

Report

Common federation protocol for public sector chat

ES2025-20





Content

1. Summary	4
2. Demarcation	6
3. Background.....	6
3.1 History.....	8
3.1.1 Email – where it all began.....	8
3.1.2 Chat – technical development.....	9
3.2 Current status	11
4. Environment	13
4.1.1 Alternative solutions to public central soil services	14
4.1.2 International examples of the application of open protocols.....	15
5. Desired new location.....	17
5.1 Principles for the future.....	18
5.2 Economic impact.....	19
5.3 Legal and information security	21
6. Decision	23
7. Final words	24



1. Summary

Employees in our agencies are entering a channel shift and new ways of working where users move from traditional email and instant chat to a more cohesive user experience with persistent chat, file sharing, video rooms, voicemail, digital whiteboards, AI, and similar capabilities. This shift also means that users expect collaboration capabilities in external collaborations to match those within their own agency.

Today's communications landscape is fragmented, with many different tools and platforms. Collaboration across government boundaries is becoming more difficult, and dependence on a few global providers is growing. This poses risks to digital sovereignty, legal uncertainty, reduced control over sensitive information, and government control over our ability to collaborate.

The public sector is facing an important choice: to continue on a path of fragmentation and supplier dependencies, or to agree on an open, interoperable and democracy-promoting communications infrastructure – a common “language”, where authorities can freely choose between both delivery form and supplier according to their unique operational needs.

The choice of communication protocol is a matter of great strategic importance for the Swedish public sector. It is about more than just technology; it is about creating the conditions for an efficient, secure, resilient and economically sustainable digital administration that can meet the current and future needs of citizens and society. In order for the communication infrastructure to maintain its fundamental properties, a common model of principles needs to be established.

The legal and strategic requirements are growing within the EU. Regulations such as NIS2, Data Act, Digital Markets Act and Interoperable Europe Act place demands on openness, security and interoperability – both within and between member states.

New legislative proposals such as "A reform for data sharing" (SOU 2023:96)¹ Reinforcing the fact that the public sector is lagging behind in terms of interoperability and data sharing, the eSam working group sees clear synergies with a common open protocol for chat federation.

Open APIs, public code bases, and standardized protocols enable organizations to develop and adapt digital infrastructure themselves. This can improve innovation

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



capacity, shorten development times, and reduce dependence on individual suppliers, as more expertise is available within the public sector.

However, for this to become a reality, a conscious investment in knowledge sharing and development is required. Taking advantage of IT as a resource requires that the public sector continuously learns, allocates time for incremental development and testing, builds common repositories for code and knowledge, and encourages collaboration across organizational boundaries. Experiences from, among others, the British Government Digital Service² and the Baltic digitalization programs show that long-term development of skills – not just a transition to new technology – is important for joint, distributed solutions to work well over time.

If authorities do not take ownership of their ability to collaborate across agency boundaries, there is a risk that the public sector will in practice standardize its conditions for collaboration around a few commercial suppliers. We have already seen this happen before – with Microsoft Skype for Business as a clear example. This results in a comprehensive lock-in effect. When a critical mass of authorities choose the same solution to be able to collaborate with each other, it becomes difficult to change solutions - who dares to take the first step away from a solution and risk losing collaboration opportunities? Another effect is that authorities adapt to the supplier – not the other way around. Or that authorities choose the same solution as “everyone else”, which can lead to reduced competition, reduced innovation and fewer solutions that are adapted to the actual needs of the public sector.

Swedish authorities need control and discretion over their conditions for cooperating with each other. This is illustrated by the consultation bodies that the working group has been in contact with:

"A federated, open solution strengthens democracy and creates robustness." – RISE

"The report is well written – we support the long-term path chosen." – Sunet

"Important to have clarity around technical standards and governance." – Internet Foundation

"A decentralized chat infrastructure, based on open standards and federated solutions, can be a way to reduce dependence on individual providers and central cloud services" -MSB

"This initiative has clear synergies with new legislative proposals in the area of interoperability and data sharing" - Government Offices

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



The report provides a basis for further decisions on how authorities within eSam can act given that they choose different communication solutions at the same time that authorities need to cooperate across authority boundaries. The working group does not take a position on specific supplier solutions, since authorities' choice of product or service is not in focus in this context. Based on this, the lowest common denominator is not product/service but instead a common protocol for cross-agency cooperation. The question being addressed is how strategic conditions can be ensured to enable supplier-independent, efficient and robust cooperation within the public sector.

These are precisely the issues at the heart of the EU's digitalisation strategy, both current and future regulations. Not making an active choice would therefore not only be passive – it would also be an active step away from the path prioritised within European cooperation on digitalisation.

2. Demarcation

This material has been produced on behalf of the steering group within the framework of the Digital Collaboration Platforms (dSam) eSam working group.

The working group consists of expert competences from various authorities. However, assessments described in the report should not be seen as formally decided or an official position within the respective authority. This is part of the recommended timeline presented in the report.

