eSam

Digital collaboration platform for the public sector

November 2021

Results

There are various legal options suitable for use within the public sector.

After consideration, and in the light of the requirements specification, we have captured a snapshot of the market and identified several solutions that, either individually or in combination, could provide a suitable digital collaboration platform for public-sector organisations. Even though it has not been possible to outline the entire market in a comprehensive manner, it is clear that suitable legal alternatives to US-based cloud services are available. A few of these alternative solutions even seem to perform better than US cloud services, and are already being used by several public-sector organisations. Some have been in use within the public sector for several years, while others have been adopted during the COVID-19 pandemic. These are therefore tried-and-tested solutions.

The overall aim has been for the report to benefit the public sector by facilitating access to the benefits of digitalisation. There is no real value in excluding individual suppliers, but we acknowledge that the application of hidden extraterritorial legislation creates an obstacle between the needs of the public sector and non-Swedish (predominantly US) service providers.

This report shows clearly that alternative options are available, and that public-sector organisations do not have to navigate a legal "grey area" to meet their needs. On the contrary: we believe that the public sector should set a good example and maintain a security margin with regard to the internal processing of information within organisations – especially given the risk of serious issues such as unauthorised access to personal data and sensitive information.

A public-sector organisation should not have to spend time and resources on protecting information from a supplier. Instead, it should select an alternative supplier that does not present a risk in terms of the unauthorised dissemination and processing of information. Establishing various means of protection, or making "special cases" in order to render a particular service usable, limits the possibilities of digitalisation. By maintaining a focus on legality, information security and digital sovereignty from the start, the public sector can avoid having to disable functions or impose restrictions on the use of services.

We can summarise our aims as a metaphor: instead of choosing a racing car that can only be driven on an enclosed track in Sweden, we opt for a simpler, more robust vehicle that can be driven freely on the roads. In other words, legislation and cybersecurity should no longer be considered limiting factors – on the contrary: they enable the use of appropriate solutions.

The public sector needs solutions now. We have important societal tasks to carry out, and can no longer wait for a solution to appear of its own accord. Besides, there is a chance of such a solution being rejected in court following lengthy negotiations on data protection. We therefore need to take the initiative and secure what is required for employees and for the tasks we have to fulfil. The options we have identified will enable the public sector to make immediate and significant advancements in the digitalisation domain.

Our approach requires the IT industry to change its approach and – in certain cases – its business model too. A one-sided effort by the public sector to adapt to existing solutions would not be an effective way of resolving the issue. Instead, we hope that the IT industry will respond to our stance by developing solutions characterised by inbuilt data protection, security, legality, and a holistic approach to the processing of information and personal data held by public authorities. The investment in suitable legal solutions is likely to result in the IT sector adapting to the changing needs of the public sector.

The impact analysis carried out indicates that major challenges lie ahead as the work proceeds. Time and resources are needed, as is a new perspective that mirrors the need for a holistic approach to the entire public sector. In the next step, we will therefore aim to highlight the options available and demonstrate their effectiveness for use both within and between public authorities.

The final report includes four annexes (only available in Swedish):

- Annexe 1: *Complete list* of suppliers and solutions encountered during the project
- Annexe 2: *Requirements specification* outlining the requirements on which the evaluation is based
- Annexe 3: an in-depth outline of *Collaboration models*
- Annexe 4: an in-depth outline of *Possible solutions*

In the report, the project working group refers to the annexes named above. Since this group is behind the work, the final report is written using the pronoun "we".

The members of the working group are: Bo Anderson, Technical Project Manager, the Swedish Companies Registration Office ("Bolagsverket"); Kenneth Edwall, IT Architect, the Swedish Social Insurance Agency ("Försäkringskassan"); Magnus Einarsson, IT Strategist, the Swedish Civil Contingencies Agency ("Myndigheten för samhällsskydd och beredskap, MSB"); Erik Enocksson, Enterprise Architect, the Swedish Transport Administration ("Trafikverket"); Sara Israelson, Deputy IT Security Manager, the County Administrative Board of Västra Götaland ("Länsstyrelsen i Västra Götaland"); Peter Nordström, Strategist, the Swedish Tax Agency ("Skatteverket"); Jenny Olivestedt, Product Manager, the Swedish Public Employment Service ("Arbetsförmedlingen"); Soheil Roshanbin, Legal Developer, the Swedish Enforcement Authority ("Kronofogden"); and Peter Witt, Project Manager, the Swedish Tax Agency ("Skatteverket").

The project steering committee approved the report on 29 October 2021, and decided it could be published on 18 November as planned. The steering group's members are:

Sofia Ekelöf, eSam ("eSamverkansprogrammet", a digital collaboration programme); Peder Sjölander, the Swedish Tax Agency ("Skatteverket"); Johan Acharius, the Swedish Enforcement Authority ("Kronofogden"); Krister Lindvall, the Swedish Transport Administration ("Trafikverket"); Magnus Peterson, the County Administrative Boards ("Länsstyrelserna"); Joel Tostar, the Swedish Companies Registration Office ("Bolagsverket"); Mats Persson, the Swedish Civil Contingencies Agency (MSB); Krister Dackland, the Swedish Public Employment Service ("Arbetsförmedlingen"); Mikael Norberg, the Swedish Social Insurance Agency ("Försäkringskassan"); and Peter

Nordström and Peter Witt, the Swedish Tax Agency ("Skatteverket"), who represent the project work group.

