul style="list-style-type: none"> - Oklart hur länge lokal leverans av Skype kommer erbjudas - Risk att myndigheter inte använder chatt sinsemellan - Risk att man skjuter på viktiga beslut/handlingsförlamning - Försämrad samverkan på sikt - Svårt att möta befintliga och kommande EU-krav - Risk för oplanerade driftproblem när stödet för Skype upphör
2. Central brygglösning	<ul style="list-style-type: none"> - Relativt snabbt införande - Kan ge samverkansmöjlighet på kort sikt - 	<ul style="list-style-type: none"> - Hög teknisk komplexitet - Risk för flaskhalsar och sårbarheter - Totalsträckskryptering (end-to-end-kryptering) kan troligen inte 	<ul style="list-style-type: none"> - Möjlighet att samordna olika verktyg i övergångsfas - Skapar ett brett ekosystem - Ger leverantörer tid att förflytta sig emot fullt 	<ul style="list-style-type: none"> - Kostsam att underhålla - Risk för att bli permanent "nödlösning" om inte tydlig övergångsstrategi finns



Vägval	Styrkor	Svagheter	Möjligheter	Risker
		erbjudas/hållas intakt mellan lösningar - Tillfällig lösning - Komplex beroendekedja mellan lösningar - Svagheter i end-to-end-kryptering -	stöd för öppet federationsprotokoll	- För komplex eller tidskrävande att underhålla - Leverantörer motvilliga till att stötta för att skapa förutsättningar för interoperabilitet
3. Federerad öppen lösning	- Hög interoperabilitet - Ger förutsättningar för digital suveränitet och egen rådighet - Långsiktig hållbarhet - Decentraliserad kommunikation som standard	- Kräver investering i gemensam styrning och kompetens - Löser inte nuvarande utmaningar ur ett kortsiktigt perspektiv - Kräver etablering av tillitsramverk och certifikathantering - Digital suveränitet förutsätter även kontroll över värdskap/infrastruktur	- Innovation och leverantörsoberoende - Kan bli europeisk förebild - Förbättrad säkerhet och insyn - Kan kombineras med brygglösningar (alt 2) - Tydligt i linje med EU:s krav på interoperabilitet, säkerhet och öppenhet	- Kräver uthållighet och gemensam målbild - Kräver aktiva val i beslut och styrning och förankring utanför eSam - Risk för motstånd från stora plattformaktörer
4. Etablera central chattlösning	- Samordnad lösning med tydlig ansvarsfördelning - Möjlig att anpassa efter svenska krav - Relativt snabbt införande	- Risk för ny central inlåsning - Kan upplevas som toppstyrd - Inte decentraliserad	- Skapa nationell standard med hög säkerhet - Möjlighet till kostnadsdelning mellan myndigheter - Ger leverantörer tid att förflytta sig emot fullt	- Risk för låg acceptans - Svårt att skala eller förändra efter behov - Driv mot ett öppet federationsprotokoll minskar - Risk för ny form av inlåsning om



Vägval	Styrkor	Svagheter	Möjligheter	Risker
			stöd för öppet federationsprotokoll	driftcentralisering sker utan öppna gränssnitt <ul style="list-style-type: none"> - Risk att öppenhet urvattnas om central lösning blir för styrande
5. Bilda kluster för samarbeten	<ul style="list-style-type: none"> - Låg tröskel - Möjligt att komma igång snabbt i vissa sektorer 	<ul style="list-style-type: none"> - Saknar gemensam riktning - Svårigheter att växla upp nationellt - Kräver omfattande koordinering 	<ul style="list-style-type: none"> - Praktisk väg för test och pilot - Stärker sektorsvis samverkan - Praktisk övergångsstrategi - Möjlighet att testa federerade koncept i mindre skala 	<ul style="list-style-type: none"> - Kräver långsiktig samordning för att bli hållbart - Risk för fortsatt fragmentering om inte vägvalet kopplas till gemensamma principer och styrning
6. Myndigheter väljer samma proprietära lösning	<ul style="list-style-type: none"> - Snabb implementation - Kända verktyg - Skalbara och effektiva lösningar 	<ul style="list-style-type: none"> - Svårt att uppfylla krav på öppenhet och kontroll - Myndigheter måste välja samma lösning för att kunna samarbeta effektivt - Betydande leverantörsberoende - Proprietärt chattprotokoll 	<ul style="list-style-type: none"> - tillgång till marknadsledande funktioner för samarbete - nyttjande av befintliga investeringar 	<ul style="list-style-type: none"> - Risk för bristande kostnadskontroll - Ökad inlåsning och begränsad rådighet - Om lösningen är en amerikansk molntjänst risk för politiskt motiverad avstängning eller åtkomstbegränsning från amerikanska leverantörer, i händelse av förändrat rättsläge eller yttre geopolitiska beslut



Vägval	Styrkor	Svagheter	Möjligheter	Risker
				<ul style="list-style-type: none">- Om amerikansk molntjänst, myndigheter gör olika bedömningar kring förutsättningar att hantera känslig information- Risk för otillräcklig kontroll över funktioner, lagring och dataflöden- Risk för juridiska och politiska påverkansmöjligheter utanför EU- Avviker från EU:s strategi för digital suveränitet och interoperabilitet

Denna bilaga har uppdaterats utifrån synpunkter från RISE, Sambruk, DIGG, MSB, Sunet och Internetstiftelsen under remissrundan våren 2025.

Promemoria 2025-11-25
Dok.bet.: Bilaga
Version: 1.0
Dnr/ref: ES2025-20





Bilaga D – Tidslinje och övergångsplan

Inledning

Den föreslagna tidslinjen utgår från att styrgruppen beslutar om fortsatt arbete efter sommaren 2025, samt att detta arbete prioriteras och får tydliga förutsättningar i form av styrning och tillgång till resurser.

Varje fas i tidsplanen är beroende av att sådana beslut fattas i tid, och att de följs av mandat och operativ kapacitet.

Det krävs en tydlig nationell styrmodell för hur arbetet med federation ska ledas, följas upp och förvaltas över tid. Detta inkluderar ansvarsfördelning, tillitsförvaltning, incidenthantering och långsiktig förvaltning av teknisk infrastruktur och kod.

Regeringens utredning (SOU 2023:96) föreslår en ny lag om offentlig förvaltnings interoperabilitet från 2026. Den ska stärka myndigheters förmåga att dela information och samverka digitalt. Det här initiativet kan utgöra ett av de första operativa stegen i riktning mot den typen av interoperabilitet – särskilt inom området kommunikation.

Följande tidslinje bygger på antagandet att styrgruppen, efter styrgruppsmöte i september 2025, fattar beslut om att arbetet med chattfederation ska fortsätta och prioriteras. Det innebär att projektet även fortsatt drivs av en liten arbetsgrupp med begränsad tillgänglighet (ca 10–20 %), varför tempot under hösten 2025 kommer vara begränsat. Ytterligare resurser föreslås tillföras våren 2026.

Tidslinjen och övergångsplanen förutsätter:

- att beslut fattas i september 2025 om fortsatt arbete
- att styrgruppen tydligt pekar ut riktningen för arbetet
- att ansvarsfördelning och mandat klargörs
- att kapacitet och kompetens säkras i form av dedikerade resurser
- att organisatoriskt stöd finns på plats för varje fas
- att förstärkning med nyckelkompetens planeras till våren 2026.

Det är också avgörande att styrgruppen gör tydliga prioriteringar. Om det finns delar i planen som inte bedöms vara genomförbara inom givna ramar – tidsmässigt, ekonomiskt eller organisatoriskt – behöver dessa prioriteras om eller strykas. Tidslinjen är därför inte att betrakta som statisk utan kommer behöva justeras utifrån hur styrgruppen väljer att inrikta och stödja arbetet.



I linje med EU:s ökande fokus på digital suveränitet, interoperabilitet och säkerhetsstyrning är det också avgörande att detta arbete bedrivs med långsiktigt ansvarstagande och uthållighet. En gemensam federationsmodell kräver inte bara teknik och juridik – utan också kontinuerlig samordning, kompetensuppbyggnad och förvaltning. Det handlar om att stegvis bygga en gemensam kommunikationsinfrastruktur med höga krav på robusthet, säkerhet och samordning över tid.

2025 - Förberedelsefas: Grundplatta och vägval

Syfte: Förankring, dialog, förbereda test och besluta om riktning

Regeringsproposition om interoperabilitet (SOU 2023:96) väntas hösten 2025, där dSam4:s arbete kan ses som ett operativt steg mot den framtida lagstiftningen.

- **Beslut & förberedelse:**

- Beslut om fortsatt arbete från eSam:s styrgrupp september 2025
- Etablera kontakt med DIGG inför höstens arbete.

Givet att arbetsgruppen består av personer med begränsad tillgänglighet kommer framdriften hösten 2025 behöva fokusera på:

- Första utkast till vägledning för myndigheter.
- Initiera förberedelser för testmiljöer i mindre skala inom arbetsgruppen.

- **Fortsatt omvärldsbevakning:**

- Omvärldsbevaka Skandinavien och starta dialog

- **Kommunikation:**

- Förankra färdplanen hos eSam:s medlemmar
- Påbörja dialoger med leverantörer och andra EU länder

- **Risker:**

- Avsaknad av styrgruppsbeslut
- Otillräcklig resurstilldelning
- Oklar ansvarsfördelning



2026 – Interna tester och vägledningsfördjupning

Syfte: Samverka, testa i verklig miljö och förbereda för gradvis uppskalning, juridisk analys

Under första halvåret 2026 fokuserar arbetsgruppen på att testa federation i liten skala. Målet är att samla praktisk erfarenhet som kan användas för att ta fram förbättrade vägledningar för andra myndigheter. Först därefter kan bredare piloter eller testmiljöer erbjudas fler aktörer. Federation behöver inte ersätta det primära kommunikationsverktyget – det kan fungera som ett komplement, särskilt vid samverkan över organisationsgränser.

Fokusområden:

- **Teknisk förmåga:**
 - Utveckla teknisk kompetens baserat på myndigheters krav, inklusive stöd för Matrix-protokollet och dialog med Matrix Foundation.
- **Starta federerade miljöer:**
 - Sätt upp ett federationskluster med minst 3–4 myndigheter (t.ex. Försäkringskassan, UBM, Hav och Pensionsmyndigheten) med minst tre olika leverantörlösningar.
 - Utvärdera pilotverksamheten och återkoppla till vägledningsstödet – tidigast hösten 2026.

Samverkan och omvärldsbevakning:

En ny lag om offentlig förvaltnings interoperabilitet (enligt SOU 2023:96) förväntas träda i kraft sommaren 2026. Det är viktigt att arbetet med federation anpassas till den lagens krav och arkitektur.

- Dialog har inletts med DIGG om möjliga kopplingar till nationell infrastruktur (ENA), men samarbetet utvecklas i takt med respektive parts prioriteringar.
- Bidra till standardisering i EU:s tekniska arbetsgrupper (t.ex. CEF).
- Inleda dialog om eventuell EU-finansiering via CEF2 eller Interoperabilitetsprogrammet.
- Utforska möjligheten att etablera en stödstruktur eller ett samverkansnätverk för federation.

Rättsliga och säkerhetsrelaterade frågor:

Ett nationellt införande kan innebära nya säkerhetskrav. Om federationen blir en bärande del av digital infrastruktur kan det krävas:

- Samråd enligt säkerhetsskyddslagen
- Säkerhetsskyddsanalyser för driftsmiljöer
- Bedömning av juridiska risker vid mellanlagring eller spridning av personuppgifter mellan noder.



Dessa frågor är komplexa och svåra att förutse i detalj, men måste inkluderas i planering, riskhantering och tidsbuffert – särskilt om lösningen ska användas vid kris eller höjd beredskap.

Kompetensförstärkning:

För att arbetet ska kunna skalas upp under 2026 föreslås att arbetsgruppen förstärks med dedikerad kompetens. Följande roller är prioriterade:

- Teknisk specialist (federation, säkerhet, E2EE)
- Juridisk expert (upphandling, interoperabilitet, samverkan)
- Projekt- och förändringsledning samt IT- och verksamhetsstrateger

Detta möjliggör:

- Design av federationsarkitektur
- Juridisk analys av delad drift
- Färdigställande av vägledningar och stödmaterial inför upphandling

Styrning och förvaltning:

Det behövs en tydlig nationell modell för hur federationen ska styras, följas upp och förvaltas över tid. Arbetet kräver långsiktigt ansvarstagande, och senast 2027 bör en permanent förvaltningsorganisation vara på plats.

2027 - Inledande federation

Syfte: Skapa förutsättningar för bredare införande och börja bygga gemensam struktur

Våren 2027 bör eSam fatta beslut om fortsatt prioritering av arbetet samt om en eventuell ny fas med breddinförande. För att det ska lyckas krävs att en koordinerande funktion eller projektledare får tydligt mandat att driva frågan mellan myndigheter. Framdriften under året beror på vilka resurser som tillförs.

Observera: Detta avsnitt beskriver målbilder – inte garanterade händelser.

Kompetensförsörjning:

- Inrätta gemensamma kunskaps- och stödfunktioner, exempelvis ett utvecklingslabb eller en testmiljö ("sandbox") för federation.
- Påbörja uppbyggnaden av ett nationellt kodarkiv med vägledningar, kodexempel och komponenter som kan återanvändas.

Teknisk implementering:

- Testa E2EE, identitetslösning (ex: Sweden Connect), närvarostatus, synkning
- Ta fram ett arkitekturförslag för en tillfällig HUB-lösning.



- Påbörja utveckling av en HUB-lösning för de myndigheter som saknar förutsättningar att själva etablera en federationsnod. Detta sker endast om behov och finansiering bekräftats utifrån tidigare tester.
- Etablera tekniskt samarbete med Matrix Foundation och andra myndigheter inom EU.

Stödmaterial och styrning:

- Publicera första versionen av gemensamma riktlinjer och principer för federation.
- Utveckla en governance-modell för teknisk konfiguration, säker federation och samordning.

Upphandling och ramverk:

- Ta fram stödmaterial för teknisk kravställning i upphandlingar.
- Upprätta en referensmiljö som andra myndigheter kan använda för tester och verifiering.

Risker att beakta:

- Brist på tydligt stödmaterial och teknisk support kan försvåra införandet.
- Otillräcklig konfiguration kan leda till oavsiktlig exponering av metadata.
- Federationsnoder riskerar att placeras i moln utanför EU, vilket strider mot målbilden om digital suveränitet.
- Framdriften kan bli långsam vid begränsad tillgång på personalresurser.
- Brist på nyckelkompetens kan fördröja arbetet med vägledningar och riktlinjer.
- Underskattning av behovet av säkerhetsskyddsanalyser och juridiska samråd kan orsaka fördröjningar.
- Tidskrävande hantering av dataskyddsavtal mellan federerade parter.
- Svårigheter att i förväg identifiera juridiska hinder för gemensam drift och ansvarsfördelning.

2028 – Utvidgning och operativ mognad

Syfte: Bygga vidare på fungerande federationskluster och skala ut stegvis

Förutsätter att pilotprojekten under 2026–2027 utvärderats positivt, och att eSam beslutat om en långsiktig styrmodell.

Kompetensförsörjning:

- Starta insatser för kompetensförsörjning, exempelvis workshops, koddelning och behovsinventering.
- Säkerställ att arbetsgrupper bemannas med tvärfunktionella team där tekniska specialister samarbetar med verksamhetsrepresentanter.
- Inför strukturer för kontinuerligt lärande: dokumentation, utbildning och kollegiala forum.
- Etablera nationella former för samverkan kring kompetensdelning, support och vidareutveckling.



Teknisk planering:

- Definiera en teknisk målbild för E2EE (end-to-end encryption) och MLS (Message Layer Security) i Matrix.
- Specificera krav för identitetshantering, federation och klientfunktionalitet.
- Påbörja tillitsförvaltning, inklusive system för certifikathantering.
- Identifiera eventuella funktionsgap utifrån myndigheternas gemensamma behov.

Parallellt bör en styrmodell för tillit etableras – med regler för certifikathantering, incidenthantering och en nationell policy för federationens säkerhet. Modellen behöver fungera både tekniskt och organisatoriskt, med tydlig rollfördelning mellan deltagande myndigheter och central samordning.

Anslutning av fler myndigheter:

- Samordna gemensam kravdialog kring funktionalitet, säkerhet och användbarhet.
- Ta fram onboardingpaket för olika sektorer.

