



## Appendix A – External monitoring

There are several initiatives underway within the EU related to open federation protocols, with Germany and France at the forefront. In addition, several pieces of legislation have been passed in recent years, all of which point to interoperability, open source and open standards.

Below is a summary of identified areas relevant to the report.

### Summary

EU regulations affect and will affect how we act strategically. Germany and France are actively working on issues such as open protocols.

"A reform for data sharing" (SOU 2023:96) clearly shows that there is a drive and a will within the public sector to improve interoperability capabilities. A law may come into force in 2026.

There is great demand from municipalities, authorities and universities for a common path forward linked to the opportunity to collaborate more effectively and seamlessly.

Identity, security, transparency and interoperability must be the cornerstones of a future solution. Open protocols are seen as a prerequisite for achieving digital sovereignty and reducing vendor dependency.

Several actors are calling for national coordination, clear principles and test environments.

To achieve real change, the public sector in the EU needs to act together, drive technology development themselves and not just wait for suppliers' initiatives or political decisions.

### EU regulations – increased requirements for interoperability and transparency

The European Union has adopted several major pieces of legislation in recent years that affect how digital infrastructure is built and governed, particularly in the public sector.



These regulations strengthen the case for using open, interoperable and auditable technical solutions, such as open federation protocols.

### ***Interoperable Europe Act<sup>1</sup>***

This regulation was adopted in April 2024 and is an important step towards harmonising digital public services across the EU. It requires public digital systems to be able to interoperate across national borders – both technically and organisationally. The aim of the act is to reduce duplication, save costs and improve the quality of public services across the Union.

The public sector is expected to choose solutions that support open federation, to ensure interoperability between countries and authorities. The application of open-source code and standards is a requirement that is raised by both the EU's Interoperable Europe Act. The act wants to promote interoperability, but aspects such as chat federation are not explicitly mentioned in the Interoperable Europe Act.

### ***Data Governance Act (DGA)<sup>2</sup>***

The DGA aims to facilitate the sharing of data between public and private actors, in a secure and reliable manner. It provides guidelines for how data should be made available, while preserving the protection of sensitive information.

Public communication services must be able to handle data sharing according to these principles – something that is benefitted by standardized and open protocols.

### ***Digital Services Regulation (DSA)<sup>3</sup>***

The Digital Services Regulation (DSA), Regulation(EU)2022/2065, is another key part of the EU's digital regulatory framework. It aims to create a safer and more transparent online environment by setting obligations for digital service providers acting as intermediaries, including hosting services and online platforms. Many messaging services may fall under these categories, especially if they offer features beyond pure peer-to-peer communication.

### ***Digital Markets Act (DMA)<sup>4</sup>***

The EU DMA, in particular Article 7, introduces a mandate for designated “gatekeepers”

---

<sup>1</sup> Interoperable Europe Act | Interoperable Europe Portal

<sup>2</sup> European Data Governance Act | Shaping Europe's digital future

<sup>3</sup> The EU's Digital Services Act

<sup>4</sup> European Data Governance Act | Shaping Europe's digital future



– large digital platforms such as Meta (with WhatsApp and Messenger) – to make their messaging services interoperable with third-party services. This regulatory framework aims to increase competition and choice in the digital market.

DMA reinforces the need for federated communications solutions, as they help break lock-in and create competition.

### ***AI Act***<sup>5</sup>

The AI Regulation is the first of its kind in the world and requires transparency, traceability and control in the use of AI systems. For high-risk applications, documentation, human oversight and security are required.

If AI is used in conjunction with messaging platforms, for example for automated response management or analysis, the infrastructure must be transparent and controllable – which speaks in favor of solutions where the public sector itself controls the technology.

### ***NIS2 Directive (Network and Information Systems Directive 2)***

This directive aims to strengthen cybersecurity within the EU by setting a high common level of security for network and information systems in key and significant sectors. The directive specifically mentions "the use of cryptography and, where appropriate, encryption as a risk management measure. This directly encourages the use of E2EE solutions for secure communications in these sectors. The NIS2 directive also states that end-to-end encryption should be used to protect public electronic communications networks and services."<sup>6</sup>

### ***Cyber Resilience Act (CRA)***<sup>7</sup>

This act focuses on cybersecurity requirements for products with digital elements. It emphasizes the need for products to be delivered without known exploitable vulnerabilities and with secure default configurations, including the use of encryption.

### ***Digital sovereignty – permeates several legal acts***

Digital sovereignty is fundamentally about the ability to exercise control over one's digital environment – including infrastructure, data and the rules that govern them.

---

<sup>5</sup> AI Act | Shaping Europe's digital future

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

<sup>7</sup> Cyber Resilience Act | Shaping Europe's digital future



Digital resilience refers to the ability of systems, organisations and society at large to withstand, adapt to and recover from digital disruptions, such as cyberattacks or technological failures.

A significant acceleration in the number of regulations has been observed in recent years, driven by technological developments, increasing threat perceptions and a political will to strengthen the EU's so-called "strategic autonomy". Key pieces of legislation such as the NIS2 Directive, the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Act, the Data Governance Act (DGA) and the proposed Cyber Resilience Act (CRA) have either recently entered into force, are under implementation or have been presented within a relatively short period of time. This rapid emergence of new legislation creates a complex and dynamic regulatory landscape that can be challenging for businesses to navigate and adapt to.

The EU Commission has developed a framework to support member states in evaluating provider solutions and their potential to offer digitally sovereign features. This support also creates a clear definition of what features a service should have to be called digitally sovereign.<sup>8</sup>

The EU legal framework, led by the Digital Markets Regulation (DMA), is reshaping the playing field for digital communications services. While no EU legal act explicitly mandates the use of specific open chat protocols, the overall effect of the legislation clearly points in a direction that advocates transparency, interoperability and user control. The DMA's requirement for interoperability of gatekeeper messaging services is the most direct driver, but its implementation must be in harmony with the fundamental data protection principles of the GDPR and the ePrivacy Directive, as well as the EU's overall policy of promoting open standards.

The EU's existing and upcoming legislation creates conditions and incentives where open chat protocols appear as a strong and logical solution to meet the multifaceted demands for interoperability, security, privacy and transparency. It is less about a direct mandate and more about shaping a market where open, standardized and user-centric solutions have a better chance to compete and thrive.

## **Swedish bill – increasing interoperability for the public sector**

"A reform for data sharing" (SOU 2023:96)<sup>9</sup>, is a report by the Inquiry on Interoperability in Data Sharing. The Inquiry was appointed to analyze the existing

---

<sup>8</sup> [09579818-64a6-4dd5-9577-446ab6219113\\_en](https://www.regeringen.se/09579818-64a6-4dd5-9577-446ab6219113_en)

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



governance and regulation of interoperability in data sharing within the public administration and with external actors, and to propose how this can be developed. The aim is to increase the public administration's ability to share data in an efficient and secure manner, which is crucial for meeting societal challenges, streamlining operations and improving service to citizens and businesses.

The report notes that current shortcomings in interoperability make it difficult and sometimes impossible to share data, which slows down digitalisation and the realisation of its benefits. Current governance is fragmented, often sectoral, and lacks a coherent national strategy. This leads to inefficiency, manual handling, poorer data quality and Sweden falling behind other comparable countries, especially the Nordic countries, which have come much further in creating regulations and systems for interoperability.

To address these shortcomings, the investigation proposes a reform that includes:

- The "Public Administration Interoperability Act" is proposed to centralize the governance to achieve interoperability in data sharing. The Act is to be applied by state authorities, municipalities, regions, municipal associations and municipal companies. However, it shall not affect existing rules on the right to access data or the protection of personal data.
- That public administration's most urgent data sharing should be fully interoperable by 2030. This is to clarify ambitions and create a measurable goal.
- The law shall contain definitions of central concepts such as:
  - Data -Information in digital format regardless of medium.
  - Data sharing -Providing data or accessing data.
  - Interoperability in data sharing -The ability to provide or access data through information systems that interact with each other.
  - Interoperability solution -A reusable resource (legal, organizational, semantic, or technical) that aims to achieve interoperability, such as frameworks, standards, and source code.
  - National interoperability solution -A solution for interoperability that is common to public administration.
- Public administrations shall use national interoperability solutions as notified by regulations. Exceptions may be made if this is inappropriate for security reasons.



- The Swedish Digital Governance Agency (Digg) will have a central role and will, among other things, develop national interoperability solutions in collaboration with public administration, communicate and issue regulations on national interoperability solutions and act as an interoperability council. Digg will also analyze the benefits and costs of the solutions and report annually to the agency on the development of interoperability. They will also be involved in standardizing the work according to the EU's upcoming interoperability regulation and taking into account international interoperability work.
- Interoperability within specific sectors or areas should be governed by sector-specific legislation. The need for further investigation to introduce such governance in more sectors is highlighted.
- It is proposed that the Swedish Civil Contingencies Agency (MSB) be tasked with investigating whether adequate, common and coordinated protection levels or other appropriate security measures can be used when sharing data throughout public administration and with external actors. This is to strengthen trust and security in increased data sharing.

The inquiry assesses that the proposals will create the conditions for a more efficient and cohesive public administration, better service and an increased ability to handle societal challenges. Although this may initially entail costs, especially for implementation, the benefits are expected to outweigh these in the long term. An important aspect is to reduce the "interoperability debt" that Sweden has built up. The proposals are assessed to restrict municipal self-government, but this is considered necessary and proportionate to achieve the desired goals. The issue of financing for municipalities and regions is addressed, where it is noted that a large part of the measures are linked to technical development that still needs to take place. The ambition is to present a bill in the autumn of 2025 in order to be able to enact new legislation in 2026 based on the inquiry's report.

## **What open protocols are used within the EU?**

The Matrix protocol is commonly used, so we have created a separate section to describe its various applications.

In addition to Matrix, XMPP is used, for example<sup>10</sup>, an open federation protocol for chat. XMPP supports federation, which allows communication between different XMPP servers. The protocol has a wide range of uses beyond instant messaging, including VoIP and IoT.

---

<sup>10</sup> XMPP | The universal messaging standard



An example of use in the public sector 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.

Another common protocol is SIP/SIMPLE.<sup>11</sup>(Session Initiation Protocol). Although the protocol is primarily intended for VoIP and presence information, it can also be used for instant messaging, but not for persistent chat. It is currently possible to federate, for example, Skype for Business with Cisco Webex and Meeting.

Like the matrix protocol, these protocols provide the opportunity to follow the EU's strategic preference to choose open standards in the public sector.

The XMPP protocol has been around for a long time and has relatively extensive use in certain areas, description of specific large-scale implementations in the public sector is lacking in comparison to e.g. the matrix protocol. Although XMPP has wide use, the protocol is considered outdated and more complicated to implement.

In addition to this, work is underway within the Internet Engineering Task Force (IETF) to develop standards for interoperability between chat solutions. Partly through the development of Message Layer Security<sup>12</sup>, a secure group key agreement protocol, designed for asynchronous messaging environments. It is not a complete chat protocol in itself, but rather a security layer intended to be integrated into other protocols, such as XMPP or potentially MIMI.

Another IETF initiative is MIMI<sup>13</sup>- the main goal of More Instant Messaging Interoperability (MIMI) is to create a standard for different messaging services to be able to communicate with each other in a standardized and secure way. In line with the needs that this report highlights. MIMI is intended to apply MLS for, among other things, E2EE encryption mechanisms. MIMI can currently be defined more as an ongoing work within a dedicated IETF working group. The group's goal is to specify the minimum set of mechanisms required to make modern, E2EE-based Internet messaging services interoperable. The working group's assessment of the work is that it is unclear what the scope will be, i.e. does it support eSam's needs, and that it is difficult to assess when/if suppliers can begin to apply MIMI.

---

<sup>11</sup> [ietf.org/rfc/rfc3261.txt](http://ietf.org/rfc/rfc3261.txt)

<sup>12</sup> RFC 9420 - The Messaging Layer Security (MLS) Protocol

<sup>13</sup> More Instant Messaging Interoperability (mimi)



## Implementation of the open Matrix protocol within the EU

The discussion and interpretation of digital sovereignty has intensified in recent years. Several European actors have expressed concern about the possibility that the US, through the CLOUD Act or political decisions, could order the interception or shutdown of cloud services in Europe. The reporting from the countries choosing alternative solutions emphasizes that open source and European-controlled platforms are a more sustainable option in the long term.

Several European countries have already taken concrete steps towards establishing national communication platforms based on open protocols, with Matrix being a commonly used federation protocol.

### *France – Tchap<sup>14</sup>*

France was an early adopter of a national chat solution based on Matrix. The solution is called Tchap and is used for internal communication between public officials.

- The project is run by DINUM – the state's digital directorate.
- Tchap is specifically developed with a focus on security, user-friendliness and digital independence.
- The service is delivered to hundreds of thousands of users in the French public sector and it has recently been decided that Tchap will be used throughout the public administration.<sup>15</sup>
- The system includes features such as encrypted calls, group chats and mobile apps – and is linked to French identity services.
- The solution is currently mainly centralized, but DINUM is working towards increasing decentralization in the solution.

France sees federated communication with open protocols as a way to reduce dependence on American cloud services and regain control of government IT infrastructure. DINUM is working to create a comprehensive solution called La Suite<sup>16</sup>, where solutions for information management and meetings are being developed.

---

<sup>14</sup> Tchap - the instant messenger of agents of the public function

<sup>15</sup> [Public sector employees required to use French-developed Tchap app | Interoperable Europe Portal](#)

<sup>16</sup> The Digital Suite



Germany and the Netherlands are also actively contributing to the development of services. Ref -The Digital Suite GitHub

### ***Luxembourg – Luxchat and Luxchat4Gov<sup>17</sup>***

Luxembourg has taken a holistic approach to digital communication through two parallel solutions.

Luxchat is aimed at individuals and businesses. Luxchat4Gov is tailored for the public sector. Both solutions are built on Matrix and offer encrypted, ad-free communication, national operation (to ensure data control and security) and integration with public services.

Luxembourg has chosen Matrix because of its flexibility, security, and the ability to keep all data within the country's own infrastructures.

### ***Germany – broad national implementation***

Germany has come a long way in introducing Matrix broadly within the public sector. The initiative covers several sectors and areas of use:

- BwMessenger<sup>18</sup>– used by the entire German Armed Forces as a secure alternative to commercial apps.
- TI Messenger<sup>19</sup>– a mandatory solution for healthcare, decided by Gematik. Over 150,000 organizations are affected, eventually 80+ million citizens.
- OpenDesk<sup>20</sup>–a new digitally superior workplace platform, developed by BMI (Ministry of the Interior) and ZenDiS.
- Data port<sup>21</sup>– state-owned IT operations provider to eight regions in Germany
- Training<sup>22</sup>and police – several states have implemented Matrix in schools, universities and police departments. 2-3 million users.

---

<sup>17</sup> Luxchat – The instant messaging solution of Luxembourg!

<sup>18</sup> Bw Messenger | Secure. Flexible. Open Source.

<sup>19</sup> TI Messenger

<sup>20</sup> The office and collaboration suite for public administration | openDesk

<sup>21</sup> Who we are | Dataport

<sup>22</sup> Why Matrix? :: Matrix Documentation



- FITKO<sup>23</sup> – together with the Ministry of the Interior, FITKO is running a pilot project to develop a federated, government communications platform.
- IT Planning Council - Justizpostfach, Zentrales Bürgerpostfach, Elster-Postfach & Co review the next generation communication solution<sup>24</sup>

Germany's strategy is based on open source, sovereign infrastructure and standardization around a single protocol – Matrix – that different sectors can implement based on their needs. In contrast to France, it applies a more decentralized federated model with several independent entities.

### *European Commission*

The European Commission plans to increase its digital sovereignty in 2026 by replacing external apps like Signal with apps based on the open protocol Matrix. The goal is to create a secure, government communications platform where they own the data themselves and offer complements to Microsoft Teams. The need is to be able to verify all users and communicate encrypted between different EU institutions – without staff needing to use their private phone numbers and to be able to run in completely isolated environments owned by the European Commission itself, rather than relying on American cloud services for everything.<sup>25</sup>

After seeing other countries (such as France, Germany and Sweden) using Matrix, the Commission launched a "Proof of Concept". They installed their own Matrix server on secure cloud servers and used the Element X client. The plan going forward is to expand the solution to the entire Commission, use it in high-security environments and connect different EU institutions in a closed, secure network.

### *Austria – ELGA and the healthcare sector<sup>26</sup>*

Austria plans to implement Matrix as a communication layer in ELGA – the country's national electronic health record system. The idea is that different healthcare providers will be able to send and receive encrypted patient information, communicate securely in real time between different healthcare actors and integrate with other systems via federated identity

---

<sup>23</sup> Matrix Conference 2024 | FITKO

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

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

<sup>26</sup> Austrian electronic health records (ELGA)



The initiative has been inspired by German Gematik and is driven by the desire to improve interoperability, federation and security in patient communication.

### ***NATO – secure communication between allies<sup>27</sup>***

NATO has developed its own chat app called NICE, a Matrix-based solution for non-classified communications for NATO allies. The aim is to provide secure, interoperable and federated communication (chat, file sharing, etc.) between different NATO countries and partners.

NICE offers the type of modern, secure and federated communications platform that NATO and its members strive for.

### **What benefits do countries see with the matrix protocol?**

Common benefits highlighted by the countries that have chosen to standardize on the matrix protocol are:

**Openness**- The protocol is open and well documented.

**Security**- Support for end-to-end encryption in all functions, control over metadata and local operation.

**Sovereignty and control**- Enables national control over digital infrastructure.

**Decentralization** –possibility to choose delivery method, location and get risk spread

**Interoperability**- Supports federation – different organizations can communicate with each other without using the same provider, service or client.