Table of contents

1 The project

1.1 Background

During the first quarter of 2021, the Swedish Tax Agency ("Skatteverket") and the Swedish Enforcement Authority ("Kronofogden") jointly investigated the prerequisites for replacing the software application Skype for Business (subsequently Skype) with the cloud service Teams as their main video conferencing and collaboration platform. The investigation was triggered by two developments: Microsoft's announcement that it would cease to support and develop Skype in approximately five years' time; and a ruling by the Court of Justice of the European Union (CJEU) to the effect that the design of US intelligence and surveillance programmes does not fulfil EU requirements on the processing of personal data. The CJEU also ruled that the transfer of personal data to the US was prohibited – unless an adequate level of data protection could be guaranteed, making the data unavailable to the US authorities.

The Swedish Tax Agency and the Swedish Enforcement Authority concluded from their investigations that the use of Teams as their main video conferencing and collaboration platform would be incompatible with the regulations governing their activities. The principal argument was that if Teams were to be used in the way Skype is used today, large amounts of data would be exposed to Microsoft in a way that would be incompatible with data protection and privacy regulations. In their report, the Swedish Tax Agency and the Swedish Enforcement Authority also considered the risks presented by the lock-in effects, costs, continuity, suitability and continuous changes associated with the solution[1]. Several other public authorities – including the Swedish Public Employment Service ("Arbetsförmedlingen"), the Swedish Social Insurance Agency ("Försäkringskassan") and the Swedish Transport Administration ("Trafikverket") – subsequently subscribed to the assessment made by the Swedish Tax Agency and the Swedish Enforcement Authority.

Following the publication of the report, the Swedish Tax Agency and the Swedish Enforcement Authority decided to establish a cross-functional working group with several other public authorities to investigate the prerequisites for a suitable legal appropriate and legal suitable legal for the public sector. The work began in May 2021, and the working group was named "Digital collaboration platform for the public sector" ("Digital samarbetsplattform för offentlig sektor").

1.2 Organisation

The working group has consisted of eight experts from the Swedish Tax Agency, the Swedish Enforcement Authority ("Kronofogden"), the Swedish Public Employment Service ("Arbetsförmedlingen"), the Swedish Companies Registration Office ("Bolagsverket"), the Swedish Social Insurance Agency ("Försäkringskassan"), the County Administrative Board of Västra Götaland ("Länsstyrelsen i Västra Götaland"),

---

See the decisionissued by the Swedish Tax Agency and the Swedish Enforcement Authority on 3 May 2021 regarding Swedish Tax Agency case 8-958696 or Swedish Enforcement Authority case KFM 10419-2021.

the Swedish Civil Contingencies Agency ("Myndigheten för samhällsskydd och beredskap, MSB") and the Swedish Transport Administration ("Trafikverket"). The Swedish Agency for Growth Policy Analysis ("Myndigheten för tillväxtpolitiska utvärderingar och analyser"), the Swedish Gender Equality Agency ("Jämställdhetsmyndigheten" and the National Board of Housing, Building and Planning ("Boverket") have also contributed to the work by providing additional resources during a certain period.

The scope, resources and timeline of the project have been governed by the steering committee, which comprises individuals from the organisations represented in the working group.

The working group has been supported by a reference group representing 121 public-sector organisations. The reference group and steering committee have been kept informed of the work in progress throughout the project. The reference group has provided input to the project in terms of requirements and experience. The reference group has also had insight into the collective requirements and alternative solutions identified by the working group.

1.3 Assignment and aim

The assignment has been to investigate solutions that could – either alone or in combination – form a digital collaboration platform for use by public-sector organisations, given the requirements that such organisations have to fulfil.

The term "digital collaboration platform" refers to a tool with the following features:

- Video conferencing
- File storage
- Permanent chat rooms
- Kanban board (used for visualising tasks, for example)
- Whiteboard

1.4 Scope

Solutions for processing secure information under the Swedish Protective Security Act (2018:585) have been excluded from the scope of our assignment. The production of supporting material for public procurement purposes has not been included in our assignment either. Consequently, the *Requirements specification* does not fully reflect requirements that may be specified in the procurement regulations.

Outlining IT support requirements for case administration purposes has not either been part of our assignment. Further, our assignment has been limited with regard to more in-depth implementation measures that may be required, depending on the operating environment and other factors specific to each organisation. There have also been clear limitations regarding our assessment of suppliers and solutions. We have used a specific review method and focused on solutions of which we were aware, those recommended to us by the reference group, and those presented to us by suppliers on their own initiative. We have also had to limit our work in view of the time available. On this basis,

we do not claim that the final report outlines all of the solutions available on the market. In other words, alternative solutions not mentioned in the report could also be suitable and legal as a digital collaboration platform for the public sector.

2 Possible solutions

General outline

We have grouped the solutions according to different areas, although some extend to more than one area. This grouping is based on our own assessment. The solutions placed in the "comprehensive solutions" category have the majority of the features that we need.

We have primarily looked at each specific solution – not the cloud service provider that offers the solution. There are, for example, several Swedish suppliers selling Nextcloud as a service. However, we have not evaluated suppliers within the framework of this project – except when a supplier has developed and added a new feature to the solution.

We can visualise the concept of a *digital collaboration platform* in different ways:

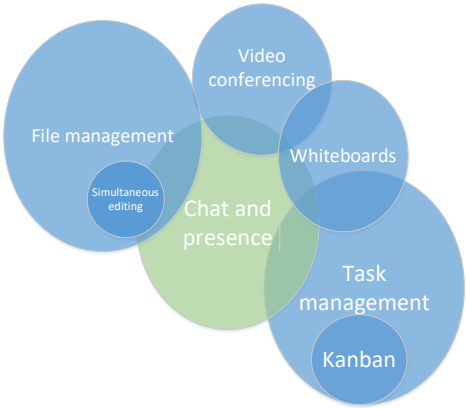

Figure 1 The chat rooms are the central feature to which the remaining features connect.