This report constitutes a basis for decision-making for further discussion within eSam. It does not contain any formal recommendations. Any suggestions for further direction will be handled separately in a letter.

3. Background

eSam members see a great need to use group chat solutions as part of a modern way of working. Email has become an outdated communication tool and lacks many of the features that modern collaboration solutions offer. Authorities that are introducing modern chat solutions testify that users are clearly reducing their use of email. There is currently no agreed standard for how chat solutions in the public sector should be interconnected. Instead, many authorities have used Microsoft Skype for Business, which has brought risks such as lock-in, unwanted dependencies and a reduced ability to digitize their operations.



As Microsoft Skype for Business can no longer be seen as a modern collaboration solution, authorities are faced with evaluating and implementing other digital solutions for collaboration. Authorities, regions and municipalities testify that this has become easier with the work done within eSam through the Digital Collaboration Platform project (dSam part 1 and part 2).

Each agency makes its own assessment based on operational needs, legal assessments, security aspects and supply strategy. This means that agencies end up with different solutions, which in itself is positive, they get solutions tailored to their operational needs, competition increases in the market, which in turn leads to reduced supplier lock-in and more alternatives tailored to the public sector.

At the same time, different solutions also pose a number of challenges. If suppliers choose to continue using proprietary technology to enable external collaboration, it will be more difficult to connect other suppliers' systems. Authorities that have chosen the same solution have the potential to cooperate, but between different solutions there is often a lack of technical capabilities to connect the systems.

As authorities now choose different chat solutions, we see growing fragmentation and risk eventually creating a situation where the public sector is forced to choose one and the same supplier or continue with fragmentation and the risks this entails.

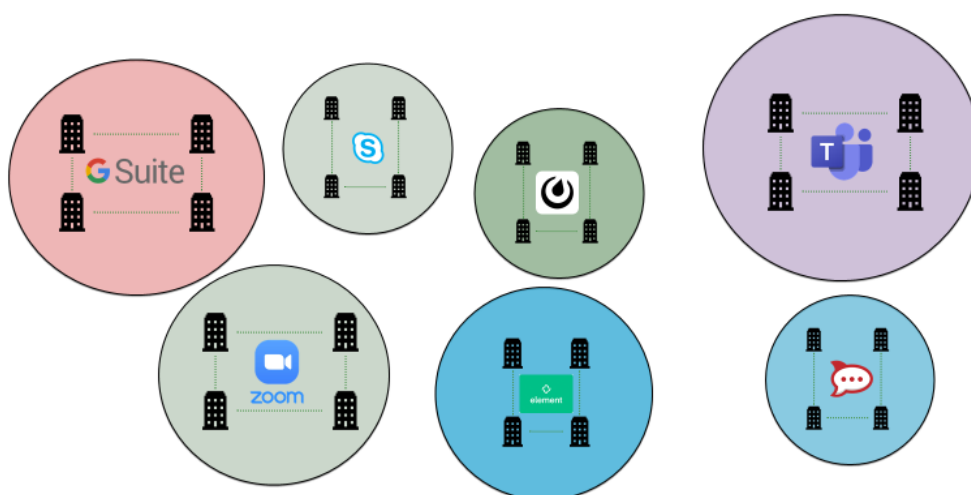


Figure 1- fragmentation increases

Several authorities have implemented or are planning to implement collaboration solutions from public cloud service providers. Several are introducing limitations in functionality or various



safeguards – technical or administrative – when they assess that:

- the legal basis is uncertain,
- digital control is weakened, or
- it is not appropriate to share sensitive information or sensitive personal data with the supplier and thereby establishes complementary solutions for information of higher protection value

Other agencies value offering users a holistic experience and choose tools where they can freely choose the form of delivery and are not affected by legal issues or the uncertain geopolitical situation. At the same time, some agencies are “forced” to establish user accounts for their employees in public cloud services so that they can collaborate effectively in external collaborations.

3.1 History

To create an understanding of the benefits that open federation protocols generate, authorities should look at how email has developed from the beginning to where we are today.

3.1.1 Email – where it all began

The need for decentralized and interoperable communication between different services has, in line with the rise of the Internet, driven the development of federation protocols for chat. The federation of standard protocols for email has its roots in the early development of the Internet. During the 1970s, researchers at ARPANET, the predecessor of the Internet, began experimenting with email systems. Ray Tomlinson introduced the "@" symbol in 1971 to separate usernames and hosts, which became a fundamental part of email addresses. At this time, the Simple Mail Transfer Protocol (SMTP) was also developed, and gradually began to be used to transfer email between different systems and solutions.

The 1980s saw major strides toward standardizing email. SMTP was formalized in 1982 in RFC 821 and established as the primary protocol for sending email. At the same time, protocols such as the Post Office Protocol (POP) and later the Internet Message Access Protocol (IMAP) were developed to enable the retrieval and management of email from servers to clients. These protocols helped make email more accessible and usable to a wider group of users.