Förbättrad funktionalitet och stöd:

- Fortsätt gemensam kravställning gentemot Matrix-protokollet.
- Ta fram utbildningspaket, lathundar, användarstöd och manualer för IT-drift.

Internationell samverkan:

- Om möjlighet ges, bidra till europeiska initiativ inom federation, t.ex. via DINUM (Frankrike) eller OpenDesk (Tyskland) och mot EU Kommissionen.

Kommunikation och förändringsledning:

- Genomför en nationell utbildningsinsats.
- Etablera stömlinje och en "Fråga federationen"-tjänst för vägledning.

Risker att beakta:

- Teknisk implementering riskerar att bli fragmenterad.
- Svagt deltagande från sektorer med höga säkerhetskrav kan skapa obalanser.
- Det kan bli svårt att upprätthålla tillit mellan noder utan gemensamma rutiner.
- Ökat beroende av ett fåtal federationsnoder kan skapa nya sårbarheter.

2029 – Nationell uppskalning

Syfte: Etablera federation som standard för digital kommunikation i offentlig sektor

Förutsätter att:

- fler myndigheter har anslutit sig under 2028



- governance-strukturen har etablerats
- tekniska, juridiska och organisatoriska modeller har testats i praktiken.

Fullskalig implementering:

- Utöka federationsnätverket baserat på fungerande kluster.
- Påbörja utfasning av eventuell HUB-lösning för myndigheter som nu etablerar egen federationsförmåga.
- Integrera fler identitetslösningar (exempelvis SITHS och eduGAIN).
- Säkerställ att teknisk implementation följer gemensamma standarder för att undvika fragmentering.

Stöd för komplexa miljöer:

- Ta fram anpassningspaket för kommuner och myndigheter med höga säkerhetskrav.
- Möjliggör integration med befintliga plattformar där federation används parallellt, till exempel Microsoft Teams, så att organisationer inte måste ersätta sina nuvarande chatt- och kommunikationsverktyg (som Teams), utan att det gemensamma federerade protokollet (Matrix) kan samexistera med befintliga system. Det kan till exempel ske genom:
 - gateway-lösningar, där meddelanden från federationen kan läsas och besvaras i Teams
 - parallell användning, där vissa chattar sker i Teams (internt) och andra i federationen (tvärorganisatoriskt)

Nationell samverkan och styrning:

- Formalisera styrmodell med tydliga roller för ansvar, tillsyn, stöd och förvaltning.
- Etablera processer för regelbundna säkerhetsrevisioner.
- Fortsätt samordning med eSam, DIGG och andra relevanta aktörer.

Den nationella governance-strukturen bör även omfatta:

- Certifiering av federerade noder
- Kontroll av efterlevnad och incidenthantering
- Versionshantering av specifikationer och stödmaterial
- En gemensam instans för samordning och tillsyn

Kompetensförsörjning:

- Förvaltning och vidareutveckling av federation bör ske i en öppen och lärande struktur.
- Prioritera kontinuerlig kompetensutveckling och teknisk innovation inom ramen för en gemensam infrastruktur.

Risker att hantera:

- Övergång från HUB till egen federation sker utan tillräcklig lokal kapacitet.
- Användning av extern molndrift kvarstår – riskerar att bryta mot målbilden om digital suveränitet.



- Försenad utveckling av certifieringssystem och styrmodell (governance) kan försena uppskalningen.

2030 – Full interoperabilitet

Syfte: Federerad kommunikation blir norm i offentlig sektor.

Om tidigare etapper genomförts enligt plan, kan 2030 vara året då federerad kommunikation är fullt etablerad som standard.

Följande kännetecknar detta skede:

- Chatt, video och fildelning fungerar sömlöst mellan alla myndigheter.
- End-to-end-kryptering är standard i all kommunikation.
- Sverige uppfyller EU:s mål om 100 % digitala och interoperabla offentliga tjänster inom chatt.
- Förvaltning och vidareutveckling sker löpande i öppen samverkan, både nationellt och inom ramen för europeiska initiativ som Interoperable Europe Act (IEA) och OpenID Foundation (OIDF).



Kompetensförsörjning:

- Förvaltning och utveckling av federationen sker i en öppen, lärande struktur.
- Det finns tydliga processer för dokumentation, erfarenhetsutbyte och vidareutbildning.
- Offentlig sektor prioriterar fortsatt kompetensutveckling och teknisk innovation inom ramen för en gemensam infrastruktur.

Efter 2030 – Gemensam förvaltning och fortsatt utveckling

När federerad kommunikation har blivit en etablerad norm i offentlig sektor, går arbetet in i en ny fas. Fokus flyttas från uppbyggnad till långsiktig förvaltning, förbättring och vidareutveckling.

Vid det här laget förväntas interoperabilitet vara en självklar och integrerad del av Sveriges digitala infrastruktur. Den federerade modellen är då en naturlig del av den nationella interoperabilitetsarkitekturen – i linje med EU:s *Interoperable Europe Act* och den svenska lagstiftning som föreslås i SOU 2023:96.

Interoperabilitet blir därmed inte bara en teknisk lösning utan ett styrande krav för offentlig sektor. Det är avgörande för att:

- skapa en sammanhållen digital förvaltning
- stärka demokratisk kontroll
- och bygga motståndskraft längs hela hotskalan.

Förvaltningen behöver säkerställa att:

- tekniken hålls uppdaterad och säker
- lösningarna är användarvänliga och tillgängliga
- gemensamma regelverk och standarder förvaltas
- erfarenhetsutbyte sker både nationellt och internationellt

Genom fortsatt öppen samverkan kan offentlig sektor inte bara möta framtida krav – utan även leda utvecklingen. Ett gemensamt chattprotokoll är mer än teknik. Det är ett verktyg för digitalt självbestämmande, ökad krisberedskap och en mer öppen offentlig dialog.

Om remissrundan

Denna tidslinje har tagits fram av arbetsgruppen inom dSam4 och har justerats utifrån synpunkter som inkommit under remissrundan våren 2025. Aktörer som Sunet, RISE, MSB, Regeringskansliet, Sambruk, Digg och Internetstiftelsen har bidragit med viktiga inspel.

Till exempel:



- RISE har betonat vikten av kompetensutveckling och lärande förvaltningsstrukturer.
- Sambruk har lyft frågor kring tillit, certifikathantering och teknisk samordning.
- MSB har pekat på behovet av säkerhetsskyddsanalyser och juridisk förberedelse för ett nationellt införande.



Bilaga E – Principer för federerad chattlösning i offentlig sektor baserat på öppna protokoll

Denna bilaga beskriver principer för en federerad chattlösning i offentlig sektor, baserat på öppna protokoll. Fokus ligger inte på ett enskilt protokoll, utan på vilka tekniska, organisatoriska och juridiska principer som krävs för att skapa en interoperabel och kontrollerbar infrastruktur mellan myndigheter. I praktiken skulle fler principer inom områden som tillit, säkerhet och användbarhet behövas. Syftet är att ge läsaren en förståelse för vilka fördelar och konsekvenser ett öppet protokoll medför.

SAMMANFATTNING

Implementation och gemensamma principer är viktiga att etablera i ett tidigt skede för att ha tydliga ramar att följa i etablering och utveckling av lösningar. Det ger också styrmedel för att ställa krav mot öppna protokoll samt för leverantörer som utvecklar och erbjuder tjänster till offentlig sektor.

Standardiserade öppna protokoll ger, i sin natur, både kortsiktiga och långsiktiga fördelar för offentlig sektor. Fortsatt arbete bör säkerställa att grundläggande principer för federerad kommunikation är överenskomna och beslutade.

Dessa principer ska fungera som ett stöd för styrning, upphandling och arkitekturella beslut under införandet av federerade chattlösningar inom offentlig sektor.

Lösningen ska kunna anvisas av en central aktör

Beskrivning: En central aktör ska kunna anvisa det gemensamma protokollet för att säkerställa interoperabilitet och främja samverkan mellan olika plattformar och system.

Motivering: Genom att följa ett gemensamt protokoll kan myndigheter kommunicera sömlöst med andra, både inom och utom offentlig sektor samtidigt som man undviker inlåsning till enskilda leverantörer.

Konsekvenser:

- Myndigheter måste anta och implementera chattlösningar som stödjer ett gemensamt antaget öppet protokoll.



- Införande av proprietära protokoll begränsas och kompletteras med brygglösningar.
- Anskaffning av chattlösningar krävs för att stödja det utpekade protokollet.

Undvik leverantörsinlåsningar

Beskrivning: Protokollet ska bidra till att undvika leverantörsinlåsning och uppmuntra till en mångfald av leverantörer med olika affärsmodeller.

Motivering: Leverantörsinlåsning leder till sämre lösningar och risk för beroenden som påverkar informationskoncentration och kostnader negativt.

Konsekvenser:

- Avtal bör struktureras för att säkerställa att myndigheter enkelt kan byta leverantörer utan att det medför omfattande arbete.
- Interoperabilitet med lösningar från flera leverantörer bör prioriteras i kravställning i upphandling.
- Protokollet och dess specifikationer ska vara fritt tillgängliga och kunna implementeras i öppna källkodslösningar.

Stöd brygglösningar för äldre system

Beskrivning: Chattlösningar utan stöd för det utpekade protokollet ska kompletteras med brygglösningar för att möjliggöra kommunikation mellan aktörer. Ansvar för att vara kompatibel med andra lösningar faller på den som inte har stöd för det gemensamma protokollet.

Motivering: Många offentliga myndigheter kan redan ha befintliga kommunikationsplattformar eller system som behöver fortsätta vara i drift under övergången till en ny lösning. Genom att den som inte förhåller sig till det gemensamma protokollet ansvarar för sin egen interoperabilitet skapas incitament för att migrera.

Konsekvenser:

- Protokollet måste kunna användas för att skapa brygglösningar med andra system.
- Kompatibilitet med äldre system kan medföra ytterligare installations- och underhållskostnader.

Stöd säkerhetsfunktioner för breda användningsmöjligheter



Beskrivning: Behovet att samverka mellan myndigheter omfattar ett stort antal informationsklasser och ett anvisat protokoll behöver omfatta säkerhetsfunktioner som möjliggör så många användningsfall som möjligt.

Motivering: Givet mångfalden av kommunikation inom och mellan myndigheter ska chattlösningar uppfylla höga säkerhetskrav för att möjliggöra olika typer av samarbeten.

Konsekvenser:

- Protokollet ska ha stöd för totalsträckskryptering.
- Möjligt att kunna använda olika identitetslösningar för användarinformation.
- Chattlösningar ska gemensamt genomgå regelbundna säkerhetsrevisioner och tester.

Tydlig och säker identitetshantering

Beskrivning: Protokollet bör ha ett robust system för att hantera användaridentiteter över det federerade nätverket. Detta inkluderar mekanismer för att skapa, verifiera och hantera användarkonton och enheter.

Motivering: En tydlig identitetshantering är avgörande för att säkerställa att kommunikationen sker med rätt personer och har en hög grad av tillit.

Konsekvenser:

- Protokollet ska stödja olika former av identitetskällor och standarder

Det är viktigt att skilja på autentisering och federation. Protokoll som OpenID Connect (OIDC) erbjuder autentiseringslösningar, men har inte inbyggt stöd för federation. För att möjliggöra federation behövs ett tillägg, som till exempel OpenID Federation (OIDF), vilket fortfarande är under utveckling men har stor potential för offentlig sektor. En framtida lösning bör därför bygga på arkitektur som är kompatibel med både nationella och europeiska identitetsfederationer.

Stöd för federation

Beskrivning: Protokollet ska ha inbyggt stöd för federation. Funktioner och förmågor som erbjuds som standard i protokollet ska fungera över en federation.

Motivering: Myndighets behöver hantera krav på resiliens, robusthet, fritt kunna välja leverans- och samarbetsformer. Detta är särskilt viktigt i kontext av totalförsvaret och civil beredskap, där kommunikation måste fungera även under påfrestning och utan beroende av externa plattformar.



Konsekvenser:

- Protokollet ska ha stöd för federation
- Protokollet ska ha säkerhetsfunktioner där myndigheter kan styra hur en federation genomförs, vem/vilka federationen sker med och vad som får ske över federationen.

Standardkompatibilitet med europeisk digital strategi

Beskrivning: Den federerade chattlösningen ska utformas i linje med europeiska regelverk och initiativ som Interoperable Europe Act, NIS2 och Cyberresiliensakten.

Motivering: Europeiska lagstiftare efterfrågar öppna, säkra och interoperabla offentliga tjänster. Genom att följa dessa ramar kan Sverige säkerställa rättslig efterlevnad och framtidssäkerhet.

Konsekvenser: Lösningen bör vara kompatibel med europeiska identitetstjänster, säkerhetsramverk och tekniska specifikationer för federation.

Gemensam tillitsmodell och styrning

Beskrivning: Det federerade nätverket behöver en tillitsmodell som reglerar hur parter autentiseras, hur certifikat hanteras och hur incidenter rapporteras.

Motivering: En fungerande federation kräver att alla deltagande parter litar på varandras identiteter och att det finns gemensamma rutiner vid avvikelser.

Konsekvenser: Kräver etablering av nationell styrning, regler för certifikathantering och rutiner för incidentrapportering.

Detta dokument har tagits fram av dSam4:s arbetsgrupp; med input från bl.a. Sunet, RISE, Digg, Sambruk, MSB och Internetstiftelsen.



Bilaga F - Tillämpningen av Matrix-protokollet inom Europeiska Unionen

Inledning

Huvudrapport och bilagor till denna rapport beskriver olika möjliga öppna protokoll. Givet att Matrix-protokollet har fått ökat nyttjande och börjat implementeras inom EU ser vi ett värde i att fördjupa oss i Matrix-protokollet genom denna bilaga. För information om andra protokoll och tillämpningar hänvisar vi till ”Bilaga_A_Omvärldsbevakning” samt ”Bilaga_B_Teknisk_jämförelse_av_protokoll”.

Sammanfattning

Matrix-protokollet **ökar kraftigt i tillämpning** inom Europeiska Unionen, vilket bekräftas på Matrix konferensen i Strasbourg oktober 2025, särskilt inom den offentliga sektorn. Till och med EU kommissionen utvärderar själva att nyttja matrix-protokollet. Denna utveckling drivs primärt av ett **behov av kommunikationslösningar som är säkra, decentraliserade, interoperabla och som respekterar digital suveränitet**. Medlemsstater som Tyskland och Frankrike har tagit en **ledande roll** i att implementera Matrix inom olika områden av den offentliga förvaltningen.

EU-direktiv och regleringar, såsom NIS2 och DMA, förväntas ytterligare accelerera användningen av protokoll som Matrix genom att betona vikten av **säker och interoperabel kommunikation**. Ett aktivt open source-community och EU-finansierade initiativ bidrar kontinuerligt till utvecklingen och förbättringen av protokollet.

Matrix har en intressant framtid framför sig inom EU. Protokollets förmåga att erbjuda en säker, öppen och federerad kommunikationsinfrastruktur gör att det skapas **förutsättningar för att möta de växande kraven på interoperabilitet, digital suveränitet och säkerhet inom unionen**. Satsningar inom EU borde **fokusera på de ekonomiska fördelarna** med att anta öppna kommunikationsstandarder som Matrix inom den offentliga sektorn samt utmaningarna med storskaliga federerade installationer över olika administrativa strukturer inom EU.



Introduktion till Matrix-protokollet

Matrix-protokollet är en öppen standard och ett kommunikationsprotokoll för realtidskommunikation. Dess främsta syfte är att möjliggöra sömlös kommunikation mellan olika tjänsteleverantörer, på ett liknande sätt som standardprotokollet SMTP (Simple Mail Transfer Protocol) fungerar för e-post ¹. Detta innebär att användare med konton hos en kommunikationstjänsteleverantör, på ett standardiserat sätt, kan kommunicera med användare hos en annan.