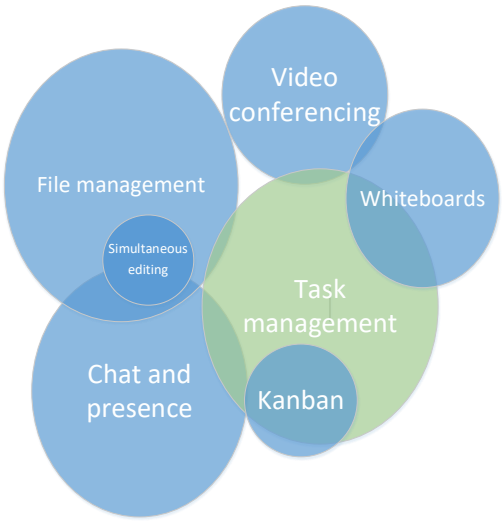

Figure 2 Task management is the central feature to which all others are connected.

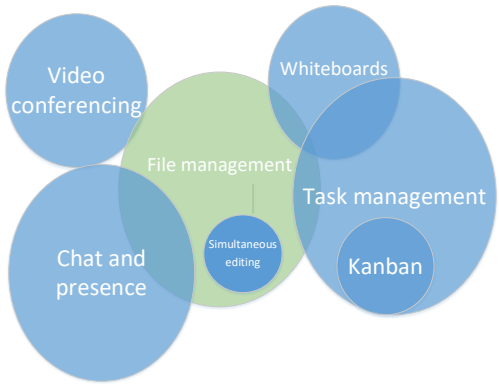

Figure 3 The document repository is the central feature to which all others are connected.

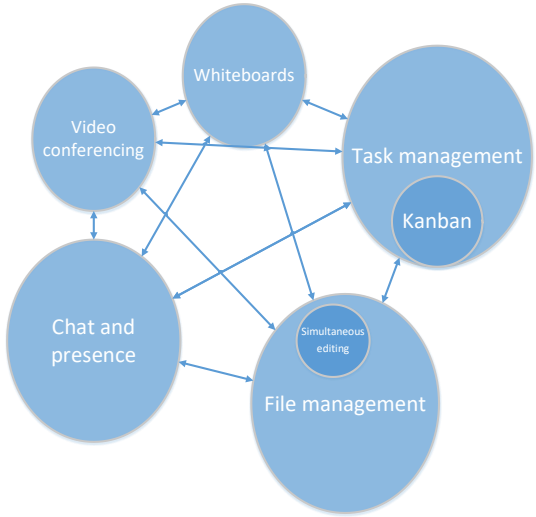

Figure 4 Equal components with connections between information objects.

The solutions that best meet our requirements are presented below. A more in-depth outline of the solutions is provided in annexe 4 *Possible solutions*. The solutions of interest for further investigation are also mentioned in this annexe.

2.1 Comprehensive solutions

Comprehensive solutions comprise a broad range of features spanning several of the areas that we have considered, as well as other areas such as email.

Two of these solutions would best meet our requirements: Nextcloud and Compliant Office. There is one main difference between them. Nextcloud is like a toolbox from which the customer can select a set of features. Compliant Office, on the other hand, offers a fixed set of features as well as email functionality for both clients and servers.

2.1.1 Nextcloud

There has been increasing interest in Nextcloud in recent years – both in Sweden and in other EU countries. Nextcloud is an open-source solution, and there is an extensive network of stakeholders and enthusiasts contributing to its development. This results in

an actively managed solution, with new features and applications being released on a continuous basis. Nextcloud is a comprehensive collaboration solution that is similar to Microsoft 365, Google Workspace, IceWarp, etc.

Nextcloud stands out as a customisable open-source solution. A wide range of features are available through around 100 selectable applications. These applications enable features such as file and document management, document editor for web with support for simultaneous collaborative editing, permanent chat rooms with support for group and one-on-one chat sessions, video meetings, email, calendars, "to do lists", online Kanban boards, survey tools, a Wiki app and a collaborative whiteboard to name a few.

In the world at large, Nextcloud is offered or used by the EU Gaia-X initiative, Deutsche Telekom (as a service), the French state, the Swedish Transport Agency ("Transportstyrelsen") and the Swedish Social Insurance Agency ("Försäkringskassan") among others. The Swedish Social Insurance Agency offers Nextcloud as a service to public authorities: "Collaboration platform for the public sector" ("Samarbetsplattform för offentlig sektor"). This service is delivered within the framework of the Swedish Social Insurance Agency's assignment to ensure coordinated and secure state IT systems.[2]

Nextcloud does not offer any cloud services, but provides business partners with its technology. It is therefore possible to procure Nextcloud as a cloud service from Swedish suppliers. The solution can be established in an organisation's own IT environment, without support requirements or licensing costs. If required, external support can be provided through support agreements with distributors, Nextcloud partners and consultants.

2.1.2 Compliant Office (IceWarp)

Compliant Office is a cloud service provided by City Network, based on the collaboration solution IceWarp. Compliant Office is delivered from Swedish data centres owned by a Swedish company. IceWarp is a comprehensive collaboration solution comparable to Google Workspace and Microsoft 365. The features included are email client, email server, calendars, chat, group chat, video conferencing, task management, document management, and Office document support including simultaneous collaborative online editing. Integration with locally installed software is also possible, enabling document editing.