**Integration**- Ability to connect via API, authentication (SAML, OIDC) and connect to other systems (e.g. Slack, Zoom, Teams, email).

See appendix "Appendix\_F\_Matrix and EU applications\_eSammallen" for an in-depth look at the matrix protocol.

---

<sup>27</sup> NI2CE Messenger – The Innovation Hub for Allied Command Transformation



## Sweden – authorities needs and conditions

In Sweden, interest in federated solutions for real-time communication within the public sector is growing. At the same time, the current situation is fragmented, where many actors are looking for guidance, technical direction and legal certainty. Below is a summary of dialogues that have taken place with central actors such as Sunet<sup>28</sup>, Co-use<sup>29</sup>, Internet Foundation<sup>30</sup>, RISE<sup>31</sup> and MSB<sup>32 33</sup>

**Sunet**, which provides network and identity services to higher education and research, express similar needs. Their experience shows that there is a growing interest in federated communication – but also uncertainty about which technical standards are best suited and how these can be linked to Swedish identity management (for example SAML, eduGAIN and Skolfederation).

Sunet also emphasizes the importance of strong identity in all federated solutions. They particularly highlight the risks with apps like Signal, where identity is effectively based on phone numbers – something that may be inappropriate in government contexts where unambiguous identification is required.

Sunet is part of an EU project where universities will collaborate on how to communicate with each other in a more seamless way. The matrix protocol is mentioned here as a potential enabler.

Sunet will also conduct a PoC on Element (matrix-based client) as a replacement for Slack, which is currently used within parts of SUNET's organization.

**The Swedish Internet Foundation** emphasizes that Sweden has historically benefited from a decentralized internet climate and a broad commitment to open protocols and warns that too much control in the hands of individual platform providers can undermine digital sovereignty. Therefore, the public sector needs to take a more active role in building or requiring open and federated solutions.

During meetings, it has been highlighted that there is a need for national coordination to create guidance – both technical and legal – on how federation can be implemented in a way that meets the requirements of GDPR, NIS2 and national security legislation. There

---

<sup>28</sup> Sunnet

<sup>29</sup> Joint use – Municipal business development

<sup>30</sup> The Internet Foundation

<sup>31</sup> Swedish research for sustainable growth | RISE

<sup>32</sup> MSB – Swedish Civil Contingencies Agency

<sup>33</sup> The following compilation is based on dialogues, consultation responses and public sources from actors such as Sunet, Sambruk, the Internet Foundation, RISE and MSB.



is currently a lack of a clear national framework that bridges technology, identity, law and business benefit.

The Internet Foundation sees identity federation as a key factor in achieving a robust and secure chat federation. Here, DIGG can play a central role in the matter as they plan to build a national identity and authorization architecture based on OI DF (OpenID Federation). This creates the potential to utilize a common federation infrastructure for real-time communication as well – so the solutions become compatible.

**RISE** have particularly emphasized that interoperability must not come at the expense of security. Their experts emphasize that end-to-end encryption should be a natural starting point for all real-time communication and open protocols, especially in the public sector. This applies regardless of whether the communication is internal, between authorities or, in the future, includes citizen contact.

RISE believes that in some cases two different systems may be needed – one that is open and interoperable, and another that is used for particularly sensitive communications where security comes first. They also highlight that it is important for the public sector to choose protocols, not products – and that control over metadata and operations is crucial to avoid future lock-in scenarios.

RISE sees the matrix protocol as an interesting alternative for chat federation because it is decentralized, based on open source, has end-to-end encryption as standard, and supports federation. They compare it favourably to the email model – where each actor runs their own server but can still communicate across borders.

It is also highlighted that the public sector should adopt open protocols and solutions for social media such as ActivityPub or the AT protocol. One of the major advantages of these protocols is that authorities gain control over their democratic communication channels.

**The Swedish Civil Contingencies Agency (MSB)** sees that there is a need to be able to maintain the functions of the authorities even in the event of disruptions in digital infrastructure, for example if parts of the country are cut off from central services. They specifically point to the following regulations from the Ordinance on State Government Emergency Preparedness (2022:524), which contains a number of paragraphs that can be directly linked to the need for secure, robust and decentralized communication solutions:



*§7: Authorities shall identify activities of national importance and analyse vulnerabilities in the face of peacetime crises and heightened preparedness. This also includes working systematically to maintain operations (continuity), and ensuring that other actors in the area do the same.*

*§10: Authorities must take into account the requirements of total defense and plan to ensure that operations can continue even during heightened readiness, based on the availability of personnel and prevailing conditions.*

*§20–21: Emergency response authorities shall have a good ability to resist threats and risks, prevent vulnerabilities and carry out their tasks in peacetime crises and heightened alert.*

In light of the above, it becomes clear that the requirements for functionality during crises and wars place special demands on the public sector's ability to communicate with each other. A decentralized chat infrastructure, based on open standards and federated solutions, can be a way to reduce dependence on individual suppliers and central cloud services. Such a solution can strengthen resilience in the event of disruptions, reduce the risk of interruptions in the event of cyberattacks, and enable continued communication even if part of the network is knocked out. This is in line with the responsibilities that authorities, especially emergency response authorities, have under current regulations.

**Sambruk**, a collaboration body for municipalities, highlights that there is a great need for better digital collaboration, especially in municipal operations where collaboration with regions and government agencies is everyday life. But technical solutions for secure chat across organizational boundaries are often lacking, or are based on temporary bridges rather than sustainable standardized protocols.

Sambruk highlights that an open protocol in itself does not address issues such as digital sovereignty and control. If many public actors still choose external operating providers that are, for example, affected by extraterritorial legislation, sovereignty can be undermined. In this way, the federation network can become vulnerable, which requires clear principles and policies.

Implementing an open chat protocol is complex and requires deep technical expertise from suppliers. A federation requires secure certificate management and managing trust chains – who actually trusts whom. In addition, Sambruk sees a need for a joint steering group that provides the opportunity to steer the work and steer the development of the public sector federation in a responsible manner.

Sambruk sees a risk that a new form of centralized lock-in will be created if only a few actors set up federation solutions.



The subject council within digitization, data and digital administration at the **Swedish Government Offices (Regeringskansliet)** believes that eSam's work on a common protocol for chat federation has clear synergies with "A reform for data sharing" (SOU 2023:96)" and could be an issue to be addressed early if the bill passes. The original ambition was for the law to come into force as early as January 1, 2025, but due to prioritized issues (including the war in Ukraine, the NATO process and the US election) the timetable has been adjusted.

## **The Nordic region – how are our neighboring countries?**

The working group has sought contact with our Nordic neighbours to understand how they work on this issue but has not yet found the right contact points. Therefore, we recommend that in any further work, we establish contact with our neighbouring countries. The only example we have intercepted so far is an SMS-like encrypted messaging system (Meshtastic<sup>34</sup>), based on open-source code, which Aarhus Municipality is piloting. The purpose of the system is to ensure communication in difficult conditions, such as the power outage that affected the Iberian Peninsula (Spain and Portugal) in April 2025.

This appendix has been updated based on reviews from RISE, Sambruk, DIGG, MSB, Sunet and the Internet Foundation during the consultation round in spring 2025.

---

<sup>34</sup> Meshtastic



# Appendix B: Technical comparison of protocols

## Summary

There is no universally "best" protocol for all purposes, but rather different protocols that are optimized for different purposes and needs.

**The XMPP protocol** is historically strong but requires more additions and configuration for full functionality, the development rate is also considered low. Application is limited within the EU.

**Signal** offers strong security but lacks federation and open integration, and limited support for identity management. Aimed at individuals.

**WebRTC**, SIP and other protocols are better suited for voice/video and supplementary features – not for end-to-end solutions within federated chat.

**ActivityPub** has great potential for the public sector in terms of social media given its support for decentralized communication. However, the protocol does not have the capabilities required for chat federation and real-time communication.

**MLS and MIMI** have the potential to become a common standard for chat federation. However, the development of MIMI in particular is in its early stages and the work is considered to be a complex and time-consuming process where several commercial actors need to find common ground before the protocol has the opportunity to become a formal RFC standard.

**The Matrix Protocol** stands out as the most complete option for federated, secure, real-time communication and chat – especially for the public sector. The protocol also provides good integration with existing infrastructure via e.g. bridges to email, Slack, Teams and other platforms. This assessment is strengthened by the fact that several EU countries have started to invest and build solutions based on the matrix protocol.

## Differences between open and proprietary protocols

A communications protocol can be described as a set of rules and specifications that define how data is formatted, sent, received, and interpreted between different computer



systems. Protocols can be either open or proprietary (“closed”), a distinction that has implications for their use and the effects they bring.

### ***Open Standards/Protocols***

A standard is often described as a common and agreed upon solution to a recurring problem or need. An open standard, and thus an open protocol, is characterized by its specification being publicly and freely available for anyone to study, implement, and use. Any intellectual property rights associated with the standard are usually licensed on fair, reasonable, and non-discriminatory (FRAND) terms<sup>1</sup>, and preferably without any royalty fees. The development and maintenance of open standards often takes place through a transparent process in which all stakeholders have the opportunity to participate and influence. Key characteristics of open protocols include the promotion of interoperability, reusability, and the absence of arbitrary restrictions on their use. They enable compatibility between products and services from different manufacturers, which in turn stimulates free competition in the market.

### ***Proprietary Standards/Protocols***

Proprietary standards and protocols, as opposed to open standards, are technical specifications controlled by a single vendor or organization. The specifications are often not publicly available, but may be protected as trade secrets or only offered under restrictive licensing terms. In many cases, they are designed so that they cannot be easily implemented by independent developers outside the ecosystem of the controlling entity. Documentation may be inadequate, or in some cases intentionally designed to hinder independent implementation and thereby protect the vendor's market position. Characteristics often associated with proprietary protocols are limited interoperability with systems outside the vendor's sphere of control and an inherent risk of vendor lock-in.

## **The market for open chat protocols**

In a digital world where communication is a central part of both private life and business, the choice of underlying protocols plays an important role. Open protocols for chat communication offer a standardized way of communicating, enabling interoperability between different applications and services. Below is a description and analysis of the most common open protocols on the market

---

<sup>1</sup> [FRAND patents - Wikipedia](#)



## ***XMPP (Extensible Messaging and Presence Protocol)***

The Extensible Messaging and Presence Protocol (XMPP) is better known from its roots in Jabber. Although it doesn't always get the spotlight that some newer protocols do, it is under continuous development driven by the XMPP Standards Foundation (XSF) and an active community. The protocol has a decentralized architecture, meaning it doesn't rely on a central server but can be distributed across multiple servers that communicate with each other. XMPP supports a range of chat features, including text messaging, presence, group chat, and file transfer. Support for voice and video calls is handled through plugins; basic support is missing in XMPP.

The pace of development for XMPP can be described as stable rather than revolutionary. The core of the protocol is well-established (specified in RFC 6120 and RFC 6121), and much of the development is done through XMPP Extension Protocols (XEPs). These XEPs allow the protocol to be extended and adapted for new features and uses without breaking compatibility with the underlying implementations. The process of standardizing XEPs involves different stages from experimental to final, which can take time but also contributes to robust and thoughtful development. The challenges sometimes lie in the volunteer-driven nature and in ensuring that implementations widely adopt new extensions.

## ***WebRTC (Web Real-Time Communication)***

WebRTC (Web Real-Time Communication) is a technology that enables real-time communication, such as voice calls, video calls, and data transfer, directly between browsers and devices in a peer-to-peer network. The goal of WebRTC is to provide these features without the need for plugins or third-party software, revolutionizing the possibilities for web-based communication applications. Essentially, WebRTC is a set of standards, protocols, and JavaScript APIs that allow browsers to exchange media streams and data directly with each other. Instead of all communication going through a central server (client-server model), WebRTC strives to establish direct connections between users' devices. This reduces latency and improves the performance of real-time applications.

WebRTC has reached a high level of maturity and is now an established and widely implemented standard. Its development has been driven jointly by the World Wide Web Consortium (W3C), which is responsible for the browser APIs, and the Internet Engineering Task Force (IETF), which specifies the underlying protocols and security aspects.



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

Session Initiation Protocol (SIP) is a signalling protocol widely used to establish, modify, and terminate real-time sessions such as voice and video calls over IP networks. The protocol is a central component of modern communication systems, especially in IP telephony (VoIP). SIP is a relatively mature protocol, standardized by the Internet Engineering Task Force (IETF). The pace of development of the core specifications is not as fast as for some newer, more agile protocols. However, continuous development occurs through the publication of Request for Comments (RFC) that either refine existing functionality or introduce extensions to meet new requirements and use cases. Development is driven by the need to improve security, interoperability, and support new communication services. Work is done within various IETF working groups and contributions from vendors and developers who implement SIP in their products and services.

Features such as multimedia sessions, including voice and video calls, and instant messaging through the SIMPLE extension are supported. The protocol does not have built-in support for persistent chat or end-to-end encryption.

### ***WebSocket***

WebSocket is a communications protocol that enables bidirectional (full-duplex) and persistent communication over a single TCP connection. Unlike the traditional HTTP model, where the client initiates each request and the server responds, WebSocket allows both the client and the server to send data to each other at any time after the connection is established. This makes WebSocket ideal for real-time applications that require low latency and frequent data updates.

WebSocket is a mature and widely implemented protocol that has been an official web standard for a long time. The WebSocket protocol was standardized by the Internet Engineering Task Force (IETF) in RFC 6455 in 2011. The World Wide Web Consortium (W3C) has specified the WebSocket API, which defines how browsers can interact with WebSocket connections via JavaScript. These standards are stable and have undergone extensive review.

### ***IRC (Internet Relay Chat)***

IRC is a text-based application layer protocol and one of the oldest text-based chat protocols, developed in the late 1980s for real-time communication in the form of chat. It allows communication in groups (channels) as well as private messages between



individual users. IRC was one of the earliest forms of real-time Internet communication to become widely popular and is the basis for many concepts found in today's messaging services.

IRC is a mature protocol in the sense that its core specifications are long-standing and well-established. However, its status and usage have changed significantly over time as newer communication technologies have emerged.

### ***MQTT (Message Queuing Telemetry Transport)***

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol designed for machine-to-machine (M2M) communication and widely used in the Internet of Things (IoT). The protocol is based on a "publish-subscribe" (pub-sub) model, which differs from the traditional client-server model where the client directly requests data from a server. This model makes MQTT very effective for environments with limited bandwidth, high latency or unreliable networks, as well as scenarios with a large number of connected devices.

MQTT is a mature, stable, and widely adopted protocol, particularly prominent in the IoT world due to its lightweight design and efficient publish-subscribe model. Its standardization and rich ecosystem of implementations make it a reliable choice for real-time data transmission in a wide variety of applications.

### ***AMQP (Advanced Message Queuing Protocol)***

AMQP (Advanced Message Queuing Protocol) is an open, standardized application-layer protocol for messaging. It is designed to enable robust and reliable message exchange between applications and systems, regardless of platform or programming language. AMQP is particularly suited for enterprise-level messaging systems, system integration, and scenarios where reliability and advanced routing are important.

AMQP is a mature and robust protocol, well-established for advanced messaging in enterprise and integration scenarios where reliability, flexible routing, and guaranteed delivery are paramount. Its standardization and broad support in the form of broker and client implementations contribute to its reliability and continued relevance.

### ***RCS (Rich Communication Services)***

RCS (Rich Communication Services) is a communications protocol that aims to replace and modernize the aging SMS and MMS standards for mobile messaging. The goal is to



offer a more interactive and app-like messaging experience directly within the phone's built-in messaging application, without requiring the download of separate "over-the-top" (OTT) apps like WhatsApp or Messenger.

Unlike SMS/MMS which primarily uses the circuit-switched network, RCS is built on the IP Multimedia Subsystem (IMS) and uses packet-based data (cellular data or Wi-Fi) for message transmission. When an RCS connection is not possible (e.g. due to lack of coverage or incompatible recipient), the message can fall back to being sent as a regular SMS or MMS.

As a protocol and ecosystem, RCS is still in a developmental and maturing phase compared to older protocols like SMS or newer but more niche protocols like MQTT. While the core standards are in place, work is still ongoing to ensure full global interoperability, a consistent user experience across platforms and carriers, and to address challenges related to roaming, privacy, and carrier business models. Google and Apple are working to enable interoperability with RCS between their messaging services. The standard protocol currently lacks end-to-end encryption.

## **MLS**

Message Layer Security (MLS) is a relatively new protocol designed specifically to provide efficient and secure end-to-end encryption for large-scale group messaging. The goal is to solve the challenges of key management and security in large group conversations, problems that become more complex the more participants there are and the more frequently members are added or removed.

MLS is formally defined in RFC 9420 and 9750 (architecture), published in July 2023 as a proposed standard. Its primary purpose is to provide a highly efficient and secure group key agreement protocol designed for asynchronous messaging environments. It is not a complete chat protocol in itself, but rather a security layer intended to be integrated into other protocols, such as XMPP, Matrix, or potentially MIMI. MLS focuses on providing a secure and efficient cryptographic layer for group communications. The protocol is used to varying degrees in chat solutions from Wire, Google, AWS (Wickr), and Matrix.

By default, the MLS protocol is considered stable after going through the IETF review process. However, the ecosystem around MLS, including a wide range of off-the-shelf solutions, is still under construction. Challenges remain in achieving widespread adoption, ensuring interoperability between different MLS implementations in practice, and managing the integration of MLS into complex existing messaging systems. The



security features have been formally reviewed by various bodies, but as with any new cryptographic protocol, time and widespread use are required to identify any unexpected vulnerabilities.