In the 1990s, the use of email expanded rapidly and became one of the most popular services on the Internet. IMAP and POP3 were further developed to give users more flexibility in how they managed their email, for example by allowing them to read messages directly on servers instead of downloading them locally. However, the growing popularity of email also led to new challenges, including spam and fraud.

In the 2000s, security issues began to receive more attention. To combat spam and forged senders, security protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC were introduced, making it more difficult for unauthorized people to send email in someone else's name. At this time, federated solutions for email were also being explored through protocols such as XMPP (Extensible Messaging and Presence Protocol), which had previously been used for instant messaging but was now being seen as a possibility for more decentralized email systems.

In the 2010s, interest in privacy and decentralization of email grew. With increased awareness of data protection, it became more important to give users more control over their email servers. Initiatives such as DANE (DNS-based Authentication of Named Entities) were introduced to improve security, while more and more services began to offer end-to-end encryption to protect users' communications.

Email is still built on these basic standard protocols and is one of the most robust federated systems on the internet. Thanks to this open structure/protocol, users on different services and domains can still communicate with each other without being tied to a specific provider. Going back to the fragmentation that email had in the beginning would be completely unthinkable today.

3.1.2 Chat – technical development

Federation protocols for chat have evolved with the rise of the Internet and the need for decentralized, interoperable communication between different services. In the 1990s, the first instant messaging networks began to emerge, often as closed systems where users were limited to a specific service. Popular platforms such as ICQ, AOL Instant Messenger (AIM), MSN Messenger, and Yahoo Messenger dominated the market, but because they lacked compatibility with each other, users were forced to have multiple accounts to communicate with different people.



During the early 2000s, interest in open standards grew, leading to the development of protocols such as XMPP (Extensible Messaging and Presence Protocol). XMPP, originally known as Jabber, was created to enable federated communication between different services and platforms. It offered an open, decentralized model where different XMPP servers could communicate with each other, similar to how email works. Google integrated XMPP into its Google Talk service, which increased the popularity of the protocol, but many commercial players continued to use closed systems.

Despite XMPP's success, federated chat solutions faced challenges in the 2010s. Many major players, including Facebook and Google, chose to abandon XMPP in favor of their own, proprietary solutions that gave them more control over the ecosystem and user data. At the same time, the need for secure and encrypted communication increased, leading to the development of protocols such as the Signal Protocol, which laid the foundation for secure messaging services such as Signal and WhatsApp.

In recent years, federated chat protocols have experienced a renaissance, particularly in open and decentralized networks. The IETF has developed an Internet standard for end-to-end encryption in groups in the form of the MLS protocol and has an ongoing investigation in the form of the MIMI working group to “specify the minimum set of mechanisms required to make modern Internet messaging services interoperable.” The Matrix protocol, launched in the 2010s, has become a popular solution in the public sector for federated communication. Unlike XMPP, Matrix focuses on synchronizing messages across multiple servers, making it more robust for modern use. Matrix has been adopted by organizations and governments that want to control their own communication channels without being dependent on a single provider.

Today, the development of federated chat protocols continues, with issues such as security, privacy, and interoperability becoming increasingly important. While many large players still prefer closed systems, alternative solutions are driven by a strong open source community and by organizations that see the value in decentralized communication.



3.2 Current status

The market for collaboration solutions is dominated by various forms of public centralized cloud services. These solutions are often user-friendly and quick to deliver new and innovative features to their users. Common to these cloud services is that they are often built on proprietary technology, with few incentives to drive interoperability and support for connecting with other vendor solutions. Third-party vendors offer various forms of bridges that connect these solutions, but this does not solve the basic problem and often loses functionality between the systems.

Public sector collaboration tools are currently characterized by a fragmented landscape where different agencies have chosen different technical solutions for instant messaging, video meetings and collaboration spaces. Several agencies are in the process of leaving Skype for Business, while several have not yet decided on a long-term solution. A shift towards public American cloud services can be seen, often in the form of limited implementations or with complementary solutions.

eSam's investigation indicates that only one of eSam's 41 members has chosen US public cloud services as their sole communications solution. Other members who have chosen US public cloud services have chosen to limit functionality or implement other solutions in parallel – often due to legal challenges, information security, and the need for digital sovereignty.

Several authorities are still in the analysis phase and some are awaiting the outcome of how the legal and geopolitical situation affects the decision made by the European Commission in July 2023.³, regarding the adequate level of protection for the transfer of personal data to the USA. Some have chosen to extend the life of Skype by switching to “Skype SE”, which has reduced the immediate need to switch.

A fundamental difference between public central solutions and Skype for Business is how the services are delivered and exposed. While Skype can be operated in government data centers or via private providers, public cloud services are centralized – without the ability to have local control or choose how the service is exposed to the internet.

The authorities' choices are illustrated in Figure 2, the survey was carried out by eSam in April 2025 within the framework of the digital collaboration platform (dSam) project. It summarizes the current situation of authorities, both within eSam and other authorities.

³ [Decision on adequate protection for secure data flows between the EU and the US](#)



Note that many are in a transitional or hybrid state, rather than in a final choice of solution.