Compliant Office (IceWarp) is of particular interest because it is a cohesive solution centred around collaboration features. It should be a particularly attractive solution for smaller organisations. IceWarp licenses can be purchased for independent operation, or for operation by an organisation's chosen IT management provider.

Composite solutions

Several Swedish and European partners can deliver a comprehensive collaboration platform based on a combination of solutions. Redpill Linpro, for example, has outlined

[2] Government decision reached on 26 September 2019 in case I2019/02515/DF.

a comprehensive solution combining Mattermost (group chat), Jitsi (video conferencing and large meetings), Focalboard (Kanban), Nextcloud (document management) and Collabora Online (office applications and collaborative editing).

2.2 Permanent chat rooms

Permanent chat rooms (also known as persistent chat rooms) can serve as a starting point in the search for cooperation solutions – for example using the approach shown in Figure 1 in Section 2. Organisations that have adopted permanent chat rooms for communication indicate that they have made a deliberate transition from email. From a chat room, users can start a meeting, edit documents or manage files, for example. It is also possible to transfer seamlessly from a client to a mobile device, using the same interface. Persistent chat solutions are currently in limited use as collaboration tools, but there is significant interest among public-sector organisations. However, usage may be largely restricted to IT departments for the time being.

The options we have considered can all be integrated with other solutions to provide enhanced functionality. The prerequisites for external collaboration between different solutions (referred to hereafter as "federation") constitute another important factor. Find out more in section 3.3 and annexe *Collaboration models*.

When a solution fulfils the prerequisites for integration and federation, it is possible to add extra features – such as Kanban and document management – and to enable communication with external organisations that have different persistent chat solutions.

Element, Rocket.Chat and Mattermost are the solutions that best meet our requirements. Our overall comparison of these shows that:

- - Element has inbuilt support for federation via the open protocol "Matrix" (matrix.org)
  - Rocket.Chat has its own built-in federation support
  - Mattermost only supports federation in its beta version.
- Element has been designed from the outset for end-to-end encryption, while only the beta version of Rocket.Chat supports end-to-end encryption. Mattermost does not offer end-to-end encryption.
- Rocket.Chat is perceived to be the most user-friendly solution. Mattermost has the most features, and Element has the best federation and encryption features.

2.2.1 Element

Several EU public-sector organisations use Element internally or when in contact with citizens. Element is used within parts of the French State, via the application Tchap. In Germany, Element is used within the armed forces and the health sector via the applications BwMessenger and Gematics respectively.

The Swedish Social Insurance Agency is currently evaluating Element in a pilot project. If the pilot is successful, the Swedish Social Insurance Agency will use the solution internally and also offer it as a service to other public authorities, within the framework of its mission.

Element offers permanent chat rooms, with support for group and one-to-one chat. It also supports one-to-one and group video calls through integration with Jitsi (see section 2.3). Other features include widgets (plugins) and bots, making Element a comprehensive collaboration platform. End-to-end encryption is available for all functionality.

Element differs from other chat solutions in that it uses the open-source Matrix protocol, reducing lock-in effects since both the client and server can be replaced with other solutions on the market. This means that organisations can still collaborate with each other even if they choose different clients and servers. The Matrix protocol is based on a decentralised design, with robust federation capabilities built in. Element also supports the standalone bridging solution Matterbridge.

2.2.2 Rocket.Chat

Rocket.Chat is an open-source solution for permanent chat rooms, with inbuilt support for group chat, one-to-one chat and video conferencing. Rocket.Chat uses Jitsi or BigBlueButton as video-conferencing solutions. It also supports file management in connection with chats. Rocket.Chat comes with APIs for enhanced functionality and systems integration. For example, it is possible to connect Rocket.Chat with other solutions via Matterbridge.

2.2.3 Mattermost

Mattermost is an open-source solution for permanent chat rooms, with inbuilt support for group chat, one-to-one chat, video conferencing and Kanban. It also includes functionality for repetitive processes such as incident management. Mattermost uses Jitsi as its standard video conferencing solution but also supports other solutions, such as BigBlueButton. The solution supports the management of files linked to the chats, and documents can be edited directly in a chat room through integration with Collabora Online. Mattermost enables integration with other systems via APIs.

The standalone bridging solution Matterbridge enables Mattermost to communicate with a wide range of other solutions. Mattermost also provides experimental support for the federation of channels between multiple Mattermost installations.

2.3 Video conferencing

The need for conferencing services is a continued focus area, even though several public-sector organisations have recently identified suitable solutions. Public-sector organisations commonly use Skype, installed in their own IT infrastructures, and this has been our basic solution for video conferencing. However, our evaluation of video conferencing solutions takes into account that some organisations wish to move away from Skype for various reasons – for example, because support for permanent chat rooms has been withdrawn in the latest release, and there is limited scope for extending the solution's functionality. Our assessment is that a richer user experience could be achieved through a combined platform – for example, incorporating video conferencing and permanent chat solutions. We have therefore primarily selected solutions that we consider to have better functionality and integration capabilities than Skype.

2.3.1 Jitsi

Jitsi features in several of the solutions that we have analysed – both as a packaged service and as a video conferencing feature integrated into comprehensive solutions. Jitsi is a collection of open-source applications owned by 8X8, a US-based company that provides support, maintenance and cloud services. Several companies – including Element – offer commercial support for Jitsi, and several European and Swedish suppliers offer Jitsi as a service. The solution is also available for operation within an organisation's own IT environment.