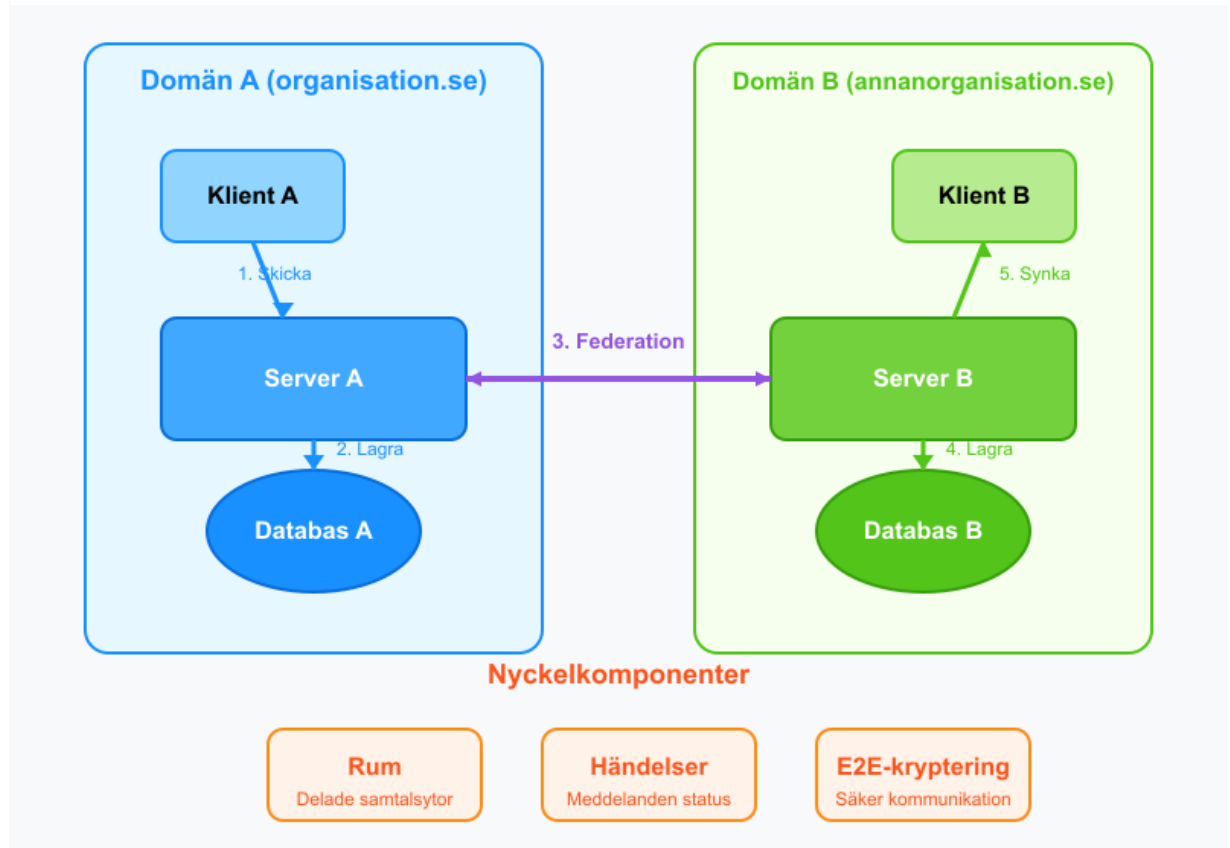
Matrix är utformat för en rad olika användningsområden, inklusive IP-telefoni (VoIP), Internet of Things (IoT) och snabbmeddelanden, samt gruppkommunikation. En central aspekt av protokollet är dess stöd för säkerhet och replikering av data, vilket säkerställer att fullständig konversationshistorik bevaras utan att det finns några enskilda kontrollpunkter eller risk för systemfel.

Flera viktiga funktioner gör Matrix särskilt intressant för användning inom EU, och speciellt inom offentlig sektor:

- **Decentralisering och Federation:** Matrix tillåter organisationer att driva sina egna servrar ("on-prem") och behålla full kontroll över sin data, samtidigt som de kan kommunicera med användare på andra servrar. Detta tillmötesgår EU:s strävan efter digital suveränitet.
- **End-to-End-Kryptering (E2EE):** Protokollet erbjuder valfri men kraftfull säkerhet (bland annat genom biblioteken Olm och Megolm, som implementerar Double Ratchet-algoritmen). Detta säkerställer att endast deltagarna i ett rum kan läsa meddelandena.
- **Interoperabilitet:** Genom så kallade bryggor kan Matrix kopplas samman med andra kommunikationsplattformar som Slack, Teams och XMPP-baserade lösningar, vilket underlättar enhetlig kommunikation över olika system.
- **Öppen Standard och öppen Källkod:** Matrix är en öppen standard med tillgängliga implementeringar i öppen källkod. Det främjar transparens, granskning, säkerhet och utveckling driven av en bred gemenskap.



Tabell 1 - Visualisering av federation mellan två domäner eller organisationer



Den ökade betydelsen av decentralisering och E2EE svarar direkt mot de växande kraven kring dataskydd och säkerhet inom EU. Detta gör Matrix till ett attraktivt alternativ till mer centraliserade och proprietära kommunikationsplattformar/protokoll. EU har aktivt främjat digital suveränitet och dataskydd genom initiativ som GDPR. Matrix grundläggande design principer överensstämmer med dessa mål genom att ge organisationer kontroll över sin kommunikationsinfrastruktur och säkerställa skydd av data genom stark kryptering.

Tekniskt sett är Matrix-protokollet ett kommunikationsprotokoll på applikationsnivå som använder HTTP-API:er och tillhandahåller referensimplementeringar med öppen källkod för säker distribution och lagring av meddelanden i JSON-format över ett öppet federerat nätverk.



Uppmärksamhet på politisk nivå

Matrix-protokollet uppmärksammas även på hög nivå inom EU-institutionerna. I "Cyber Blueprint - Proposal Council Recommendation" nämner en rekommendation om att använda Matrix för kommunikation mellan regeringar i frågor som rör cybersäkerhet. Rekommendationen från EU-rådet kan leda till framtida officiella projekt som involverar protokollet där man överväger det för säker kommunikation mellan offentlig verksamhet inom ett kritiskt område som cybersäkerhet. EU-rådets fokus på cybersäkerhetskommunikation understryker vikten av säkra kanaler på de högsta nivåerna av EU-styret. Att Matrix rekommenderas, ett öppet och granskningsbart protokoll med stark kryptering, antyder en strategisk inriktning mot att utnyttja sådana tekniker för känslig kommunikation inom EU.

Den politiska viljan stärks i och med att EU kommissionen genomfört en "Proof of Concept" på Matrix-baserad app (Element) efter att ha sett andra länder (som Frankrike, Tyskland och Sverige) använda Matrix. Målet är att skapa en säker, statlig kommunikationsplattform för medlemsländerna där de äger data själva och erbjuder komplement till Microsoft Teams och kan ersätta appar som t.ex. Signal.

Liknande dialoger sker i USA där senatorer har skickat en uppmaning till departementet att tillämpa Matrix-protokollet för att skydda information som kommuniceras.

Teknisk arkitektur och implementering inom EU

En typisk Matrix-installation involverar klientapplikationer som kommunicerar med servrar via HTTP-API:er. Servrarna federerar sedan med varandra för att replikera data i så kallade rum. Kommunikation sker i dessa virtuella rum genom utbyte av händelser (events), som är den grundläggande dataenheten i protokollet. Matrix använder en modell för slutlig konsistens (eventual consistency) för datareplikering.

Inom EU-kontexten är flera arkitektoniska aspekter särskilt viktiga:

- **Säkerhet:** End-to-end-kryptering med Olm/Megolm, HTTPS för federation och signering av servrar och meddelanden för integritet är centrala säkerhetsfunktioner.
- **Interoperabilitet:** Användningen av ett öppet protokoll för federation, bryggor för att ansluta till andra system och andra plattformar är avgörande för att underlätta kommunikation över olika tekniska miljöer.
- **Skalbarhet och Hög Tillgänglighet:** Professionella backend-lösningar som Element Server Suite erbjuder funktioner för att hantera stora installationer och säkerställa kontinuerlig drift.
- **Datasuveränitet:** Den decentraliserade naturen gör det möjligt för organisationer att lagra



sin data inom EU:s gränser, vilket är viktigt för att uppfylla kraven i GDPR och andra dataskyddsförordningar ¹.

Matrix design som ett protokoll är avgörande för det mångfacetterade landskapet inom EU:s offentliga sektor, där olika medlemsstater och institutioner har varierande krav på säkerhet, interoperabilitet och datahantering. Den öppna källkoden är viktig för transparens, möjligheten till säkerhetsgranskningar och för att främja innovation inom EU:s digitala ekosystem.

Det exemplifieras av att specifika implementeringar som BwMessenger, TI-Messenger och Tchap har sina egna arkitektoniska särdrag och anpassningar. Exempelvis integrerar TI-Messenger elektroniska hälso- och sjukvårdspersonalens kort och en FHIR-katalog. Det finns även initiativ som CoMatrix som syftar till att möjliggöra användning av Matrix på begränsade IoT-enheter. Möjligheten att anpassa och utöka protokollet, vilket syns i implementeringar som TI-Messenger med dess hälso- och sjukvårdsspecifika integrationer, ökar dess värde för specialiserade applikationer.

Det finns också ett flertal olika klientapplikationer för Matrix, såsom Element, FluffyChat, Cinny och andra, som utvecklats av både kommersiella aktörer och community.

För fler exempel, se ”Bilaga_A_Omvärldsbevakning”.

Hur finansieras utvecklingen av matrix-protokollet?

Kärnan i Matrix-protokollets styrning är The Matrix.org Foundation, en ideell organisation baserad i Storbritannien (Community Interest Company). Stiftelsens huvudsakliga uppgift är att agera som en neutral väktare av Matrix-standarden och säkerställa dess fortsatta utveckling som ett öppet och ofragmenterat kommunikationsnätverk

Historiskt sett har företaget Element (tidigare New Vector), som grundades av Matrix-skaparna, varit en huvudsaklig finansiär. Element anställer en stor del av kärnutvecklarna och har tagit in betydande kapital) samt genererar intäkter från tjänster som Element Matrix Services (EMS).

Matrix stiftelsen har sedan cirka 2022–2023 intensifierat sin egen insamling. Detta inkluderar medlemskap, donationer, företagssponsorskap eller bidrag. En relativt vanlig lösning, för större organisationer att bidra till ekosystemet är antingen genom kod eller finansiellt stöd, för att på så sätt motarbeta "Allmänningens dilemma" - många använder protokollet men ett begränsat antal organisationer bidrar ekonomiskt.



Referensimplementationerna för Matrix-servrar - (Synapse och Dendrite) - är under AGPLv3, vilket innebär att en slutanvändare som modifierar servrarna måste dela med sig av ändringarna. Alternativt finns också möjligheten att köpa en kommersiell licens ifrån Element och på så sätt stödja vidareutvecklingen av matrix-protokollet.

Att hitta hållbara och rättvisa finansieringsmodeller som balanserar öppenhetens fördelar med de kommersiella realiteterna i ett växande ekosystem är avgörande. Matrix-protokollets framtid och dess förmåga att fortsätta fungera som ett fritt, säkert och decentraliserat kommunikationsalternativ beror i hög grad på om dess community och de organisationer som drar nytta av det gemensamt kan lösa denna centrala finansiella utmaning. Det kommer fortsatt kräva samarbete, transparens och ett delat gemensamt ansvar.

Teknisk mognad och risker

Matrix har nått en betydande mognadsgrad sedan version 1.0 släpptes 2019. Regelbundna specifikationsuppdateringar, ett aktivt ekosystem av klienter och servrar (med Synapse som den etablerade referensimplementationen och Dendrite som ett lovande alternativ), samt pågående arbete med Matrix 2.0 visar på ett dynamiskt och framåtblickande projekt. Tillämpningen inom offentlig sektor i flera europeiska länder understryker förtroendet för protokollets kapacitet.

Matrix-protokollet, och särskilt dess federationsmekanismer kan anses vara komplext att implementera på serversidan. Denna komplexitet är delvis en konsekvens av designvalet att ha decentraliserade rum, där varje deltagande server upprätthåller en egen kopia av rummets tillstånd och historik. Jämfört med protokoll som XMPP, som traditionellt har använt mer centraliserade rumskontroller (även om decentraliserade MUC:er har diskuterats), medför Matrix design större utmaningar för serverutvecklare.

Matrix-protokollets federationsmodell, där oberoende servrar kommunicerar med varandra för att skapa ett sammanhängande nätverk, är en av dess kärnstyrkor. Den medför dock också specifika risker och operativa utmaningar som måste beaktas. Den kanske mest uppenbara risken i ett federerat system är beroendet av administratörer för en organisations federationsnod. En illasinnad eller komprometterad server utgör ett hot mot sina egna användare och potentiellt mot andra servrar den federerar med. Risker som avlyssning/manupilation, obehörig åtkomst till chattrum, nyckelmanupilation. Totalsträckskryptering (E2EE) ger ett visst skydd men hanterar inte samtliga risker.

En enskild server med bristfällig drift kan få stor negativ inverkan på den bredare användarupplevelsen, vilket är en risk som enskilda användare och serveradministratörer



har begränsad kontroll över (förutom att eventuellt blockera federation med problematiska servrar).

Myndigheter kommer behöva acceptera en högre grad av teknisk och administrativ komplexitet, driftkostnader, samt de specifika säkerhets- och operativa risker som är starkt förknippade med federationsmodellen.

Öppen källkods- och community-drivna initiativ inom EU

Matrix är ett protokoll baserat på öppen källkod, och det finns flera implementeringar baserade på Matrix-protokollet tillgängliga. Matrix.org Foundation spelar en central roll i underhållet och utvecklingen av protokollet.

Inom EU finns en aktiv community som bidrar till utvecklingen och användningen av Matrix; Fairkom erbjuder en Matrix-server och har varit involverad i Schulchat RLP, en meddelandelösning för skolor i Rheinland-Pfalz. På Matrix Conference 2024 presenterades flera community-projekt och diskussioner, inklusive "Polychat - Interoperability for the masses" och analys av Matrix-ekosystemet.

Vid European Open Source Awards tilldelades Amandine Le Pape, medgrundare av Element och Matrix.org, priset Business & Impact Award, vilket understryker betydelsen av matrix-protokollets betydelse inom open source området inom EU.

Öppen källkods-community kring Matrix inom EU är en avgörande del, som driver innovation, tillhandahåller olika klientalternativ och bidrar till protokollets robusthet och säkerhet genom offentlig granskning och kollaborativ utveckling. Matrix öppna egenskaper uppmuntrar till deltagande och bidrag från individer och organisationer över hela EU och världen. Denna samarbetsmiljö leder till en snabbare innovationstakt, utveckling av lösningar som är anpassade till specifika europeiska behov och en högre grad av förtroende för tekniken på grund av dess transparens och granskningsbarhet.

Matrix konferensen 2025

Den andra konferensen av sitt slag – den första var i Berlin september 2025, hölls i Strasbourg 15–18 oktober 2025. Intresset och deltagandet var stort och många av föredragen genomfördes av representanter från offentlig sektor. Konferensen markerade en tydlig vändpunkt där Matrix gick från att vara en "nischad" teknik till att bli ryggraden för digital suveränitet i Europa, särskilt inom offentlig sektor och sjukvård.



Offentlig Sektor

- **Trialing Matrix within the European Commission** - EU-kommissionen testar Matrix för att ersätta Signal och Teams för säkrare, självstyrd kommunikation.
- **BundesMessenger** - Flera föredrag handlade om Tysklands massiva satsningar på matrix-protokollet. B.l.a om hur de konsoliderar landets administrativa kommunikation till en gemensam Matrix-arkitektur.
- **Frankrikes "Tchap"** - Frankrike var tidiga med sin chattlösning Tchap, nu arbetar man med att öppna upp privata federationer på ett säkert sätt för att kunna kommunicera bredare.
- **Luxemburgs myndighet och medborgar-app** - Staten tillhandahåller chattlösning för offentlig sektor ("från brandman till politiker") och erbjuder även en separat app för privatpersoner
- **Sveriges offentliga sektor** - Försäkringskassan och eSam presenterade sin resa mot en säker och interoperabel samarbetsplattform (SAFOS) och gemensamt öppet federationsprotokoll för svensk offentlig sektor

Sjukvård och skola

- **74 miljoner användare i Tyskland (TI-Messenger)** - Gematik höll ett föredrag om utrollningen av TI-Messenger, som ska binda samman hela det tyska sjukvårdssystemet. Detta är troligen världens största Matrix-projekt.
- **SchulchatRLP (Skolchatt)** – Ett exempel där man rullat ut en krypterad meddelandetjänst till en halv miljon elever i Rheinland-Pfalz.