### ***More instant Messaging Interoperability (MIMI)***

MIMI (More Instant Messaging Interoperability) is not a single protocol in the same way as WebRTC, WebSocket, Matrix, MQTT, AMQP or MLS. Instead, MIMI is an initiative and working group within the IETF (Internet Engineering Task Force) whose goal is to specify a framework and related protocols to enable secure and interoperable messaging between different messaging services and platforms. The primary purpose is to break down the “silos” that exist today, where users on different chat platforms cannot communicate with each other.

MIMI is a standards initiative within the IETF that is intended to address the complex challenge of interoperability between messaging services with a focus on security. The framework and its related specifications are under development and have not yet reached full standards status. However, implementation and widespread adoption is most likely several years away. MIMI is therefore in the early stages of its maturity cycle compared to more established Internet protocols. Its success will depend on the completion of the standards and on a sufficient number of messaging providers choosing to implement and collaborate based on the MIMI framework.

### ***ActivityPub***

ActivityPub is a decentralized social networking protocol that enables different social platforms and applications to communicate with each other in a federated network, often referred to as the "Fediverse". Unlike traditional centralized social networks (run by a single company), ActivityPub allows users on one platform (an "instance" or server) to interact with users on another platform that also supports the protocol. The goal is to create an open and interconnected social web ecosystem where users have more control over their data and their online experience.

ActivityPub is an open, decentralized social networking protocol that was standardized by the World Wide Web Consortium (W3C) in 2018. It forms the backbone of the so-called "Fediverse" (a federation of diverse, interoperable social networks).

ActivityPub is a mature and standardized protocol that successfully powers Fediverse as a decentralized alternative to traditional social networks. The specification itself is stable and widely implemented, but the ecosystem as a whole is still evolving in terms of



solving challenges related to large-scale operation, moderation, and user experience. Its maturity lies in being an established and working standard with a growing base of implementations and users.

### ***Matrix***

Matrix is an open, standardized protocol for secure, decentralized real-time communication. It differs from more traditional protocols in its federated architecture, where different servers can exchange messages with each other, giving users greater control over their data and freedom of choice of client and server.

The development pace of the Matrix protocol is fast and dynamic. The project is actively driven by the Matrix.org Foundation and a committed global community of developers. Development is done openly with a focus on rapid iteration and implementation of new features and improvements. This includes continuous work on improving performance, scalability, user experience and security. The concept of "Matrix 2.0" demonstrates a drive to introduce significant improvements, such as faster synchronization ("Sliding Sync"), more modern authentication mechanisms (Native OIDC) and built-in support for end-to-end encrypted group calls (MatrixRTC).

Matrix offers end-to-end encryption as standard for private conversations and supports bridges to many other popular communication protocols and services.

Matrix is actively working on integrating MLS into the Matrix protocol, including the development of "Decentralized MLS" (DMLS) to adapt MLS to federated and decentralized environments.

### ***SimpleX Chat Protocol***

SimpleX Chat Protocol is a modern, decentralized messaging protocol that deliberately uses the concept of one-way message queues (simplex) to achieve a high degree of privacy and anonymity for its users. Unlike most other messaging services that rely on user identifiers (such as phone numbers, email addresses, or usernames), SimpleX does not link users to permanent identities.

The development pace of the SimpleX Chat Protocol and its associated applications is relatively high and is driven by the SimpleX project. As it is a newer protocol, active development is underway to add features, improve performance, and strengthen security based on community feedback and new insights into privacy-preserving communications. Development is open and follows a clear roadmap.



Due to its centralized architecture and lack of formal standardization, the protocol is considered difficult to scale to inter-agency federation at present.

The table below summarizes the main technical characteristics of each protocol based on criteria such as federation, encryption, media support, scalability, and maturity.

**Table 1: Technical characteristics and comparison of selected communication protocols**

Protocol	Support for federation	Support for E2EE	Media support	Bridging	Scalability	Maturity
<b>XMPP</b>	Yes	Via add-on	Text, Files (Jingle/HTTP), VoIP (Jingle)	Yes	High	Mature (IETF RFCs, XSF XEPs).  Slow development pace
<b>Matrix</b>	Yes	Built-in	Text, Files, Images, Audio, Video, VoIP	Yes, comprehensive	High	Mature (Matrix.org Spec, no IETF RFC)
<b>Signal</b>	No	Built-in	Text, Files, Images, Audio, Video, Calls	No	High (Centralized infrastructure)	Mature (Protocol well established, App popular)
<b>WebRTC</b>	No	Built-in	Real-time Audio/Video, Arbitrary Data (Data Channels)	Yes	High (P2P), Limited by signaling/TURN	Mature (W3C Rec, IETF RFCs)
<b>IRC</b>	Yes	Via add-on	Primarily Text, Files (DCC - insecure/obsolete)	Yes	Medium (Limited by netsplits, older design, depends on IRCd)	Mature (but aging, IETF RFCs)
<b>RCS</b>	Yes (Operator-controlled)	Implementation-specific	Text, Files, High-resolution media, Rich Cards (replaces SMS/MMS)	Limited	High (Depending on operators' IMS infrastructure)	Maturing (GSMA Universal Profile, increasing applic.)



<b>MLS</b>	N/A	Yes	N/A	Yes	Yes	Maturation (standard RFC 9420)
<b>MIMI</b>	Yes (draft)	Yes, through MLS	Too early to say	Too early to say	Too early to say	Low maturity (IETF status Internet-Drafts). Not a protocol
<b>Activity Pub</b>	Yes	No (Work in progress via addendum /FEPs)	Text, Links, Media Objects (AS2), Binary Data (depending on impl.)	Possible	Medium/High (Depending on server implementation, fan-out/inbox load)	Mature (W3C Rec)
<b>MQTT</b>	No	Via application layer	Arbitrary binary data (Payload), optimized for small messages (IoT)	Yes	Very High (Depending on broker impl. and clustering, designed for millions)	Mature (OASIS Standard, ISO/IEC)
<b>SIP</b>	Yes	Signaling only	Audio/Video (via RTP), Other via SDP negotiation	Yes	Very High (Carrier-grade implementations available)	Mature (IETF RFCs, VoIP backbone)
<b>SimpleX</b>	No	Built-in	Text, Files (XFTP), Images, Audio, Video, Calls (WebRTC signaling)	No	Unknown /Experimental	Early (No formal standard)

## Bridge solutions

Two main strategies are applied to achieve interoperability: building bridges between existing, often proprietary, platforms and applying open federation protocols.



Existing bridging solutions create the conditions to connect open chat solutions with proprietary chat solutions such as Slack, Microsoft Teams and Zoom. An example is m.io.

The challenge of interoperability in the chat landscape is complex, and there is no one-size-fits-all solution. The choice between using bridges to connect existing closed systems and using open federation protocols requires a trade-off between immediate convenience and long-term control, transparency, and security.

Open source bridging solutions, such as Matterbridge and Matrix bridging, offer a way to connect to the dominant platforms where users are already present. Their strength lies in enabling communication across ecosystem boundaries without requiring everyone to switch platforms. However, this convenience comes at the cost of significant drawbacks such as compatibility and API dependencies, not maintaining end-to-end encryption, dropped features, and continued reliance on the underlying closed platforms and any bridging vendors.

A form of hybrid strategy may become relevant for the public sector, where a federated protocol forms the core and bridges are used selectively for necessary external connections.

This appendix has been updated based on reviews from RISE, Sambruk, DIGG, MSB, Sunet and the Internet Foundation during the consultation round in spring 2025.



## Appendix C – SWOT of possible paths

### Summary

Overall, the SWOT analysis shows that the choices involve different trade-offs between speed, control, cost and long-term sustainability.

Options 1 and 6 offer temporary convenience but carry significant risks of long-term fragmentation and dependency. Options 2 and 5 can serve as transitional solutions, but lack stability and coordinated direction.

Options 3 and 4 both build on openness and interoperability, but option 3 is the only alternative that is currently considered to meet all known requirements for openness, EU compatibility, security and the possibility of independent further development.

Based on the analysis, option 3 – a federated open solution – appears to be the most sustainable option in the long term. Options 3 and 4 can be combined.

To succeed, a clear framework for governance, resources, and management of trust and certificates is required – especially if the federation is to become a long-term, societally sustainable solution.

### Strengths, Weaknesses, Opportunities and Threats (SWOT)

This SWOT analysis shows six possible options for how the public sector can organize its digital chat communication. The purpose is to highlight the strengths, weaknesses, opportunities and risks for each option. The analysis is not a definitive answer, but a tool for discussion and prioritization.



The timeline in Appendix D is based on Pathway 3 (federated open solution), but the analysis here helps to understand the consequences if other strategies were proposed, supplementing or replacing the main track.

Also keep in mind that the path choices are not mutually exclusive – some can function as steps or parallel solutions in a transitional phase.

What we mean by the six (6) proposals

**1 - Continue as today** means that many authorities will retain the Skype tool for their chat communication for the time being. Most authorities have established a federation between their respective Skype environments. This will be maintained until Skype disappears as a product. Authorities that have already chosen or are choosing a solution other than Skype will either end up outside the previous “community” or will be forced to maintain Skype in parallel as a solution for interacting with others.

**2 - Central bridging solutions** 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 - Federated open solution** means that eSam requires its members (and other partners) to ensure that the chat tools they use comply with the standard for this open protocol. The requirement should also be anchored in ministries and authorities outside eSam. Each authority that meets the requirements can then more easily become interoperable with other parties that also comply with the current standard. Each authority knows which path leads to federation and can create the conditions by following the standard.

**4 - Establish a central chat solution** means that a party is assigned to make available “a common Swedish government chat” which will be the only channel through which authorities and their employees can/should communicate with each other. Examples can be found from France (Tchap<sup>1</sup>). This route choice could be an interim solution while waiting for route choice 3 to be established.

---

<sup>1</sup>Tchap — Tchap



**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. Typically, this could happen between authorities that have chosen or are choosing the same products for internal chat and where the threshold for federation is lower.

**6 - Authorities choose the same proprietary solution** which means that authorities put the issue of authority aside and all choose to let, for example, an American cloud service company, handle all communication via their platforms. This is done at the expense of control and adaptation.



## SWOT: Choice of path for government communication

Table1- A comparison of six strategic alternatives based on strengths, weaknesses, opportunities and risks

Path selection	Strengths	Weaknesses	Facilities	Risks
<b>1. Continue as today</b>	<ul style="list-style-type: none"> <li>- Low threshold</li> <li>- Existing functionality</li> <li>- Platforms already established</li> </ul>	<ul style="list-style-type: none"> <li>- Increased fragmentation</li> <li>- Decreasing interoperability in the US</li> <li>- Lock-in to supplier(s)</li> </ul>	<ul style="list-style-type: none"> <li>- Temporary convenience for some users</li> <li>- Buy time to establish a strategy</li> </ul>	<ul style="list-style-type: none"> <li>- Unclear how long local delivery of Skype will be offered</li> <li>- Risk that authorities do not use chat among themselves</li> <li>- Risk of postponing important decisions/action paralysis</li> <li>- Impaired collaboration in the long term</li> <li>- Difficult to meet existing and future EU requirements</li> <li>- Risk of unplanned operational issues when Skype support ends</li> </ul>
<b>2. Central bridging solution</b>	<ul style="list-style-type: none"> <li>- Relatively quick implementation</li> <li>- Can provide collaboration opportunities in the short term</li> </ul>	<ul style="list-style-type: none"> <li>- High technical complexity</li> <li>- Risk of bottlenecks and vulnerabilities</li> <li>- End-to-end encryption probably cannot be</li> </ul>	<ul style="list-style-type: none"> <li>- Possibility to coordinate different tools in the transition phase</li> <li>- Creates a broad ecosystem</li> </ul>	<ul style="list-style-type: none"> <li>- Costly to maintain</li> <li>- Risk of becoming a permanent "emergency solution" unless a clear transition strategy is in place</li> </ul>



Path selection	Strengths	Weaknesses	Facilities	Risks
	-	<ul style="list-style-type: none"> <li>offered/maintained intact between solutions</li> <li>- Temporary solution</li> <li>- Complex dependency chain between solutions</li> <li>- Weaknesses in end-to-end encryption</li> <li>-</li> </ul>	<ul style="list-style-type: none"> <li>- Gives vendors time to move towards full support for open federation protocol</li> </ul>	<ul style="list-style-type: none"> <li>- Too complex or time-consuming to maintain</li> <li>- Suppliers reluctant to support creating conditions for interoperability</li> </ul>
<b>3. Federated open solution</b>	<ul style="list-style-type: none"> <li>- High interoperability</li> <li>- Provides conditions for digital sovereignty and self-determination</li> <li>- Long-term sustainability</li> <li>- Decentralized communication as standard</li> </ul>	<ul style="list-style-type: none"> <li>- Requires investment in joint governance and expertise</li> <li>- Does not solve current challenges from a short-term perspective</li> <li>- Requires establishment of trust framework and certificate management</li> <li>- Digital sovereignty also requires control over hosting/infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>- Innovation and supplier independence</li> <li>- Could become a European role model</li> <li>- Improved security and transparency</li> <li>- Can be combined with bridge solutions (option 2)</li> <li>- Clearly in line with EU requirements for interoperability, security and transparency</li> </ul>	<ul style="list-style-type: none"> <li>- Requires perseverance and a shared goal</li> <li>- Requires active choices in decisions and governance and anchoring outside eSam</li> <li>- Risk of resistance from large platform players</li> </ul>
<b>4. Establish a central chat solution</b>	<ul style="list-style-type: none"> <li>- Coordinated solution with clear division of responsibilities</li> <li>- Possible to adapt to Swedish requirements</li> </ul>	<ul style="list-style-type: none"> <li>- Risk of new central locking</li> <li>- Can be experienced as top-down</li> <li>- Not decentralized</li> </ul>	<ul style="list-style-type: none"> <li>- Create a national standard with high security</li> <li>- Possibility of cost sharing between authorities</li> </ul>	<ul style="list-style-type: none"> <li>- Risk of low acceptance</li> <li>- Difficult to scale or change as needed</li> <li>- The push towards an open federation protocol is waning</li> </ul>



Path selection	Strengths	Weaknesses	Facilities	Risks
	<ul style="list-style-type: none"> <li>- Relatively quick implementation</li> </ul>		<ul style="list-style-type: none"> <li>- Gives vendors time to move towards full support for open federation protocol</li> </ul>	<ul style="list-style-type: none"> <li>- Risk of new form of lock-in if operations centralization occurs without open interfaces</li> <li>- Risk of transparency being diluted if central solution becomes too controlling</li> </ul>
<b>5. Form clusters for collaborations</b>	<ul style="list-style-type: none"> <li>- Low threshold</li> <li>- Possible to get started quickly in certain sectors</li> </ul>	<ul style="list-style-type: none"> <li>- Lack of common direction</li> <li>- Difficulty in upgrading nationally</li> <li>- Requires extensive coordination</li> </ul>	<ul style="list-style-type: none"> <li>- Practical path for testing and piloting</li> <li>- Strengthen sectoral collaboration</li> <li>- Practical transition strategy</li> <li>- Opportunity to test federated concepts on a smaller scale</li> </ul>	<ul style="list-style-type: none"> <li>- Requires long-term coordination to become sustainable</li> <li>- Risk of continued fragmentation unless the choice of path is linked to common principles and governance</li> </ul>
<b>6. Authorities choose the same proprietary solution</b>	<ul style="list-style-type: none"> <li>- Fast implementation</li> <li>- Well-known tools</li> <li>- Scalable and efficient solutions</li> </ul>	<ul style="list-style-type: none"> <li>- Difficult to meet transparency and control requirements</li> <li>- Authorities must choose the same solution to be able to collaborate effectively</li> <li>- Significant supplier dependency</li> <li>- Proprietary chat protocol</li> </ul>	<ul style="list-style-type: none"> <li>- access to market-leading collaboration features</li> <li>- utilization of existing investments</li> </ul>	<ul style="list-style-type: none"> <li>- Risk of lack of cost control</li> <li>- Increased lockdown and limited availability</li> <li>- If the solution is a US cloud service, there is a risk of politically motivated shutdown or access restriction from American suppliers, in the event</li> </ul>



Path selection	Strengths	Weaknesses	Facilities	Risks
				of changed legal situations or external geopolitical decisions - Authorities make different assessments regarding the conditions for handling sensitive information in American cloud services - Risk of insufficient control over functions, storage and data flows - Risk of legal and political influence opportunities outside the EU - Deviates from the EU's strategy for digital sovereignty and interoperability

This appendix has been updated based on reviews from RISE, Sambruk, DIGG, MSB, Sunet and the Internet Foundation during the consultation round in spring 2025.

Memorandum 2025-11-25  
Doc. payment: Appendix  
Version: 1.0  
No./ref: ES2025-20





# Appendix D – Timeline and Transition Plan

## Introduction

The proposed timeline assumes that the steering group decides on continued work after the summer of 2025, and that this work is prioritized and given clear conditions in the form of governance and access to resources.

Each phase of the timetable is dependent on such decisions being made on time, and being followed by mandate and operational capacity.

A clear national governance model is required for how the federation work will be led, monitored and managed over time. This includes the division of responsibilities, trust management, incident management and long-term management of technical infrastructure and code.

The government's inquiry (SOU 2023:96) proposes a new law on public administration interoperability from 2026. It will strengthen the ability of authorities to share information and collaborate digitally. This initiative could be one of the first operational steps towards this type of interoperability – especially in the area of communication.

The following timeline is based on the assumption that the steering group, after the steering group meeting in September 2025, decides that the work on chat federation should continue and be prioritized. This means that the project will continue to be run by a small working group with limited availability (approximately 10–20%), which is why the pace during the fall of 2025 will be limited. Additional resources are proposed to be added in the spring of 2026.

The timeline and transition plan assume:

- that a decision be made in September 2025 on continued work
- that the steering group clearly points out the direction of the work
- that the division of responsibilities and mandate are clarified
- that capacity and expertise are secured in the form of dedicated resources
- that organizational support is in place for each phase



- that reinforcement with key competence is planned for spring 2026.

