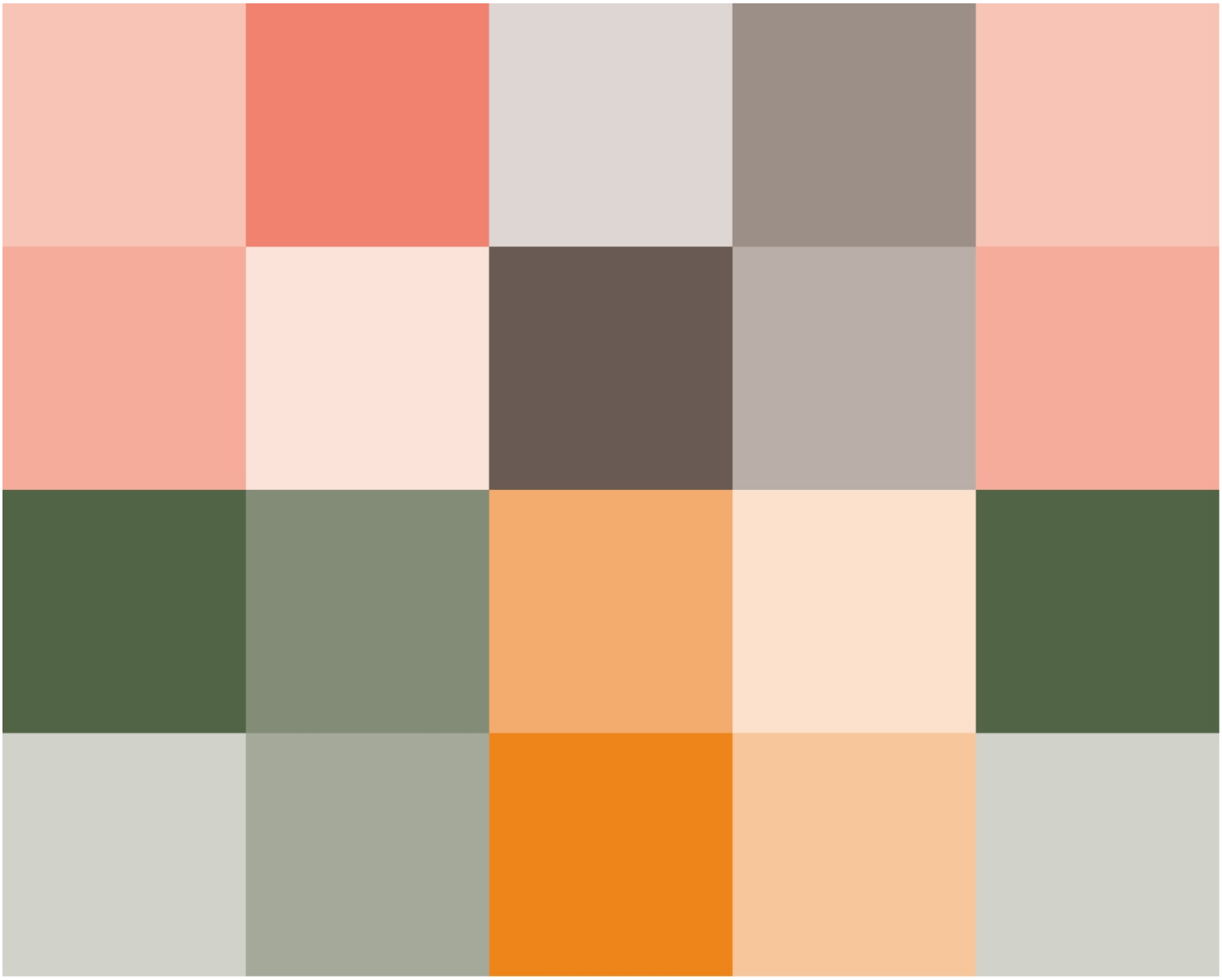


Secure and efficient electronic information exchange in the public sector

Final report of government assignment Fi2018/02150/DF, FI2018/03037/DF and I2019/01061/DF

DIGG Dnr: 2019-100

Summary

The Swedish Companies Registration Office, the Swedish National Courts Administration, the Swedish eHealth Agency, the Swedish Social Insurance Agency, Lantmäteriet (the Swedish mapping, cadastral and land registration agency), and the Swedish Agency for Digital Government (DIGG) were jointly tasked with analysing and submitting proposals aimed at improving the security and efficiency of electronic information exchange within and with the public sector.

The authorities performed a needs analysis which identified and prioritised the common public-sector needs. The needs analysis highlights prioritised needs related to information management, trust and security, information exchange and digital services.