Samtliga föredrag spelades in och kan ses i efterhand via [Matrix Conference 2025 :: pretalx](#)

Denna bilaga har uppdaterats utifrån synpunkter från RISE, Sambruk, DIGG, MSB, Sunet och Internetstiftelsen under remissrundan våren 2025.

Fördjupning

1. Matrix (protocol) - Wikipedia, [https://en.wikipedia.org/wiki/Matrix_\(protocol\)](https://en.wikipedia.org/wiki/Matrix_(protocol))
2. Matrix | Germany | Digital sovereignty - Element, <https://element.io/matrix-in-germany>
3. Matrix | Germany | openDesk | ZenDiS - Element, <https://element.io/matrix-in-germany/projects/opendesk>
4. Matrix.org, <https://matrix.org/>
5. Watch The Matrix Conference's talks - Matrix.org, <https://2024.matrix.org/watch/>
6. Blog - Matrix.org, <https://matrix.org/blog/>
7. The European Union must keep funding free software - Matrix.org, <https://matrix.org/blog/2024/07/17/ngi-open-letter/>
8. Next Generation Internet Discovery and Search | NGI Search | Project | Fact sheet | HORIZON | CORDIS | European Commission, <https://cordis.europa.eu/project/id/101069364>
9. European Commission cuts funding support for Free Software projects, <https://edri.org/our-work/european-commission-cuts-funding-support-for-free-software->



- [projects/](#)
10. Next Generation Internet Zero | Association for Progressive Communications, <https://www.apc.org/en/project/next-generation-internet-zero>
 11. The NGI Initiative: An Internet of Trust, <https://ngi.eu/about/>
 12. Elm Matrix SDK - NLnet Foundation, <https://nlnet.nl/project/Elm-Matrix-SDK/>
 13. Fractal | Next Generation Internet, https://ngi.eu/funded_solution/fractal/
 14. Security & Defence European, https://euro-sd.com/wp-content/uploads/2024/08/ESD_8_2024_BAAINBw_WEB.pdf
 15. Matrix | Germany | BwMessenger | Bundeswehr - Element, <https://element.io/matrix-in-germany/projects/bwmessenger>
 16. BundesMessenger: shared, reused and interoperable., <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/bundesmessenger-shared-reused-and-interoperable>
 17. TI-Messenger | gematik | Matrix | German healthcare - Element, <https://element.io/solutions/ti-messenger-gematik-matrix>
 18. tim+: The TI Messenger from Arvato Systems, <https://www.arvato-systems.com/industries/industries-overview/healthcare-pharma/ti-messenger>
 19. The TI-Messenger: Advancing Secure Healthcare Communication within Germany - The Matrix Conference, https://2024.matrix.org/documents/talk_slides/LAB4%202024-09-20%2013_30%20Jan%20Kohnert%20-%20The%20TI-Messenger_%20Advancing%20Secure%20Healthcare%20Communication%20within%20Germany.pdf
 20. The TI Messenger: Advancing Secure Healthcare Communication with Matrix - Jan Kohnert, <https://www.youtube.com/watch?v=MoA2cYfHlyA>
 21. Matrix Specification, <https://spec.matrix.org/>
 22. CoMatrix, <https://comatrix.eu/>
 23. fairmatrix - Fairkom, <https://www.fairkom.eu/en/fairmatrix>
 24. Matrix of EUPL compatible open source licences | Interoperable Europe Portal, <https://interoperable-europe.ec.europa.eu/collection/eupl/matrix-eupl-compatible-open-source-licences>
 25. EU celebrates open source excellence | Science | Business, <https://sciencebusiness.net/news/eu-celebrates-open-source-excellence>
 26. NIS2 Directive: new rules on cybersecurity of network and information systems, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
 27. The NIS 2 Directive | Updates, Compliance, Training, <https://www.nis-2-directive.com/>
 28. NIS2 Requirements | 10 Minimum Measures to Address - The NIS2 Directive, <https://nis2directive.eu/nis2-requirements/>
 29. Cyber Resilience Act (CRA) | Updates, Compliance, Training, <https://www.european-cyber-resilience-act.com/>
 30. Cyber Resilience Act - BSI, [https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber Resilience Act/cyber_resilience_act_node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber%20Resilience%20Act/cyber_resilience_act_node.html)
 31. Cyber Resilience Act - Shaping Europe's digital future - European Union, <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
 32. Policy and regulation update 2024: Matrix and the GDPR, <https://matrix.org/blog/2024/06/regulatory-update/>



Bilaga G - Ekonomiska fördelar och nyttoeffekter med öppna chattprotokoll

Valet av kommunikationsteknologi utgör en strategisk beslutspunkt med omfattande konsekvenser för offentlig sektors effektivitet, ekonomi, säkerhet och digitala suveränitet. I en tid då kraven på digitalisering, tillgänglighet och effektivisering kontinuerligt ökar, blir behovet av moderna, flexibla och säkra kommunikationslösningar alltmer framträdande.¹ E-förvaltning syftar till att förbättra kvaliteten och tillgängligheten på offentliga tjänster, samtidigt som kostnader reduceras och öppenheten i förvaltningen stärks.¹ En central förutsättning för att realisera dessa mål är interoperabilitet – förmågan hos olika system och organisationer att utbyta information och samverka på ett smidigt sätt. Interoperabilitet har identifierats som en avgörande faktor för ett effektivt tillhandahållande av europeiska offentliga tjänster och för att stärka den inre marknaden.² Detta understryker vikten av att välja öppna chattprotokoll som aktivt främjar, snarare än passivt hindrar, sådan samverkan.

Valet av gemensamt chattprotokoll är därmed inte enbart ett tekniskt beslut, utan ett policybeslut som påverkar offentlig sektors förmåga att uppfylla sina kärnuppdrag och anpassa sig till framtida utmaningar. Offentlig sektor har ett brett och komplext uppdrag som kräver effektiv kommunikation, mellan myndigheter och externt med medborgare och företag. Proprietära system, som ofta kontrolleras av enskilda leverantörer, kan medföra begränsningar i flexibilitet och interoperabilitet, vilket försvårar utvecklingen av en sammanhållen digital förvaltning.³ Öppna protokoll, å andra sidan, erbjuder genom sin natur större möjligheter till anpassning, leverantörsberoende och samverkan. Följaktligen är typen av protokoll direkt kopplad till hur väl offentlig sektor kan styra sin digitala utveckling, samverka effektivt och undvika kostsamma och begränsande inlåsnings effekter.

Denna bilaga analyserar de ekonomiska fördelarna och de bredare nyttoeffekterna för offentlig sektor vid valet av ett öppet protokoll för chattfederation, i jämförelse med proprietära alternativ.

Chattfederation och protokolltyper

För att kunna bedöma de ekonomiska och strategiska fördelarna med olika ansatser till digital kommunikation är det nödvändigt att först förstå de grundläggande koncepten federerad kommunikation och de skilda egenskaperna hos öppna respektive proprietära protokoll.



Kärnkonceptet federerad kommunikation

Federation, i kontexten digital kommunikation, beskriver en arkitektur där oberoende system eller servrar har förmågan att kommunicera och utbyta information med varandra. Mer specifikt definieras federation som ett sätt för olika instanser av en tjänst, exempelvis en chatttjänst, att kopplas samman så att användare kan samarbeta och kommunicera över organisationsgränser.⁵ Detta är av särskild relevans för offentlig sektor, där en mångfald av myndigheter, kommuner, regioner och andra enheter har behov av att samverka effektivt.

Distribuerade snabbmeddelandetjänster kan realiserars genom federation, vilket möjliggör kommunikation mellan användare som är anslutna till olika tjänsteinstanter.⁵ En vanlig analogi är e-postsystemet, där användare på olika domäner (t.ex. olika organisationers e-postservrar) kan skicka och ta emot meddelanden sömlöst, trots att de använder skilda tekniska implementationer under ytan.⁶ Detta står i kontrast till centraliserade system, där all kommunikation och datahantering typiskt sett sker via en enda leverantörs infrastruktur och kontroll.

Federation utgör en arkitektonisk förutsättning för att uppnå en balans mellan å ena sidan autonomi för de enskilda organisationerna, och å andra sidan interoperabilitet och sömlös kommunikation mellan dem. Offentliga organisationer har ofta specifika och legitima krav gällande säkerhet, datalagring, regelefterlevnad och intern styrning av sin kommunikation. Centraliserade system kan tvinga alla anslutna parter att anpassa sig till en standardiserad modell som dikteras av en extern leverantör, vilket potentiellt kan komma i konflikt med dessa individuella organisatoriska krav. Federation tillåter däremot varje organisation att, om så önskas, driva och administrera sin egen server eller tjänsteinstans.⁵ Detta medför att organisationen kan behålla kontrollen över sin egna data, sina säkerhetspolicyer och sin tekniska miljö. Samtidigt säkerställer federationsprotokollet att kommunikation mellan dessa autonoma instanser kan ske på ett standardiserat och effektivt sätt. Implikationen är att en federerad modell ofta är bättre anpassad till den heterogena och till viss del självständiga naturen hos offentliga organisationer än vad en strikt centraliserad modell kan erbjuda.

Ekonomiska fördelar med öppna protokoll för chattafederation

Valet mellan öppna och proprietära protokoll för chattafederation har direkta och betydande ekonomiska konsekvenser för offentlig sektor. En analys av dessa konsekvenser sträcker sig bortom initiala anskaffningskostnader och inkluderar den



totala ägandekostnaden över tid, effekterna av licensmodeller, risken för leverantörsinlåsning samt påverkan på marknadsdynamik och konkurrens.

Minskade direkta kostnader och undvikande av licensavgifter

En av de mest omedelbara och påtagliga ekonomiska fördelarna med att välja öppna protokoll och öppen källkod är möjligheten att kraftigt reducera eller helt undvika de direkta kostnader som är förknippade med licensavgifter. Det är däremot av stor vikt att offentliga organisationer på olika sätt ändå bidrar, med resurser eller pengar, till att förvalta och vidareutveckla öppna lösningar. Proprietära protokoll, särskilt de som riktar sig till stora organisationer, medför ofta betydande licenskostnader som kan baseras på antal användare, antal servrar, specifika funktioner eller årliga prenumerationer.³

För offentlig sektor, som ofta hanterar stora volymer användare (anställda, medborgare, elever etc.) och driver omfattande IT-system, kan dessa licenskostnader ackumuleras till avsevärda summor. Genom att välja lösningar baserade på öppen källkod, där källkoden är fritt tillgänglig och användningen sällan är belagd med dyra licensavgifter, kan organisationer uppnå direkta och stora besparingar.³ Detta är särskilt fördelaktigt för organisationer med begränsade budgetar, en situation som inte är ovanlig inom många delar av den offentliga förvaltningen.

Besparingen från uteblivna eller kraftigt reducerade licenskostnader är inte enbart en passiv minskning av utgifter. Dessa frigjorda medel representerar en aktiv möjlighet för offentlig sektor. De kan återinvesteras i kärnverksamheten, användas för att finansiera angelägen innovation, eller allokeras till anpassning och vidareutveckling av de öppna lösningarna för att bättre möta specifika lokala eller nationella behov. Medlen kan också användas för att stärka den egna IT-kompetensen och minska beroendet av externa konsulter. På detta sätt kan valet av öppna protokoll och öppen källkod skapa en positiv ekonomisk dynamik, där initiala besparingar driver ytterligare värdeskapande och förbättrar den offentliga sektorns förmåga att leverera tjänster effektivt.

Leverantörsinlåsning och dess ekonomiska konsekvenser

Leverantörsinlåsning, eller "vendor lock-in", är ett fenomen där en kund blir så pass beroende av en specifik leverantörs produkter eller tjänster att kostnaden eller svårigheten att byta till en alternativ leverantör blir oproportionerligt hög eller till och med oöverstiglig.¹⁵ Proprietära protokoll och de slutna ekosystem de ofta skapar är en vanlig orsak till sådan inlåsning. När en organisation väljer en kommunikationsplattform baserad på ett proprietärt protokoll, blir den ofta beroende av den enskilda leverantören för kritisk support, nödvändiga uppdateringar, framtida utveckling och underhåll.³



De ekonomiska konsekvenserna av leverantörsinlåsning där samtliga myndigheter väljer samma leverantör för myndighetsövergripande samarbete kan vara omfattande. När en leverantör har en kund i ett inlåst läge minskar deras förhandlingsstyrka drastiskt. Leverantören kan då, medveten om kundens begränsade alternativ, höja priser, ändra licensvillkor på ett ofördelaktigt sätt, eller tvinga på kunden dyra uppgraderingar utan större risk att förlora affären.¹⁵ Detta kan leda till oförutsedda och eskalerande kostnader över tid, vilket är särskilt problematiskt för offentlig sektor som måste planera långsiktigt och ansvarsfullt med skattemedel.

Öppna protokoll motverkar aktivt leverantörsinlåsning.¹⁴ Genom att baseras på standardiserade och fritt tillgängliga specifikationer möjliggör de att flera olika leverantörer kan utveckla kompatibla produkter och tjänster. Om en organisation inte är nöjd med sin nuvarande leverantör, eller om leverantörens prissättning blir oskälig, finns möjligheten att byta till en annan leverantör som erbjuder en lösning baserad på samma öppna protokoll, utan att behöva byta ut hela den underliggande teknologistacken. Detta bibehåller en sund konkurrens på marknaden och stärker offentlig sektors position som kund. Valet av öppna protokoll är därmed en proaktiv åtgärd för att säkerställa sund ekonomisk förvaltning och undvika att bli gisslan hos en enskild kommersiell aktörs affärsintressen och prisstrategier. Det handlar inte bara om att undvika direkta kostnader, utan även om att bevara strategisk flexibilitet och kontroll över den egna digitala infrastrukturen.

Främjande av sund konkurrens och marknadsdynamik

Användningen av öppna protokoll inom offentlig sektor har potentialen att agera som en kraftfull katalysator för en mer dynamisk och konkurrensutsatt marknad för IT-lösningar. När offentliga organisationer standardiserar sin kommunikation kring öppna, väldokumenterade och icke-diskriminerande protokoll, skapas förutsättningar för en bredare och mer diversifierad leverantörsmarknad, vilket i slutändan gynnar offentlig sektor som en stor upphandlare.

Öppna standarder är utformade för att möjliggöra kompatibilitet (interoperabilitet) mellan produkter och tjänster från olika tillverkare.⁹ Detta innebär att om offentlig sektor, eller en betydande del därav, enas om att använda ett specifikt öppet federationsprotokoll för chatt och samarbete, kan olika myndigheter och organisationer välja de klientapplikationer och servertjänster som bäst passar deras unika behov och budgetar, samtidigt som de bibehåller förmågan att kommunicera och samarbeta sömlöst med varandra.⁵ Detta skapar en marknad där leverantörer konkurrerar på lika villkor baserat på kvalitet, funktionalitet, service och pris, snarare än på inlåsnings effekter skapade av proprietära teknologier. En sådan ökad konkurrens har en direkt positiv



inverkan på prissättningen och kan leda till betydande kostnadsbesparingar för det offentliga. Som tidigare nämnts uppskattas att även en relativt liten förbättring i pris i förhållande till prestanda, driven av ökad konkurrens inom mjukvaruområdet, kan resultera i årliga besparingar på hundratals miljoner kronor för stora offentliga inköpare.¹⁵

Genom att aktivt efterfråga och specificera lösningar baserade på öppna protokoll i sina upphandlingar kan offentlig sektor agera som en betydelsefull marknadsformare. Offentlig sektor är ofta den största enskilda köparen av IT-produkter och tjänster i ett land.¹⁵ När denna stora köpkraft riktas mot öppna lösningar, skickas en tydlig signal till marknaden om att det finns en betydande och långsiktig efterfrågan på sådana produkter och tjänster. Detta uppmuntrar inte bara etablerade leverantörer att anpassa sina erbjudanden, utan sänker också inträdeshindren för nya och mindre aktörer, inklusive lokala små och medelstora företag, att utveckla och erbjuda kompatibla lösningar. En bredare och mer diversifierad leverantörsbas ökar inte bara konkurrensen, utan minskar också beroendet av ett fåtal stora, ofta globala, teknikleverantörer. Detta kan ha positiva spridningseffekter på den nationella ekonomin genom att stimulera lokal innovation, kompetensutveckling och sysselsättning inom IT-sektorn. Offentlig sektor övergår därmed från att vara en passiv konsument av teknologi till att bli en aktiv och strategisk aktör som formar marknaden till sin egen och samhällets fördel.