It is also crucial that the steering group sets clear priorities. If there are parts of the plan that are not considered feasible within the given framework – in terms of time, finances or organisation – these need to be reprioritised or deleted. The timeline is therefore not to be considered static but will need to be adjusted based on how the steering group chooses to focus and support the work.

In line with the EU's increasing focus on digital sovereignty, interoperability and security governance, it is also crucial that this work is carried out with long-term responsibility and perseverance. A common federation model requires not only technology and law – but also continuous coordination, capacity building and management. It is about gradually building a common communication infrastructure with high demands on robustness, security and coordination over time.

## **2025 Preparation phase - Foundation and path selection**

**Purpose:** Anchoring, dialogue, preparing tests and deciding on direction

A government bill on interoperability (SOU 2023:96) is expected in the fall of 2025, where dSam4's work can be seen as an operational step towards future legislation.

### **Decision & preparation:**

- Decision on continued work from eSam's steering group September 2025
- Establish contact with DIGG for the autumn's work.
- Given that the working group consists of people with limited availability, progress in the fall of 2025 will need to focus on:
- First draft of guidance for authorities.
- Initiate preparations for smaller-scale test environments within the working group.

### **Continued monitoring of the world:**

- Monitor Scandinavia and start a dialogue

### **Communication:**

- Anchor the roadmap with eSam's members



- Start dialogues with suppliers and other EU countries

#### Risks:

- Lack of steering group decisions
- Insufficient resource allocation
- Unclear division of responsibilities

## 2026 Internal tests and guidance deepening

**Purpose:** Collaborate, test in real-world environment and prepare for gradual scale-up, legal analysis

During the first half of 2026, the working group will focus on testing federation on a small scale. The goal is to gather practical experience that can be used to develop improved guidance for other authorities. Only then can broader pilots or test environments be offered to more actors. Federation does not need to replace the primary communication tool – it can function as a complement, especially when collaborating across organizational boundaries.

#### Focus areas:

- Technical ability:
  - Develop technical expertise based on government requirements, including support for the Matrix protocol and dialogue with the Matrix Foundation.
- Start federated environments:
  - Set up a federation cluster with at least 3–4 authorities (e.g. Försäkringskassan, UBM, Hav and the Swedish Pensions Agency) with at least three different vendor solutions.
  - Evaluate the pilot activities and provide feedback to the guidance support – no earlier than autumn 2026.



Collaboration and monitoring of the external environment:

A new law on public administration interoperability (according to SOU 2023:96) is expected to come into force in the summer of 2026. It is important that the work on federation is adapted to the requirements and architecture of that law.

- Dialogue has been initiated with DIGG about possible connections to national infrastructure (ENA), but the collaboration is developing in line with each party's priorities.
- Contribute to standardization in EU technical working groups (e.g. CEF).
- Initiate dialogue about possible EU funding via CEF2 or the Interoperability Programme.
- Explore the possibility of establishing a support structure or collaboration network for federation.

***Legal and security-related issues:***

A national implementation may entail new security requirements. If the federation becomes a core part of the digital infrastructure, this may be required:

- Consultation according to the Security Protection Act
- Security protection analyses for operating environments
- Assessment of legal risks when storing or distributing personal data between nodes.

These issues are complex and difficult to predict in detail, but must be included in planning, risk management and time buffers – especially if the solution is to be used in a crisis or heightened alert.

***Competence enhancement:***

In order to scale up the work in 2026, it is proposed that the working group be strengthened with dedicated expertise. The following roles are prioritized:

- Technical Specialist (Federation, Security, E2EE)
- Legal expert (procurement, interoperability, collaboration)
- Project and change management as well as IT and business strategists



This enables:

- Federation architecture design
- Legal analysis of shared operation
- Completion of guidelines and support materials for procurement

***Governance and administration:***

A clear national model is needed for how the federation will be governed, monitored and managed over time. The work requires long-term responsibility, and a permanent management organization should be in place by 2027 at the latest.

## **2027 - Broader implementation**

**Purpose:** Create conditions for broader implementation and start building a common structure

In the spring of 2027, eSam should make a decision on continued prioritization of the work and on a possible new phase with broad implementation. For this to be successful, a coordinating function or project manager must be given a clear mandate to drive the issue between authorities. Progress during the year depends on the resources that are provided.

**Note:** This section describes target images – not guaranteed events.

***Competence supply:***

- Establish shared knowledge and support functions, such as a development lab or a federation sandbox.
- Begin building a national code repository with guidelines, code examples, and reusable components.

***Technical implementation:***

- Test E2EE, identity solution (ex: Sweden Connect), presence status, synchronization
- Develop an architectural proposal for a temporary HUB solution.
- Begin development of a HUB solution for those authorities that lack the capacity to establish a federation node themselves. This will only happen if the need and funding have been confirmed based on previous tests.



- Establish technical cooperation with the Matrix Foundation and other authorities within the EU.

***Support materials and guidance:***

- Publish the first version of common guidelines and principles for federation.
- Develop a governance model for technical configuration, secure federation, and coordination.

***Procurement and framework:***

- Produce support material for technical requirements in procurements.
- Establish a reference environment that other authorities can use for testing and verification.

***Risks to consider:***

- Lack of clear support materials and technical support can make implementation difficult.
- Inadequate configuration can lead to unintentional exposure of metadata.
- Federation nodes risk being placed in clouds outside the EU, which conflicts with the goal of digital sovereignty.
- Progress may be slow due to limited access to human resources.
- Lack of key competence can delay work on guidance and guidelines.
- Underestimating the need for security assessments and legal consultations can cause delays.
- Time-consuming management of data protection agreements between federated parties.
- Difficulties in identifying legal obstacles to joint operation and division of responsibilities in advance.

## **2028 – Expansion and operational maturity**

**Purpose:** Build on a functioning federation cluster and scale out incrementally

Assumes that the pilot projects in 2026–2027 have been evaluated positively, and that eSam has decided on a long-term governance model.



### ***Competence supply:***

- Start initiatives for skills provision, such as workshops, code sharing and needs assessments.
- Ensure that workgroups are staffed with cross-functional teams where technical specialists collaborate with business representatives.
- Introduce structures for continuous learning: documentation, training and collegial forums.
- Establish national forms of collaboration around skills sharing, support and further development.

### ***Technical planning:***

Define a technical roadmap for E2EE (end-to-end encryption) and MLS (Message Layer Security) in Matrix.

- Specify requirements for identity management, federation, and client functionality.
- Begin trust management, including certificate management systems.
- Identify any functional gaps based on the common needs of the authorities.

In parallel, a governance model for trust should be established – with rules for certificate management, incident management and a national policy for the security of the federation. The model needs to function both technically and organizationally, with a clear division of roles between participating authorities and central coordination.

### ***Connection of more authorities:***

- Coordinate joint requirements dialogue around functionality, security and usability.
- Develop onboarding packages for different sectors.

### ***Improved functionality and support:***

- Continue joint demands towards the Matrix protocol.
- Develop training packages, walkthroughs, user support and manuals for IT operations.

### ***International collaboration:***



If given the opportunity, contribute to European initiatives within the federation, e.g. via DINUM (France) or OpenDesk (Germany) and towards the EU Commission.

***Communication and change management:***

Implement a national training initiative.

Establish a helpline and an "Ask the Federation" service for guidance.

***Risks to consider:***

- Technical implementation risks becoming fragmented.
- Weak participation from sectors with high security requirements can create imbalances.
- It can be difficult to maintain trust between nodes without common routines.
- Increased dependence on a few federation nodes can create new vulnerabilities.

## **2029 – National scale-up**

**Purpose:** Establish federation as the standard for digital communication in the public sector

Assumes that:

- more authorities have joined in 2028
- the governance structure has been established
- Technical, legal and organizational models have been tested in practice.

***Full-scale implementation:***

- Expand the federation network based on functioning clusters.
- Begin phasing out any HUB solution for authorities that are now establishing their own federation capabilities.
- Integrate more identity solutions (for example, SITHS and eduGAIN).
- Ensure that technical implementation follows common standards to avoid fragmentation.



***Support for complex environments:***

Develop adaptation packages for municipalities and authorities with high security requirements.

Enable integration with existing platforms where federation is used in parallel, such as Microsoft Teams, so that organizations do not have to replace their current chat and communication tools (such as Teams), but the common federated protocol (Matrix) can coexist with existing systems. This can be done, for example, by:

- gateway solutions, where messages from the federation can be read and replied to in Teams
- parallel use, where some chats take place in Teams (internally) and others in the federation (cross-organizationally)

***National collaboration and governance:***

Formalize a governance model with clear roles for responsibility, supervision, support and management.

Establish processes for regular security audits.

Continue coordination with eSam, DIGG and other relevant actors.

***The national governance structure should also include:***

Certification of federated nodes

Compliance monitoring and incident management

Version management of specifications and supporting materials

A joint body for coordination and supervision

***Competence supply:***

Management and further development of the federation should take place in an open and learning structure.

Prioritize continuous skills development and technical innovation within the framework of a common infrastructure.

***Risks to manage:***

Transition from HUB to own federation occurs without sufficient local capacity.



Use of external cloud operations remains – risking violating the goal of digital sovereignty.

Delayed development of certification systems and governance models may delay scale-up.

## **2030 – Full interoperability**

**Purpose:** Federated communication is becoming the norm in the public sector.

If previous stages are implemented according to plan, 2030 could be the year when federated communications is fully established as a standard.

*The following characterize this stage:*

Chat, video and file sharing work seamlessly between all agencies.

End-to-end encryption is standard in all communications.

Sweden meets the EU's goal of 100% digital and interoperable public services in chat.

Management and further development take place continuously in open collaboration, both nationally and within the framework of European initiatives such as the Interoperable Europe Act (IEA) and the OpenID Foundation (OIDF).

**Competence supply:**

Management and development of the federation takes place in an open, learning structure.

There are clear processes for documentation, exchange of experiences and further training.

The public sector prioritizes continued skills development and technical innovation within the framework of a common infrastructure.

## **After 2030 – Joint management and continued development**

Once federated communication has become an established norm in the public sector, the work enters a new phase. The focus shifts from construction to long-term management, improvement and further development.

At this point, interoperability is expected to be a self-evident and integrated part of Sweden's digital infrastructure. The federated model is then a natural part of the national



interoperability architecture – in line with the EU's Interoperable Europe Act and the Swedish legislation proposed in SOU 2023:96.

Interoperability thus becomes not just a technical solution but a governing requirement for the public sector. It is crucial for:

- create a cohesive digital administration
- strengthen democratic control
- and build resilience along the entire threat spectrum.

The administration needs to ensure that:

- the technology is kept up-to-date and secure
- the solutions are user-friendly and accessible
- common regulations and standards are managed
- exchange of experience takes place both nationally and internationally

Through continued open collaboration, the public sector can not only meet future demands – but also lead the way. A common chat protocol is more than technology. It is a tool for digital self-determination, increased crisis preparedness and a more open public dialogue.

## About the consultation round

This timeline has been developed by the dSam4 working group and has been adjusted based on comments received during the consultation round in spring 2025. Actors such as Sunet, RISE, MSB, the Government Offices, Sambruk, Digg and the Internet Foundation have contributed important input.

For example:

**RISE** has emphasized the importance of skills development and learning management structures.

**Sambruk** has raised issues around trust, certificate management and technical coordination.



**MSB** has pointed to the need for security protection analyses and legal preparation for a national implementation.



# Appendix E – Principles for a federated chat solution in the public sector based on open protocols

This appendix describes principles for a federated chat solution in the public sector, based on open protocols. The focus is not on a single protocol, but on the technical, organizational and legal principles required to create an interoperable and controllable infrastructure between authorities. In practice, more principles in areas such as trust, security and usability would be needed. The aim is to give the reader an understanding of the benefits and consequences of an open protocol.

## Summary

Implementation and common principles are important to establish at an early stage to have a clear framework to follow in the establishment and development of solutions. It also provides a means to set requirements for open protocols and for suppliers who develop and offer services to the public sector.

Standardized open protocols, by their nature, provide both short-term and long-term benefits for the public sector. Continued work should ensure that fundamental principles for federated communication are agreed and decided.

These principles should serve as a support for governance, procurement and architectural decisions during the introduction of federated chat solutions in the public sector.

Example

### ***The solution should be assignable by a central actor***

**Description:** A central actor should be able to specify the common protocol to ensure interoperability and promote collaboration between different platforms and systems.

**Justification:** By following a common protocol, authorities can communicate seamlessly with others, both within and outside the public sector, while avoiding lock-in to individual providers.



### **Consequences:**

- Governments must adopt and implement chat solutions that support a commonly adopted open protocol.
- Introduction of proprietary protocols is limited and supplemented with bridging solutions.
- Procurement of chat solutions is required to support the designated protocol.

### ***Avoid vendor lock-in***

**Description:** The protocol should help avoid supplier lock-in and encourage a diversity of suppliers with different business models.

**Justification:** Supplier lock-in leads to inferior solutions and the risk of dependencies that negatively affect information concentration and costs.

### **Consequences:**

- Agreements should be structured to ensure that authorities can easily change suppliers without it entailing extensive work.
- Interoperability with solutions from multiple suppliers should be prioritized in procurement requirements.
- The protocol and its specifications should be freely available and can be implemented in open source solutions.

### ***Support bridge solutions for legacy systems***

**Description:** Chat solutions without support for the designated protocol should be supplemented with bridge solutions to enable communication between actors. The responsibility for being compatible with other solutions falls on the one that does not support the common protocol.

**Justification:** Many public authorities may already have existing communication platforms or systems that need to remain operational during the transition to a new solution. By making those who do not adhere to the common protocol responsible for their own interoperability, incentives are created to migrate.



### **Consequences:**

- The protocol must be able to be used to create bridge solutions with other systems.
- Compatibility with older systems may incur additional installation and maintenance costs.

### ***Support security features for wide application possibilities***

**Description:** The need to interact between authorities encompasses a large number of information classes and a designated protocol needs to include security features that enable as many use cases as possible.

**Justification:** Given the diversity of communication within and between authorities, chat solutions must meet high security requirements to enable different types of collaboration.

### **Consequences:**

- The protocol must support end-to-end encryption.
- Possible to use different identity solutions for user information.
- Chat solutions should collectively undergo regular security audits and tests.

### ***Clear and secure identity management***

**Description:** The protocol should have a robust system for managing user identities across the federated network. This includes mechanisms for creating, authenticating, and managing user accounts and devices.

**Justification:** Clear identity management is crucial to ensure that communication occurs with the right people and has a high degree of trust.

### **Consequences:**

- The protocol should support various forms of identity sources and standards

It is important to distinguish between authentication and federation. Protocols such as OpenID Connect (OIDC) offer authentication solutions, but do not have built-in support for federation. To enable federation, an add-on is needed, such as OpenID Federation (OIDF), which is still under development but has great potential for the



public sector. A future solution should therefore be based on an architecture that is compatible with both national and European identity federations.

### ***Support for federation***

**Description:** The protocol should have built-in support for federation. Functions and capabilities offered as standard in the protocol should work across a federation.

**Justification:** Authorities need to manage demands for resilience, robustness, and the freedom to choose delivery and collaboration methods. This is especially important in the context of total defense and civil preparedness, where communication must function even under stress and without dependence on external platforms.

### **Consequences:**

- The protocol should support federation
- The protocol should have security functions where authorities can control how a federation is implemented, who/what federations are implemented with, and what is allowed to happen over the federation.

### ***Standard compatibility with European digital strategy***

**Description:** The federated chat solution will be designed in line with European regulations and initiatives such as the Interoperable Europe Act, NIS2 and the Cyber Resilience Act.

**Justification:** European legislators are demanding open, secure and interoperable public services. By following this framework, Sweden can ensure legal compliance and future security.

**Consequences:** The solution should be compatible with European identity services, security frameworks, and federation technical specifications.

### ***Common trust model and governance***

**Description:** The federated network needs a trust model that governs how parties are authenticated, how certificates are managed, and how incidents are reported.



**Justification:** A functioning federation requires that all participating parties trust each other's identities and that there are common procedures in case of deviations.

**Consequences:** Requires establishment of national governance, rules for certificate management and procedures for incident reporting.

This document has been produced by the dSam4 working group; with input from, among others, Sunet, RISE, Digg, Sambruk, MSB and the Internet Foundation.



# Annex F - Application of the Matrix Protocol within the European Union

## Introduction

The main report and appendices to this report describe various possible open protocols. Given that the Matrix protocol has gained increased use and has begun to be implemented within the EU, we see a value in delving into the Matrix protocol through this appendix. For information on other protocols and applications, please refer to “Appendix\_A\_External\_Monitoring” and “Appendix\_B\_Technical\_Comparison\_of\_Protocols”.

## Summary

The Matrix protocol is rapidly gaining traction in the European Union, as confirmed at the Matrix conference in Strasbourg in October 2025, especially in the public sector. Even the EU Commission itself is evaluating the use of the Matrix protocol. This development is primarily driven by the need for communication solutions that are secure, decentralized, interoperable and respect digital sovereignty. Member States such as Germany and France have taken a leading role in implementing Matrix in various areas of public administration.

**EU directives and regulations**, such as NIS2 and DMA, are expected to further accelerate the adoption of protocols like Matrix by emphasizing the importance of secure and interoperable communication. An active open source community and EU-funded initiatives are continuously contributing to the development and improvement of the protocol.

**Matrix has an interesting future within the EU**, the protocol's ability to provide a secure, open and federated communications infrastructure creates the conditions to meet the growing demands for interoperability, digital sovereignty and security within the Union. Efforts within the EU should focus on the economic benefits of adopting open communications standards such as Matrix in the public sector as well as the challenges of large-scale federated deployments across different administrative structures within the EU.



