

Abridged report

Common federation protocol for public sector chat

ES-2025-23





Content

1.	Introduction.....	4
2.	Background and current situation.....	4
3.	Mission.....	6
4.	Summary of the analysis.....	6
4.1	EU legal context.....	8
4.2	International examples show the way.....	8
4.3	Recommendations.....	9
4.4	Guiding principles for an open federation protocol.....	9
5.	Summary of alternative paths forward.....	9



1. Introduction

The Swedish public sector needs a robust, open and interoperable communications infrastructure. A common federation protocol for chat lays the foundation for efficient, secure and vendor-independent collaboration. With clear principles, structured governance and targeted investments, Sweden can take a strategic and long-term sustainable step towards increased digital sovereignty and better service to citizens and businesses.

This report is an abbreviated and accessible version of "Common Federation Protocol for Chat in the Public Sector". The purpose is to highlight the need for and the possibility of a common communication infrastructure in the Swedish public sector. The report is based on the work within eSam's Digital Collaboration Platform (dSam4) project and includes insights from associated appendices.

The analysis shows that there is a strong need and broad support for a common, open solution for federated communication in the public sector. Fragmentation and vendor lock-in are clear risks today.

An open protocol-based model can provide:

- better conditions for cooperation
- increased security and control
- reduced lock-in
- greater innovation capacity and flexibility

Recommendations:

- Prioritize open standards in procurement.
- Invest in expertise around federated systems.
- Participate in standardization and exchange of experiences.
- Conduct TCO analyses that weigh strategic benefits and risks.
- Establish policies and guidelines for federated chat services.

2. Background and current situation

Agencies are phasing out Skype for Business without a mutually agreed replacement. Some are choosing public cloud services (e.g. Microsoft Teams, Google Meet), often with restrictions on sensitive information; others are exploring proprietary or hybrid



solutions. The result is a fragmented landscape that makes collaboration across agency boundaries more difficult.

In parallel, the EU is tightening the requirements for interoperability, security and transparency (including NIS2, Data Act, Interoperable Europe Act and DMA). Nationally, SOU 2023:96 A reform for data sharing shows the need for a comprehensive strategy for digital communications infrastructure.

Email is increasingly being replaced by persistent chats, file sharing and video. The lack of common standards for collaboration between government chat solutions increases the risk of lock-in and reduces digital sovereignty. eSam members point to a great need for group chat as part of a modern way of working, but there is no agreed standard for interconnection.

Public, centralized cloud services dominate the market and deliver fast functionality, but are often proprietary with weak incentives for interoperability. Third-party bridges can temporarily link systems but often result in loss of functionality and do not address the underlying problem.

The public sector will continue to be dependent on large, often international, suppliers, at least for parts of its digital communication. This means that lock-in effects and lack of control over data may persist in the long term. This feasibility study does not aim to replace existing solutions, but to complement them with alternative, open and federated communication channels.

A common federation protocol could therefore be used in parallel with other tools. In this way, we gradually reduce dependence on individual suppliers, increase the robustness of communication and improve digital interoperability. It is not about choosing either or, but about creating more paths to secure and controlled collaboration.

The need for better digital collaboration is great, but a common infrastructure that enables secure, standardized and interoperable communication is missing. Actors such as Sunet, Sambruk, the Internet Foundation and RISE are calling for national coordination, technical guidance and legal clarity. Strong identity management, end-to-end encryption (E2EE), openness and interoperability are central. DIGG (2024) emphasizes that increased coordination is likely to be the most important trend-breaking measure in digitalization policy.



3. Mission

The report was produced within the Digital Collaboration Platforms (dSam) project on behalf of the eSam steering group. The assignment is to analyze the conditions, alternatives and consequences of introducing a common federation protocol for chat within the public sector. The goal is to enable secure, interoperable and vendor-independent collaboration across authority boundaries.

4. Summary of the analysis

Today's public sector communications landscape is characterized by a large number of different tools and platforms. This proliferation makes it difficult to collaborate across agency boundaries and increases dependence on a few global players. It negatively affects digital sovereignty and creates uncertainty around legal issues and the handling of sensitive information.

The public sector is therefore faced with a strategic choice:

- to continue on a fragmented path where different authorities create their own solutions, or
- to agree on a common, open and interoperable communications infrastructure.

The choice of communication protocol is therefore not only a technical issue, but one that affects efficiency, security and long-term economic sustainability. In order to be able to collaborate effectively, a common model with clear principles for how communication should be organized is required.

At the same time, both total defense and new EU regulations place higher demands on robustness, security and collaboration. Nationally, the investigation SOU 2023:96 A reform for data sharing emphasizes that the Swedish public sector is lagging behind in interoperability and data sharing. A common protocol for chat solutions is seen as a concrete step in the right direction.

Technically, open APIs, public code bases, and standardized protocols enable governments to develop, adapt, and further develop digital infrastructure themselves. This strengthens internal expertise, reduces dependence on external suppliers, and shortens development times.



However, for such a development to become a reality, conscious efforts are required in knowledge sharing and collaboration – for example, common code repositories, test environments and competence development across agency boundaries. Experience from initiatives such as the British Government Digital Service and similar efforts in the Baltics show that competence is crucial for long-term success.