Nyttoeffekter

Utöver de direkta ekonomiska besparingarna medför valet av öppna protokoll för chattfederation en rad betydande strategiska nyttoeffekter för offentlig sektor. Dessa vinster sträcker sig från förbättrad samverkan och innovationsförmåga till stärkt säkerhet, ökad resiliens och säkrad digital suveränitet.

Förbättrad interoperabilitet och sömlös samverkan

Interoperabilitet är en fundamental förutsättning för en modern och effektiv offentlig förvaltning. Öppna, federerade protokoll spelar här en nyckelroll för att bryta ner de kommunikationssilos som ofta existerar mellan olika myndigheter, förvaltningsnivåer och till och med inom enskilda stora organisationer. Öppen källkod och öppna standarder lyfts ofta fram som viktiga beståndsdelar för att garantera interoperabilitet och dataportabilitet i den digitala infrastrukturen.⁸

Fullständig interoperabilitet, möjliggjord av öppna federerade protokoll, transformerar samverkan från att vara en återkommande teknisk utmaning till att bli en strategisk möjlighet. Offentlig sektor består av en mångfald av organisationer – kommuner, regioner, statliga myndigheter – som alla har ett behov av att utbyta information och



koordinera insatser.²⁰ Bristande interoperabilitet leder oundvikligen till ineffektivitet, informationssilos, dubbelarbete¹⁸ och en fragmenterad serviceleverans, vilket i slutändan drabbar medborgare och företag. Öppna federerade protokoll skapar en gemensam teknisk grund, vilket gör det tekniskt enklare för olika system att "förstå" varandra och utbyta data på ett meningsfullt sätt.² När de tekniska hindren för kommunikation sänks, kan organisationer istället fokusera sina resurser och sin uppmärksamhet på *vad* de behöver samarbeta kring och *varför*, snarare än på de tekniska detaljerna i *hur* de ska få sina system att fungera tillsammans. Detta möjliggör mer agila, flexibla och effektiva samarbetsformer, vilket är ovärderligt vid exempelvis hantering av samhällskriser, i komplexa vårdkedjor som involverar flera vårdgivare, eller vid ärendehantering som spänner över flera myndighetsgränser. Investeringar i öppna federerade kommunikationslösningar är därmed i grunden investeringar i en mer sammanhållen, kapabel och lyhörd offentlig förvaltning.

Katalysator för innovation, anpassningsbarhet och lokal utveckling

Öppenhet i protokoll och tillhörande programvara ger en unik frihet att anpassa, modifiera och bygga vidare på befintliga lösningar. Detta skapar en grogrund för innovation som kan skräddarsys för att möta offentlig sektors specifika och ofta unika behov, snarare än att vara begränsad av de standardiserade erbjudanden som dominerar på den proprietära marknaden. Öppen källkod har visat sig signifikant öka innovationstakten genom att möjliggöra för olika aktörer att samutveckla, dela kunskap, anpassa lösningar och bygga vidare på varandras arbete.¹⁷ Detta leder till ökad flexibilitet och anpassningsbarhet, vilket är kritiskt i en föränderlig värld.³

Möjligheten att fritt anpassa och skräddarsy programvara efter specifika verksamhetsbehov och arbetsflöden är en av de främsta fördelarna med öppen källkod.³ Offentlig sektor har ofta komplexa och lagstyrda processer som inte alltid enkelt låter sig fångas av generiska kommersiella produkter. Med tillgång till källkoden kan offentliga organisationer, antingen med egen personal eller genom att anlita lokala utvecklare, skapa tillägg, integrationer eller helt nya funktioner som är optimerade för deras behov. Detta främjar inte bara utvecklingen av mer ändamålsenliga verktyg, utan kan också stimulera lokal IT-kompetens och näringsliv. Offentlig sektor kan också samarbeta kring utvecklingen av gemensamma digitala lösningar och standarder, vilket kan leda till stordriftsfördelar och undvikande av dubbelarbete.²² EU-kommissionen har uppmärksammat den makroekonomiska potentialen i detta och noterat att en ökning med endast 10% i bidrag till öppen källkodsutveckling inom EU skulle kunna generera en ökning av EU:s BNP med 0,4–0,6%, vilket motsvarar betydande summor.¹⁷



Öppna protokoll och öppen källkod kan sägas demokratisera innovationsprocessen genom att sänka trösklarna för deltagande. Till skillnad från proprietära system, där utvecklingsagendan och produktcyklerna styrs av den enskilda leverantörens kommersiella intressen och där anpassningar kan vara dyra, tidskrävande eller helt omöjliga, ger öppenhet en annan dynamik. Tillgången till källkod och öppna specifikationer³ gör det möjligt för offentliga organisationer att själva, eller i samarbete med andra (inklusive akademi, ideell sektor och lokala företag), identifiera behov, utveckla lösningar, åtgärda buggar eller integrera system på ett sätt som direkt adresserar deras utmaningar.³ Detta skapar en innovationsmodell där offentlig sektor kan vara proaktiv och drivande, istället för att vara en reaktiv och beroende kund. Implikationen är att offentlig sektor kan få tillgång till lösningar som är bättre anpassade till lokala förhållanden och medborgarnas behov. Samtidigt kan detta bidra till att bygga upp en "innovationsallmänning", där förbättringar och ny funktionalitet som utvecklas av en aktör kan delas och komma andra offentliga organisationer till godo, vilket främjar en kultur av samarbete och kunskapsdelning.³

Stärkt informationssäkerhet, transparens och granskningsbarhet

En vanlig missuppfattning är att öppenhet i källkod och protokollspecifikationer skulle innebära en säkerhetsrisk. Tvärtom argumenterar många experter och erfarenheter för att transparens och möjligheten till bred granskning kan leda till en högre nivå av informationssäkerhet. När källkoden till en programvara eller specifikationen för ett protokoll är öppet tillgänglig, kan den granskas ingående av en stor och diversifierad grupp av utvecklare, säkerhetsexperter och forskare världen över.³ Denna kollektiva granskning leder ofta till en snabbare identifiering och åtgärdande av potentiella sårbarheter och säkerhetsbrister, jämfört med slutna system där endast leverantörens interna team har insyn.

Transparensen i sig kan också bidra till ett ökat förtroende för programvaran och dess säkerhet.³ Användare och organisationer är inte enbart beroende av leverantörens utfästelser om säkerhet, utan har möjlighet att (eller låta oberoende experter) själva verifiera påståenden och bedöma säkerhetsnivån. Det är dock viktigt att understryka att säkerheten inte enbart beror på öppenheten i sig, utan även på ett aktivt och engagerat ekosystem kring programvaran som snabbt hanterar och åtgärdar upptäckta problem.³ Decentraliserade system, vilka federerade kommunikationssystem kan vara en form av, kan erbjuda ytterligare säkerhetsfördelar genom att minska antalet centrala attackpunkter och ge organisationer större kontroll över sin egna data och säkerhetskfiguration.²⁴

För offentlig sektor, som hanterar stora mängder känsliga personuppgifter och ofta ansvarar för samhällskritisk digital infrastruktur, är transparensen och



granskningsbarheten som följer med öppna protokoll en avgörande tillitsfaktor och ett viktigt medel för att säkerställa ansvarsskyldighet. Proprietära system fungerar ofta som "svarta lådor", där den interna funktionen och de exakta säkerhetsmekanismerna inte är fullt synliga eller verifierbara för kunden. Offentlig sektor har ett särskilt och lagstadgat ansvar för transparens och för att kunna demonstrera hur medborgarnas data hanteras på ett säkert och korrekt sätt. Öppna protokoll och öppen källkod möjliggör en oberoende granskning av både kod och protokollspecifikationer.³ Detta gör det möjligt att objektivt verifiera säkerhetsanspråk, identifiera potentiella svagheter och säkerställa att systemet fungerar som avsett utan dolda funktioner. Denna möjlighet till oberoende verifiering är fundamental för att bygga och upprätthålla medborgarnas förtroende för den digitala förvaltningen och för att kunna hålla systemleverantörer ansvariga. Valet av öppna protokoll är därmed inte bara en teknisk fråga om säkerhetsimplementering, utan också en demokratisk och förtroendeskapande åtgärd. Det minskar även risken för oupptäckta bakdörrar eller oönskad datainsamling från leverantörens sida, vilket är en viktig aspekt av dataskydd och integritet.

Ökad resiliens, driftskontinuitet och minskat beroende av enskilda aktörer

Resiliens, förmågan hos ett system att motstå, anpassa sig till och återhämta sig från störningar, är av yttersta vikt för offentlig sektors kommunikationsinfrastruktur. Decentraliserade och federerade arkitekturer, som bygger på öppna protokoll, är i sin natur ofta mer motståndskraftiga mot olika typer av störningar och problem jämfört med centraliserade system. Ett resilient informationssystem är konstruerat för att kunna stå emot och snabbt återhämta sig från störningar och hot, och därigenom minimera negativa effekter och bibehålla kontinuiteten i verksamheten.²⁶

Federerade arkitekturer erbjuder förbättrad feltolerans och resiliens eftersom fel eller avbrott i en enskild del av nätverket (t.ex. ett datacenter hos en specifik organisation) inte nödvändigtvis leder till att hela kommunikationssystemet slås ut.²⁷ Eftersom resurser och data ofta är distribuerade över flera oberoende men sammankopplade noder, finns en form av naturlig redundans inbyggd i systemet.²⁷ En decentraliserad infrastruktur minskar risken för så kallade "single points of failure" – enskilda kritiska punkter vars fallerande skulle lamslå hela systemet.²⁸ Även om storskaliga centraliserade molntjänster kan vara mycket kraftfulla och erbjuda hög tillgänglighet och säkerhet, utgör deras centraliserade natur en inneboende sårbarhet om den centrala tjänsten drabbas av ett omfattande avbrott.²⁸

Oberoendet av enskilda leverantörer, som är en central fördel med öppna protokoll, bidrar också starkt till ökad resiliens.³ Om offentlig sektor är beroende av en enda proprietär leverantör för sina förutsättningar att kommunicera mellan



organisationsgränserna, och den leverantören drabbas av tekniska problem, ekonomiska svårigheter, upphör med en tjänst/funktion eller blir uppköpt av ett annat företag med andra prioriteringar, kan det få allvarliga konsekvenser för vår förmåga att kommunicera med varandra. Med öppna protokoll finns möjligheten att byta till en annan leverantör som erbjuder en kompatibel lösning, eller till och med att organisationen själv, eller i samarbete med andra, tar över driften eller vidareutvecklingen av programvaran. Detta skapar en "kollektiv resiliens" som är svår att uppnå med en monolitisk, proprietär lösning som kontrolleras av en enda aktör.

Genom att adoptera öppna federerade protokoll bygger offentlig sektor en kommunikationsinfrastruktur som är mer robust, inte bara mot tekniska fel och cyberattacker, utan även mot geopolitiska spänningar eller kommersiella beslut från enskilda globala teknikleverantörer som kan påverka tjänstetillgängligheten i ett visst land eller en viss region. Detta är avgörande för att säkerställa samhällets funktionalitet och kontinuitet, särskilt i kristider. Valet av öppna protokoll stärker därmed den nationella digitala infrastrukturens motståndskraft, vilket i förlängningen är en fråga om nationell säkerhet och förmåga att upprätthålla samhällsviktig verksamhet.

Säkrad digital suveränitet och kontroll över kritisk kommunikationsinfrastruktur

Digital suveränitet handlar om en nations eller organisations förmåga att ha kontroll över sin egen digitala framtid – vilket inkluderar data, hårdvara och mjukvara som man förlitar sig på och skapar.²⁹ Det är ett begrepp som syftar till att öka autonomi och minska beroendet av externa aktörer, särskilt i en alltmer digitaliserad och globaliserad värld.³⁰ För offentlig sektor är digital suveränitet inte bara en teknisk fråga, utan en grundläggande aspekt av nationell säkerhet, skydd av medborgares integritet och förmågan att självständigt fatta beslut om den egna digitala infrastrukturen. Öppna protokoll utgör en viktig förutsättning för att offentlig sektor ska kunna utöva verklig digital suveränitet över sina förutsättningar att kommunicera med varandra.

Att enbart lagra data inom ett lands geografiska gränser är inte tillräckligt för att uppnå digital suveränitet; tillgängligheten till, och kontrollen över, den underliggande teknologin och infrastrukturen är minst lika avgörande.³¹ Användningen av utlandsbaserade, kommunikationsplattformar kan innebära att känsligt data lagras eller processas utanför nationell kontroll och jurisdiktion. Det kan också innebära att plattformens funktion, säkerhetsuppdateringar och framtida utveckling styrs av en extern kommersiell aktörs policyer och affärsintressen, vilka inte nödvändigtvis sammanfaller med nationella eller offentliga intressen för samarbete. Detta kan skapa risker kopplade till dataskydd (t.ex. exponering för utländsk lagstiftning som tillåter myndighetsåtkomst till data för



underrättelseändamål), samt ett teknologiskt beroende som kan påverkas av geopolitiska spänningar eller handelspolitiska beslut.

Öppna standarder och öppen källkod ger ett avgörande oberoende från enskilda leverantörer³, vilket är en grundpelare för digital suveränitet. Öppna protokoll tillåter offentlig sektor att själv, eller genom valfria leverantörer, bestämma var servrar ska placeras, vem som ska administrera dem, och hur data ska hanteras i enlighet med nationell lagstiftning och egna policyer. De möjliggör även utveckling och anpassning av egna, nationellt eller lokalt anpassade klientprogram och serverimplementationer, vilket ger en djupare nivå av kontroll och förståelse för den teknologi som används.³ Detta ger en konkret och verifierbar kontroll över den digitala kommunikationsinfrastrukturen, vilket är kärnan i begreppet digital suveränitet. EU har också identifierat digital suveränitet som ett viktigt strategiskt mål och arbetar aktivt med regleringar och initiativ för att främja utvecklingen och användningen av europeiska digitala lösningar och standarder.²⁹

Valet av öppna protokoll för federerad chatt är därmed ett konkret uttryck för en strävan efter digital suveränitet. Det ger offentlig sektor makten att definiera och kontrollera sina egna kommunikationsvägar, fria från sådana utländska eller kommersiella beroenden som potentiellt kan strida mot nationella intressen eller grundläggande demokratiska värden. Detta val stärker nationens förmåga att skydda sina medborgares integritet, säkerställa robusta och tillförlitliga informationsflöden även under kriser, och undvika att bli en passiv bricka i spelet mellan globala teknikjättar.

Öppet eller Proprietärt

När offentlig sektor står inför valet mellan gemensamma öppna respektive proprietära protokoll, är det viktigt att väga in de unika krav, ansvarsområden och principer som styr offentlig verksamhet. De tidigare diskuterade ekonomiska fördelarna och strategiska nyttoeffekterna får en särskild tyngd i denna kontext.

Offentlig upphandling är en process som omgärdas av striktare regelverk och högre krav på transparens, ickediskriminering och lika möjligheter för alla leverantörer än vad som ofta är fallet inom privat sektor.³² Öppna standarder och protokoll kan underlätta denna process genom att tillhandahålla tydliga, väldokumenterade och icke-diskriminerande tekniska specifikationer som kan ligga till grund för upphandlingsunderlag. Detta främjar en rättvis konkurrens. I kontrast kan situationer uppstå där en dominerande leverantör av ett proprietärt system i praktiken "bestämmer" villkoren och förordar sina egna helhetslösningar, vilket kan begränsa konkurrensen och leda till inlåsning.³³ Om en offentlig organisation försöker integrera ett proprietärt system med lösningar baserade på



öppna protokoll, och detta inte har krävts korrekt från början, kan risken och kostnaden för eventuella integrationsproblem hamna hos systemägaren (den offentliga organisationen) snarare än hos leverantören av det proprietära systemet.³³

Myndigheten för digital förvaltning (DIGG) i Sverige har i sina riktlinjer betonat vikten av öppenhet – inkluderande öppna data, öppna API:er, öppen programvara och öppna standarder – som en grundläggande princip för utvecklingen av en gemensam och sammanhållen digital förvaltning.⁸ Detta understryker en nationell strategisk inriktning som harmonierar väl med fördelarna hos öppna protokoll.