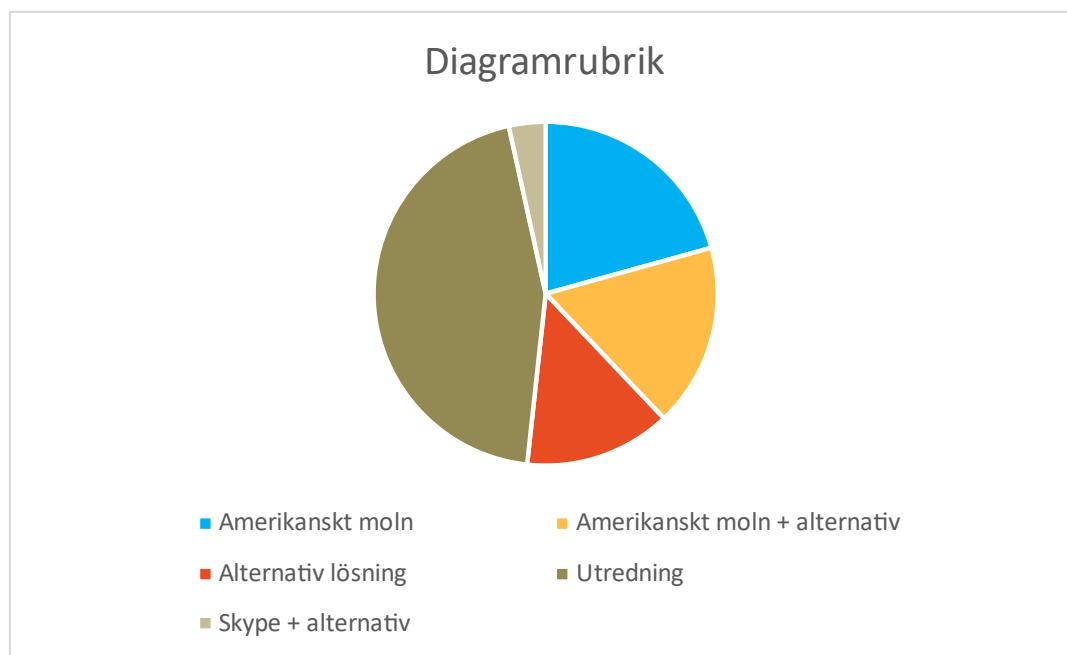


Figure 2. Overview of government agencies' choices and strategies for collaboration tools (April 2025).

The figure shows that several authorities already use different technologies and solutions. This fragmentation underlines the need to start from common protocols rather than common products.

There is a great demand for better digital collaboration within the public sector, but there is currently a lack of a common communication infrastructure that enables secure, standardized and interoperable communication between authorities, which risks reducing the public sector's efficiency, coordination and resilience. Actors such as Sunet, Sambruk, the Internet Foundation and RISE have in other contexts raised the need for national coordination, technical guidance and legal clarity. Key aspects raised are strong identity management, security (E2EE), openness and interoperability.

These issues were also previously raised by eSam within the framework of the Digital Collaboration Platform 2021-2022 project. Guiding principles⁴ such as legality, suitability, federation and standardization were advocated as the cornerstones of a strategic shift in this area.

⁴ [Digital collaboration platform - there are suitable and legal alternatives for the public sector - eSamverka](#)



Interest in open standards for collaboration solutions has increased in recent years, not least within the EU.⁵ In countries like Germany⁶ and France⁷. The uncertain geo- and security-political situation has once again put issues such as authority and digital sovereignty on the agenda within a number of different organisations within the EU, both in the public and private sectors. It is no longer a “GDPR issue”, but authorities are weighing up more perspectives in their strategic choices. The need for national coordination in Sweden has also been raised by DIGG, they write in the report “A society in change (2024)”⁸ that –

"The single most important trend-breaking measure in the digitalization policy area is increased coordination, something that can be achieved through a greater element of the right kind of governance."

Suppliers with existing products and solutions that have begun to implement and analyze open protocols report a fear of being “last in the ball” compared to other suppliers that have implemented open protocols from the start. They also see complexity and increased costs in adapting their product to work with open protocols.

4. Environment

At the EU policy level, the issue of interoperability is addressed through various forms of regulations or acts. In recent years, the EU has intensified its efforts to regulate the digital sphere, with a clear focus on promoting competition, protecting fundamental rights and ensuring a fair internal market. Several key pieces of legislation, notably the Digital Markets Regulation (DMA), the Digital Services Regulation (DSA), the General Data Protection Regulation (GDPR) and the ePrivacy Directive, together form a complex but increasingly clear framework that directly and indirectly influences the choice of chat protocols.