The authorities performed a comparative international analysis in which existing national solutions for information exchange and solutions from the rest of the world are described and analysed in order to benefit from lessons learnt and insights. The comparative international analysis shows that the existing national solutions need to be supplemented by common regulatory frameworks and standards and common public-sector building blocks to allow for barrier-free exchange between sectors in the public and private sector. It is not considered appropriate to replace the existing infrastructure with a solution from the outside world.

Based on the analyses, the authorities propose that there should be four categories of common public-sector building blocks in an ecosystem with a common public-sector digital infrastructure for information exchange. The solution is described as a conceptual architecture and proposals are also made regarding governance models and arrangements for allocating responsibility for the building blocks. The four categories are digital services, information exchange, information management, and trust and security.

To implement the building blocks, the authorities propose some fundamental measures that are considered to be a necessary first step towards more secure and more efficient information exchange. The authorities propose that the government should establish a national governance model to allow decisions to be made about activities relating to the development and implementation of a common public-sector digital infrastructure for information exchange. New government assignments and funding are also proposed in order to analyse, develop and implement a roadmap and to implement the prioritised building blocks. Finally, a legal commission is proposed to ensure that the necessary long-term legal arrangements are in place allowing the building blocks to be developed.

Contents

1 Introduction

1.1 Assignment and background

In early 2018, the Swedish Companies Registration Office, the Swedish National Courts Administration, the Swedish eHealth Agency, the Swedish Social Insurance Agency, Lantmäteriet (the Swedish mapping, cadastral and land registration agency)[1], and the Swedish Agency for Digital Government (DIGG) were jointly tasked with analysing and submitting proposals aimed at improving the security and efficiency of electronic information exchange within and with the public sector, for example through greater standardisation.

Electronic information exchange in this context refers to the systematic provision of basic data and other exchanges of structured and unstructured information, such as the status and messages between actors.

A previous assignment found that the responsibility for basic data needs to be clarified and that a national framework should be established. The provision of basic data in the form of technical services and infrastructure is addressed in this assignment, but it is not confined to managing basic data but also covers information exchange with and within the public sector in general.

Sweden lacks several of the common public-sector basic components and solutions that are available in comparable countries. The lack of a national digital infrastructure has resulted in a large number of authority-specific and sector-specific solutions that differ from one another, which has largely produced an inefficient regime for the public sector as a whole. Government authorities and municipalities have so far mainly developed solutions for electronic information exchange based on the needs and circumstances of their own operations. The lack of governance and coordination at the common public-sector level, and the diverging sectoral responsibilities, mean that legal and security issues continue to present obstacles which cannot be overcome between the individual parties.

To summarise the issues, in Sweden there are:

- Solutions for information exchange in different sectors and domains that are not universal.
- Different information exchange solutions that serve the same purpose.

[1] Assignment concerning secure and efficient electronic information exchange in the public sector (*Uppdrag om ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn*) (FI2018/02150/DF, FI2018/03037/DF and I2019/01061/DF).

- Information exchange solutions developed for specific purposes and often bilaterally between two actors. They cannot be reused or scaled up as there is no basis in law, for example.
- An absence of common standards and reusable technical components and building blocks for information exchange.
- A lack of clarity as to who should be responsible for common public-sector or national building blocks and standards for information exchange.
- An absence of governance and coordination at the common public-sector level, and diverging sectoral responsibilities for different sectors.
- Legal and security issues that present obstacles that cannot be overcome in individual projects, requiring information to be exchanged on paper, with private individuals and companies acting as couriers between authorities.

1.2 Objectives

According to the government assignment, the governance and coordination of public sector information provision needs to be strengthened by clarifying the division of responsibilities and increasing standardisation. The authorities' interpretation of the objectives of the assignment is that in Sweden there should be a common public-sector digital infrastructure, with common public-sector solutions that contribute to efficient and secure information exchange and that are clearly regulated in terms of the responsibility of authorities.

1.3 Methodology and execution of the assignment

The assignment was carried out in project form, with a project steering group composed of one representative from each organisation involved in the assignment and the Swedish Association of Local Agencies and Regions (SALAR). DIGG occupied the role of coordinating project leader, and all the organisations involved in the assignment and SALAR contributed resources to a number of different working groups. The working groups focused on different aspects of the report, namely the needs analysis, comparative international analysis, architecture, law, security, and coordination and communication. All the participants attended monthly meetings for information sharing, analysis and planning. The steering group and several of the working groups have been shared with the government assignment entitled “Secure and efficient access to basic data” (*Säker och effektiv tillgång till grunddata*) and both assignments attended the monthly meetings described above.

1.4 Constraints

According to the assignment remit, the proposals made by the authorities must be accommodated within the existing law.

In the assignment, the authorities did not address the handling of classified information. This is because this type of information must meet special security standards under the Protective Security Act (*säkerhetsskyddslagen*) (2018:585) and only a limited amount of such information is exchanged between authorities and companies. When information exchange does take place, it is almost exclusively between well-defined actors using strictly regulated methods.