Jitsi includes functionality for hosting smaller video meetings (currently with up to 75 participants), and it is compatible with most modern web browsers. Features include chat during meetings, screen sharing, own or blurred background, recording of meetings, audio and video sharing, streaming, and end-to-end encryption.

The Swedish Social Insurance Agency is also evaluating Jitsi as part of its pilot programme. If the results are positive, the solution will be available internally and as a service to other public authorities – as with Element.

We have assessed Jitsi in various different contexts – as a standalone solution, for example, and as a tool integrated into Mattermost, Element, Nextcloud or IceWarp. Our review indicates that there are many opportunities for integration of Jitsi with the other solutions that have been analysed.

2.3.2 Pexip

Pexip is a solution offered by the Norwegian company of the same name. It can be run in an organisation's own IT environment and is also available as a cloud service. Several Swedish suppliers offer Pexip as a cloud service. We have excluded Pexip's own cloud service since it is deployed through Amazon Web Services.

Pexip offers features such as audio, video, chat and integration with video conferencing systems. Video conferencing is the principal feature, and chat features are connected to ongoing meetings. Pexip's interface can be customised or transformed to reflect an organisation's own branding, for example. The solution can be scaled up to manage large meetings. Pexip is already in use by some of Sweden's regional and municipal authorities.

2.3.3 Cisco Meeting

Cisco Meeting is a solution created by the US company Cisco. There are European suppliers offering the solution as a service, and it can also be operated in an organisation's own IT environment. We have excluded Cisco's cloud service Webex from our evaluation.

Cisco Meeting is a video conferencing product that supports chat, group chat and one-to-one chat. It also supports integration with video conferencing equipment. The chat and group chat features use the XMPP protocol (for the exchange of structured information) and support XMPP federation.

2.3.4 Large meetings

A number of public-sector organisations want to be able to hold meetings with many participants (1,000 people or more). There is no agreed definition of a large meeting, but we have considered factors such as the number of participants, who can make themselves heard, moderators and chat management features. In the course of our work, we have not identified any specific solutions for large meetings. However, several suppliers have stated that their solutions can meet at least the requirement for a large number of participants, through investment in servers and network infrastructure.

2.3.5 Streaming

As with large meetings, it must be possible to deal with large numbers of participants, through the use of effective administrative features for moderators and video and audio streaming solutions, for example. Some organisations also wish to be able to broadcast live or manage video recordings via external video players. In the annexe *Possible solutions*, we therefore outline the solutions Screen9, Quickchannel and Wowza.

2.4 Kanban

There is a demand for opportunities to create Kanban boards. Solutions for this are integrated into services such as Nextcloud and Mattermost, and the sticky note features in whiteboard solutions can also be used to some extent. Several options, such as Kanboard and Wekan, offer open source code for installation in organisations' own operations, but we have not been able to examine them in detail.

A Kanban solution can be designed in many different ways, depending on requirements. We have focused on evaluating solutions that can be integrated with other collaboration platforms, since this approach would best meet our requirements.

2.4.1 Nextcloud

Nextcloud has a simple Kanban feature that supports task-planning visualisation. The Kanban board is integrated with calendar and tasks modules.

2.4.2 Mattermost Boards

Mattermost Boards includes a simple Kanban feature that enables a board to be created for each discussion channel. However, the boards are not linked to the other Mattermost features.

2.4.3 Stackfield

Stackfield is a task-focused tool that supports collaboration within working groups. Task planning can be visualised on a Kanban board. A more in-depth outline of the solution is provided in the annexe *Possible solutions*.

2.4.4 Jira

Jira is a comprehensive case-management system that supports agile working methods. Cases can be visualised using Kanban and scrum boards. Jira can be configured to support different process flows. The solution can be purchased as a cloud service or for independent operation. Since the cloud service is deployed through Amazon Web Services, we have excluded it from our evaluation. Jira has primarily been developed to support software development teams, and it can therefore be perceived as too advanced for other users.

2.5 Whiteboard

There is great demand for a feature that enables collaboration on a visual basis in a shared space – before, during and after a meeting. Many organisations conduct workshops using a combination of whiteboards and video conferencing. Whiteboards can be used to document the outcome of a video conference directly, reducing the post-meeting workload.

We have identified Collaboard, Nuiteq Stage, Bluescape and iObeya as the solutions that best match our requirements.

2.5.1 Collaboard

Collaboard is a well-developed whiteboard application that runs directly in web browsers and can be used independently. We have excluded the associated cloud service that can be purchased within Microsoft Azure. Collaboard has an unlimited workspace and includes about 50 ready-made templates for workshops, brainstorming and flow diagrams.

2.5.2 Nuiteq Stage

Nuiteq Stage is also run directly in web browsers, and its whiteboards are complemented by the option of audio and video meeting integration. The solution includes most of the tools required for a workshop, and provides for an infinite number of whiteboards of predetermined size.

2.5.3 Bluescape

Bluescape is a UK company that offers its solution for independent operation or as a service via Amazon Web Services. We have excluded the latter option. Bluescape's online whiteboards enable real-time virtual collaboration. The solution comprises a broad range of features including drawing tools, multicoloured digital sticky notes, shapes and brainstorming templates. Users can add comments to a board directly, or start a video call with other users in the same board.