At the heart of the EU’s approach, particularly through the DMA, is the requirement for interoperability of major consumer messaging services designated as “gatekeepers” (e.g. WhatsApp and Messenger). This forces previously closed ecosystems to open up, creating a potential space for open protocols to offer standardised and transparent solutions. While the DMA does not explicitly mandate the use of specific open protocols, its requirements for fair, reasonable and non-discriminatory (FRAND) access

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

⁶ [About us | openDesk](#)

⁷ [The Digital Suite](#)

⁸ [A society in change – basis for the government's strategic priorities | Digg](#)



and the preservation of security, including end-to-end encryption (E2EE), point in the direction of solutions that are robust and well-defined.

Other directives such as the NIS2 Directive (Network and Information Systems Directive 2), the Cyber Resilience Act (CRA) also point out in various ways the importance of interoperability and secure and open communication protocols. See “Appendix_A_Environmental Monitoring” for more information.

A Swedish bill "A reform for data sharing" (SOU 2023:96)⁹, aimed to analyze the existing governance and regulation of interoperability in data sharing within public administration. The aim is to increase the ability to share data efficiently and securely in order to streamline public operations and services to citizens and businesses. It highlights, just like this report, a form of fragmentation and the lack of a national strategy for interoperability. The government's ambition is to be able to submit a bill on the bill to the Riksdag in the autumn of 2025 with hopes of new legislation in 2026.

It is important to note that ‘openness’ in the context of chat protocols is multifaceted. While open source is an important aspect for transparency and joint development, it is likely that the EU’s primary interest lies in ‘open standards’. Such standards are crucial to ensure true interoperability between different services and to prevent lock-in effects by dominant providers, which is a core principle of the EU’s drive to promote competition. This focus on standardised interfaces is likely to be the main driver behind EU countries’ possible preference for ‘open’ communication solutions, although open source and open standards often go hand in hand.

4.1.1 Alternative solutions to public central soil services

In addition to the popular public cloud services from Microsoft, Google, Zoom, Slack, etc., there are a number of collaboration solutions on the market, which enable your own choice of delivery method, decentralization and your own data control. Organizations can purchase support and also gain access to enterprise-specific features such as support for multi-factor authentication, antivirus integrations, managing large-scale IT operations, multi-customer support, custom apps, etc.

The working group has not focused on external analysis of ready-made collaboration solutions, but on open protocols. In light of this, the list of suppliers below should be seen as an example and not as a recommendation or “net list” of suppliers. The market

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



is considerably more diverse. Below are some examples of clients and services offered on the market with different forms of chat capabilities.

Element¹⁰ - Element is a popular client and also offers hosting services (Element Services) where you can choose a hosting region (including EU) and your own IT operations (on-premise).

Mattermost¹¹ - Often described as an alternative to Slack/Teams. Can be installed on your own servers (on-premise) or in any cloud (including European providers).

Nextcloud Talk¹² - Included as an app in a Nextcloud platform solution along with other functions such as document management, digital whiteboard, kanban, etc. Can be self-hosted or as a service with several cloud service providers.

Rocket.Chat¹³ - Offers flexibility with self-hosting or via cloud services from partners in Sweden and other countries within the EU.

AWS Wickr¹⁴ - E2EE based chat solution that is offered both as a SaaS service but can also be set up for your own IT operations on Kubernetes.

Other more niche solutions such as SimpleX, Delta chat and Session are also options chosen by some organizations.

4.1.2 International examples of the application of open protocols

Developments within some EU countries show a clear trend towards open standards and solutions that reduce dependency on individual suppliers. Several countries have already implemented national or sector-specific communication platforms based on the open federation protocol Matrix.

The French government uses a service based on the Matrix protocol, called Tchap, for communication between public officials. The service currently has over 400,000 users and targets large parts of the French public administration. The project is run by the Direction interministérielle du Numérique (DINUM) with a focus on security and digital sovereignty.¹⁵

The European Commission plans to replace third-party apps like Signal with apps based on the open Matrix protocol by 2026. The goal is to create a secure, government communications platform that owns the data and can offer complements to Microsoft Teams.

¹⁰ [Digital collaboration platform - there are suitable and legal alternatives for the public sector - eSamverka](#)

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

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

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

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

¹⁵ [Tchap - the instant messenger of agents of the public function](#)



Luxchat is a messaging service for the general public and businesses, while Luxchat4Gov is intended for the public sector in Luxembourg. Both services are interoperable and offer secure, encrypted communication without advertising or use of personal data. They are delivered as a service in data centers located in Luxembourg.¹⁶

Germany has a clear strategy to apply open protocol (Matrix) in the public sector in several areas. This includes, among other things:

- BwMessenger: A version of Element used by the entire German Armed Forces as a secure alternative to commercial messaging apps¹⁷
- TI-Messenger: A Matrix-based system that has been made mandatory by Gematik for secure communication in the German healthcare sector, involving over 150,000 organizations¹⁸
- openDesk: The Federal Ministry of the Interior (BMI) and ZenDiS have chosen Matrix and Element as the communication layer for the open and sovereign workplace platform openDesk¹⁹
- Universities: Many universities in Germany and Austria use Matrix as their primary communication platform
- Schools: Several German states have introduced Matrix for secure communication in online education
- Police (P20 Program): A subgroup within the police has recommended the use of Matrix as a unified messaging protocol
- FITKO (Federal IT Cooperation): Together with the German Ministry of the Interior, FITKO has initiated a pilot project to develop a modern communication platform based on Matrix²⁰

ELGA (Elektronische Gesundheitsakte) is Austria's national electronic health record system, designed to improve information exchange in healthcare. It enables healthcare professionals to quickly and securely access patients' medical data, leading to better coordination and quality of care. ELGA plans to implement the Matrix protocol as a basis, similar to Gematik, for exchanging sensitive data between different partners including citizens.