1.5 Concepts

In digitalised collaboration, it is important to establish a common concept structure. By using concepts that have already been agreed, we reinforce established usage in the collaboration between different actors. This report uses the concepts below.

Important concepts	Description	Source
Actor	Person or organisation acting in collaboration.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Asynchronous communication	In asynchronous communication, the parties are independent of each other in terms of time. Asynchronous means transmission that is not simultaneous.	Swedish Centre for Terminology TNC: Basic terms in our languages for special purposes (*Basord i våra fackspråk*) 2012.
Concept model	Graphical representation of the relationship between concepts in a coherent concept system.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Building block	A building block is basic digital service infrastructure which enables, and can be reused in, more complex digital services. A building block may consist of technical capabilities, but also standardised models and paradigms that must be reusable in digital information exchange.	CEF Definitions Regulation (EU) No 283/2014
Data	Representation of facts, ideas, etc. in a form suitable for transmission, interpretation or processing by humans or by automatic equipment.	Rikstermbanken (Sweden's national term bank)

Domain coordinator, basic data domain	Responsible for national coordination of production, collaboration and provision of basic data in the basic data domain.	Cf. interim report on detailed plans (*Delrapport Detaljplaner*) (Lantmäteriet)
Common public-sector digital infrastructure	Infrastructure consisting of different building blocks or components enabling digital development. It is used by many actors and sectors in public-sector administration to address cross-border and cross-sectoral needs.	Own definition
Common public-sector solutions	Solutions such as building blocks or components that can be used by many actors and sectors in public-sector administration to address cross-border and cross-sectoral needs.	Own definition
Basic data domain	Area of responsibility within basic data, such as personal information, company information, property information and geographical information.	Own definition
Information	Defined under data.	Rikstermbanken (Sweden's national term bank)
Information model	Graphical representation of information objects.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Information object	Carrier of information in an information model.	IRM
Information exchange model	Model describing the content of the information exchange between two or more parties.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Information owner	Actor responsible for the information created and handled internally.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Interoperability	The capacity or ability of systems, organisations or business processes to work together and communicate with each other by following common rules.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Component	A defined part of an infrastructure that can be used in different contexts but is independent. Synonymous with building block.	
Consumer	Actor receiving or using a service or information.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)

Customer	Person or organisation needing a service or information.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Source	Service from which an actor can obtain data.	Cf. Swedish Companies Registration Office (concept model for composite basic service)
Metadata	Data about data, for example the date of a decision.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Producer	Actor providing a service or information.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Collaboration	Different actors collaborating to achieve defined impact objectives and value for customers.	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
SLA – Service Level Agreement	Agreement describing the service level of a service. For example it could define response times, or when a service can be suspended for updates.	CEF Glossary
Standard	A standard is a common solution to a recurring problem.	Swedish Institute for Standards
Synchronous communication	Synchronous communication takes place in real time, in other words simultaneous communication between a number of parties.	Swedish Centre for Terminology TNC. Basic terms in our languages for special purposes (*Basord i våra fackspråk*) 2012.
Service	Packaged service or solution offered to satisfy a need	Guidance on digital collaboration (*Vägledning för digital samverkan*) (eSamverka)
Open data	Open data means all information that satisfies the requirements of so-called open knowledge, in other words information that is freely provided without charge and with few or no technical or legal limitations on how it may be used.	Report on digitalisation rights (*Digitaliseringsrättsutredningen*)

2 Needs analysis

Summary: The authorities consider that there is need for clear governance in the following categories of common public-sector needs:

- *Information handling.* This need concerns the ability to rely on the information and to assess the quality of information.
- *Trust and security.* This need includes the ability to verify that an identified actor is entitled to receive the information.
- *Information exchange.* This need includes the ability to search, compile, filter, share, access and receive updates on information from multiple sources (this includes so-called synchronous and asynchronous messaging).
- *Digital services.* This need includes the ability to impose conditions on information exchange in applications such as "Min profil" (My profile).

According to the assignment, the authorities must carry out a needs analysis regarding information exchange within and with the public sector. The needs analysis considered around 260 use cases from the Swedish Companies Registration Office, the Swedish National Courts Administration, the Swedish eHealth Agency, the Swedish Social Insurance Agency, Lantmäteriet (the Swedish mapping, cadastral and land registration agency), the Swedish Environmental Protection Agency, the Swedish Tax Agency and SALAR. Needs described in the assignment entitled "Secure and efficient access to basic data" (*Säker och effektiv tillgång till grunddata*) (Fi2018/02149/DF, Fi2018/03036DF och I2019/01060/DF) were also taken into account.