## Introduction to the Matrix Protocol

The Matrix protocol is an open network/protocol for secure and decentralised communications. Its primary purpose is to enable seamless communication between different service providers, in a similar way to the standard SMTP (Simple Mail Transfer Protocol) protocol for email. This means that users with accounts at one communications service provider can communicate with users at another in a standardized way.

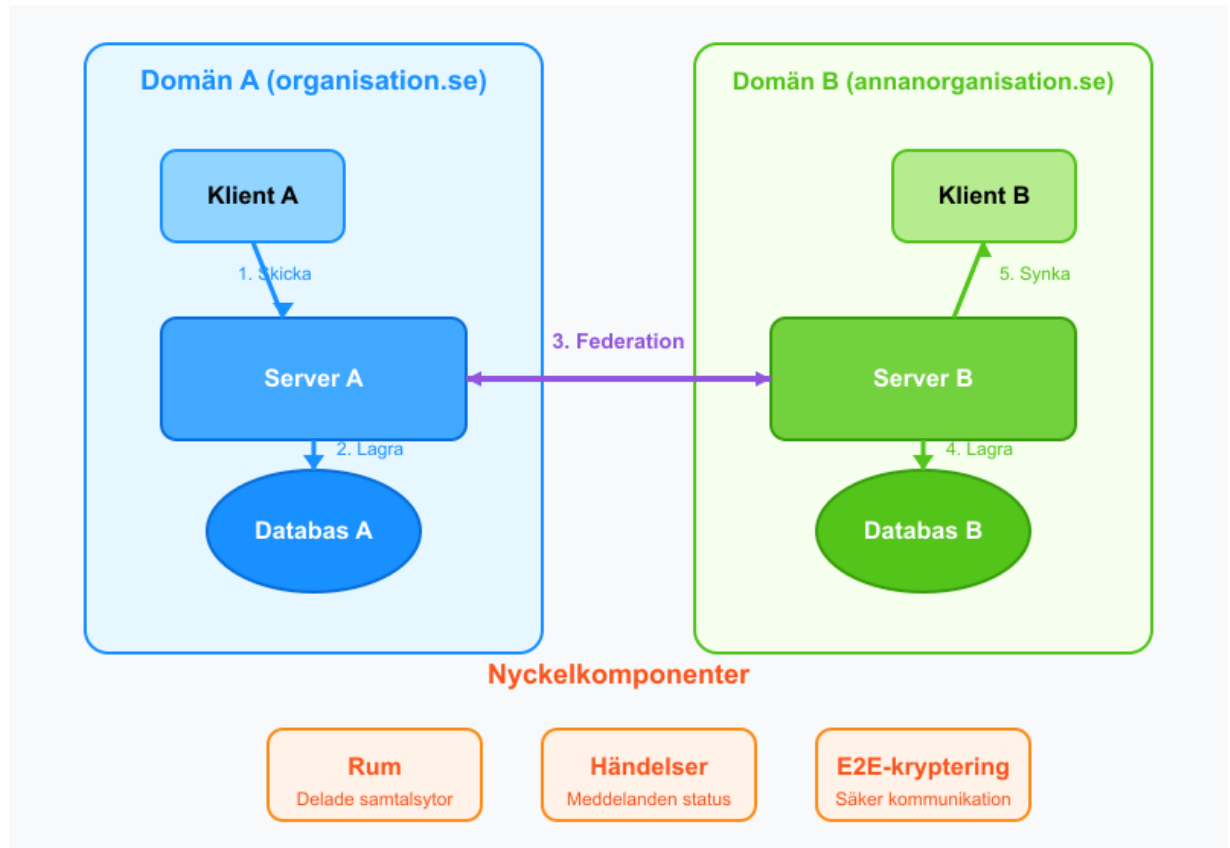
Matrix is designed for a variety of use cases, including Voice over IP (VoIP), Internet of Things (IoT) and instant messaging, as well as group communications. A key aspect of the protocol is its support for security and data replication, ensuring that complete conversation history is preserved without any single checkpoints or risk of system failure.

Several important features make Matrix particularly interesting for use within the EU, and especially in the public sector:

- **Decentralization and Federation:** Matrix allows organizations to run their own servers (“on-prem”) and maintain full control over their data, while still being able to communicate with users on other servers. This meets the EU’s drive for digital sovereignty.
- **End-to-End Encryption (E2EE):** The protocol offers built in E2EE (including through the Olm and Megolm libraries, which implement the Double Ratchet algorithm). This ensures that only participants in a room can read the messages.
- **Interoperability:** Through so-called bridges, Matrix can be connected to other communication platforms such as Slack, Teams and XMPP-based solutions, which facilitates unified communication across different systems.
- **Open Standard and Open Source:** Matrix is an open standard with available open source implementations. It promotes transparency, auditability, security, and community-driven development.



Table1- Visualization of federation between two domains or organizations



The increasing importance of decentralization and E2EE directly responds to the growing demands for data protection and security within the EU. This makes Matrix an attractive alternative to more centralized and proprietary communication platforms/protocols. The EU has actively promoted digital sovereignty and data protection through initiatives such as the GDPR. Matrix's fundamental design principles align with these goals by giving organizations control over their communication infrastructure and ensuring data protection through strong encryption.

Technically, the Matrix protocol is an application-level communications protocol that uses HTTP APIs and provides open-source reference implementations for secure distribution and storage of messages in JSON format over an open federated network.



## Attention at the political level

The Matrix protocol is also receiving high-level attention within the EU institutions. The draft of the "Cyber Blueprint - Proposal Council Recommendation" mentions a recommendation to use Matrix for government-to-government communication on cybersecurity issues. The EU Council recommendation may lead to future official projects involving the protocol, considering it for secure communication between public services in a critical area such as cybersecurity. The EU Council's focus on cybersecurity communications underlines the importance of secure channels at the highest levels of EU governance. The recommendation of Matrix, an open and auditable protocol with strong encryption, suggests a strategic direction towards using such technologies for sensitive communications within the EU.

The political will is strengthened by the fact that the EU Commission has carried out a "Proof of Concept" on a Matrix-based app (Element) after seeing other countries (such as France, Germany and Sweden) using Matrix. The goal is to create a secure, state-owned communication platform for member states where they own the data themselves and offer complements to Microsoft Teams and can replace apps such as Signal.

Similar dialogues are taking place in the United States, where senators have sent a call to the departments to apply the Matrix protocol to protect information being communicated.

## Technical architecture and implementation within the EU

A typical Matrix deployment involves client applications communicating with servers via HTTP APIs. The servers then federate with each other to replicate data in so-called rooms. Communication occurs in these virtual rooms through the exchange of events, which are the basic data unit of the protocol. Matrix uses an eventual consistency model for data replication.

Within the EU context, several architectural aspects are particularly important:

**Security:** End-to-end encryption with Olm/Megolm, HTTPS for federation, and server signing and message integrity are key security features.

**Interoperability:** The use of an open protocol for federation, bridges to connect to other systems, and other platforms is essential to facilitate communication across different technological environments.



**Scalability and High Availability:** Professional backend solutions like Element Server Suite offer features to manage large installations and ensure continuous operation.

**Data sovereignty:** The decentralized nature allows organizations to store their data within the EU borders, which is important for meeting the requirements of GDPR and other data protection regulations.

Matrix design as a protocol is crucial for the multifaceted landscape of the EU public sector, where different Member States and institutions have varying requirements for security, interoperability and data management. The open-source code is important for transparency, the possibility of security audits and to promote innovation within the EU digital ecosystem.

This is exemplified by the fact that specific implementations such as BwMessenger, TI-Messenger and Tchap have their own architectural features and customizations. For example, TI-Messenger integrates electronic health records and a FHIR directory. There are also initiatives such as CoMatrix that aim to enable the use of Matrix on limited IoT devices. The ability to customize and extend the protocol, as seen in implementations such as TI-Messenger with its healthcare-specific integrations, increases its value for specialized applications.

There are also several different client applications for Matrix, such as Element, FluffyChat, Cinny and others, developed by both commercial players and the community.

For more examples, see “Appendix\_A\_External\_Monitoring”.

## **How is the development of the matrix protocol funded?**

At the heart of the Matrix protocol's governance is The Matrix.org Foundation, a UK-based non-profit organization (Community Interest Company). The Foundation's primary mission is to act as a neutral guardian of the Matrix standard and ensure its continued development as an open and unfragmented communications network.

Historically, the company Element (formerly New Vector), founded by the Matrix creators, has been a major financier. Element employs a large portion of the core developers and has raised significant capital) as well as generating revenue from services such as Element Matrix Services (EMS).



The Matrix Foundation has since around 2022-2023 intensified its own fundraising. This includes memberships, donations, corporate sponsorships or grants. A relatively common solution for larger organizations to contribute to the ecosystem is either through code or financial support, thus counteracting the "Commons' Dilemma" - many use the protocol but a limited number of organizations contribute financially.

The reference implementations for Matrix servers - (Synapse and Dendrite) - are under AGPLv3, which means that an end user who modifies the servers must share the changes. Alternatively, there is also the option to purchase a commercial license from Element and thus support the further development of the matrix protocol.

Finding sustainable and equitable funding models that balance the benefits of transparency with the commercial realities of a growing ecosystem is crucial. The future of the Matrix protocol and its ability to continue to function as a free, secure, and decentralized communications alternative depends largely on whether its community and the organizations that benefit from it collectively can solve this central financial challenge. It will continue to require collaboration, transparency, and shared accountability.

## Technical maturity and risks

Matrix has reached a significant level of maturity since version 1.0 was released in 2019. Regular specification updates, an active ecosystem of clients and servers (with Synapse as the established reference implementation and Dendrite as a promising alternative), and ongoing work on Matrix 2.0 demonstrate a dynamic and forward-looking project. Public sector adoption in several European countries underscores the confidence in the protocol's capabilities.

The Matrix protocol, and especially its federation mechanisms, can be considered complex to implement on the server side. This complexity is partly a consequence of the design choice to have decentralized rooms, where each participating server maintains its own copy of the room's state and history. Compared to protocols such as XMPP, which have traditionally used more centralized room controls (although decentralized MUCs have been discussed), the Matrix design poses greater challenges for server and app developers.

The Matrix protocol's federation model, where independent servers communicate with each other to create a cohesive network, is one of its core strengths. However, it also



brings with it specific risks and operational challenges that must be considered. Perhaps the most obvious risk in a federated system is the reliance on administrators for an organization's federation node. A malicious or compromised server poses a threat to its own users and potentially to other servers it federates with. Risks include eavesdropping/tampering, unauthorized access to chat rooms, key tampering. End-to-end encryption (E2EE) provides some protection but does not address all risks.

A single server with poor performance can have a major negative impact on the broader user experience, which is a risk over which individual users and server administrators have limited control (other than possibly blocking federation with problematic servers).

Authorities will need to accept a higher degree of technical and administrative complexity, operational costs, as well as the specific security and operational risks that are strongly associated with the federation model.

## **Open source and community-driven initiatives within the EU**

Matrix is open source, and there are several implementations based on the Matrix protocol available. The Matrix.org Foundation plays a central role in the maintenance and development of the protocol.

Within the EU, there is an active community contributing to the development and use of Matrix; Fairkom offers a Matrix server and has been involved in Schulchat RLP, a messaging solution for schools in Rhineland-Palatinate. At the Matrix Conference 2024, several community projects and discussions were presented, including "Polychat - Interoperability for the masses" and analyses of the Matrix ecosystem.

At the European Open-Source Awards, Amandine Le Pape, co-founder of Element and Matrix.org, was awarded the Business & Impact Award, underscoring the importance of the Matrix protocol in the open-source field within the EU.

The open-source community around Matrix within the EU is a crucial part, driving innovation, providing diverse client options, and contributing to the robustness and security of the protocol through public review and collaborative development. Matrix's open nature encourages participation and contributions from individuals and organizations across the EU and the world. This collaborative environment leads to a faster pace of innovation, the development of solutions tailored to specific European needs, and a higher level of trust in the technology due to its transparency and auditability.



## Matrix Conference 2025

The second conference of its kind – the first was in Berlin in September 2025, was held in Strasbourg from 15-18 October 2025. The interest and participation were high and many of the presentations were delivered by representatives from the public sector. The conference marked a clear turning point where Matrix went from being a “niche” technology to becoming the backbone of digital sovereign communication in Europe, especially in the public sector and healthcare.

A few of the talks during the “Public Sector”-track

- **Trialing Matrix within the European Commission** - The European Commission is testing Matrix to replace Signal and Teams for more secure, self-directed communication.
- **BundesMessenger** - Several presentations were about Germany's massive investments in the matrix protocol. For example, how they are consolidating the country's administrative communication into a common Matrix architecture.
- **France's "Tchap"** - France was early with its chat solution Tchap, now they are working on opening up private federations in a secure way to be able to communicate more broadly.
- **Luxembourg government and citizen app** - The state provides a chat solution for the public sector (“from firefighter to politician”) and also offers a separate app for private individuals
- **Sweden's public sector** - Försäkringskassan and eSam presented their journey towards a secure and interoperable collaboration platform (SAFOS) and a common open federation protocol for the Swedish public sector

Healthcare and school

- **74 million users in Germany (TI-Messenger)** - Gematik gave a talk about the rollout of TI-Messenger, which will connect the entire German healthcare system. This is probably the world's largest Matrix project.
- **SchulchatRLP (School Chat)** – An example where an encrypted messaging service has been rolled out to half a million students in Rhineland-Palatinate.



All talks were recorded and can be viewed afterwards via [Matrix Conference 2025 :: pretalx](#)

This appendix has been updated based on reviews from RISE, Sambruk, DIGG, MSB, Sunet and the Internet Foundation during the consultation round in spring 2025.



Recess

Matrix (protocol) - Wikipedia,[https://en.wikipedia.org/wiki/Matrix\\_\(protocol\)](https://en.wikipedia.org/wiki/Matrix_(protocol))

Matrix | Germany | Digital sovereignty - Elements,<https://element.io/matrix-in-germany>

Matrix | Germany | openDesk | ZenDiS - Elements,<https://element.io/matrix-in-germany/projects/opendesk>

Matrix.org,<https://matrix.org/>

Watch The Matrix Conference's talks - Matrix.org,<https://2024.matrix.org/watch/>

Blog - Matrix.org,<https://matrix.org/blog/>

The European Union must keep funding free software -  
Matrix.org,<https://matrix.org/blog/2024/07/17/ngi-open-letter/>

Next Generation Internet Discovery and Search | NGI Search | Project | Fact sheet |  
HORIZON | CORDIS | European  
Commission,<https://cordis.europa.eu/project/id/101069364>

European Commission cuts funding support for Free Software  
projects,<https://edri.org/our-work/european-commission-cuts-funding-support-for-free-software-projects/>

Next Generation Internet Zero | Association for Progressive  
Communications,<https://www.apc.org/en/project/next-generation-internet-zero>

The NGI Initiative: An Internet of Trust,<https://ngi.eu/about/>

Elm Matrix SDK - NLnet Foundation,<https://nlnet.nl/project/Elm-Matrix-SDK/>

Fractal | Next Generation Internet,[https://ngi.eu/funded\\_solution/fractal/](https://ngi.eu/funded_solution/fractal/)

Security & Defence European,[https://euro-sd.com/wp-content/uploads/2024/08/ESD\\_8\\_2024\\_BAAINBw\\_WEB.pdf](https://euro-sd.com/wp-content/uploads/2024/08/ESD_8_2024_BAAINBw_WEB.pdf)

Matrix | Germany | BwMessenger | Bundeswehr -  
Elements,<https://element.io/matrix-in-germany/projects/bwmessenger>



BundesMessenger: shared, reused and interoperable.,<https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/bundesmessenger-shared-reused-and-interoperable>

TI Messenger | gematics | Matrix | German healthcare - Elements,<https://element.io/solutions/ti-messenger-gematik-matrix>

tim+: The TI Messenger from Arvato Systems,<https://www.arvato-systems.com/industries/industries-overview/healthcare-pharma/ti-messenger>

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](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)

The TI Messenger: Advancing Secure Healthcare Communication with Matrix - Jan Kohnert,<https://www.youtube.com/watch?v=MoA2cYfHlyA>

Matrix Specification,<https://spec.matrix.org/>

CoMatrix,<https://comatrix.eu/>

fairmatrix - Fairkom,<https://www.fairkom.eu/en/fairmatrix>

Matrix of EUPL compatible open source licenses | Interoperable Europe Portal,<https://interoperable-europe.ec.europa.eu/collection/eupl/matrix-eupl-compatible-open-source-licences>

EU celebrates open source excellence | Science | Business,<https://sciencebusiness.net/news/eu-celebrates-open-source-excellence>

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

The NIS 2 Directive | Updates, Compliance, Training,<https://www.nis-2-directive.com/>

NIS2 Requirements | 10 Minimum Measures to Address - The NIS2 Directive,<https://nis2directive.eu/nis2-requirements/>



Cyber Resilience Act (CRA) | Updates, Compliance, Training,<https://www.european-cyber-resilience-act.com/>

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>

Cyber Resilience Act - Shaping Europe's digital future - European Union,<https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

Policy and regulation update 2024: Matrix and the GDPR,<https://matrix.org/blog/2024/06/regulatory-update/>



## Appendix G - Economic benefits and benefits of open chat protocols

The choice of communication technology is a strategic decision point with far-reaching consequences for the efficiency, economy, security and digital sovereignty of the public sector. In an era where demands for digitalisation, accessibility and efficiency are continuously increasing, the need for modern, flexible and secure communication solutions is becoming increasingly prominent. E-government aims to improve the quality and accessibility of public services, while reducing costs and strengthening the transparency of administration. A key prerequisite for realising these goals is interoperability – the ability of different systems and organisations to exchange information and interact smoothly. Interoperability has been identified as a crucial factor for the efficient provision of European public services and for strengthening the internal market. This underlines the importance of choosing open chat protocols that actively promote, rather than passively hinder, such interaction.