Den inneboende transparensen och den icke-diskriminerande naturen hos öppna protokoll ligger bättre i linje med offentlig sektors grundläggande principer om öppenhet, ansvarsskyldighet och främjande av rättvis konkurrens, än vad de ofta slutna, leverantörsstyrda och kommersiellt drivna proprietära alternativen gör. Offentlig sektor verkar under lagar och principer som kräver öppenhet i beslutsprocesser och en ansvarsfull användning av offentliga medel (exempelvis offentlighetsprincipen och lagen om offentlig upphandling). Proprietära protokoll, med sina ofta hemlighållna specifikationer och starka leverantörskontroll⁴, kan skapa en informationsasymmetri som försvårar oberoende insyn, utvärdering och granskning. Öppna protokoll och standarder, med sina offentligt tillgängliga specifikationer och ofta transparenta utvecklings- och förvaltningsprocesser⁸, erbjuder en betydligt högre grad av granskningsbarhet och minskar risken för godtycke eller dolda agendor från leverantörshåll. Detta gör det enklare för offentliga organisationer att motivera sina teknikval för samverkan, säkerställa en rättvis behandling av potentiella leverantörer i upphandlingsprocesser, och demonstrera en ansvarsfull och effektiv användning av skattemedel. Ett strategiskt val för öppna protokoll kan därmed inte bara leda till tekniska och ekonomiska fördelar, utan även stärka medborgarnas förtroende för den digitala förvaltningens integritet och funktion.

Nedan följer en tabell som sammanfattar de centrala skillnaderna och nyttoeffekterna:

Tabell 1: Jämförelse av egenskaper: Öppna kontra proprietära protokoll för chattafederation

Egenskap	Öppna protokoll	Proprietära protokoll
Kostnadsaspekter		



Initial kostnad	Ofta låg för själva protokollet/mjukvaran; kostnader kan uppstå för implementation, anpassning, support.	Kan variera; ofta licenskostnader från start, men kan ibland paketeras för att verka lägre initialt.
Löpande kostnader	Primärt för drift, underhåll, support; sällan direkta licenskostnader för protokollet.	Ofta återkommande licensavgifter (per användare/år), supportavtal, kostnader för påtvingade uppgraderingar.
TCO (Total Cost of Ownership)	Potentiellt lägre över tid p.g.a. frånvaro av licenskostnader och större flexibilitet. ¹²	Kan bli hög p.g.a. licenser, inlåsning och begränsad flexibilitet. ¹⁵
Licenskostnader	Sällsynta eller inga för själva protokollet; licenser kan gälla specifika implementationer. ³	Vanligt förekommande och kan vara betydande. ³
Beroende		
Leverantörsberoende	Lågt; möjlighet att byta leverantör av implementationer/tjänster. ³	Högt; starkt beroende av en enskild leverantör för utveckling, support och prissättning. ³
Risk för inlåsning	Låg; öppna specifikationer möjliggör alternativa lösningar. ¹⁴	Hög; svårt och kostsamt att byta system eller leverantör. ¹⁵
Teknisk flexibilitet		
Interoperabilitet	Hög; designade för att möjliggöra kommunikation mellan olika system. ²	Ofta begränsad till leverantörens eget ekosystem; kan försvåra samverkan med externa system. ¹⁸
Anpassningsbarhet	Hög; tillgång till specifikationer och ofta källkod möjliggör anpassning. ³	Låg; anpassningar styrs och begränsas av leverantören.
Skalbarhet	Goda möjligheter genom federerad arkitektur och valfria implementationer. ²⁷	Beror på leverantörens arkitektur; kan vara begränsad av licensmodeller.
Innovation		



Innovationstakt	Kan vara hög genom samverkan och bidrag från en bred gemenskap. ¹⁷	Styrs av leverantörens FoU-budget och prioriteringar.
Möjlighet till egen utveckling	Hög; offentlig sektor kan delta i eller driva utveckling. ³	Mycket begränsad eller obefintlig.
Säkerhet & Kontroll		
Transparens	Hög; specifikationer och ofta källkod är öppna för granskning. ³	Låg; "svart låda"-princip, begränsad insyn.
Granskningsbarhet	Hög; möjliggör oberoende säkerhetsgranskningar. ³	Begränsad till leverantörens interna processer eller dyra tredjepartsrevisioner.
Datakontroll	Hög; organisationen kan kontrollera var data lagras och hur den hanteras. ²⁴	Kan vara begränsad, särskilt vid användning av molntjänster styrda av leverantören.
Digital suveränitet	Stärks genom oberoende och kontroll. ²⁹	Kan undermineras av beroende av externa, ofta utländska, leverantörer. ³¹
Standardisering		
Tillgång till specifikation	Offentlig och ofta kostnadsfri. ⁸	Begränsad, skyddad eller kostnadsbelagd. ⁴
Standardiseringsprocess	Ofta öppen, inkluderande och konsensusdriven. ⁸	Sluten och kontrollerad av leverantören.

Tabell 2: Sammanfattning av ekonomiska fördelar och nyttoeffekter vid val av öppna protokoll för chattfederation

Nyttokategori	Nyttoeffekt	Stödjande principer
Kostnadsreduktion	Lägre Total Cost of Ownership (TCO) över tid.	Undvikande av återkommande licenskostnader, minskad risk för



		påtvingade dyra uppgraderingar, flexibilitet i hårdvaruval.
	Minskade direkta kostnader.	Inga eller låga licensavgifter för användning av protokollet/grundläggande programvara.
	Undvikande av kostnader för leverantörsinlåsning.	Ökad förhandlingsstyrka, minskad risk för oskäliga prisökningar från enskild leverantör.
Effektivitetsvinster	Förbättrad interoperabilitet och sömlös samverkan.	Standardiserad kommunikation mellan olika system och organisationer, minskade silos, undvikande av dubbelarbete.
	Ökad anpassningsbarhet till specifika behov.	Möjlighet att modifiera och skräddarsy lösningar för att passa unika verksamhetsprocesser och krav.
Förbättrad Samverkan	Effektivare kommunikation över organisationsgränser.	Federation möjliggör direkt och säker kommunikation mellan användare i olika anslutna organisationer.
	Stöd för nationell och internationell samverkan.	Gemensamma standarder underlättar gränsöverskridande informationsutbyte och projekt.
Innovationspotential	Katalysator för innovation och lokal utveckling.	Möjlighet för offentlig sektor och lokala företag att utveckla nya tjänster och funktioner baserade på öppna plattformar.
	Ökad innovationstakt genom samutveckling.	Delning av kod och kunskap inom en öppen gemenskap kan accelerera utvecklingen.
Säkerhetsförbättring	Stärkt informationssäkerhet genom transparens.	Möjlighet till bred och oberoende granskning av källkod och protokollspecifikationer identifierar och åtgärdar sårbarheter.
	Ökad granskningsbarhet och ansvarsskyldighet.	Tydlig insyn i hur system fungerar och hur data hanteras, vilket bygger förtroende.



Ökad Resiliens	Förbättrad driftskontinuitet.	Decentraliserad och federerad arkitektur minskar risken för "single points of failure".
	Minskat beroende av enskilda aktörer.	Möjlighet att byta implementation eller tjänsteleverantör utan att byta underliggande standard, vilket ökar robustheten.
Digital Suveränitet	Säkrad kontroll över kritisk kommunikationsinfrastruktur.	Möjlighet att bestämma över datalagring, administration och teknisk utveckling i linje med nationella intressen.
	Oberoende från enskilda, ofta utländska, leverantörers affärsstrategier och potentiella påtryckningar.	Minskad risk för beroende av teknologi som kan påverkas av geopolitiska faktorer eller kommersiella beslut utanför egen kontroll.

Referenser och fördjupning

1. E-förvaltning - EUR-Lex.europa.eu. - European Union - <https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=uriserv:l24226b>
2. Interoperabilitet för europeiska offentliga tjänster - <https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52010DC0744&from=PT>
3. Proprietär – Wikipedia <https://sv.wikipedia.org/wiki/Propriet%C3%A4r>
4. www.esamverka.se, - <https://www.esamverka.se/download/18.596c52ae184a362422a546/1669194851235/221121%20Federation-Utv%C3%A4rdering.pdf>
5. Standarder - Kommerskollegium - <https://www.kommerskollegium.se/importera--exportera/paverka-handelsreglerna/standarder/>
6. www.digg.se, - <https://www.digg.se/download/18.129a4fef1939e2e1c1f113d8/1664286148293/riktlinjer-for-utveckling-och-publicering-av-oppen-programvara.pdf>
7. Öppen standard – Wikipedia, https://sv.wikipedia.org/wiki/%C3%96ppen_standard
8. Öppna standarder – tillgång till och vidareutnyttjande av offentlig information i elektroniskt format - Insyn Sverige, <https://insynsverige.se/documentHandler.ashx?did=105492>
9. Jämförelse Total Cost of Ownership (TCO) och livscykelkostnad (LCC), hämtad maj 12, 2025, <https://www.upphandlingsmyndigheten.se/frageportalen/2023708/jamforelse-total-cost-of-ownership-tco-och-lcc/>
10. Open Source Myth: That It Has a Higher Total Cost of Ownership (TCO), <https://www.lpi.org/blog/2023/03/10/open-source-myth-it-has-higher-total-cost-ownership-tco/>



11. Vendor Lock | NetChoice, https://netchoice.org/wp-content/uploads/2023/01/NetChoice_Garland_The-Pernicious-Consequences-of-Vendor-Lock.pdf
12. Öppen källkod - Sveriges Dataportal, <https://www.dataportal.se/oppen-kallkod>
13. Förslag till en europeisk interoperabilitetsram för smarta städer och samhällen (EIF4SCC), <https://digital-strategy.ec.europa.eu/sv/news/proposal-european-interoperability-framework-smart-cities-and-communities-eif4scc>
14. En reform för datadelning, SOU 2023:96 - Regeringen, <https://www.regeringen.se/contentassets/6866c386b0ec492c8171c92c9c8922cf/en-reform-for-datadelning-sou-202396.pdf>
15. Offentligkod - Öppen programvara i svenska offentliga organisationer, <https://offentligkod.se/>
16. Öppen programvara - RISE, <https://www.ri.se/sv/expertisomraden/expertiser/oppen-programvara>
17. DigResiliens - Om resilienta informationssystem - RISE, <https://www.ri.se/sv/resilienta-informationssystem/digresiliens-om-resilienta-informationssystem>
18. What is digital sovereignty and how are countries approaching it? | World Economic Forum, , <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>
19. Digital sovereignty: the end of the open Internet as we know it? (Part 1) - DiploFoundation, <https://www.diplomacy.edu/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/>
20. NCS3 – Industriella protokoll i Sverige - MSB, <https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/industriella-informations--och-styrssystem/industriella-protokoll-i-sverige.pdf>



Bilaga H - Identitetsfederation som möjliggörare för federerad kommunikation

Denna bilaga fokuserar främst på hur identitetsfederationer kan möjliggöra en säker och interoperabel åtkomst till kommunikationstjänster mellan organisationer i offentlig sektor – inte bara autentisering, utan även gemensam infrastruktur och styrning.

Bilagan beskriver nuläge och möjlig väg framåt för identitetsfederation i offentlig sektor, i relation till framtida federerad kommunikation (t.ex. Matrix).

Slutsats och rekommendation

Genom att successivt bygga stöd för federerad inloggning enligt OIDC och framtida federationsstandarder som OIDF kan offentlig sektor skapa en säker, interoperabel och framtidssäkrad infrastruktur för digital kommunikation.

Denna infrastruktur stöder målen om federerad samverkan inom offentlig sektor, och ligger i linje med principerna som beskrivs i Bilaga E och i rapportens huvuddel.

Identitetsfederation

Det finns många fördelar med en identitetsfederation, som minskad administration av användare för varje enskild tjänst, ökad säkerhet, förbättrad användarupplevelse. Ett öppet federationsprotokoll kräver säkra identitetsfederationer för att få full effekt.

Givet dess verksamhetskritiska funktion behöver identitetsfederationer hantera totalförsvars- och beredskapsperspektivet för att skapa en robust och resilient implementation.¹

Idag finns flertalet etablerade identitetsfederationer i Sverige med olika syften:

Organisationsfederationer för samverkan:

- [Sambi](#) (för vård och omsorg, drivs av Inera AB) - stöder samverkan mellan vårdorganisationer
- [Skolfederation](#) (för utbildningssektorn) - möjliggör samverkan mellan utbildningsinstitutioner
- [Swamid](#) och [eduGain](#) - för akademisk sektor

¹ [Förordning \(2022:524\) om statliga myndigheters beredskap | Sveriges riksdag](#)



Individuell legitimering:

- [Sweden Connect](#) - nationell identitetsfederation som standardiserar integrationsmönstret för direkt legitimering (government-to-citizen/business-to-consumer), där förlitande part beställer identitetskontroll från e-legitimationsutfärdare
- SITHS - SITHS (Säker IT för Hälso- och Sjukvården) är en e-legitimation och ett tillitsramverk som används inom vård och omsorg för stark autentisering och behörighetsstyrning. Det förvaltas av Inera och bygger på certifikat kopplade till smarta kort eller mjukvarulösningar.
- EFOS - EFOS (Elektronisk FörskrivarOrganisation och Signering) är ett federationsramverk som används inom e-hälsa och offentlig sektor för att möjliggöra säker autentisering och elektroniska underskrifter. Det används bland annat för att koppla samman vårdgivare och apotek via e-receptsystem.
- FrejaOrgID - Freja OrgID är en variant av e-legitimationen Freja eID anpassad för organisationer. Den möjliggör säker identifiering av medarbetare i tjänsten och kan användas som en del av identitetsfederationer inom offentlig sektor.

Sweden Connect används idag främst för G2C-identifiering. För myndighetsgemensam (G2G) federation kan andra lösningar som OpenID Federation eller Ena vara mer ändamålsenliga, enligt exempelvis Internetstiftelsen.

Ena, Digg:s ramverk för digital samverkan, kan också spela en roll i att samordna federationslösningar inom offentlig sektor – särskilt vad gäller interoperabilitet och tillitsförvaltning.

Dessa federationer har olika användningsområden beroende på om syftet är samverkan mellan organisationer (B2B/G2G) eller individuell legitimering (B2C/G2C).

Tekniken bakom en identitetsfederation

Globalt flyttar organisationer från äldre protokoll som SAML till modernare lösningar baserade på OIDC. För offentlig sektor är det avgörande att förstå skillnaderna mellan dessa teknologier – särskilt i arbetet med att etablera framtidens federerade digitala infrastruktur.

SAML har inbyggt federationsstöd som en del av protokollet, medan OIDC i sig är ett autentiseringsprotokoll. Den moderna motsvarigheten till SAML:s federationsmodell är OpenID Federation (OIDF), som fortfarande är under utveckling men har stor potential för offentlig sektor.

- **OIDC är ett autentiseringsprotokoll** som är bättre anpassat för moderna system med sitt REST/JSON-format, enklare att implementera, och bättre stöd för mobila enheter.



Det har blivit standarden för nya identitetsautentisering tack vare att det tillgodoser dagens behov av identitetshantering över olika plattformar.

- **SAML har inbyggt federationsstöd** som del av protokollet.
- **OIDF ([OpenID Federation](#))** är den moderna motsvarigheten till SAML:s federationsmodell. OIDF är för närvarande i draft-stadiet men utvecklas aktivt och kan få stor betydelse för offentlig sektor i framtiden.

Även i Sverige pågår en förflyttning mot OIDC för autentisering. [OIDC Sweden](#) har definierat en profil för OIDC som stöds av bl.a. BankID, Freja, Digg, Inera med flera. Sweden Connects profilering för e-legitimering utgår från denna profilering och kompletterar med specifik detaljering för just Sweden Connect.

En möjlig väg framåt i detta ekosystem för offentlig sektor

Inom ramen för Digg:s arkitektur för identitets- och behörighetshantering planeras stöd för OIDF. Det innebär att offentliga tjänster, inklusive framtida chattlösningar, kan använda samma federationsinfrastruktur som exempelvis vårdtjänster. Detta ger både teknisk samordning och förbättrad användarupplevelse genom återanvändbara tillitsrelationer.