The needs were described on the basis of use cases and patterns of need. The use cases were developed from different perspectives, both "looking out" where the benefits are felt by parties outside the organisation and also "looking in", which means that benefits are felt within the organisation. The majority of the use cases described are based on the needs of the organisation in question.

This part of the assignment is described in a shortened form, and for more detailed information you are referred to project reports and the background documentation produced by the authorities in the context of the assignment. The conclusions of the needs analysis are summarised in this chapter on the basis of the common public-sector needs that were identified and prioritised.

The purpose of the needs analysis was to produce a basis upon which proposals could be made regarding a conceptual architecture for common public-sector solutions, as described in chapter 4.

2.1 Identified needs

Using the collected actor-specific use cases, the authorities identified the following 16 fundamental needs that are universally applicable to all actors:

For information handling

1. To be able to trust the information.
2. To be able to assess the quality of the information.

For trust and security

3. To know that an actor is entitled to receive information.

For information exchange

4. To exchange information in an individual case.
5. To exchange information comprising facts in cases.
6. To exchange information in different cases concerning the same issue.
7. To search, compile, and filter information from multiple sources.
8. To exchange information with third parties.
9. To handle common plans concerning an object.
10. To be able to arrange meetings digitally.
11. To be able to prepare documents without an official case/to be able to have a digital dialogue about incomplete documents.
12. To notify actors about decisions/proposals/messages.
13. To notify actors about decisions/proposals/messages and receive acknowledgement.
14. To search, compile, and filter information from multiple sources.
15. To exchange information about the business.

For digital services

16. To impose conditions on information exchange in applications such as "Min profil" (My profile).

The authorities analysed the actor-specific needs according to the quality standard ISO 25010[2] in order to identify those elements which are common to all actors. The standard is based on a number of areas that describe common denominators in a use case. The areas in the standard concern the following categories: actor, interaction, importance/weight, confidence, flexibility and responsiveness. The following conclusions have been drawn from the standard. The conclusions are presented as general requirements for an architecture of the common public-sector digital infrastructure for information exchange.

[2] ISO/IEC 25010:2011 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models

Actor: An architecture that satisfies the needs should not be constrained to any particular types of actor. The needs concern public as well as private actors. In an information exchange there are two categories of principal actors, normally referred to as the producer and the consumer.

Interaction: An architecture that satisfies the needs should include information exchange from one producer to one consumer, one producer to many consumers, many producers to one consumer, and many producers to many consumers.

Importance/weight: An architecture that satisfies the needs should create the conditions necessary for capabilities and functions such as the ability to create, read, update, search, and delete information in order to allow the authorities to perform their fundamental duties.

Confidence: An architecture that satisfies the needs must include capabilities and functions for monitoring, logging, etc. Secure identities and trust are needed in order to decide whether a consumer is allowed access to certain information or not. Greater digitalisation is a common need in which information that is already known must be reused. This is in line with established principles for secure and efficient information exchange, such as "obtain from the source", "one task at a time" and "reduce the administrative burden". Other aspects in this area include the ability to carry out quality checks on the basis of common profiles, or to provide services to different stakeholders.

The area also contains several aspects about the actual information, for example quality, status, source, sensitivity, etc. A consumer must know where the information comes from, what its quality is, whether it has been issued by an authority, whether it needs protection with regard to secrecy and privacy, and what level of protection must be given to the information before it can be received. A producer must also take these aspects into account before it can ever disclose the information to the consumer.

In the context of research and development there is a need to create so-called test beds, which require anonymisation of information.

Flexibility: An architecture that satisfies the needs must be flexible in terms of adaptation and development. One thing the needs have in common is a requirement, arising from the outside world and from technological development, to easily adapt systems and modify operating rules to make information exchange more efficient and secure. All types of information exchange require immediate changes to be made in response to incidents, sometimes within a week. Use in real time requires faster delivery times, which is considered to mean the capacity for changes within one month. New legislation implies changes with a timescale of about one year.

Responsiveness: An architecture that satisfies the needs should take into account requirements concerning how quickly the information needs to be accessed. Self-service and real-time information must be immediately accessible by the consumer.

The producer's need to check a request for information can delay access by up to an hour. Complex processing can take up to one day.

The authorities consider that all 16 needs and the requirements they impose on an architecture are to an extent already satisfied where the need for digital information exchange exists. The question then is what is lacking in order to achieve more efficient and secure information exchange? The main problems surrounding the needs are that the various existing solutions

- are not reused nationally,
- are not comprehensive in terms of the needs and
- are very different from each other for the same or similar needs.

What is considered to be lacking is national governance of common elements in an information exchange that recur in the different needs.

2.2 Prioritised common needs

In conclusion, the overall common need concerns the ability to share or obtain relevant information within and with a public administration in a straightforward and secure way. It must be easy to know where, how, when and to whom information can be made available.