Another example is ActivityPub, an open, decentralized social networking protocol, best known as the technology behind the "Fediverse" (a collection of interconnected social platforms such as Mastodon, PeerTube, Lemmy, etc.). There has been a recent shift

¹⁶ [Luxchat – The instant messaging solution of Luxembourg!](#)

¹⁷ [Bw Messenger | Secure. Flexible. Open Source.](#)

¹⁸ [TI-Messenger | gematics](#)

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

²⁰ [FITKO](#)



away from the X platform (formerly Twitter) towards other alternatives given the organizational and principle changes that have occurred since Twitter was acquired. Some EU bodies and officials have started to explore and use platforms based on ActivityPub. For example, the European Data Protection Supervisor (EDPS) launched the EU Voice initiative, which is a dedicated Mastodon instance (Mastodon uses ActivityPub), to give EU institutions a presence in the Fediverse.

Other protocols such as XMPP and SIP are common open protocols in the public sector, where the latter is primarily intended for voice and video and presence management. An example of XMPP's use is Cisco Webex, a chat solution that uses XMPP for chat with support for federation. There are a number of public XMPP servers in EU countries such as Germany, the Netherlands, France, Austria, the Czech Republic, Poland, Latvia and Finland.

In parallel, work is underway within the Internet Engineering Task Force (IETF) on two different forms of protocols, Message Layer Security (MLS) and More Instant Messaging Interoperability (MIMI). These two in combination have the potential to become standard protocols for interoperability for chat solutions, but it is too early to judge given that the MIMI working group has not yet presented a proposal. The work has been fraught with conflicts of interest and complex issues, which in itself is a natural part of the process of arriving at a common open standard.

5. Desired new location

There are several possible strategies for how the public sector can organize its communications infrastructure going forward. The SWOT analysis in Appendix C describes six options in detail.

The most prominent options are:

- To continue as today, with different tools and without joint coordination.
- To introduce a central bridge solution that temporarily connects existing systems.
- To introduce a common federated and open protocol, with decentralized operation and standardized interoperability.

Other options include introducing a central government chat solution, forming sectoral clusters around current tools. All authorities agreeing on a common commercial service/product is not considered a realistic option as authorities make different



assessments and are guided by different requirements and needs. The presented options have different degrees of complexity, lock-in effect, cost and adaptability.

The working group's assessment is that the choice of an open federated solution provides long-term sustainability, opportunities for innovation and control in line with the EU's strategic goals. However, the assessment is that we may need interim solutions in the short term to reach the desired new situation and that authorities should be able to make their own assessments regarding solutions for, for example, internal cooperation.

5.1 Principles for the future

As part of the work, the working group has developed a proposal for principles for an open federation protocol for chat. The principles should not be seen as a complete list of requirements, but rather as examples of how work to harmonize the choice of chat solutions can work in the future.

The basis for the principles is that they should support interoperability, not be tied to a supplier, have full transparency and support authorities' requirements for robustness and crisis and emergency planning within total defense and Swedish sovereignty.

For a protocol to be "open" in this context means more than just access to the source code. The European Committee for Interoperable Systems (ECIS) has formulated principles for open standards that illustrate this. These principles include:

- A collaborative and democratic development and management process.
- A transparent development and management process open to all interested parties.
- Approval through a due process with consensus among the participants.
- That correct implementations of the standard must be interoperable.
- That they are platform-independent, vendor-neutral and usable by an unlimited number of competing implementations.
- That they are openly published, including specifications and documentation.
- That they are available royalty-free or at minimal cost, with the only licensing restrictions being reciprocity and defensive shutdown.

This principle-based view would result in authorities avoiding shaping their collaboration around individual solutions, and instead coming together around a technical and organizational foundation that enables freedom of choice and competitive advantages.



The "open" aspect of a protocol is not just a technical detail; it is a fundamental guarantee of long-term availability, adaptability and control, which is of particular importance for the public sector. When a protocol is proprietary, it means that a single commercial actor owns and controls its specification and future development. This gives the provider a significant position of power to dictate terms, pricing and technical direction, which can lead to a strong dependency on the organizations that use the protocol.

Open protocols, with their freely available specifications and transparent development processes, limit this exclusive control by a single actor. For the public sector, which has a pronounced long-term responsibility and a need for stability, predictability and responsible use of tax funds, this means that the risk of sudden and disadvantageous license changes, cessation of support for older versions, or forced and costly upgrades is significantly reduced. The choice of an open protocol can therefore be seen as a strategic risk minimization measure and an active investment in securing and maintaining digital autonomy.