2.5.4 iObeya

iObeya's whiteboard solution is also run via a web browser. It provides digital rooms, with several whiteboards of different sizes stored in each room. The solution includes

different backgrounds, templates and various types of sticky notes. iObeya can also be used as a Kanban.

2.6 File storage

There is high demand for a file storage solution that enables sharing with external collaboration partners. As outlined previously with reference to permanent chat rooms, file storage and/or management can be a basis for collaboration – for example, as illustrated in Section 2, Figure 3. We are also investigating other solutions, which are outlined in the annexe *Possible solutions*.

We have identified Nextcloud and Storegate as the solutions that best match our requirements.

2.6.1 Nextcloud

Nextcloud's file storage features are customisable. The solution's functionality can be limited to file management only. We consider Nextcloud to be a good file management solution. The Swedish Social Insurance Agency ("Försäkringskassan") uses Nextcloud for the provision of services to other public authorities.

2.6.2 Storegate

Storegate is a Swedish cloud service (that has been Norwegian-owned since November 2021) used for synchronised file storage – comparable to Dropbox or Microsoft OneDrive, for example – which can be used for backup and file sharing with external organisations. There are options for integration with Microsoft Outlook, for example. The Swedish Board of Student Finance ("Centrala studiestödsnämnden") uses this solution.

3 Considerations

3.1 Legal considerations

A digital collaboration platform for the public sector needs to live up to the legal prerequisites that apply to public authorities. The relevant legal prerequisites will be identified according to the amount of data to be handled. Since the group's mandate does not include analysis of issues specific to individual cases or public authorities, the framework for the group's legal considerations is rather based on general legal issues that typically arise in connection with the outsourcing of IT services.

A variety of provisions apply to public-sector activities, such as public access to documents, registration of public records, Swedish administrative law regarding service and accessibility, and rules on the archiving and culling of public records, to name a few. During the course of the work, it has been confirmed that it is generally possible to combine a code of good practice with IT solutions, as long as they are properly implemented within the public authority. The working group's considerations are outlined in the annexe *Requirements Specification*.

In matters of confidentiality regarding outsourcing and third-country transfers under the EU Data Protection Regulation,[3] we have mainly based our work on the legal assessments that have been made previously during the review of Teams.[4] We have therefore ruled out solutions that are under the direct or indirect control of a foreign company – for example, through infrastructure – where there is a risk of disclosure of classified information, or of direct or indirect transfer of personal data to third countries without legal basis under the EU Data Protection Regulation.

This excludes suppliers that may unlawfully expose data to foreign authorities – in particular those of the United States – through operation, infrastructure, service delivery, support, license activation, etc.

3.2 Information security considerations

There is one common aspect to the use of all IT services: given the amount of data involved, there is a call for data security with the right level of protection. This usually makes information classification and risk analysis necessary. This in turn means that information is required about the data in question, the applicable regulations, and the organisation's internal requirements and conditions. To that end, we have had to make several assumptions.

A given starting point has been that the target groups are public sector organisations that are affected – to a greater or lesser extent – by information security regulations as well as specific operating rules. The requirements specification therefore includes specific

[3]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[4]See the decisionissued by the Swedish Tax Agency and the Swedish Enforcement Authority on 3 May 2021 relating to Swedish Tax Agency case 8-958696 or Swedish Enforcement Authority case KFM 10419-2021.

requirements designed to protect the information from disclosure to unauthorised recipients, while ensuring that it is accurate and accessible to authorised recipients.

A fictitious service is assumed to handle data for various purposes, including administration, use, access management, lifecycle management, operation, maintenance, support and troubleshooting. Examples of such data include:

- user register data
- meeting data
- streamed and stored meeting materials
- uploaded and shared files
- metadata and version history
- statistical data
- access management data
- design sketches and system diagrams
- system and event logs
- databases and backups
- support information
- user support data
- analyses
- agreements

Based on assumptions about the target group, legislation and information sets, we have carried out a fictitious information classification and drafted a complete list of proposed safety measures from SS-EN ISO/IEC 27002, which are included in the requirements specification.

3.3 Technology considerations

User experience has a major impact on how a solution is received by an organisation. The underlying technologies must also support the organisation's current and future needs with regard to user numbers, external cooperation requirements and mobility, for example. The evaluation of technical functions and capabilities has therefore been an important part of the assessment of the solutions.

The requirements specification partially reflects the technical assessments in the solution categories analysed. It indicates how well different technical functions, capabilities and components are executed in a solution. Since the focus has been on finding solutions for a broad range of public-sector organisations, we have chosen to focus on common requirements rather than specific technical applications required by only a few authorities. The working group has discussed a wide range of issues in formulating these requirements. Since it is not possible to recount all the arguments in their entirety, we have listed the following examples of technical issues that we have considered.

- What are the components of the solution?
- How customisable is the solution?
- How scalable is the solution?
- Is the solution platform independent?

- Is there support for mobility: i.e., can employees use different devices to consume and produce information?
- Which safety components and mechanisms are used in the solution?
- To what extent is external collaboration (federation) supported?
- What support is available for two-factor authentication?
- How is the solution applied to clients? Is customisation required? Which platforms are supported?
- Are third-party solutions supported?
- Is the solution a niched technology application or can it create value on a broader scale?
- Are there lock-in effects that needs to be considered?
- Specifically for video conferencing services: does the solution support traditional telephony?

Building a combined solution from multiple "best of breed" solutions

The working group has taken into account the fact that several organisations already have solutions in place that they need to continue using indefinitely, where these solutions need to be complemented with additional functionality.