This should be *simple* and *secure*, which creates a need for standardisation and consequently for national digital solutions that can be reused in information exchange.

The authorities consider that joint governance is needed for the following overall common needs, which are therefore considered to be prioritised.

A common framework is needed that can be applied to the following needs.

- *Information exchange.* This need concerns the ability to search, compile, filter, share, access and receive updates on information from multiple sources, in different stages and states (including messaging). Bidirectional communication must be possible. This general paradigm is about the need for easier digital access to information in an information exchange. Public actors often need to obtain information from a variety of sources when dealing with a case, common issues, inspection or various reporting obligations. In these situations, there is a need to easily find and access information among many actors that produce the information and many actors that need to consume the information. Examples include case handling in social services, collaborative projects to counteract errors, fraud and organised crime, rehabilitation cases and the detailed planning process, etc. This need includes asynchronous and synchronous messaging.

- *Security and trust.* This need concerns the ability to verify that an identified actor is entitled to receive the information. This general paradigm is an example of the

need for digital functions that provide secure access to information and thus a secure information exchange. Examples of such functions include secure identification, common permission management, and classification of information based on data protection rules (secrecy, privacy and security).

- *Information handling:* This need concerns the ability to rely on the information and be able to assess the quality of information. This general paradigm is an aspect that affects efficient as well as secure digital information management by an actor. The paradigm demands a common quality model for information that must be nationally accessible. Corresponding requirements regarding the content of the information were identified in the analysis of basic data carried out in the government assignment entitled "Secure and efficient access to basic data".[3]

- *Digital services.* This need concerns the ability to impose conditions on information exchange in applications such as "Min profil" (My profile).

The needs identified above are not sufficient in themselves, but should be considered alongside the needs analysis in the specified assignments. From the point of view of basic data, there is a need for a common framework allowing basic data and other structured or unstructured information to be used digitally. This general paradigm concerns the standardisation of the information that must be nationally accessible. On its own, straightforward and secure access is not sufficient to achieve efficiency.

It must also be possible to use information digitally, requiring it to be prepared for standardised use. Standardisation means that the information is described and structured according to common models and information standards, for example so that it can be combined with other data. The concept of basic data is used here as a generic term for information that is important in society and is therefore repeatedly requested. This need is described in more detail in the government report on the assignment concerning secure and efficient access to basic data (*uppdraget om säker och effektiv tillgång till grunddata*).

[3] Swedish Companies Registration Office, the Swedish Agency for Digital Government (DIGG), Lantmäteriet (the Swedish mapping, cadastral and land registration agency), and the Swedish Tax Agency, *Uppdrag om säker och effektiv tillgång till grunddata – slutrapport för regeringsuppdragen (Assignment concerning secure and efficient access to basic data) (Fi2018/02149/DF and I2019/01060/DF), DIGG dnr 2018-31*

3 Comparative international analysis

Summary: The comparative international analysis shows that there are important lessons and insights to glean from the EU, from the analysed countries, and from existing national solutions and initiatives.

The existing Swedish information exchange infrastructure satisfies or at least has the technical prerequisites to satisfy most of the needs identified in different sectors and domains. The existing national solutions need to be supplemented by common regulatory frameworks and standards and common public-sector building blocks to become more efficient and secure and to allow for cross-border exchange between sectors and with the private sector.

It is not considered appropriate to replace the existing infrastructure with a solution from the outside world. However, there are numerous components in the form of common public-sector building blocks that can be taken as inspiration and reused. The building blocks must be designed to meet Swedish needs and adapted to Swedish legal circumstances.

The process of establishing common public-sector solutions in Sweden can also benefit from valuable insights and experiences from other countries, mainly concerning governance, economic impacts and legislation.

The countries with successful common public-sector information exchange have established barrier-free exchange (within and with the public sector) by creating fundamental components. The countries did not consider information exchange primarily as a technical challenge, but instead worked on reviewing the legislation, created central funding models and established clear national governance and political leadership in issues such as mandatory connection and strategies.

The assignment tasked the authorities with a comparative international analysis of relevant international and national solutions for secure information exchange. The analysis must cover national as well as international information exchange initiatives and solutions. The comparative international analysis must describe the advantages and disadvantages of each solution with reference to the prioritised needs, and state how compatible it is with other existing solutions. Particular account must be taken of costs, economic impacts, security, secrecy and privacy aspects, as well as any legal obstacles. The assignment also provides scope for highlighting and benefiting from other relevant experiences from other countries.

On the basis of the comparative international analysis, the authorities are expected to submit proposals for possible common public-sector solutions. The solutions must be

compatible with applicable law, such as the personal data processing rules and the principle of freedom of information, and must observe the security considerations. The primary purpose of the comparative international analysis is therefore to serve as input for proposals on common public-sector solutions and proposals for actions within the assignment.