The choice of a common chat protocol is therefore not only a technical decision, but a policy decision that affects the public sector's ability to fulfil its core missions and adapt to future challenges. The public sector has a broad and complex mission that requires effective communication, both within authorities and externally with citizens and businesses. Proprietary systems, often controlled by individual suppliers, can lead to limitations in flexibility and interoperability, which makes it difficult to develop a coherent digital administration. Open protocols, on the other hand, by their very nature offer greater opportunities for adaptation, vendor independence and collaboration. Consequently, the type of protocol is directly linked to how well the public sector can steer its digital development, collaborate effectively and avoid costly and restrictive lock-in effects.

This appendix analyses the economic benefits and broader public sector benefits of choosing an open protocol for chat federation, compared to proprietary alternatives.

### Chat federation and protocol types

In order to assess the economic and strategic benefits of different approaches to digital communication, it is necessary to first understand the basic concepts of federated communication and the different characteristics of open and proprietary protocols.



### *The core concept of federated communication*

Federation, in the context of digital communications, describes an architecture where independent systems or servers have the ability to communicate and exchange information with each other. More specifically, federation is defined as a way for different instances of a service, such as a chat service, to be connected so that users can collaborate and communicate across organizational boundaries.<sup>3</sup>This is of particular relevance to the public sector, where a variety of authorities, municipalities, regions and other units need to collaborate effectively.

Distributed instant messaging services can be established through federation, which enables communication between users connected to different service instances.<sup>3</sup>A common analogy is the email system, where users on different domains (e.g., different organizations' email servers) can send and receive messages seamlessly, despite using different technical implementations underneath the surface.<sup>4</sup>This contrasts with centralized systems, where all communication and data management typically occurs through a single provider's infrastructure and control.

Federation is an architectural prerequisite for achieving a balance between autonomy for individual organizations on the one hand, and interoperability and seamless communication between them on the other. Public organizations often have specific and legitimate requirements regarding security, data storage, regulatory compliance, and internal governance of their communications. Centralized systems can force all connected parties to adapt to a standardized model dictated by an external provider, which can potentially conflict with these individual organizational requirements. Federation, on the other hand, allows each organization to operate and administer its own server or service instance, if desired.<sup>5</sup>This means that the organization can retain control over its own data, security policies, and technical environment. At the same time, the federation protocol ensures that communication between these autonomous entities can take place in a standardized and efficient manner. The implication is that a federated model is often better suited to the heterogeneous and somewhat autonomous nature of public organizations than a strictly centralized model can offer.

### **Economic benefits of open protocols for chat federation**

The choice between open and proprietary protocols for chat federation has direct and significant economic consequences for the public sector. An analysis of these consequences extends beyond initial acquisition costs and includes the total cost of ownership over time, the effects of licensing models, the risk of vendor lock-in, and the impact on market dynamics and competition.



### ***Reduced direct costs and avoidance of licensing fees***

One of the most immediate and tangible economic benefits of choosing open protocols and open source is the ability to greatly reduce or completely avoid the direct costs associated with licensing fees. However, it is of great importance that public organizations still contribute in various ways, with resources or money, to the maintenance and further development of open solutions. Proprietary protocols, especially those aimed at large organizations, often entail significant licensing costs that can be based on the number of users, number of servers, specific features or annual subscriptions.<sup>3</sup>

For the public sector, which often handles large volumes of users (employees, citizens, students, etc.) and operates extensive IT systems, these licensing costs can accumulate to considerable amounts. By choosing solutions based on open source, where the source code is freely available and use is rarely subject to expensive licensing fees, organizations can achieve direct and significant savings.<sup>3</sup> This is particularly beneficial for organizations with limited budgets, a situation that is not uncommon in many parts of public administration.

The savings from eliminated or greatly reduced licensing costs are not just a passive reduction in expenses. These freed up funds represent an active opportunity for the public sector. They can be reinvested in core operations, used to finance urgent innovation, or allocated to adapting and further developing the open solutions to better meet specific local or national needs. The funds can also be used to strengthen their own IT competence and reduce dependence on external consultants. In this way, the choice of open protocols and open-source code can create a positive economic dynamic, where initial savings drive further value creation and improve the public sector's ability to deliver services efficiently.

### ***Vendor lock-in and its economic consequences***

Vendor lock-in is a phenomenon where a customer becomes so dependent on a specific supplier's products or services that the cost or difficulty of switching to an alternative supplier becomes disproportionately high or even insurmountable.<sup>15</sup> Proprietary protocols and the closed ecosystems often create a common cause of such lock-in. When an organization chooses a communications platform based on a proprietary protocol, it often becomes dependent on that single vendor for critical support, necessary updates, future development, and maintenance.<sup>3</sup>



The economic consequences of vendor lock-in, where all agencies choose the same vendor for cross-agency collaboration, can be extensive. When a vendor has a customer in a locked-in situation, their bargaining power is drastically reduced. The vendor, aware of the customer's limited options, can then raise prices, change licensing terms in an unfavorable way, or force expensive upgrades on the customer without much risk of losing the deal.<sup>15</sup> This can lead to unforeseen and escalating costs over time, which is particularly problematic for the public sector, which must plan long-term and responsibly with tax funds.

Open protocols actively counteract vendor lock-in.<sup>14</sup> By being based on standardized and freely available specifications, they enable multiple vendors to develop compatible products and services. If an organization is not satisfied with its current vendor, or if the vendor's pricing becomes unreasonable, there is the option to switch to another vendor that offers a solution based on the same open protocol, without having to replace the entire underlying technology stack. This maintains healthy competition in the market and strengthens the public sector's position as a customer. The choice of open protocols is therefore a proactive measure to ensure sound financial management and avoid becoming hostage to the business interests and pricing strategies of a single commercial actor. It is not only about avoiding direct costs, but also about preserving strategic flexibility and control over one's own digital infrastructure.

### ***Promoting healthy competition and market dynamics***

The use of open protocols in the public sector has the potential to act as a powerful catalyst for a more dynamic and competitive market for IT solutions. When public organizations standardize their communication around open, well-documented and non-discriminatory protocols, the conditions are created for a broader and more diversified supplier market, which ultimately benefits the public sector as a major procurer.

Open standards are designed to enable compatibility (interoperability) between products and services from different manufacturers.<sup>9</sup> This means that if the public sector, or a significant portion of it, agrees to use a specific open federation protocol for chat and collaboration, different agencies and organizations can choose the client applications and server services that best suit their unique needs and budgets, while maintaining the ability to communicate and collaborate seamlessly with each other.<sup>3</sup> This creates a market where suppliers compete on equal terms based on quality, functionality, service and price, rather than on lock-in effects created by proprietary technologies. Such increased competition has a direct positive impact on pricing and can lead to significant cost savings for the public sector. As previously mentioned, it is estimated that even a relatively small improvement in price relative to performance, driven by increased



competition in the software area, can result in annual savings of hundreds of millions of kronor for large public sector purchasers.<sup>15</sup>

By actively requesting and specifying solutions based on open protocols in their procurements, the public sector can act as a significant market shaper. The public sector is often the largest single buyer of IT products and services in a country.<sup>16</sup> When this large purchasing power is directed towards open solutions; a clear signal is sent to the market that there is a significant and long-term demand for such products and services. This not only encourages established suppliers to adapt their offerings, but also lowers the barriers to entry for new and smaller players, including local SMEs, to develop and offer compatible solutions. A broader and more diversified supplier base not only increases competition, but also reduces dependence on a few large, often global, technology suppliers. This can have positive spillover effects on the national economy by stimulating local innovation, skills development and employment in the IT sector. The public sector thus moves from being a passive consumer of technology to becoming an active and strategic player shaping the market to its own benefit and that of society.

## **Benefits**

In addition to the direct financial savings, choosing open protocols for chat federation brings a number of significant strategic benefits for the public sector. These benefits range from improved collaboration and innovation capacity to strengthened security, increased resilience and secured digital sovereignty.

### ***Improved interoperability and seamless collaboration***

Interoperability is a fundamental prerequisite for a modern and efficient public administration. Open, federated protocols play a key role here in breaking down the communication silos that often exist between different authorities, levels of administration and even within individual large organizations. Open source and open standards are often highlighted as important components for ensuring interoperability and data portability in the digital infrastructure.<sup>8</sup>

Full interoperability, enabled by open federated protocols, transforms collaboration from a recurring technical challenge to a strategic opportunity. The public sector consists of a diverse set of organizations – municipalities, regions, state agencies – all of which have a need to exchange information and coordinate efforts.<sup>20</sup> Lack of interoperability inevitably leads to inefficiency, information silos, duplication of effort<sup>19</sup> and fragmented service delivery, which ultimately affects citizens and businesses. Open federated protocols create a common technical foundation, making it technically easier for different systems



to "understand" each other and exchange data in a meaningful way.<sup>2</sup> When the technical barriers to communication are lowered, organizations can instead focus their resources and attention on what they need to collaborate on and why, rather than on the technical details of how to make their systems work together. This enables more agile, flexible and effective forms of collaboration, which is invaluable when, for example, managing societal crises, in complex care chains involving multiple healthcare providers, or when handling cases that span multiple agency boundaries. Investments in open federated communication solutions are therefore fundamentally investments in a more cohesive, capable and responsive public administration.

### ***Catalyst for innovation, adaptability and local development***

Openness in protocols and associated software provides a unique freedom to adapt, modify and build upon existing solutions. This creates a fertile ground for innovation that can be tailored to meet the specific and often unique needs of the public sector, rather than being limited by the standardized offerings that dominate the proprietary market. Open source has been shown to significantly increase the pace of innovation by enabling different actors to co-develop, share knowledge, adapt solutions and build on each other's work.<sup>17</sup> This leads to increased flexibility and adaptability, which is critical in a changing world.<sup>3</sup>

The ability to freely adapt and tailor software to specific business needs and workflows is one of the main advantages of open source.<sup>3</sup> The public sector often has complex and legally-driven processes that are not always easily captured by generic commercial products. With access to the source code, public organizations can, either with their own staff or by hiring local developers, create extensions, integrations or completely new functions that are optimized for their needs. This not only promotes the development of more appropriate tools, but can also stimulate local IT skills and business. The public sector can also collaborate on the development of common digital solutions and standards, which can lead to economies of scale and the avoidance of duplication.<sup>22</sup> The European Commission has highlighted the macroeconomic potential of this, noting that an increase of just 10% in contributions to open-source development within the EU could generate an increase in EU GDP of 0.4–0.6%, which represents significant sums.<sup>17</sup>

Open protocols and open source can be said to democratize the innovation process by lowering the thresholds for participation. Unlike proprietary systems, where the development agenda and product cycles are driven by the commercial interests of the individual supplier and where adaptations can be expensive, time-consuming or even impossible, openness provides a different dynamic. The availability of source code and open specifications enables public organizations to, by themselves, or in collaboration



with others (including academia, the nonprofit sector, and local businesses), identify needs, develop solutions, fix bugs, or integrate systems in a way that directly addresses their challenges.<sup>3</sup> This creates an innovation model where the public sector can be proactive and driving, instead of being a reactive and dependent customer. The implication is that the public sector can access solutions that are better adapted to local conditions and the needs of citizens. At the same time, this can help build an "innovation commons", where improvements and new functionality developed by one actor can be shared and benefit other public organizations, promoting a culture of collaboration and knowledge sharing.<sup>3</sup>

### ***Strengthened information security, transparency and auditability***

A common misconception is that openness in source code and protocol specifications would pose a security risk. On the contrary, many experts and experiences argue that transparency and the possibility of broad review can lead to a higher level of information security. When the source code of a software or the specification of a protocol is openly available, it can be scrutinized in detail by a large and diverse group of developers, security experts and researchers around the world.<sup>3</sup> This collective review often leads to faster identification and remediation of potential vulnerabilities and security flaws, compared to closed systems where only the vendor's internal team has visibility.

Transparency itself can also contribute to increased trust in the software and its security.<sup>3</sup> Users and organizations are not solely dependent on the vendor's security claims, but have the opportunity to verify claims themselves (or have independent experts) and assess the level of security. However, it is important to emphasize that security does not only depend on openness per se, but also on an active and engaged ecosystem around the software that quickly addresses and fixes discovered problems.<sup>3</sup> Decentralized systems, of which federated communication systems can be a form, can offer additional security benefits by reducing the number of central attack points and giving organizations greater control over their own data and security configuration.<sup>24</sup>

For the public sector, which handles large amounts of sensitive personal data and is often responsible for critical digital infrastructure, the transparency and auditability that come with open protocols are a crucial trust factor and an important means of ensuring accountability. Proprietary systems often act as "black boxes", where the internal functioning and exact security mechanisms are not fully visible or verifiable to the customer. The public sector has a special and statutory responsibility for transparency and to be able to demonstrate how citizens' data is handled in a secure and correct manner. Open protocols and open-source code enable independent review of both code and protocol specifications.<sup>3</sup> This makes it possible to objectively verify security claims,



identify potential weaknesses and ensure that the system works as intended without hidden features. This possibility of independent verification is fundamental to building and maintaining citizens' trust in digital government and to be able to hold system providers accountable. The choice of open protocols is therefore not only a technical issue of security implementation, but also a democratic and trust-building measure. It also reduces the risk of undetected backdoors or unwanted data collection by the provider, which is an important aspect of data protection and privacy.

### ***Increased resilience, operational continuity and reduced dependence on individual actors***

Resilience, the ability of a system to withstand, adapt to, and recover from disruptions, is of paramount importance to public sector communications infrastructure. Decentralized and federated architectures, which are built on open protocols, are inherently more resilient to various types of disruptions and problems than centralized systems. A resilient information system is designed to withstand and quickly recover from disruptions and threats, thereby minimizing negative impacts and maintaining business continuity.<sup>26</sup>

Federated architectures offer improved fault tolerance and resilience because failures or outages in a single part of the network (e.g., a data center at a specific organization) do not necessarily lead to the entire communications system being down.<sup>27</sup> Because resources and data are often distributed across multiple independent but interconnected nodes, there is a form of natural redundancy built into the system.<sup>27</sup> A decentralized infrastructure reduces the risk of so-called "single points of failure" – individual critical points whose failure would paralyze the entire system.<sup>28</sup> While large-scale centralized cloud services can be very powerful and offer high availability and security, their centralized nature presents an inherent vulnerability if the central service suffers a major outage.<sup>28</sup>

The independence from individual vendors, which is a key advantage of open protocols, also contributes greatly to increased resilience.<sup>3</sup> If the public sector is dependent on a single proprietary provider for its ability to communicate across organizational boundaries, and that provider experiences technical problems, financial difficulties, ceases to provide a service/function, or is acquired by another company with different priorities, it can have serious consequences for our ability to communicate with each other. With open protocols, there is the possibility of switching to another provider that offers a compatible solution, or even for the organization itself, or in collaboration with others, to take over the operation or further development of the software. This creates a "collective resilience" that is difficult to achieve with a monolithic, proprietary solution controlled by a single actor.



By adopting open federated protocols, the public sector is building a communications infrastructure that is more robust, not only against technical failures and cyberattacks, but also against geopolitical tensions or commercial decisions by individual global technology providers that may affect service availability in a given country or region. This is crucial to ensuring the functionality and continuity of society, especially in times of crisis. The choice of open protocols thus strengthens the resilience of the national digital infrastructure, which is ultimately a matter of national security and the ability to maintain essential activities.

### ***Secured digital sovereignty and control over critical communications infrastructure***

Digital sovereignty is about a nation or organization's ability to have control over its own digital future – which includes the data, hardware, and software it relies on and creates.<sup>29</sup> It is a concept that aims to increase autonomy and reduce dependence on external actors, especially in an increasingly digitalized and globalized world.<sup>30</sup> For the public sector, digital sovereignty is not just a technical issue, but a fundamental aspect of national security, the protection of citizens' privacy and the ability to independently make decisions about their own digital infrastructure. Open protocols are an important prerequisite for the public sector to be able to exercise true digital sovereignty over its ability to communicate with each other.

Simply storing data within a country's geographical borders is not enough to achieve digital sovereignty; access to, and control over, the underlying technology and infrastructure is at least as crucial.<sup>31</sup> The use of foreign-based communication platforms may mean that sensitive data is stored or processed outside national control and jurisdiction. It may also mean that the platform's operation, security updates and future development are governed by the policies and business interests of an external commercial actor, which may not necessarily coincide with national or public interests for cooperation. This may create risks related to data protection (e.g. exposure to foreign legislation that allows government access to data for intelligence purposes), as well as a technological dependency that may be affected by geopolitical tensions or trade policy decisions.

Open standards and open source provide crucial independence from individual vendors, which is a cornerstone of digital sovereignty. Open protocols allow the public sector to decide for itself, or through providers of choice, where servers should be located, who should administer them, and how data should be handled in accordance with national legislation and its own policies. They also enable the development and adaptation of its own, nationally or locally adapted client applications and server implementations, which provides a deeper level of control and understanding of the technology used.<sup>32</sup> This



provides tangible and verifiable control over the digital communications infrastructure, which is at the core of the concept of digital sovereignty. The EU has also identified digital sovereignty as a key strategic objective and is actively working on regulations and initiatives to promote the development and use of European digital solutions and standards.<sup>29</sup>

The choice of open protocols for federated chat is thus a concrete expression of a quest for digital sovereignty. It gives the public sector the power to define and control its own communication channels, free from foreign or commercial dependencies that could potentially conflict with national interests or fundamental democratic values. This choice strengthens the nation's ability to protect the privacy of its citizens, ensure robust and reliable information flows even during crises, and avoid becoming a passive pawn in the game between global technology giants.