Genom att i framtiden kombinera:

- ENA infrastruktur för identitets- och behörighetshantering
- [OIDC Sweden Profile](#)²
- [OpenID Federation \(OIDF\)](#) för federationslagret (när det blir färdigt)
- [Matrix-projektets pågående implementering av OIDC-stöd](#)

kan en framtida vision ses där:

1. Matrix inom organisationsfederation:

Matrix-tjänster (server) fungerar som "Relying Parties" i OIDC-terminologi inom en organisationsfederation. De kan använda OIDC Sweden Profile för att acceptera inloggningar från betrodda svenska identitetsleverantörer. För offentlig sektor är det ofta mer lämpligt att ansluta till en sektorsfederation som i sin tur litar på Sweden Connect, istället för att varje tjänst själv ansluter direkt. Det skapar bättre kontroll, återanvändning och tydligare styrning.

² Se mer: oidc.se/profilering (om den finns, annars skriv: "Profilen definieras av DIGG, Inera, Freja eID, BankID m.fl.")



2. Federerad identitetshantering:

Användare kan logga in på Matrix-tjänster med sin organisationsidentitet. Inloggning kan ske via arbetsgivares, skolas eller andra sektors federationers identiteter. Matrix-server hanterar inte längre lösenord utan förlitar sig på betrodda externa identitetsleverantörer.

3. Enhetlig säkerhetsmodell:

Samma säkerhetskrav och tillitsramverk som används inom offentlig sektor kan då tillämpas på Matrix-tjänster. E-legitimationer kan användas för att säkert identifiera användare när det behövs. Krypterade meddelanden (E2EE) i Matrix behåller sin integritet samtidigt som identitetshandlingen federeras

Denna utveckling skapar synergier med andra initiativ inom offentlig sektor. Identitets- och auktorisationslösningarna för chatttjänsterna kan utnyttja samma federationsinfrastruktur som etableras för andra offentliga sektortillämpningar, vilket ger enhetlighet, säkerhet och kostnadseffektivitet.

Denna utveckling passar väl in i [ENA:s målbild](#) om en enhetlig, nationell modell för säker identitetshantering som stödjer både människor, organisationer och i digitala ekosystem.

En nationellt samordnad federationslösning kräver även tydlig styrning av tillitsramverk, certifikathandtering och incidenthantering. Juridiska aspekter såsom krav på säkerhetsskyddsanalyser, personuppgiftsansvar och avtal mellan parter behöver beaktas. Tidig koordinering med berörda aktörer kan minska risken för förseningar i implementationen.

Digg har särskild kompetens inom behörighets- och auktorisationsmodeller, och skulle kunna bidra i ett vidare arbete med att säkerställa att en federerad chattlösning integreras i en gemensam identitetsinfrastruktur med hög tillit och spårbarhet.

Denna bilaga har tagits fram med inspel från bl.a. Digg, Sambruk och RISE inom ramen för remissrunda i dSam4-arbetsgruppen under våren 2025



Så förbereder du din organisation för det gemensamma protokollet för digital samverkan

Den här vägledningen är ett strategiskt stöd för eSam:s medlemmar och andra offentliga aktörer som vill förbereda sig för ett gemensamt, öppet protokoll för chatt och digital kommunikation – med målet att stärka säkerhet, interoperabilitet och samverkan över organisationsgränser.

1. Bakgrund och förankring inom eSam

Det strategiska stödet bygger på det analysarbete som arbetsgruppen inom dSam4 har genomfört under 2025. Arbetsgruppen har utvärderat sex möjliga vägval och rekommenderar att ett gemensamt, öppet kommunikationsprotokoll införs – Matrix – som möjliggör federation och interoperabilitet.

2. Vad innebär ett gemensamt protokoll för chatt och samverkan?

Ett **gemensamt protokoll** är en teknisk standard som olika system kan använda för att kommunicera med varandra – oavsett vilket program eller vilken leverantör som används. Det gör det möjligt för organisationer att använda olika verktyg men ändå kunna chatta och samarbeta över gränser, på ett säkert och effektivt sätt.

Matrix är ett sådant öppet protokoll. Det fungerar på ett liknande sätt som e-post: varje myndighet kan välja egna lösningar, men eftersom de talar samma "språk" via Matrix kan de ändå utbyta meddelanden, delta i gemensamma kanaler och kommunicera i realtid.

Protokollet möjliggör så kallad **federation**, vilket betyder att systemen kan prata med varandra utan att vara centralt styrda eller inlåsta till en specifik leverantör. Detta stärker:

- **Självbestämmande:** varje organisation behåller kontroll över sin egen miljö.
- **Säkerhet:** trafiken kan krypteras (end-to-end) och hanteras inom Sveriges gränser.
- **Skalbarhet:** det är möjligt att börja i liten skala och utöka över tid.
- **Redundans:** decentralisering minskar sårbarheten vid driftstörningar.

Det gör det möjligt att:

- samverka i vardagen utan att behöva särskilda installationer
- kommunicera effektivt vid kris eller samhällsstörningar
- bygga en långsiktigt hållbar digital kommunikationsinfrastruktur för offentlig sektor.



Det är viktigt att understryka att federationen inte behöver ersätta befintliga kommunikationsverktyg, som till exempel Microsoft Teams. Det federerade protokollet kan användas som ett komplement, särskilt för extern samverkan.

3. Vad innebär det här för min organisation?

Att införa ett gemensamt protokoll för digital kommunikation innebär vissa konsekvenser för varje myndighet – tekniskt, organisatoriskt och resursmässigt.

Exempelvis behöver myndigheten:

- Förstå principerna bakom federation och öppna protokoll
- Se över befintliga verktyg och framtida behov
- Ställa krav på stöd för Matrix vid upphandling eller avrop
- Bedöma behov av kompetens och resurser

Vägledningen är framtagen för att ge stöd i detta arbete, men varje myndighet behöver själv bedöma när ett införande är relevant, och i vilken takt det är möjligt att förbereda sig.

4. Varför är detta viktigt?

- För att kunna samverka effektivt i vardag och kris.
- För att uppfylla framtida lagstiftning, som SOU 2023:96 och Interoperable Europe Act.
- För att säkerställa digital suveränitet och minska beroende av enskilda leverantörer.
- För att bidra till målen i Sveriges nya digitaliseringsstrategi: "Ena – Sveriges digitala infrastruktur".

5. Vad behöver myndigheten göra?

Under 2026, kan myndigheter börja förbereda sig för att kunna använda det gemensamma protokollet.

Redan nu:

- Ta del av rapport och bilagor från dSam4.
- Förankra frågan internt: behov, möjligheter, risker.
- Säkerställ att ledningen är informerad om syftet och arbetets koppling till strategiska mål.
- Har ni system idag som kan använda sig av Matrix-protokoll?
- Hur säkerställer ni juridisk och teknisk förberedelse inför upphandling eller avrop?
- Vilken kompetens behöver ni bygga upp internt för att kunna införa och förvalta en federerad lösning?
- Verifiera om myndigheten kan bidra med kapacitet och kompetens från våren 2026: teknisk expertis (federation, säkerhet), juridiskt stöd (upphandling, interoperabilitet) samt förändringsledning och kommunikation är resurser som behövs.



Under 2026:

- Se över kommande upphandlingar eller avrop – ställ krav på stöd för Matrix-protokollet.
- Utse kontaktperson på myndigheten för samordning med dSam4 och internt på myndigheten.
- Bidra med kompetens om det är möjligt

Dessa förberedelser kan hjälpa er organisation att ligga steget före och vara redo när bredare införande inleds från 2027.

6. Plan för införande i tre steg

Steg 1 – Arbetsgruppen testar i liten skala (höst 2025 – vår 2026)

- Myndigheterna i arbetsgruppen kommer att delta i mindre pilotprojekt för att testa federation praktiskt.
- Erfarenheterna används som grund för att ta fram mer detaljerade riktlinjer till andra myndigheter.

Not: Under hösten 2025 kommer arbetet främst att drivas av befintlig arbetsgrupp, där deltagarna har begränsad arbetstid avsatt. För att kunna skala upp arbetet och ta fram en mer omfattande vägledning rekommenderas förstärkning med nyckelkompetenser från våren 2026. Det kan handla om teknisk expertis (federation, säkerhet), juridiskt stöd (upphandling, interoperabilitet) samt förändringsledning och kommunikation.

Steg 2 – Vägledning och samverkan (hösten 2026)

- Baserat på testresultaten skapas ett mer komplett stöd till myndigheter.
- Fler myndigheter bjuds in att delta.
- Stödmaterial anpassas efter olika organisationers behov och förutsättningar.

Steg 3 – Införande (2027 och framåt)

- Myndigheter som har behov ska kunna börja federera via gemensamt protokoll för digital samverkan.
- Samordning sker inom eSam och i samverkan med DIGG.

7. Rekommenderade principer

- Använd öppna standarder för kommunikation.
- Tänk på informationsklassning och behov av E2EE (end-to-end encryption).
- Bygg lösningar som är förvaltningsbara och interoperabla.
- Beakta tillgänglighet, robusthet och beredskap för incidenter.



- Säkerställ att lösningar uppfyller krav på tillgänglighet enligt WCAG och svenska språklagen.

8. Stöd och samverkan

- Arbetsgruppen inom eSam (dSam4) samordnar fortsatt arbete.
- Arbetsgruppen planerar att sätta upp en första testmiljö under hösten 2026. Denna kommer utgå från praktiska tester som genomförs i mindre skala.
- Kontakt med DIGG etableras för att säkra koppling till den nationella digitala infrastrukturen (ENA).
- Stödmaterial och erfarenhetsutbyte kommer löpande.

9. Uppdatering av vägledningen

Vägledningen underhålls av arbetsgruppen inom dSam4. Innehållet kommer att uppdateras löpande utifrån:

- Erfarenheter från pilotprojekt och tester under 2025–2026
- Förändringar i lagstiftning, styrdokument eller digitaliseringsstrategier
- Synpunkter och behov från eSams medlemmar
- Samordning med DIGG och andra relevanta initiativ (som ENA)

Målet är att vägledningen ska vara ett praktiskt stöd som följer utvecklingen – från förberedelse till införande.

Arbetsgruppen ansvarar för att uppdaterade versioner publiceras i samverkan med eSam.



Bilaga J - En jämförelse mellan MLS, MIMI och Matrix-protokollet

Denna bilaga fokuserar på att ge en teknisk jämförelse mellan tre centrala teknologier - Messaging Layer Security (MLS), More Instant Messaging Interoperability (MIMI) och Matrix-protokollet.

Messaging Layer Security (MLS)

Denna sektion analyserar MLS status, dess kärnarkitektur, de säkerhetsgarantier den erbjuder och dess roll som en möjliggörande teknologi för nästa generations interoperabla meddelandesystem.

Standardisering och aktuell status

Messaging Layer Security (MLS) har övergått från ett experimentellt utkast till en formell internetstandard. Protokollet publicerades officiellt av Internet Engineering Task Force (IETF) som RFC 9420 i juli 2023. Denna standardisering är av stor betydelse eftersom den för första gången ger industrin ett enhetligt, öppet och rigoröst granskat protokoll för end-to-end-kryptering i grupper. Tidigare har landskapet varit fragmenterat med olika proprietära implementationer eller varianter av Signal-protokollet, vilka ofta saknat en fullständig och öppen specifikation.

IETF har publicerat ett kompletterande dokument, RFC 9750, som är en informativ guide till MLS-arkitekturen. Detta dokument, publicerat i april 2025, beskriver hur man bygger ett komplett meddelandesystem runt MLS-protokollets kärna. Dokumentet belyser en viktig aspekt - MLS är en grundläggande komponent för nyckelhantering och kryptering, inte en komplett, fristående meddelandelösning. Det faktum att IETF inte bara standardiserade kryptografin (RFC 9420) utan även tillhandahöll en arkitekturguide (RFC 9750) visar på en insikt om att ett protokolls säkerhetsgarantier lätt kan undermineras av en felaktig implementation.

Arkitektoniska kärnprinciper

Kärnan i MLS ligger i dess metod för att hantera gruppnycklar, känd som "Continuous Group Key Agreement". Till skillnad från tidigare metoder som Signal-protokollets "Double Ratchet", som bygger på parvisa krypteringssessioner, använder MLS en trädstruktur för att representera gruppens tillstånd. I denna modell, kallad



"Asynchronous Ratcheting Trees" (ART), representeras varje medlem som ett löv i ett binärt träd.

Denna trädstruktur är nyckeln till MLS effektivitet. När en medlem läggs till eller tas bort från gruppen krävs endast ett fåtal uppdateringar längs sökvägen från lövet till trädets rot för att generera en ny gruppnyckel. Detta innebär att de kryptografiska operationerna, både beräkningsmässigt och kommunikationsmässigt, skalar logaritmiskt ($\log(N)$) med gruppens storlek (N). Detta står i kontrast till äldre metoder där "kostnaden" kunde skala linjärt (N) eller till och med kvadratisk (N^2). Denna logaritmiska skalbarhet är vad som gör MLS praktiskt användbart för mycket stora chattgrupper/kanaler, med stöd för upp till 50 000 medlemmar.

Avancerade säkerhetsgarantier

MLS är designat för att erbjuda en robust uppsättning moderna säkerhetsgarantier som går utöver grundläggande kryptering. Dessa egenskaper, definierade i de officiella specifikationerna, är avgörande för att bygga förtroende i ett interoperabelt ekosystem.

Meddelandekonfidentialitet, integritet och autentisering: Säkerställer att meddelanden är privata, oförändrade och kommer från den påstådda avsändaren.

Forward Secrecy (FS): Garanterar att om en medlems långsiktiga nycklar komprometteras, kan en angripare inte dekryptera tidigare meddelanden.

Post-Compromise Security (PCS): Om en medlems enhet blir komprometterad kan protokollet automatiskt "läka" sig självt. Efter att användaren har vidtagit åtgärder för att säkra sin enhet kommer framtida meddelanden återigen att vara skyddade från angriparen.

Medlemskapsautentisering: Alla medlemmar i en grupp har en konsekvent och kryptografiskt verifierbar bild av vilka andra som ingår i gruppen. Detta förhindrar att en angripare i smyg kan lägga till en spion i konversationen.

Tillämpningar och och framtida utveckling

Protokollet har fått stöd från och aktörer i branschen planerar tillämpa protokollet. Google har meddelat sin avsikt att integrera MLS i end-to-end-krypteringen för Google Messages över Rich Communication Services (RCS). GSMA, som styr RCS-standarden, och Apple har också meddelat att de kommer att stödja RCS med MLS. Företag som Cisco och Wire har också varit tidiga med att implementera och stödja MLS.



Även Matrix-protokollet har deklarerat sin avsikt att utvärdera och potentiellt nyttja MLS. Det pågår även forskning och IETF-utkast för att integrera postkvantkryptografi (PQC), vilket syftar till att säkerställa långsiktig säkerhet mot framtida hot från kvantdatorer.

MIMI-arbetsgruppen

Medan MLS löser det grundläggande problemet med säker grupp-kryptering, återstår den större utmaningen att få olika meddelandetjänster att kunna kommunicera med varandra. Detta är uppdraget för IETF:s arbetsgrupp "More Instant Messaging Interoperability" (MIMI).

Stadgar och målsättningar

Kärnuppdraget för MIMI-arbetsgruppen är att "specificera den minimala uppsättning mekanismer som krävs för att göra moderna internetmeddelandetjänster interoperabla". Det är viktigt att notera att detta uttryckligen gäller för tjänster med end-to-end-kryptering och att målet är att uppnå interoperabilitet utan att underminera de säkerhetsgarantier som användarna förväntar sig.

Arbetsgruppens stadgar identifierar fyra centrala problemområden som kräver standardisering för att detta ska bli möjligt:

Identitet: Hur en användares kryptografiska identitet kan etableras och verifieras över olika tjänsteleverantörers gränser.

Introduktion: Hur en användare på tjänst A kan upptäcka och initiera en konversation med en användare på tjänst B.

Innehållsformat: Ett gemensamt format för meddelanden och funktioner (som svar, reaktioner och bilagor) som fungerar i en E2EE-kontext.

Leverans: En gemensam leveranstjänst och ett transportprotokoll för kommunikation mellan de federerade domänerna.

MIMI:s fokus på en "minimal uppsättning" är en medveten strategi för att undvika tidigare misslyckanden. Tidigare försök till interoperabilitet, som XMPP, försökte standardisera ett mycket brett spektrum av funktioner, vilket ledde till komplexa specifikationer som var svåra att implementera fullt ut. MIMI:s stadgar anger explicit att man ska "dra lärdom av dessa tidigare försök" och fokusera på det absolut nödvändiga för att lösa kärnproblemet först.