The comparative international analysis focused mainly on the countries' solutions for the supply and exchange of information in the public sector. These solutions are essentially technical solutions, but bearing in mind the issues in the assignment, a broader approach has been chosen in order to also cover other aspects and circumstances.

Seven countries were selected for closer scrutiny (Finland, Norway, Denmark, Belgium, Singapore, the Netherlands and Estonia). The main focus was on Estonia, Finland and Denmark as they are specifically mentioned in the assignment. Other countries were selected because they have made good progress on a national digital infrastructure, and several of the countries are highlighted as best practice by various EU initiatives and international comparisons and measurements in this area.

In addition to information exchange solutions in various countries, an analysis was conducted of EU-initiated projects and initiatives that have or will have an impact on the area. A selection of existing national solutions and initiatives is also described in the report, in particular the SHS dissemination and retrieval system (*Spridnings och hämtningssystemet*), Inera's service platform (based on RIV-TA) and the SDK project for secure digital communication (*Säker digital kommunikation*), which is based on eDelivery.

3.1 Procedure

The main method for the comparative international analysis is literature studies in the form of broad initial comparative international observations and an inventory of existing analyses and reports in the field that have bearing on the assignment. The aim is to benefit from previous experience and knowledge gathered in the field and to give an indication of which countries, initiatives and solutions are appropriate to analyse further and highlight.

The comparative international observations were supplemented by experience sharing with representatives from selected countries and the national solutions in order to find out more about the country's information exchange solutions and to describe them in more detail. The aim was to obtain a more nuanced picture of previous analyses and to capture insights and lessons that may not be evident from official reports. The method used for experience sharing is semi-structured interviews.

The comparative international analysis addresses the specific aspects set out in the assignment, supplemented by other relevant experience. These are analysed by presenting general paradigms and common features, and illustrating them with examples from different countries.

Appendix 1 contains descriptions of solutions and initiatives, and analysis based on specific aspects and relevant experience with examples.

3.2 Lessons from the comparative international analysis

The existing infrastructure in Sweden satisfies or has the prerequisites to broadly satisfy the needs identified in the needs analysis in the different sectors and domains. The principal need is therefore where there is currently no structured interaction, mainly considered to be in the form of cross-sectoral interoperability and information exchange, as well as transnational information exchange across national boundaries.

In a memo, Inera and SKL have noted and recommended[4] that existing information provision solutions should continue to be rolled out and strengthened in the sectors where they already exist and that supplementary solutions should be developed where there are none.

Ramböll too, in its report[5], follows similar reasoning and believes that no social benefit is likely to be gained in the short or medium term by replacing existing solutions with another solution from the outside world.

Information provision in the public sector is not primarily a technical challenge. The technical solutions can usually be adapted according to the relevant circumstances and needs. Compared with other analysed countries, there are some common public-sector building blocks, such as identification and permission solutions, of which there are none in Sweden and which are deemed to be important prerequisites for efficient information exchange.

Sweden has a choice to make regarding the technical solution and whatever the result, it is important to decide whether existing solutions should exist in parallel, be further developed or be replaced. What is clear from the experience of the other countries is that there is no simple answer to the question and there is not one solution that is preferable to another, but that they all have their own advantages and disadvantages.

The experience of the analysed countries indicates some important success factors – early scrutiny of the legislation, central funding models, clear national governance and political leadership. Mandatory connection and the use of common public-sector solutions are highlighted by several countries as crucial, and national governance can be achieved in several different ways, either through legislation or through collaboration and contractual solutions. In the absence of legislation, strong alternative incentives are required to promote the use of common public-sector solutions.

In some cases, Sweden may not even be able to make an independent choice, and in the context of EU cooperation it is likely that statutes and regulations will specify the use of

[4] A memo concerning national interoperability (*Ett kunskaps PM om nationell interoperabilitet*), Inera 2018-09-10
[5] Report on X-Road (*Rapport om X-road*) – Ramböll 2016-01-29

specific building blocks and technical solutions for the bilateral exchange of data. In the publicity for the Europe 2020 strategy, however, the European Commission states that it is up to the member states to choose their own technical platform and system support and also to decide whether the infrastructure is to be decentralised or centralised.

Many of the countries we analysed are subject to EU legislation and therefore have similar legal arrangements to Sweden regarding personal data handling for example. In principle there is no reason to doubt the extent to which components from the analysed countries could be reused in Sweden, especially as they are highly configurable.

The need for information exchange within a sector or domain is largely already being met by the many different authority-specific solutions that have been developed. It is not considered to make financial sense to replace the existing solutions with new ones. A national digital infrastructure and architecture consisting of common public-sector components and building blocks is a way to supplement, standardise and streamline the current situation.