## Open or Proprietary

When the public sector is faced with the choice between common open and proprietary protocols, it is important to weigh the unique requirements, responsibilities, and principles that govern public operations. The previously discussed economic benefits and strategic benefits take on particular weight in this context.

Public procurement is a process surrounded by stricter regulations and higher requirements for transparency, non-discrimination and equal opportunities for all suppliers than is often the case in the private sector.<sup>32</sup> Open standards and protocols can facilitate this process by providing clear, well-documented and non-discriminatory technical specifications that can be used as the basis for procurement documents. This promotes fair competition. In contrast, situations can arise where a dominant supplier of a proprietary system effectively "sets" the terms and conditions and advocates its own end-to-end solutions, which can limit competition and lead to lock-in.<sup>33</sup> If a public organization tries to integrate a proprietary system with solutions based on open protocols, and this has not been required correctly from the beginning, the risk and cost of any integration problems may end up with the system owner (the public organization) rather than the provider of the proprietary system.<sup>33</sup>

The Swedish Digital Governance Agency (DIGG) has emphasized in its guidelines the importance of openness – including open data, open APIs, open software and open standards – as a fundamental principle for the development of a common and cohesive digital governance.<sup>34</sup> This underlines a national strategic direction that harmonizes well with the benefits of open protocols.



The inherent transparency and non-discriminatory nature of open protocols align better with the public sector’s fundamental principles of openness, accountability and promotion of fair competition than do the often closed, vendor-controlled and commercially driven proprietary alternatives. The public sector operates under laws and principles that require transparency in decision-making processes and the responsible use of public funds (e.g. the principle of openness and the law on public procurement). Proprietary protocols, with their often secret specifications and strong vendor control, can create an information asymmetry that hinders independent transparency, evaluation and review. Open protocols and standards, with their publicly available specifications and often transparent development and management processes, offers a significantly higher degree of auditability and reduces the risk of arbitrariness or hidden agendas on the part of suppliers. This makes it easier for public organizations to justify their technology choices for collaboration, ensure fair treatment of potential suppliers in procurement processes, and demonstrate responsible and efficient use of tax funds. A strategic choice for open protocols can thus not only lead to technical and economic benefits, but also strengthen citizens' trust in the integrity and functioning of digital government.

Below is a table summarizing the key differences and benefits:

**Table 1: Comparison of features: Open vs. proprietary chat federation protocols**

Property	Open protocol	Proprietary protocols
<b>Cost aspects</b>		
Initial cost	Often low for the protocol/software itself; costs may arise for implementation, customization, support.	Can vary; often licensing costs from the start, but can sometimes be packaged to appear lower initially.
Running costs	Primarily for operation, maintenance, support; rarely direct licensing costs for the protocol.	Frequently recurring license fees (per user/year), support agreements, costs for forced upgrades.
Total Cost of Ownership (TCO)	Potentially lower over time due to absence of licensing costs and greater flexibility. <sup>12</sup>	Can be high due to licenses, lock-in and limited flexibility. <sup>15</sup>
License costs	Rare or none for the protocol itself; licenses may apply to specific implementations. <sup>3</sup>	Common and can be significant. <sup>3</sup>



<b>Dependent</b>		
Supplier dependency	Low; possibility of changing implementation/service provider. <sup>3</sup>	High; strong dependence on a single supplier for development, support and pricing. <sup>3</sup>
Risk of lock-in	Low; open specifications allow for alternative solutions. <sup>14</sup>	High; difficult and costly to change system or supplier. <sup>15</sup>
<b>Technical flexibility</b>		
Interoperability	High; designed to enable communication between different systems. <sup>2</sup>	Often limited to the supplier's own ecosystem; can make interoperability with external systems difficult. <sup>18</sup>
Adaptability	High; access to specifications and often source code allows for customization. <sup>3</sup>	Low; customizations are controlled and limited by the provider.
Scalability	Good opportunities through federated architecture and optional implementations. <sup>27</sup>	Depends on vendor architecture; may be limited by licensing models.
<b>Innovation</b>		
Innovation rate	Can be high through collaboration and contributions from a broad community. <sup>17</sup>	Controlled by the supplier's R&D budget and priorities.
Opportunity for personal development	High; the public sector can participate in or drive development. <sup>3</sup>	Very limited or non-existent.
<b>Security &amp; Control</b>		
Transparency	High; specifications and often source code are open for review. <sup>3</sup>	Low; "black box" principle, limited transparency.
Auditability	High; enables independent security audits. <sup>3</sup>	Limited to supplier internal processes or expensive third-party audits.



Data control	High; the organization can control where data is stored and how it is managed. <sup>24</sup>	May be limited, especially when using cloud services controlled by the provider.
Digital sovereignty	Strengthened through independence and control. <sup>29</sup>	Can be undermined by dependence on external, often foreign, suppliers. <sup>31</sup>
<b>Standardization</b>		
Access to specification	Public and often free of charge. <sup>8</sup>	Limited, protected or cost-based. <sup>4</sup>
Standardization process	Often open, inclusive and consensus-driven. <sup>8</sup>	Closed and controlled by the supplier.

**Table 2: Summary of economic benefits and benefits of choosing open protocols for chat federation**

Benefit category	Benefit	Supporting principles
<b>Cost reduction</b>	Lower Total Cost of Ownership (TCO) over time.	Avoidance of recurring license costs, reduced risk of forced expensive upgrades, flexibility in hardware choices.
	Reduced direct costs.	No or low licensing fees for using the protocol/basic software.
	Avoiding supplier lock-in costs.	Increased bargaining power, reduced risk of unreasonable price increases from individual suppliers.
<b>Efficiency gains</b>	Improved interoperability and seamless collaboration.	Standardized communication between different systems and organizations, reduced silos, avoidance of duplication of work.
	Increased adaptability to specific needs.	Ability to modify and tailor solutions to fit unique business processes and requirements.



<b>Improved Collaboration</b>	More effective communication across organizational boundaries.	Federation enables direct and secure communication between users in different connected organizations.
	Support for national and international collaboration.	Common standards facilitate cross-border information exchange and projects.
<b>Innovation potential</b>	Catalyst for innovation and local development.	Opportunity for the public sector and local companies to develop new services and functions based on open platforms.
	Increased pace of innovation through co-development.	Sharing code and knowledge within an open community can accelerate development.
<b>Security improvement</b>	Strengthened information security through transparency.	Ability to conduct broad and independent review of source code and protocol specifications identifies and addresses vulnerabilities.
	Increased auditability and accountability.	Clear insight into how systems work and how data is handled, which builds trust.
<b>Increased Resilience</b>	Improved business continuity.	Decentralized and federated architecture reduces the risk of "single points of failure".
	Reduced dependence on individual actors.	Ability to change implementation or service provider without changing the underlying standard, which increases robustness.
<b>Digital Sovereignty</b>	Secure control over critical communications infrastructure.	Ability to decide on data storage, administration and technical development in line with national interests.
	Independence from the business strategies and potential pressures of individual, often foreign, suppliers.	Reduced risk of dependence on technology that can be affected by geopolitical factors or commercial decisions beyond one's control.



## References and in-depth study

1. E-Government - EUR-Lex.europa.eu. - European Union -<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:l24226b>
2. Interoperability of European public services -<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0744&from=PT>
3. Proprietor – Wikipedia <https://sv.wikipedia.org/wiki/Proprietary%C3%A4r>
4. www.esamverka.se, -  
<https://www.esamverka.se/download/18.596c52ae184a362422a546/1669194851235/221121%20Federation-Utv%C3%A4rdering.pdf>
5. Standards - Swedish Board of Trade -<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-software.pdf>
7. Open standard - Wikipedia,[https://sv.wikipedia.org/wiki/%C3%96ppen\\_standard](https://sv.wikipedia.org/wiki/%C3%96ppen_standard)
8. Open standards – access to and reuse of public information in electronic format - Insyn Sweden,<https://insynsverige.se/documentHandler.ashx?did=105492>
9. Comparison of Total Cost of Ownership (TCO) and Life Cycle Cost (LCC), retrieved May 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](https://netchoice.org/wp-content/uploads/2023/01/NetChoice_Garland_The-Pernicious-Consequences-of-Vendor-Lock.pdf)
12. Open source - Sweden's Data Portal,<https://www.dataportal.se/oppen-kallkod>
13. Proposal for a European Interoperability Framework for Smart Cities and Communities (EIF4SCC), <https://digital-strategy.ec.europa.eu/sv/news/proposal-european-interoperability-framework-smart-cities-and-communities-eif4sc>
14. A reform for data sharing, SOU 2023:96 - Government,<https://www.regeringen.se/contentassets/6866c386b0ec492c8171c92c9c8922cf/en-reform-for-datadelning-sou-202396.pdf>
15. Public code - Open source software in Swedish public organizations,  
<https://offentligkod.se/>
16. Open source software - RISE,<https://www.ri.se/sv/expertisomraden/expertise/oppen-software>
17. DigResiliens - About resilient information systems - 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 – Industrial protocols in Sweden - MSB,  
<https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet->

Memorandum 2025-11-25  
Doc. payment: Appendix  
Version: 1.0  
No./ref: ES2025-20



[cybersakerhet-och-sakra-kommunikationer/industriella-informations--och-styrssystem/industriella-protokoll-i-sverige.pdf](#)



# Appendix H - Identity Federation as an Enabler for Federated Communication

This appendix focuses primarily on how identity federations can enable secure and interoperable access to communication services between public sector organizations – not just authentication, but also shared infrastructure and governance.

The appendix describes the current state and possible path forward for identity federation in the public sector, in relation to future federated communication (e.g. Matrix).

## Conclusion and recommendation

By gradually building support for federated login according to OIDC and future federation standards such as OIIF, the public sector can create a secure, interoperable and future-proof infrastructure for digital communication.

This infrastructure supports the goals of federated collaboration within the public sector, and is in line with the principles described in Appendix E and in the main body of the report.

## Identity Federation

There are many benefits to identity federation, such as reduced user administration for each individual service, increased security, improved user experience. An open federation protocol requires secure identity federations to be fully effective.

Given its mission-critical function, identity federations need to manage the total defense and preparedness perspective to create a robust and resilient implementation.<sup>1</sup>

Today, there are several established identity federations in Sweden with different purposes:

### *Organizational federations for collaboration:*

- [Sambi](#) (for healthcare and social care, run by Inera AB) - supports collaboration between healthcare organizations
- [School Federation](#) (for the education sector) - enables collaboration between educational institutions

---

<sup>1</sup> [Ordinance \(2022:524\) on the preparedness of government agencies | Swedish Parliament](#)



- [Swami](#) and [eduGain](#)- for the academic sector

#### *Individual identification:*

- [Sweden Connect](#)- national identity federation that standardizes the integration pattern for direct identification (government-to-citizen/business-to-consumer), where the relying party orders identity verification from e-identification issuers
- SITHS - SITHS (Säker IT för Hälso- och Sjukvården) is an e-identification and trust framework used in healthcare for strong authentication and authorization control. It is managed by Inera and is based on certificates linked to smart cards or software solutions.
- EFOS - EFOS (E-identitet för offentlig sektor) is a federation framework used in e-health and the public sector to enable secure authentication and electronic signatures. It is used, among other things, to connect healthcare providers and pharmacies via e-prescription systems.
- FrejaOrgID - Freja OrgID is a variant of the e-identification Freja eID adapted for organizations. It enables secure identification of employees in the service and can be used as part of identity federations in the public sector.

Sweden Connect is currently used primarily for G2C identification. For government-to-government (G2G) federation, other solutions such as OpenID Federation or Ena may be more appropriate, according to, for example, the Swedish Internet Foundation.

Ena, Digg's digital collaboration framework, can also play a role in coordinating federation solutions in the public sector – especially in terms of interoperability and trust management.

These federations have different uses depending on whether the purpose is collaboration between organizations (B2B/G2G) or individual authentication (B2C/G2C).

## **The technology behind identity federation**

Globally, organizations are moving from legacy protocols like SAML to more modern solutions based on OIDC. For the public sector, understanding the differences between these technologies is crucial – especially as they work to establish the federated digital infrastructure of the future.

SAML has built-in federation support as part of the protocol, while OIDC is itself an authentication protocol. The modern equivalent of SAML's federation model is OpenID Federation (OIDF), which is still under development but has great potential for the public sector.



- **OIDC is an authentication protocol** which is better suited for modern systems with its REST/JSON format, easier to implement, and better support for mobile devices. It has become the standard for new identity authentication thanks to its ability to meet today's needs for identity management across different platforms.
- **SAML has built-in federation support** as part of the protocol.
- **OIDF ([OpenID Federation](#))** is the modern equivalent of SAML's federation model. OIDF is currently in draft stage but is being actively developed and could have significant significance for the public sector in the future.

There is also a move towards OIDC for authentication in Sweden. [OIDC Sweden](#) has defined a profile for OIDC that is supported by, among others, BankID, Freja, Digg, Inera, etc. Sweden Connect's profiling for e-identification is based on this profiling and supplemented with specific details for Sweden Connect.

## **A possible way forward in this public sector ecosystem**

Digg's identity and authorization architecture plans to support OIDF. This means that public services, including future chat solutions, can use the same federation infrastructure as healthcare services, for example. This provides both technical coordination and an improved user experience through reusable trust relationships.

By combining in the future:

- ENA infrastructure for identity and authorization management
- [OIDC Sweden Profile](#)<sup>2</sup>
- [OpenID Federation \(OIDF\)](#) for the federation warehouse (when it is completed)
- [The Matrix project's ongoing implementation of OIDC support](#)

### **Matrix within organizational federation:**

Matrix services (server) act as "Relying Parties" in OIDC terminology within an organizational federation. They can use the OIDC Sweden Profile to accept logins from trusted Swedish identity providers. For the public sector, it is often more appropriate to connect to a sector federation that in turn trusts Sweden Connect, instead of each service connecting directly. This creates better control, reuse and clearer governance.

---

<sup>2</sup>See more: [oidc.se/profilering](https://oidc.se/profilering) (if it exists, otherwise write: "The profile is defined by DIGG, Inera, Freja eID, BankID, etc.")



### **Federated identity management:**

Users can log in to Matrix services using their organizational identity. Login can be done via employer, school or other sector federation identities. Matrix server no longer manages passwords but relies on trusted external identity providers.

### **Unified security model:**

The same security requirements and trust frameworks used in the public sector can then be applied to Matrix services. E-credentials can be used to securely identify users when needed. Encrypted messages (E2EE) in Matrix maintain their integrity while identity management is federated

This development creates synergies with other public sector initiatives. Identity and authorization solutions for chat services can leverage the same federation infrastructure established for other public sector applications, providing consistency, security and cost-effectiveness.

This development fits well into the [ENAs vision](#) about a unified, national model for secure identity management that supports both people, organizations and digital ecosystems.

A nationally coordinated federation solution also requires clear governance of trust frameworks, certificate management and incident management. Legal aspects such as requirements for security protection analyses, personal data responsibility and agreements between parties need to be considered. Early coordination with relevant actors can reduce the risk of delays in implementation.

Digg has particular expertise in permission and authorization models, and could contribute to further work to ensure that a federated chat solution is integrated into a common identity infrastructure with high trust and traceability.

This appendix has been developed with input from, among others, Digg, Sambruk and RISE within the framework of a consultation round in the dSam4 working group in the spring of 2025.



# Appendix I Guidelines – How can your organization prepare itself for the chat collaboration protocol

This guidance is a strategic support for eSam members and other public actors who want to prepare for a common, open protocol for chat and digital communication – with the goal of strengthening security, interoperability and collaboration across organizational boundaries.

## Background and anchoring within eSam

The strategic support is based on the analytical work that the dSam working group has carried out in 2025. The working group has evaluated six possible paths and recommends that a common, open communication protocol be introduced – Matrix – that enables federation and interoperability.

## What does a common protocol for chat and collaboration mean?

A **common open protocol** is a technical standard that different systems can use to communicate with each other – regardless of the software or vendor used. It enables organizations to use different tools but still be able to chat and collaborate across borders, securely and efficiently.

**Matrix** is one such open protocol. It works in a similar way to email: each agency can choose its own solutions, but because they speak the same "language" via Matrix, they can still exchange messages, participate in common channels, and communicate in real time.

The protocol enables so-called federation, which means that systems can talk to each other without being centrally controlled or locked into a specific vendor. This strengthens:

- Self-determination: each organization retains control over its own environment.
- Security: traffic can be encrypted (end-to-end) and handled within Sweden's borders.
- Scalability: it is possible to start small and expand over time.



- Redundancy: decentralization reduces vulnerability to operational disruptions.

It makes it possible to:

- interact in everyday life without the need for special installations.
- communicate effectively in times of crisis or social disruption.
- build a long-term sustainable digital communications infrastructure for the public sector.

It is important to emphasize that federation does not need to replace existing communication tools, such as Microsoft Teams. The federated protocol can be used as a complement, especially for external collaboration.

### **What does this mean for my organization?**

Implementing a common protocol for digital communication entails certain consequences for each authority – technically, organizationally and in terms of resources. For example, the authority needs to:

- Understand the principles behind federation and open protocols
- Review existing tools and future needs
- Set requirements for support for Matrix during procurement or call-off
- Assess needs for skills and resources

The guidance is designed to provide support in this work, but each authority needs to assess for itself when implementation is relevant, and at what pace it is possible to prepare.

### **Why is this important?**

- To be able to collaborate effectively in everyday life and in crisis.
- To comply with future legislation, such as SOU 2023:96 and the Interoperable Europe Act.
- To ensure digital sovereignty and reduce dependence on individual suppliers.