If the public sector does not take active ownership of its communications capabilities, there is a risk that the sector will standardize around a few commercial solutions. This leads to lock-in effects – where authorities are forced to adapt to the suppliers' terms rather than their own needs. Skype for Business is a previous example of this.

The reference bodies that the working group has been in contact with agree that the public sector needs to strengthen its control and authority over digital collaboration:

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

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

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

MSB: "A decentralized chat infrastructure, based on open standards and federated solutions, can reduce dependence on individual vendors and central cloud services."

Government Offices: "The initiative has clear synergies with new legislative proposals in the areas of interoperability and data sharing."

The working group has not evaluated or taken a position on individual products or services. Instead, the focus is on a common protocol for communication across agency boundaries – a lowest common denominator that enables robust, efficient and vendor-independent collaboration.

The technical analysis points out in particular that open protocols, such as Matrix, offer good conditions for secure and interoperable communication. The feasibility study can conclude that such a solution provides long-term sustainability, but that it also requires investments in governance, operations and skills development.

Interoperability has received increased political attention within the EU in recent years. Several key pieces of legislation regulate the digital market and directly affect which technical solutions are possible to use in the public sector.



4.1 **EU legal context**

Together, these rules create a clear framework that influences the choice of communication protocols within the public sector:

- *DMA* (Digital Markets Act) imposes interoperability requirements on those actors classified as digital “gatekeepers”. It opens up previously closed ecosystems and creates the possibility of using open protocols while maintaining security (including end-to-end encryption) and fair terms (FRAND).
- *NIS2 Directive* and the Cyber Resilience Act focuses on robust, secure and interoperable solutions.
- *GDPR* and the ePrivacy Directive requires the correct handling of personal data and communication confidentiality.

4.2 **International examples show the way**

Several countries have already introduced federated and open solutions in the public sector. These initiatives show that it is possible to implement secure and robust chat infrastructure at a national level – even in complex public environments.

- **France:** Tchap, a Matrix-based chat service with over 400,000 users.
- **Luxembourg:** Luxchat and Luxchat4Gov – interoperable and encrypted solutions for the public sector.
- **Germany:** Uses Matrix in several sectors, including the Bundeswehr (BwMessenger), healthcare (TI Messenger) and as a communication layer in openDesk.
- **EU Commission:** Will test an open chat solution (using Matrix as a protocol) to eventually replace private chat solutions for the member countries

From a legal perspective, the importance of clear responsibility for personal data, handling of public documents and information security is highlighted. Identity management, storage and regulatory compliance are also key aspects.

Economically, an open solution is not necessarily considered the cheapest in the short term, but the strategic cost remains lower in the long term thanks to increased control, reduced lock-in, and improved collaboration capabilities.

Open protocols may require greater initial capacity (implementation, integration, governance/procurement), but strengthen innovation capacity and reduce long-term lock-in effects.



4.3 Recommendations

- Prioritize open standards in procurement.
- Invest in expertise around federated systems.
- Participate in standardization and exchange of experiences.
- Conduct TCO analyses that weigh strategic benefits and risks.
- Establish policies and guidelines for federated chat services.

4.4 Guiding principles for an open federation protocol

- Interoperability and vendor independence
- A transparent and inclusive standardization process
- Specifications that are openly published and royalty-free (or close to zero)
- Robustness, including end-to-end encryption (E2EE) and disaster recovery support
- Digital sovereignty: control over data, operations and jurisdiction

It is important to note that an open protocol does not automatically imply sovereignty. If the operation takes place outside the EU/EEA or under foreign legislation, control over the information may be negatively affected.

5. Summary of alternative paths forward

The analysis identifies six possible paths for how the public sector can organize its digital chat communication:

- 1) **Continue as today** means that each agency chooses its own solution without coordination. This risks hindering cooperation, increasing costs and creating technical dependence on specific suppliers. This path means that today's challenges remain – or worsen.
- 2) **Central brewing solution** means that some party takes responsibility for giving authorities the ability to connect their chat tools to a national integration hub. As long as these authorities' chat tools meet the specification, they will be able to connect. The bridging solution will, if it is to work, be forced to support a variety of different protocols and products.

- 3) **Joint open protocol** means that the public sector agrees on a common, federated and open protocol. It enables decentralized operation and ensures interoperability between authorities.
- 4) **Establish a central chat solution** means that one party is assigned to make available "a Swedish government chat" which will be the only channel through which authorities and their employees can/should communicate with each other. This option could be an interim solution while waiting for option 3 to be established.
- 5) **Form clusters for collaborations** means that authorities in groups of two, three or more create their own federated chat clusters where these authorities can communicate.
- 6) **Authorities choose the same proprietary solution.** This means that authorities are putting the issue of authority aside and all choose to let one solution handle all communication via their platforms. This comes at the expense of control and adaptation.

Option number three, is considered the most sustainable and strategically advantageous. However, it requires careful preparation, political and organizational support, and joint governance. During implementation, interim solutions may need to be used in parallel to maintain cooperation.

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.)