A number of solutions provide the opportunity to connect collaboration solutions from different suppliers through application programming interfaces (APIs), federation, bridging technology or built-in system integration. Open-source software has the added advantage of being able to support other competing solutions through open APIs. In section 2, we present comprehensive, standalone and combined solutions.

Considerations regarding collaboration between organisations

We have also considered the solution's ability to connect with other organisations' solutions. At the most basic level, the solution should allow guests to be invited. However, our assessment is that this creates definite limitations.

Many users expect collaborative solutions to offer flexible ways to interact with other organisations. One example is that many Skype users are used to being able to seek out people at other public authorities and to send instant messages via chat or initiate video meetings. Our assessment is that users will continue to expect to be given these opportunities through future solutions, and we have taken this into account during our considerations.

The following functionalities have been assessed in the solutions under consideration:

- Guest access – for example, the ability to send a link to a document or invite an external user into a chat room.
- Bridging – for example, making it possible to establish a chat room between organisations with different chat solutions.
- Federation – for example, making it possible to search for people, chat, create chat rooms and conduct video meetings with other organisations using the same solution or protocol. This is a feature that Skype offers today.

Our considerations are outlined in more detail in the annexe *Collaboration models*.

3.4 Considerations regarding dependency, lock-in effects and digital sovereignty

3.4.1 Dependency and lock-in effects

The working group's understanding is that the public sector has long been dependent on Microsoft as a supplier of office support tools and digital collaboration solutions. There are many reasons for this, including some historical factors. One explanation is the volume agreement negotiated by the Legal, Financial and Administrative Services Agency ("Kammarkollegiet"), Adda and Microsoft, which has benefited the public sector but has also increased the level of dependence. Many organisations have extended, expanded and upgraded their Microsoft licences over a long period, and there has been little incentive for competitive procurement. This has led to significant lock-in effects – for example, with regard to technology, data formats, training and habits.

The phasing out of locally installed software in favour of cloud services also creates additional lock-in effects. In many cases, the public sector is unable to use these cloud services due to legal obstacles, for example. In other words, many organisations face the dilemma of being dependent on Microsoft who at the same time is phasing out locally installed software in favour of cloud services that the organisations cannot use.

When evaluating solutions, our focus has been on ensuring that future solutions are characterised by transparency, with the possibility for organisations to freely choose local installation, service delivery, hybrid solutions, service management by a partner that can provide sufficient protection, or service management by another public authority. Increasing the use of open-source software can be a way to achieve this. The essential consideration is that the solution should enable internal and external interaction and provide opportunities for customisation and integration with other solutions, according to the needs of the organisation.

3.4.2 Digital sovereignty

Despite the fact that the work has been limited to solutions falling within the scope of the Swedish Protective Security Act, the issues of dependence and lock-in effects raise an important overarching perspective.

The report *Cybersecurity in Sweden – Threats, methods, deficiencies and dependencies*, published in 2020 by the Swedish National Defence Radio Establishment, the Swedish Armed Forces, the Swedish Civil Contingencies Agency, the Swedish Police and the Swedish Security Service, states the following:

"Outsourcing of IT infrastructure also creates dependence on the service provider. When IT services are outsourced, global service providers are often contracted, which means the resulting dependence is international. This is sometimes expressed as the risk of loss of digital sovereignty – a concept used in the EU context which means that a state loses some of its control over its independence, autonomy and freedom of action in the digital sphere."

When public authorities assess the type of data they will store and process in a public cloud service, they typically only consider their own organisation's information. However, cloud service providers store and process many public authorities' data, which means both aggregation and accumulation of data by a party. We consider it to be difficult to oversee the consequences for Swedish society of, for example, a cloud service becoming inaccessible. However, it is easy to determine that the interruption or severe disruption of several public-sector operations could quickly lead to a serious crisis for our society. Other examples of consequences include significant costs and additional work, reduced operational capacity, and a decreased level of trust in the organisation or in society as a whole.

Against this background, we have assumed that a cloud service provider should also be prepared to conduct its own assessment of aggregated and accumulated information in its solution – for example, through a protective security analysis. Placing such requirements on public-sector suppliers would create opportunities to strengthen Sweden's digital sovereignty in the long term.

4 Methodology

4.1 General considerations

The work to identify and evaluate solutions has been based on the considerations set out in chapter 3 and has informed the selection rules and requirements specification developed by the group. From this perspective, it is important to emphasise that the requirements have been developed based on a fictitious delivery scenario.

Data security issues have been considered during this work, but the list of requirements was not preceded by the standard information classification and risk assessment outlined in section 3.2. However, the starting point was that the solution must be able to manage both internal and external communications, including case handling. Naturally, authorities whose activities are largely subject to the provisions of the Swedish Protective Security Act may impose higher requirements than the working group has done. The need for such specialised security solutions is outside the scope of our assignment.

It is also important to mention that, in many cases, we have based our assessments on solution descriptions that have been provided to us. It is therefore possible that some solutions may not live up to the promises of the description provided. It should also be noted that the solutions assessed are under continuous development. Functionality that is missing in some solutions may be added in the near future. And conversely, existing functionality may be discontinued in future releases. For this reason, the working group has primarily tried to form an opinion based on existing information, and we have not placed any faith in suppliers' promises of future functionality.

Suggestions regarding solutions came from the reference group, from our own research, and from suppliers who have contacted us independently. Analysis of solutions of which we were made aware after 6 September 2021 was limited according to the time available.

Several demonstrations of solutions were carried out for the reference group, which the group has found interesting. Public-sector organisations with experience and available testing environments participated in several demonstrations.