The proposed principles are based on a balance between technical neutrality and operational discretion. They should support the design of solutions that take into account both operational needs, legality and security. By starting from a common protocol, the public sector can maintain freedom of choice between clients, operating modes and suppliers – without sacrificing interoperability.

However, a common open chat protocol does not automatically mean digital sovereignty and increased control. When public actors choose external operating providers for inter-agency cooperation where, for example, ownership/operation takes place in a third country or is dependent on legislation outside the EU, control can be undermined.²¹

The working group's developed examples of principles for open federation protocol for chat are exemplified in Appendix E, Principles_for_federated_communication

5.2 Economic impact

It is easy to think that it would be most economically beneficial if authorities invested in the same solution and maximized their use of already implemented investments. However, the working group's assessment is that standardizing the authorities'

²¹It is important to distinguish between, for example, the Matrix protocol and clients such as Element. The report's recommendations are based on the properties of the protocol – not on specific implementations or vendors.



conditions for cooperation on a few proprietary solutions risks having negative economic effects in the long term for the public sector.

For the public sector to successfully leverage the economic and strategic benefits that open protocols for chat federation offer, a number of conscious strategic considerations and proactive action are required. It is not just a technical choice, but a direction that affects procurement, skills, collaboration and policy development.

- Prioritize open standards and protocols
- Invest in building skills around open technologies and federated systems
- Promote and participate in national and international collaborations on development and standardization
- Conduct thorough TCO analyses that include long-term strategic costs and benefits
- Develop clear guidelines and policies for the use of federated chat services

Successful transition to and effective use of open federation protocols in the public sector requires more than just appropriate technical choices. It requires a clear strategic direction from management, a readiness for organizational adaptation, and an active, long-term commitment to the ecosystem surrounding open technology. Simply “choosing” an open protocol is not enough if the organization is not equipped to manage and fully leverage the opportunities that follow.

Proprietary federation protocols are often delivered as part of a comprehensive solution with extensive support from a single supplier, which may appear simpler and less resource-intensive in the short term. Open protocols, on the other hand, may require more internal knowledge and commitment for implementation, adaptation, integration and governance. Therefore, investing in open protocols must be seen as a strategic investment in the digital capacity and maturity of your own organization. This requires leadership commitment, resource allocation for skills development and a willingness to change established working methods and procurement models.

However, chat-based federation brings with it complexity in the form of operating and securing the federation network, such as chains of trust - who trusts whom and how malicious code is prevented from spreading between authorities needs to be managed with clear models.

Beyond the direct economic aspects, open protocols for chat federation bring a number of benefits. Improved interoperability is central to enabling a truly cohesive public sector



where information can flow and collaboration can occur smoothly across organizational boundaries. Openness acts as a catalyst for innovation and adaptability, allowing the public sector to develop and tailor solutions that are optimized for its unique needs. The transparency and auditability of open systems strengthen information security and build trust, while the decentralized and federated nature contributes to increased resilience and business continuity. Perhaps most importantly, the choice of open protocols for collaboration is a concrete step towards securing digital sovereignty, giving the public sector greater control over its critical communication infrastructure and reducing dependence on individual, often external, actors.

However, these benefits are not without their trade-offs. Realizing the full economic potential of open federated solutions requires a purposeful approach and a different type of investment than that required for proprietary solutions. Instead of primarily paying license fees, the organization must invest in other solutions – either by building its own technical capabilities for its own operations or by purchasing managed services and support agreements.

5.3 *Legal and information security*

Federation of chat-based solutions between Swedish authorities is a complex process that involves several important legal aspects. Data of different nature and information class will be shared between authorities.

When personal data is processed in the federated chat solution, it must be clearly established which authority is the data controller for each processing. All processing of personal data must have a lawful basis according to the GDPR. Personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes. This is particularly important in federation where information may be shared between different authorities with different mandates. Only the personal data that is necessary for the purpose may be processed. Personal data may not be stored for longer than necessary. Routines for culling and erasure are important and that appropriate technical and organizational measures must be taken to protect the personal data. This includes encryption, access controls and logging.

If the processing is likely to result in a high risk to the rights and freedoms of individuals, an impact assessment must be carried out by the respective authority.



When a chat message becomes a public document is not always obvious - generally speaking, when it has been received by the authority or created there and is stored with the authority. How are chat messages that are of a more temporary nature and not necessarily to be preserved as public documents handled? Clear guidelines are required for all authorities.

Depending on the assessment of the authorities, information exchanged via the chat solution may constitute public documents. This means that they can be requested by the public. The authorities must have procedures for handling such requests, including being able to search and compile information from chat logs. Before a document is released, a confidentiality assessment must be carried out to assess whether any information is subject to confidentiality under the OSL. This can be complicated when information is shared between authorities with different confidentiality provisions.