Aktuell status och tidsplan för standardisering

MIMI är ett pågående arbete, och dess tekniska utveckling sker genom en serie offentliga "Internet-Drafts". Dessa dokument representerar de tekniska förslag som för närvarande diskuteras och förfinas inom arbetsgruppen. De centrala utkasten inkluderar:

- draft-ietf-mimi-protocol: Definierar kärnprotokollet för kommunikation mellan leverantörer, med användning av HTTPS och MLS.
- draft-ietf-mimi-content: Specificerar formatet för meddelandehåll.
- draft-ietf-mimi-room-policy: Beskriver hur policyer för ett "rum" (t.ex. medlemskapsregler) ska hanteras.

Arbetsgruppens officiella milstolpar ger en indikation på den förväntade tidsplanen som pekar mot en möjlig publicering som RFC-standarder under slutet av 2025 eller början av 2026, även om sådana tidsplaner alltid är preliminära. Arbetet hade initialt ett aktivt deltagande från olika representanter från industrin, men IETF meddelar att intresset har svalnat och endast ett fåtal arbetar i MIMI-arbetsgruppen i dagsläget. Det pågår därför en dialog inom IETF om scopet för arbetet ska ändras.

Den arkitektoniska ramen för MIMI

MIMI:s arkitektur är utformad för att fungera som ett lager ovanpå MLS. Den förutsätter att MLS används för nyckelablering, konfidentialitet och autentisering av gruppmedlemmar. MIMI specificerar hur leverantörer ska interagera med varandra, men lämnar i stort sett kommunikationen mellan en klients app och dess egen server ospecificerad. Detta är ett medvetet designval för att minimera de ändringar som befintliga appar behöver göra för att bli kompatibla.

En central del av den föreslagna arkitekturen är en "hub"-baserad modell för att säkerställa ordningen på meddelanden. Eftersom MLS kräver att vissa meddelanden (särskilt de som ändrar gruppens tillstånd) levereras i en strikt och konsekvent ordning till alla medlemmar, föreslås att en server för varje konversation agerar som en central "hub". Denna hub ansvarar för att tidsstämpla och distribuera meddelanden till alla deltagande leverantörer. Även om detta löser ordningsproblemet, introducerar det en spänning mellan decentralisering och centralisering. Systemet som helhet är federerat, men varje enskild konversation får en centraliserad punkt för ordningsföljd. Detta skapar en ny förtroendegräns och en potentiell attackvektor, då en illvillig hub teoretiskt skulle kunna censurera, fördröja eller ändra ordningen på meddelanden. Denna risk har redan



uppmärksammas i akademisk forskning som föreslår revisionslager för att upptäcka sådant missbruk.

Centrala utmaningar för standardisering

MIMI-arbetsgruppens framgång beror inte bara på teknisk implementation, utan också på att navigera i ett komplext landskap av praktiska och strategiska utmaningar. För att bibehålla fokus har gruppen medvetet valt att exkludera vissa komplexa problem från sitt initiala uppdrag.

Bearbetning av metadata för att hantera spam och missbruk, samt interoperabla mekanismer för gruppadministration och moderering, är för närvarande "out of scope". Detta pragmatiska tillvägagångssätt syftar till att först etablera en fungerande grund för interoperabilitet.

Den kanske största utmaningen är dock inte teknisk. För att MIMI ska lyckas krävs samarbete och konsensus mellan kommersiella konkurrenter som historiskt har skyddat sina egna ekosystem.

Drivkrafter som EU:s Digital Markets Act (DMA) skapar ett regulatoriskt tryck som kan tvinga fram detta samarbete, men den praktiska implementationen kommer att kräva att tjänsteleverantörer lutar på varandra för att hantera autentisering, nyckelmateriale och missbrukspolicyer på ett ansvarsfullt sätt.

En etablerad modell för decentraliserad kommunikation: Matrix-protokollet

Parallellt med IETF:s standardiseringsarbete existerar Matrix, ett moget och väletablerat öppet protokoll för decentraliserad kommunikation som skapat ett stort avtryck för offentlig sektor inom EU. För att kunna göra en jämförelse med MIMI är det nödvändigt att först förstå Matrix kärnarkitektur, dess säkerhetsmodell och dess strategi kring interoperabilitet.

Kärnan

Matrix definieras som en öppen standard för interoperabel, decentraliserad realtidskommunikation. Dess uttalade mål är att fungera likt e-post, dvs. att låta användare kommunicera med varandra oavsett vilken app eller serverleverantör de använder. Tekniskt sett är Matrix ett federerat system bestående av "homeservers" som synkroniserar konversationshistorik med varandra via ett Server-Server API, vanligtvis över HTTPS med JSON som dataformat.



Den mest utmärkande egenskapen hos Matrix är dess datastruktur. Istället för en linjär lista av meddelanden lagras all data i ett "rum" som en "event graph", en riktad acyklisk graf (DAG). Varje handling – ett skickat meddelande, en användare som går med, ett rumsnamn som ändras – är en "händelse" (event) som kryptografiskt länkar till sin föregångare (eller sina föregångare). Detta möjliggör konceptet "eventual consistency". Om nätverksanslutningen mellan två servrar bryts kan båda fortsätta att ta emot nya händelser i rummet. När anslutningen återupprättas kan serverna synkronisera och slå samman sina respektive historikgrafer. Denna arkitektur, som prioriterar systemets motståndskraft (resiliens) och varje servers autonomi, är robust mot nätverksfel men medför också komplexitet, särskilt när det gäller att lösa konflikter om rummets tillstånd ("state resolution").

Inbyggd end-to-end-kryptering

Matrix har haft inbyggt stöd för end-to-end-kryptering sedan 2020, och det är aktiverat som standard för alla nya privata konversationer. Krypteringen bygger på två separata men samverkande protokoll, implementerade i bibliotek som libolm och det nyare, granskade vodozemac:

- **Olm** är en implementation av Double Ratchet-algoritmen, populariserad av Signal. Olm används för att etablera säkra en-till-en-krypteringssessioner mellan två specifika enheter. Dess primära användning i gruppchattar är att säkert distribuera nycklarna för Megolm.
- **Megolm** är en kryptografisk "ratchet" designad specifikt för gruppchattar. Varje deltagare i ett krypterat rum skapar sin egen utgående Megolm-session. När de skickar ett meddelande krypteras det med denna sessionsnyckel, som sedan roteras. Nyckeln för att dekryptera meddelanden från denna session delas säkert med de andra medlemmarna i rummet via deras individuella Olm-sessioner. Denna modell är väl anpassad för Matrix decentraliserade natur men har kända skalbarhetsutmaningar i mycket stora grupper, ett problem som MLS är designat för att lösa.

Matrix-ekosystemet

Matrix är mer än bara ett protokoll; det är ett helt ekosystem. Detta inkluderar öppen källkod för serverimplementationer (där Synapse är den mest mogna), ett brett utbud av klientapplikationer för alla plattformar (där Element är den mest kända), och väldefinierade API:er för kommunikation mellan klient och server.



En av de unika aspekterna med Matrix är dess koncept av överbrygning ("bridging"). En brygga är en applikationstjänst som ansluter ett Matrix-rum till ett externt, icke-Matrix-nätverk som Slack, IRC, Discord eller Telegram. Detta gör det möjligt för Matrix-användare att kommunicera med användare på dessa plattformar från sin Matrix-klient. Denna funktion visar Matrix långvariga och praktiska fokus på interoperabilitet. Det representerar en annan filosofi än MIMI:s. Medan MIMI syftar till att skapa ett gemensamt protokoll för direktkommunikation mellan leverantörer, fungerar Matrix på samma sätt, men utöver det som ett universellt översättningslager eller en "meta-interoperabilitets-hub" som kan ansluta till vilket annat protokoll som helst via en anpassad brygga.

Jämförelse mellan Matrix och MIMI

Med en grundläggande förståelse för MLS, MIMI och Matrix är det lättare att göra en direkt jämförelse mellan protokollen.

Matrix händelsegraf (DAG) mot MIMI:s ordnade meddelandemodell

Den största tekniska skillnaden mellan Matrix och MIMI ligger i deras datamodeller för konversationshistorik.

Matrix: Använder en decentraliserad händelsegraf (DAG) som optimerar för motståndskraft och "eventual consistency". Inget enskilt system äger rummet eller dess historik; data replikeras över alla deltagande servrar. Detta är en mycket robust modell men kräver komplexa algoritmer för att hantera sammanslagning av historik och lösa tillståndskonflikter.

MIMI/MLS: Kräver implicit ett linjärt, ordnat flöde av meddelanden. Detta är ett direkt arv från MLS, som behöver en entydig ordning på kontrollmeddelanden för att säkerställa att alla deltagare har ett konsekvent kryptografiskt tillstånd. Denna modell leder till en arkitektur med en "hub" eller "sequencer" per konversation, vilket är enklare att implementera men introducerar en centraliserad punkt för ordningsföljd och förtroende. Detta försämrar motståndskraften i arkitekturen.

Matrix prioriterar decentralisering och autonomi, medan MIMI prioriterar garanterad konsistens, även till priset av en centraliserad komponent per konversation.



"Linearized Matrix"

Som ett svar på den arkitektoniska klyftan har Matrix-ekosystemet självt utvecklat och föreslagit "Linearized Matrix".

"Linearized Matrix" är en förenklad version av Matrix rumsmodell. Istället för en komplex DAG, representeras historiken som en dubbellänkad lista av händelser. Denna linjära historik hanteras av en utsedd "hub"-server för det specifika rummet. Denna modell är designad för att vara kompatibel med vanliga, icke-linjära Matrix-serverar. En fullvärdig Matrix-server kan agera som "hub" för Linearized Matrix-klienter och översätta sin interna DAG till en linjär historik för dem.

Decentralized MLS

MLS-standarden (RFC 9420) utgår ofta från en linjär ordning av händelser, vilket är svårt att garantera i en decentraliserad miljö som Matrix där serverar kan vara osynkade. Matrix måste bygga ett lager (DMLS) som hanterar denna faktor.

Matrix arbetar därför med att ersätta eller komplettera sitt nuvarande krypteringsprotokoll (Olm/Megolm) med MLS (Messaging Layer Security). Målet är att möjliggöra effektivare och säkrare kryptering för väldigt stora gruppchattar (end-to-end-kryptering som skalar bättre) samt att lösa problem med synkronisering och nyckelhantering.

Projektet har ett specifikt Rust-baserat bibliotek kallat *matrix-dmls* som är kärnan i detta arbete.

Säkerhetsmodeller i kontext

Jämförelsen av säkerhetsmodellerna visar en konvergens.

- **Matrix (Olm/Megolm):** Ett moget och granskat system baserat på Double Ratchet. Det är väl beprövat och anpassat för Matrix decentraliserade modell men har skalbarhetsbegränsningar.
- **MIMI (MLS):** Bygger från grunden på MLS, som är designat för effektivitet och skalbarhet i stora grupper.

Omfattning och filosofi

Protokollen skiljer sig åt i sin övergripande ambition och filosofi.

- **Matrix:** Siktar på att vara ett "generiskt system för meddelanden och datasynkronisering för hela webben". Det är ett komplett ekosystem med



specifikationer som täcker allt från klient-server-kommunikation till identitetshantering, applikationstjänster och realtidskommunikation.

- **MIMI:** Har det uttalade målet att definiera en "minimal uppsättning mekanismer" för interoperabilitet mellan meddelandesystem. MIMI försöker inte bygga en komplett kommunikationsplattform, utan snarare det tunnaste möjliga lagret för att koppla samman befintliga plattformar.

Strategiska perspektivet

Jämförelsen visar att framtiden för säker och interoperabel meddelandehantering inte handlar om en kamp där en vinnare tar allt. Istället rör vi oss mot en framtid präglad av konvergens och samexistens, där standardiserade lager bygger på varandra för att skapa ett rikare och mer sammankopplat ekosystem.

Scenariot är inte "Matrix mot MIMI", utan snarare "Matrix i en värld med MIMI"(eller tvärtom). MIMI utvecklas fortfarande och IETF kan ändra scope, framtiden får utvisa hur detta påverkar Matrix och andra existerande lösningar på marknaden.

I denna kontext är Matrix väl positionerat. Genom att tillämpa MLS och erbjuda ett förslag på kompatibilitetslösningar med "Linearized Matrix" eller "Decentralized MLS" kan Matrix utvecklas till en IETF-kompatibel plattform. Ett annat scenario kan vara att IETF samarbetar med Matrix Foundation för att hitta gemensamma lösningar.

Sammanfattning

Den behovsbild som beskrivs i huvudrapporten för detta eSam projekt kräver en långsiktigt hållbar lösning samtidigt som de mest prioriterade behoven behöver hanteras så snart som möjligt. Detta för att myndigheter ska kunna fortsätta samarbeta effektivt och sömlöst även om marknaden inte har anpassat sig.

Messaging Layer Security (MLS) är en färdig och publicerad IETF-standard och ger en ny lösning för att utbyta nycklar i säkra gruppkommunikationslösningar. More Instant Messaging Interoperability (MIMI) är ett aktivt IETF-projekt som bygger på MLS, bara framtiden kan utvisa vad slutresultatet blir av det arbetet.

Matrix-protokollet står inte i opposition till denna utveckling. Tvärtom anpassar det sig för att säkerställa sin fortsatta relevans och unika position. Genom sin vilja att tillämpa MLS och anpassa sin egen protokollstack, visar Matrix en framåtblickande strategi. Den omfattar öppna standarder samtidigt som den behåller de unika arkitektoniska fördelar som har definierat protokollet. Vi ser bilden av ett ekosystem i rörelse mot en mer



öppen, säker och federerad framtid, där olika arkitekturer kan behöva samexistera och samverka genom gemensamma, standardiserade lager.

Fördjupning

1. Messaging Layer Security - Wikipedia, https://en.wikipedia.org/wiki/Messaging_Layer_Security
2. RFC 9420 - The Messaging Layer Security (MLS) Protocol - IETF Datatracker, <https://datatracker.ietf.org/doc/rfc9420/>
3. Information on RFC 9750 - » RFC Editor, <https://www.rfc-editor.org/info/rfc9750> 6.
RFC 9750 - The Messaging Layer Security (MLS) Architecture - IETF Datatracker, <https://datatracker.ietf.org/doc/rfc9750/>
4. A giant leap forwards for encryption with MLS - Matrix.org, <https://matrix.org/blog/2023/07/a-giant-leap-with-mls/>
5. More Instant Messaging Interoperability (mimi) - IETF Datatracker, <https://datatracker.ietf.org/wg/mimi/about/>
6. draft-ietf-mimi-protocol-04 - More Instant Messaging Interoperability (MIMI) using HTTPS and MLS - IETF Datatracker, <https://datatracker.ietf.org/doc/draft-ietf-mimi-protocol/>
7. draft-ietf-mimi-content-07 - More Instant Messaging Interoperability (MIMI) message content, <https://datatracker.ietf.org/doc/draft-ietf-mimi-content/>
8. Room Policy for the More Instant Messaging Interoperability (MIMI) Protocol - GitHub Pages, <https://ietf-wg-mimi.github.io/mimi-room-policy/draft-ietf-mimi-room-policy.html>
9. Matrix-protokollet - [https://en.wikipedia.org/wiki/Matrix_\(protocol\)](https://en.wikipedia.org/wiki/Matrix_(protocol))
10. FAQ - Matrix.org, <https://matrix.org/faq/>
11. Matrix Specification, <https://spec.matrix.org/>
12. Matrix as a Messaging Framework - IETF, <https://www.ietf.org/archive/id/draft-ralston-mimi-matrix-framework-01.html>
13. Message Security in Matrix - Sumner Evans, <https://sumnerevans.com/posts/matrix/megolm/>
14. End-to-End Encryption implementation guide - Matrix.org, <https://matrix.org/docs/matrix-concepts/end-to-end-encryption/>
15. DMLS, MIMI, etc - Matrix Conference 2024, https://2024.matrix.org/documents/talk_slides/LAB3%202024-09-20%2016_15%20Travis%20Ralston%20-%20DMLS,%20MIMI,%20etc.pdf
16. turt2live/ietf-mimi-linearized-matrix - GitHub, <https://github.com/turt2live/ietf-mimi-linearized-matrix>
17. Linearized Matrix - GitHub Pages, <https://turt2live.github.io/ietf-mimi-linearized-matrix/draft-ralston-mimi-linearized-matrix.html>