In terms of socio-economic benefit, the private sector will gain the most from improved accessibility of basic data and other types of data held by authorities. It is therefore essential to configure common public-sector solutions to exchange information with the private sector too, where legal requirements are met.

The use of common public-sector solutions can be encouraged either with regulations and laws mandating connection or with financial incentives.

Several countries mention that the use of common public-sector services needs to reach a critical mass before the benefits can be realised. In order to encourage use of the solution, mandatory connection for the public sector is the law in several countries. In Finland, for example, there was also a financial incentive for public sector actors to connect with the option of co-funding.

The solution that Sweden chooses should be tailored to the specific needs and the existing infrastructure in the different domains and sectors. A solution based on APIs and common public-sector reusable building blocks and mandatory standards and regulations, like the solutions in Singapore and Finland, is considered to be the most appropriate route in order to standardise and streamline cross-domain and cross-sectoral information exchange.

This also enables and prepares for a more straightforward exchange with the private sector where legal requirements are met. Several authorities (including the Swedish Tax Agency, the Swedish eHealth Agency and Lantmäteriet) have already begun to develop strategies and solutions based on APIs.

4 Proposals for common solutions

Proposal: The authorities propose that there should be four categories of common public-sector building blocks in an ecosystem with a common public-sector digital infrastructure for information exchange.

1. *Digital services.* This category includes building blocks that enable standardised digital public-sector services for businesses and citizens. The building blocks are

- Mina ombud (My representatives) (prioritised)
- Mina ärenden (My cases)
- Mina meddelanden (My messages)
- Min profil (My profile)

2. *Information exchange.* This category includes building blocks that contain standardised paradigms and common infrastructure services providing easy digital access to information and exchange of information among information sources. This category aims to support category 1, but also allows private actors to build digital services that use public data and information. The building blocks are

- API management (prioritised)
- Address register
- Messaging

3. *Information handling.* This category includes building blocks that enable indexing and standardised, machine readable interpretation of information attributes and information services. These capabilities and components aim to support category 2.

- Metadata management
- Indexing

4. *Trust and security.* This category includes building blocks that enable standardised digital functions for secure information exchange, and aims to support the above categories 1 to 3.

- Identity (prioritised)
- Authorisation (prioritised)
- Trust rules (prioritised)
- Traceability

- Availability

The authorities consider that the relevant law needs to be developed in order to provide a sound legal basis for the building blocks. Initially it is proposed that the necessary feasibility studies, investigations and development of the national building blocks are performed on the basis of government assignments. In-depth security analyses are required for all building blocks.

The responsibility for the building blocks is proposed to be part of the public commitment (*det offentliga åtagandet*) relating to the common public-sector digital infrastructure for information exchange (legal governance model). This means that as a point of departure, it must form part of the responsibility of the relevant government authorities to develop and manage proposed building blocks.

The assignment requires the authorities to submit proposals for possible common public-sector solutions on the basis of the needs analysis and comparative international analysis. The authorities' proposals for common public-sector solutions are presented in this chapter according to the following points of departure.

- *Private actors*, including businesses and citizens, are the engine of digital development (demand-driven development). The development of more efficient and secure digital information exchange must involve private actors, presupposing and safeguarding their need to influence, scrutinise and trust the development process.
- *Existing architectures and solutions* are a starting point for development. For fundamental and rational reasons, it does not make sense to replace them with completely new solutions. Instead, they should be developed and shored up so they can operate in an ecosystem with common public-sector digital infrastructure. Nevertheless, models, international standards and principles from the outside world need to be reused as far as possible.
- *Basic common public-sector components* are, from a national perspective, a prerequisite in order to meet the needs of efficient and secure information exchange.
- *Coordinated governance* is a success factor in achieving secure and efficient common public-sector solutions. Clearly demarcated national responsibility for government authorities in the digital infrastructure is part of this success factor.
- *Agile development*, in other words development in small increments, is a success factor in realising benefits and helping organisations adapt more quickly in line with the general developments in digitalisation.

In order to turn the results of the needs analysis and comparative international analysis into proposals for solutions and actions, the authorities grouped the results into national capabilities in a number of areas. The identified capabilities were then used to create a conceptual architecture of national building blocks in an ecosystem with a common public-sector digital infrastructure for information exchange. The purpose of the conceptual architecture is to illustrate in general terms what is necessary in order to achieve efficient

and secure digital information exchange. This final report defines building blocks as those common public-sector solutions which the authorities have been tasked with proposing.

4.1 Proposed conceptual architecture for common public-sector information exchange solutions

The existing architectures have evolved over time with the aim of overcoming the challenges arising at various stages. The authorities consider the existing architectures for information exchange to be a good basis for further development. The aim of such further development is to achieve standardisation, uniformity and flexibility based on innovation and non-compulsion. This is to increase the pace of digitalisation and thereby enjoy the benefits of digitalisation more quickly.