Even if the information is classified, it can in some cases be disclosed to other authorities if there is legal support for it (so-called confidentiality-breaking provisions). This must be assessed in each individual case.

Authorities also have obligations regarding the registration and record-keeping of public documents and when they may be discarded (deleted). This must be done in accordance with applicable discard regulations. The information must be able to be preserved and readable over time, even if technology changes. This must be taken into account for information that is created and shared in the chat solution.

If information is temporarily stored (e.g. on servers of a service provider or in a shared infrastructure), authorities must ensure that the storage meets all relevant requirements (security protection, GDPR, OSL). The physical location of the servers may be important, especially if they are outside the EU/EEA (which may entail additional requirements under GDPR).

Authorities need to map out who has access to the temporarily stored information and under what conditions.

Federation of chat-based solutions is a complex legal and technical challenge. A thorough review of all these aspects, and the involvement of legal expertise in each area, is necessary to ensure a legal and secure implementation. It is important to see this as a whole where the different legislations interact and impose requirements on processes, technology and organization.



These legal issues need to be investigated regardless of which path authorities choose to collaborate between chat-based solutions.

6. Decision

Based on the analysis carried out, the working group proposes that the steering group decides that work on an open federation protocol should continue in the fall of 2025 and that authorities allocate financial resources and expertise for continued anchoring and development.

This includes appointing a coordinating actor with responsibility for governance, support and follow-up. Identified synergies with the bill regarding "A reform for data sharing" (SOU 2023:96)²² needs to be analyzed and acted upon. In addition, authorities need to work to integrate the work with other digitalization initiatives in Sweden and the EU.

Against this background, the working group proposes that eSam establish a collaboration to eventually establish a common, open federation protocol for persistent chat and messaging services in the public sector. The solution should be based on open standards, be vendor-independent, and support decentralized operation.

The advantages of this choice of path are:

- Better collaboration between authorities, regions and municipalities
- Better conditions for offering secure citizen services
- Better control over data, operations, security and the ability to collaborate across the full threat spectrum
- Reduced lock-in to individual suppliers
- The investment that will have an impact on surrounding areas
- Opportunity for innovation and European leadership

The working group recommends that the steering group decide on the following next steps:

- Prioritizes continued work on federated chat as a strategic goal for eSam
- Secures funding and capacity from autumn 2025
- Decides on the division of responsibilities and governance model
- Enshrines the principles proposed in Annex E
- The continued work will include the establishment of a governance framework, including a model for a joint federation.
- Involve DIGG's work in authorization and identity management to establish synergies between identity and chat federation solutions
- Uses the timeline in Appendix D as a roadmap for implementation

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

7. Final words

Several European countries have already started to implement federated chat solutions based on open protocols such as Matrix. Sweden risks falling behind – both in terms of technical development and the possibility of collaboration within and outside the country's borders.

The positive thing is that there is a realistic path forward – but it requires long-term thinking, determination, resources and a common direction.

Embracing open protocols for federated communication is not just a technical upgrade. It represents a cultural and strategic shift for the public sector – a movement towards greater autonomy, improved collaboration, and a more sustainable and responsible digitalization in the long term. Upcoming Swedish legislation can act as a catalyst for this shift.

The path forward requires conscious decisions, investments in skills and active engagement, but the potential gains in the form of more efficient, secure, innovative and superior digital communication make it a strategically important and economically advantageous direction for the Swedish public sector in the digital age. This is a journey that fundamentally strengthens the public sector's own digital maturity and its ability to navigate an increasingly complex digital landscape, which is crucial for the welfare and public services of the future.

The purpose of the eCollaboration programme (eSam) is to facilitate the digitalization of public administration through voluntary collaboration between authorities. Our members want to seize the opportunities of digitalization

All publications are available at esamverka.se

The eCollaboration programme includes the Swedish Public Employment Service, the Swedish Work Environment Authority, the Swedish Companies Registration Office, the Swedish National Board of Housing, Building and Planning, the Swedish Central Student Support Board, the National Courts Administration, the e-Health Authority, the Swedish Public Health Authority, the Swedish Social Insurance Agency, the Swedish Marine and Water Authority, the Health and Care Inspectorate, the Swedish Board of Agriculture, the Swedish Chemicals Inspectorate, the Swedish Coast Guard, the National Land Survey, the Swedish National Food Administration, the County Administrative Boards, the Swedish Migration Board, the Swedish Environmental Protection Agency, the Swedish Pensions Authority, the Swedish National Heritage Board, the National Archives, the Swedish National Board of Forensic Medicine, Sida, The Swedish Medical Products Agency, the Swedish Tax Agency, the National Agency for Education, the State Institution Board, the State Service Center, the State Occupational Pensions Board, the State Veterinary Institute, Statistics Sweden, the Swedish Agency for Economic and Social Growth, The Swedish Agency for Public Management, the Swedish Transport Administration, the Swedish Transport Agency, the Swedish Customs Agency, the Swedish Council for Higher Education and the Payments Authority. (Jan 2026.)