4.2 Selection of solutions at an overall level

As a first step, we developed rules for the selection of solutions. The purpose of the selection rules was to enable an initial sorting of the solutions proposed to us. Suppliers excluded due to the selection rules were not subject to an in-depth evaluation.

According to the considerations set out in section 3.1, any solution delivered as a service and dominating owner interests present a risk of extraterritorial application of foreign law has been excluded. The same applies to any solution that may – either directly or indirectly – transfer personal data to countries outside the EU/EEA, with the exception of countries that the European Commission deems to have an adequate level of protection. The group therefore makes a distinction between software that can be run in an organisation's own IT environment, and software that is delivered as a service from another party's infrastructure.

Solutions that are not yet fully developed have also been excluded. This includes solutions that are at the prototype level, lack basic features, are not possible to procure, or have a very small customer base. In this category, we have also included solutions that lack important features for the proper use of the service, such as meeting services without chat functionality.

4.3 Requirements specification and evaluation of requirements

An important part of the work has been to develop a *Requirements specification*, which is annexed to the report, and against which solutions have been evaluated. The requirements have been developed in collaboration with the reference group. In addition to the selection rules, they specify our technical, legal and security considerations. The requirements specification was published on 28 September 2021 at esamverka.se

Solutions that have been evaluated against the requirements specification and largely meet its demands are presented in the section "Possible solutions". Please note that, in some instances, the evaluation has been based on information supplied by the solution provider. In some cases, we have had access to test environments and have had the opportunity to evaluate the actual solution in question.

5 Impact assessment

The impact assessment is based on the assumption that organisations will choose one of the solutions presented in this report. The following considerations are particularly relevant:

- Many public-sector organisations currently use Skype. This solution enables public authorities to create federations with other organisations that use Skype. Some authorities are part of an open federation, which has become a standard for cooperation between public authorities. Another aspect of Skype as an established external collaboration solution is that many organisations have adjusted their firewall and security settings for Skype federations – particularly during the COVID-19 pandemic. If several public authorities turn to a variety of different solutions for digital collaboration instead, this standard is likely to become eroded over time.
- A collaborative platform used on a daily basis for internal and external communication becomes a critical operational function – especially if sensitive information is available through such a service. The scope for disturbances or interruptions to such a function could have serious consequences for the organisation, making reliable continuity plans a requirement.
- The replacement of established solutions involves costs – which could double in cases where complementary solutions are required. Other challenges include competence and change management. Another possible consequence is that organisations are forced to work with different solutions in parallel, negatively affecting information management. In our experience, it can take considerable time to replace an established solution altogether. It is therefore necessary to adopt a position on the parallel use of different document storage systems, or to draft an action plan for phasing out existing solutions. The implementation work will also require specific competence, and risks can result from a lack of skills and resources – especially if there is competition between public authorities with regard to staff recruitment and the procurement of consultants.
- The growing trend towards solutions delivered as a service, and thus available via any type of client, requires both a technical and a mental shift in terms of ways of working. When solutions are seamlessly available to public-sector employees even outside of work, higher demands are placed on both public authorities and the individual. In other words, the digital availability of information that was previously limited to the public authority's own environment poses challenges for the use, storage and culling of information. In this context, particular attention should be paid to the challenges of proper handling of information when data and documents flow across organisational boundaries and are considered to be processed, and to public documents in accordance with the provisions of Sweden's Freedom of the Press Act.
- If several large government authorities specify similar requirements with regard to collaboration solutions, this is likely to have an impact on the market. There is reason to assume that the *Requirements specification* annexed to this report could influence the design of future solutions.
- An important consideration with regard to potential solutions is that a long-term shift will take place. When an organisation makes a comparison with a

view to replacing an existing modern digital collaboration platform in a short time, some functions are likely to be lacking. For this reason, it is important for the public sector and the IT industry to work together to achieve a gradual shift from locked-in solutions towards open, customisable alternatives.

- Today's market consists of a few very large suppliers and many smaller suppliers. One risk is that a public-sector organisation implements a solution from a smaller supplier, which is subsequently acquired by a larger supplier operating in the US, for example. This type of risk is always present – as is the risk of suppliers closing down or significantly changing their solutions. One way to counteract this risk is to use open-source solutions.
- Finally, a move towards modern collaborative solutions gives the public sector a greater opportunity to establish solutions to enable contact and interaction with individuals. For example, video conferencing solutions with end-to-end encryption can be an alternative to customer meetings that currently require a physical visit.

6 Continued work

At an early stage in the project, there was already a clear need for further work. Information, thoughts and ideas that could not be considered in the initial stage may still be vital for ensuring suitable digital collaboration solutions for the public sector.

The starting point for our continued efforts is to build on the conclusions of this report. In subsequent steps, we will aim to ascertain that the options work, are suitable, and can be implemented by public-sector organisations. Collaboration within and between public authorities should provide at least the same level of functionality offered by Skype today, but the long-term goal is to enable the entire public sector to interact fully.

The pursuit of the following areas of work therefore remains significant within the eSam project:

1) Develop a specification for federation between various video conferencing and chat services/solutions.
2) Further develop the requirements specification for the technical, functional and regulatory aspects of a procurement document.
3) Create a knowledge centre where the public sector can meet, exchange experiences, share procurement documents, test solutions, and manage joint pilot projects.

These three areas of work should be pursued as eSam projects and managed by the eSam steering group. The project requires a full-time project manager, who should belong to one of the eSam member organisations. A decision on continued work is currently under consideration.