- To contribute to the goals of Sweden's new digitalization strategy: "Ena – Sweden's digital infrastructure".

## **What does the authority need to do?**

In 2026, authorities can begin preparing to use the common protocol.

### **Already now:**

- Take a look at the report and attachments from dSam.
- Anchor the issue internally: needs, opportunities, risks.
- Ensure that management is informed about the purpose and the connection of the work to strategic goals.
- Do you have systems today that can use Matrix protocols?
- How do you ensure legal and technical preparation for procurement or call-off?
- What skills do you need to build internally to be able to implement and manage a federated solution?
- Verify whether the authority can contribute capacity and expertise from spring 2026: technical expertise (federation, security), legal support (procurement, interoperability) as well as change management and communication are resources needed.

### **In 2026:**

- Review upcoming procurements or call-offs – require support for the Matrix protocol.
- Appoint a contact person at the authority for coordination with dSam and internally at the authority.
- Contribute expertise if possible

These preparations can help your organization stay ahead of the curve and be ready when broader adoption begins from 2027.



## **Three-step implementation plan**

### **Step 1 – Working group tests on a small scale (fall 2025 – spring 2026)**

- The authorities in the working group will participate in smaller pilot projects to test federation in practice.
- The experiences are used as a basis for developing more detailed guidelines for other authorities.

**Note:** During the fall of 2025, the work will primarily be driven by the existing working group, where participants have limited working hours. In order to scale up the work and produce more comprehensive guidance, reinforcement with key competencies is recommended from spring 2026. This may include technical expertise (federation, security), legal support (procurement, interoperability) and change management and communication.

### **Step 2 – Guidance and collaboration (autumn 2026)**

- Based on the test results, more complete support is created for authorities.
- More authorities are invited to participate.
- Support materials are adapted to the needs and conditions of different organizations.

### **Stage 3 – Implementation (2027 onwards)**

- Authorities that need it should be able to start federating via a common open protocol for digital collaboration.
- Coordination takes place within eSam and in collaboration with DIGG.

## **Recommended principles**

- Use open standards for communication.
- Consider information classification and the need for E2EE (end-to-end encryption).
- Build solutions that are manageable and interoperable.
- Consider availability, robustness and incident preparedness.



- Ensure that solutions meet accessibility requirements according to WCAG and the Swedish Language Act.

## **Support and collaboration**

- The working group within eSam (dSam) coordinates continued work.
- The working group plans to set up a first test environment in the fall of 2026. This will be based on practical tests carried out on a smaller scale.
- Contact with DIGG is established to ensure connection to the national digital infrastructure (ENA).
- Support materials and exchange of experiences will be provided on an ongoing basis.

## **Update of the guidance**

The guidance is maintained by the dSam working group. The content will be updated continuously based on:

- Experiences from pilot projects and tests in 2025–2026
- Changes in legislation, policy documents or digitalization strategies
- Views and needs from eSam members
- Coordination with DIGG and other relevant initiatives (such as ENA)

The goal is for the guidance to be practical support that follows developments – from preparation to implementation.

The dSam working group is responsible for publishing updated versions in collaboration with eSam.



# Appendix J - A comparison between MLS, MIMI and the Matrix protocol

This appendix focuses on providing a technical comparison between three key technologies - Messaging Layer Security (MLS), More Instant Messaging Interoperability (MIMI), and the Matrix protocol.

## Messaging Layer Security (MLS)

This section analyses the status of MLS, its core architecture, the security guarantees it offers, and its role as an enabling technology for next-generation interoperable messaging systems.

### Standardization and current status

Messaging Layer Security (MLS) has moved from an experimental draft to a formal Internet standard. The protocol was officially published by the Internet Engineering Task Force (IETF) as RFC 9420 in July 2023. This standardization is significant because it provides the industry with the first unified, open, and rigorously reviewed protocol for end-to-end encryption in groups. Previously, the landscape was fragmented with various proprietary implementations or variants of the Signal protocol, which often lacked a complete and open specification.

The IETF has published a companion document, RFC 9750, which is an informative guide to the MLS architecture. This document, published in April 2025, describes how to build a complete messaging system around the core MLS protocol. The document highlights an important aspect - MLS is a fundamental component for key management and encryption, not a complete, stand-alone messaging solution. The fact that the IETF not only standardized the cryptography (RFC 9420) but also provided an architecture guide (RFC 9750) demonstrates an understanding that a protocol's security guarantees can easily be undermined by a faulty implementation.

### Core architectural principles

The core of MLS lies in its method of managing group keys, known as "Continuous Group Key Agreement". Unlike previous methods such as the Signal protocol's "Double Ratchet", which relies on pairwise encryption sessions, MLS uses a tree structure to represent the state of the group. In this model, called "Asynchronous Ratcheting Trees" (ART), each member is represented as a leaf in a binary tree.



This tree structure gives efficiency to the MLS key management. When a member is added or removed from the group, only a few updates along the path from the leaf to the root of the tree are required to generate a new group key. This means that the cryptographic operations, both computationally and communicationally, scale logarithmically ( $\log(N)$ ) with the size of the group ( $N$ ). This is in contrast to older methods where the “cost” could scale linearly ( $N$ ) or even quadratically ( $N^2$ ). This logarithmic scalability is what makes MLS practical for very large chat groups/channels, supporting up to 50,000 members.

## Advanced security guarantees

MLS is designed to offer a robust set of modern security guarantees that go beyond basic encryption. These features, defined in the official specifications, are essential for building trust in an interoperable ecosystem.

- **Message confidentiality, integrity and authentication:** Ensures that messages are private, unaltered, and come from the purported sender.
- **Forward Secrecy (FS):** Guarantees that if a member's long-term keys are compromised, an attacker cannot decrypt previous messages.
- **Post-Compromise Security (PCS):** If a member's device is compromised, the protocol can automatically "heal" itself. After the user takes steps to secure their device, future messages will once again be protected from the attacker.
- **Membership authentication:** All members of a group have a consistent and cryptographically verifiable picture of who else is in the group, preventing an attacker from secretly adding a spy to the conversation.

## Applications and future developments

The protocol has received support by leading industry players. Google has announced its intention to integrate MLS into the end-to-end encryption for Google Messages over Rich Communication Services (RCS). The GSMA, which governs the RCS standard, and Apple have also announced that they will support RCS with MLS. Companies such as Cisco and Wire have also been early adopters and supporters of MLS. The Matrix protocol has declared its intention to find ways to adopt MLS

This broad adoption makes MLS a potential contender as a future standard for secure group key management for chat based solutions. There is also ongoing research and



IETF drafts to integrate post-quantum cryptography (PQC), which aims to ensure long-term security against future threats from quantum computers.

## MIMI working group

While MLS solves the fundamental problem of secure group encryption, the larger challenge remains of getting different messaging services to communicate with each other. This is the mission of the IETF's "More Instant Messaging Interoperability" (MIMI) working group.

## Statutes and objectives

The core mission of the MIMI working group is to "specify the minimum set of mechanisms required to make modern Internet messaging services interoperable". It is important to note that this explicitly applies to services with end-to-end encryption and that the goal is to achieve interoperability without undermining the security guarantees that users expect.

The working group's charter identifies four central problem areas that require standardization to make this possible:

1. **Identity:** How a user's cryptographic identity can be established and verified across service provider boundaries.
2. **Introduction:** How a user on service A can discover and initiate a conversation with a user on service B.
3. **Content format:** A common format for messages and features (such as replies, reactions, and attachments) that work in an E2EE context.
4. **Delivery:** A common delivery service and transport protocol for communication between the federated domains.

MIMI's focus on a "minimal set" is a deliberate strategy to avoid past failures. Previous attempts at interoperability, such as XMPP, attempted to standardize a very broad range of features, resulting in complex specifications that were difficult to fully implement. MIMI's charter explicitly states that it should "learn from these previous attempts" and focus on what is absolutely necessary to solve the core problem first.



## Current status and timetable for standardization

MIMI is a work in progress, and its technical development is taking place through a series of public "Internet Drafts". These documents represent the technical proposals currently being discussed and refined within the working group. The key drafts include:

- draft-ietf-mimi-protocol: Defines the core protocol for communication between providers, using HTTPS and MLS.
- draft-ietf-mimi-content: Specifies the format for message content.
- draft-ietf-mimi-room-policy: Describes how policies for a "room" (e.g. membership rules) should be handled.

The working group's official milestones provide an indication of the expected timeline, pointing towards a possible publication as RFC standards in late 2025 or early 2026, although such timelines are always tentative. The work had active participation initially from industry but the interest has declined since then and only a few members are participating in the MIMI-working group. Based on this the MIMI working group is considering whether to change the scope of the work.

## The architectural framework of MIMI

MIMI's architecture is designed to act as a layer on top of MLS. It assumes that MLS is used for key establishment, confidentiality, and authentication of group members. MIMI specifies how providers should interact with each other, but leaves the communication between a client app and its own server largely unspecified. This is a deliberate design choice to minimize the changes that existing apps need to make to become compatible.

A central part of the proposed architecture is a "hub"-based model for ensuring the ordering of messages. Since MLS requires that certain messages (especially those that change the group's state) be delivered in a strict and consistent order to all members, it is proposed that a server for each conversation act as a central "hub". This hub is responsible for timestamping and distributing messages to all participating providers. While this solves the ordering problem, it introduces a tension between decentralization and centralization. The system as a whole is federated, but each individual conversation is given a centralized point of ordering. This creates a new trust boundary and a potential attack vector, as a malicious hub could theoretically censor, delay, or change the order of



messages. This risk has already been noted in academic research proposing audit trails to detect such abuse.

## Key challenges for standardization

The MIMI working group's success depends not only on technical implementation, but also on navigating a complex landscape of practical and strategic challenges. To maintain focus, the group has deliberately chosen to exclude certain complex problems from its initial mandate.

Metadata processing to address spam and abuse, as well as interoperable mechanisms for group administration and moderation, are currently “out of scope.” This pragmatic approach aims to first establish a working foundation for interoperability.

Perhaps the biggest challenge, however, is not technical. For MIMI to succeed, it will require cooperation and consensus among commercial competitors who have historically protected their own ecosystems.

Drivers such as the EU's Digital Markets Act (DMA) are creating regulatory pressure that could force this collaboration, but practical implementation will require service providers to trust each other to manage authentication, key material, and abuse policies responsibly.

## **An established model for decentralized communication: the Matrix protocol**

Parallel to the IETF's standardization work, Matrix, a mature and well-established open protocol for decentralized communication, exists, which has created a large footprint for the public sector in the EU. In order to make a comparison with MIMI, it is necessary to first understand the core architecture of Matrix, its security model and its philosophy around interoperability.

### **The core**

Matrix is defined as an open standard for interoperable, decentralized real-time communication. Its stated goal is to function like email, i.e. to allow users to communicate with each other regardless of the app or server provider they use. Technically, Matrix is a federated system consisting of "homeservers" that synchronize conversation history with each other via a Server-Server API, typically over HTTPS with JSON as the data format.



The most distinctive feature of Matrix is its data structure. Instead of a linear list of messages, all data in a "room" is stored as an "event graph," a directed acyclic graph (DAG). Each action—a message sent, a user joining, a room name changing—is an "event" that cryptographically links to its predecessor (or predecessors). This enables the concept of "eventual consistency." If the network connection between two servers is broken, both can continue to receive new events in the room. When the connection is reestablished, the servers can synchronize and merge their respective history graphs. This architecture, which prioritizes system resilience and each server's autonomy, is robust to network failures but also introduces complexity, especially when it comes to resolving conflicts over the state of the room ("state resolution").

## Built-in end-to-end encryption

Matrix has had built-in support for end-to-end encryption since 2020, and it is enabled by default for all new private conversations. The encryption is based on two separate but interoperable protocols, implemented in libraries such as libolm and the newer, reviewed vodozemac:

- **Olm** is an implementation of the Double Ratchet algorithm, popularized by Signal. Olm is used to establish secure one-to-one encryption sessions between two specific devices. Its primary use in group chats is to securely distribute keys for Megolm.
- **Megolm** is a cryptographic "ratchet" designed specifically for group chats. Each participant in an encrypted room creates their own outgoing Megolm session. When they send a message, it is encrypted with this session key, which is then rotated. The key to decrypt messages from this session is securely shared with the other members of the room via their individual Olm sessions. This model is well suited for the decentralized nature of Matrix but has known scalability challenges in very large groups, a problem that MLS is designed to solve.

## The Matrix Ecosystem

Matrix is more than just a protocol; it's an entire ecosystem. This includes open-source server implementations (with Synapse being the most mature), a wide range of client applications for all platforms (with Element being the most well-known), and well-defined APIs for client-server communication.



One of the unique aspects of Matrix is its concept of bridging. A bridge is an application service that connects a Matrix room to an external, non-Matrix network such as Slack, IRC, Discord, or Telegram. This allows Matrix users to communicate with users on these platforms from their Matrix client. This feature demonstrates Matrix's long-standing and practical focus on interoperability. It represents a different philosophy than MIMI. While MIMI aims to create a common protocol for direct communication between vendors, Matrix acts as a universal translation layer or "meta-interoperability hub" that can connect to any other protocol via a custom bridge.

## Comparison between Matrix and MIMI

With a basic understanding of MLS, MIMI, and Matrix, it is easier to make a direct comparison between the protocols.

### Matrix event graph (DAG) versus MIMI's ordered message model

The biggest technical difference between Matrix and MIMI lies in their conversation history data models.

- **Matrix:** Uses a decentralized event graph (DAG) that optimizes for resilience and eventual consistency. No single system owns the space or its history; data is replicated across all participating servers. This is a very robust model but requires complex algorithms to handle merging of history and resolving state conflicts.
- **MIMI/MLS:** Implicitly requires a linear, ordered flow of messages. This is a direct inheritance from MLS, which requires a unique ordering of control messages to ensure that all participants have a consistent cryptographic state. This model leads to an architecture with one "hub" or "sequencer" per conversation, which is simpler to implement but introduces a centralized point of ordering and trust. This degrades the resiliency of the architecture.

Matrix prioritizes decentralization and autonomy, while MIMI prioritizes guaranteed consistency, even at the cost of a centralized component per conversation.

### "Linearized Matrix"

In response to the architectural gap, the Matrix ecosystem itself has developed and proposed the "Linearized Matrix."



"Linearized Matrix" is a simplified version of the Matrix spatial model. Instead of a complex DAG, the history is represented as a doubly linked list of events. This linear history is managed by a designated "hub" server for that specific space. This model is designed to be compatible with regular, non-linear Matrix servers. A full-fledged Matrix server can act as a "hub" for Linearized Matrix clients and translate its internal DAG into a linear history for them.

## Decentralized MLS

The MLS standard (RFC 9420) often relies on a linear order of events, which is difficult to guarantee in a decentralized environment like Matrix where servers may be out of sync. Matrix must therefore build a layer (DMLS) to handle this factor.

Consequently, Matrix is working to replace or complement its current encryption protocol (Olm/Megolm) with MLS (Messaging Layer Security). The goal is to enable more efficient and secure encryption for very large group chats (end-to-end encryption that offers better scalability) as well as to solve issues regarding synchronization and key management.

The project utilizes a specific Rust-based library called matrix-dmls which is the foundation of this effort.

## Security models in context

The comparison of the security models shows convergence.

- **Matrix (Olm/Megolm):** A mature and vetted system based on Double Ratchet. It is well proven and adapted for the Matrix decentralized model but has scalability limitations.
- **MIMI (MLS):** Built from the ground up on MLS, which is designed for efficiency and scalability in large groups.

## Scope and philosophy

The protocols differ in their overall ambition and philosophy.



- **Matrix:** Aiming to be a "generic messaging and data synchronization system for the entire web", it is a complete ecosystem with specifications covering everything from client-server communication to identity management, application services and real-time communication.
- **MIMI:** With the stated goal of defining a "minimal set of mechanisms" for interoperability between messaging systems, MIMI does not attempt to build a complete communications platform, but rather the thinnest possible layer to connect existing platforms.

## Strategic perspective

The comparison shows that the future of secure and interoperable messaging is not about a winner-takes-it-all battle. Instead, we are moving towards a future of convergence and coexistence, where standardized layers build on each other to create a richer and more connected ecosystem.

The scenario is not "Matrix vs. MIMI", but rather "Matrix in a world with MIMI(or the other way around)". MIMI is still evolving and the future will tell what the end result will be.

In this context, Matrix is well positioned. By adopting MLS and offering compatibility solutions like "Linearized Matrix" or "Decentralized MLS", Matrix can evolve into an IETF-compliant platform. Another potential scenario could be that the IETF MIMI working group starts collaborating with the Matrix Foundation, based on that Matrix is growing in popularity within the EU.

## Summary

The needs picture described in the main report for this eSam project requires a long-term sustainable solution while the most prioritized needs need to be addressed as soon as possible. This is so that authorities can continue to collaborate effectively and seamlessly even if the market has not adapted.

Messaging Layer Security (MLS) is a completed and published IETF standard that provides the new solution for key exchange in secure group communications. More Instant Messaging Interoperability (MIMI) is an active IETF project that builds on MLS only the future can tell what the outcome will be.



The Matrix protocol is not in opposition to this development. On the contrary, it is adapting to ensure its continued relevance and unique position. Through its willingness to adopt MLS and adapt its own protocol stack, Matrix demonstrates a forward-looking strategy. It embraces open standards while retaining the unique architectural advantages that have defined the protocol. We see the picture of an ecosystem moving towards a more open, secure and federated future, where different architectures need to coexist and interoperate through common, standardized layers.

## Recess

1. Messaging Layer Security - Wikipedia, [https://en.wikipedia.org/wiki/Messaging\\_Layer\\_Security](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. The Matrix Protocol - [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://sumner-evans.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](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>