The common public-sector solutions are presented below as building blocks in a conceptual vision, in an ecosystem with the common public-sector information exchange infrastructure. A building block may consist of legal, organisational, semantic and technical capabilities[6] and standardised models and paradigms that can be reused in digital information exchange.

An ecosystem is the way actors and services behave in synergy and symbiosis with each other in a balanced system. Being part of the ecosystem requires every actor to be "ecosystem ready". For example, it may be necessary to comply with regulations and standards. By defining this ecosystem, solutions and architectures for security and efficiency can be further developed. For example more efficient contract models can be established.

In general terms, the ecosystem architecture can be said to consist of a paradigm with central availability, based on loosely connected building blocks that enable development among many parallel actors simultaneously. Basic services allow access to information (stored centrally or distributed) through information exchange interfaces or APIs (Application Programming Interfaces) which are published near the information storage.

Gartner describes how APIs are published in an ecosystem to enable and promote service innovation[7]. The EU's CEF building block eDelivery also describes information exchange in ecosystems[8].

[6] EU, The New European Interoperability Framework, https://ec.europa.eu/isa2/eif_en – read 2019-06-27
[7] Gartner – Government APIs Are About Delivering Outcomes, Not Technology
[8] EU CEF eDelivery, "The future is reuse of the CEF building blocks" 2017

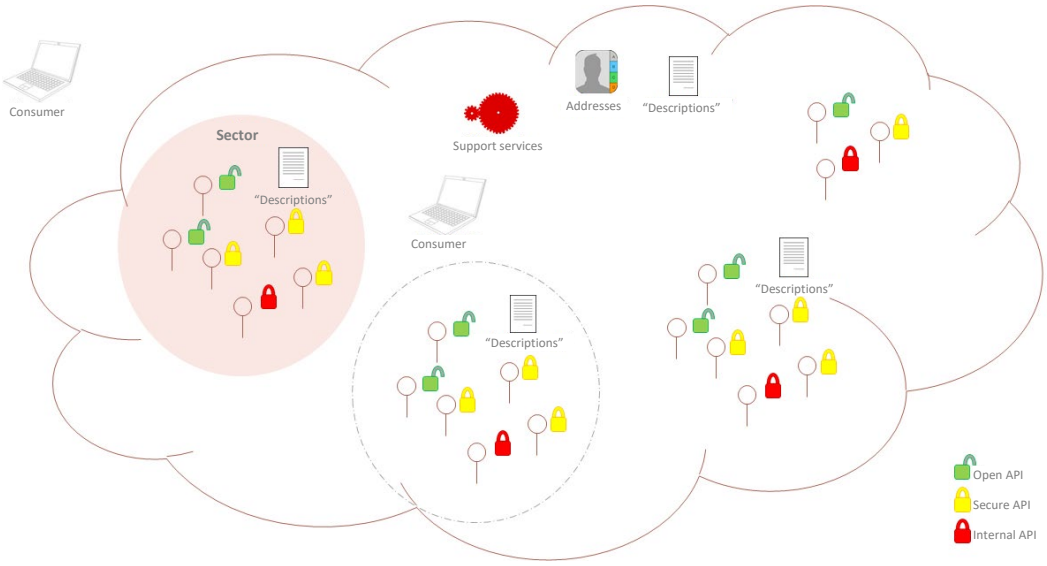


Figure A. Ecosystem for information exchange with and in the public sector

This architecture allows loosely connected components to be created that can gradually evolve over time. This provides the dynamism required between uniformity and flexibility. An API can be:

- Open – fully searchable and visible APIs, for example for open data
- Open secure – searchable and visible APIs that require secure identification, with rules-based authorisation controlling connection and information disclosure
- Internal – APIs that are only visible and available for internal use

The authorities propose that there should be four categories of common public-sector building blocks, namely:

1. *Digital services.* This category comprises capabilities and building blocks that enable standardised digital public-sector services for businesses and citizens. The category is not intended to address the actual exchange of information between machines and humans – user interfaces, user services. This is beyond the scope of this assignment.
2. *Information exchange.* This category comprises capabilities and building blocks that contain standardised paradigms or common infrastructure services for easy digital access to information and exchange of information among information sources. This category aims to support category 1, but also allows private actors to build digital services that use the information.
3. *Information handling.* This category comprises capabilities and building blocks that enable indexing and standardised, machine readable interpretation of information attributes and information services. These capabilities and components aim to support category 2.
4. *Trust and security.* This category comprises capabilities and building blocks that enable standardised digital functions for secure information exchange, and aims to support the above categories 1 to 3.

Below, the different categories and their building blocks are illustrated as a conceptual vision. Conceptual means that the proposal may need to evolve as progress is made in the coming years. The development is proposed to take place gradually.

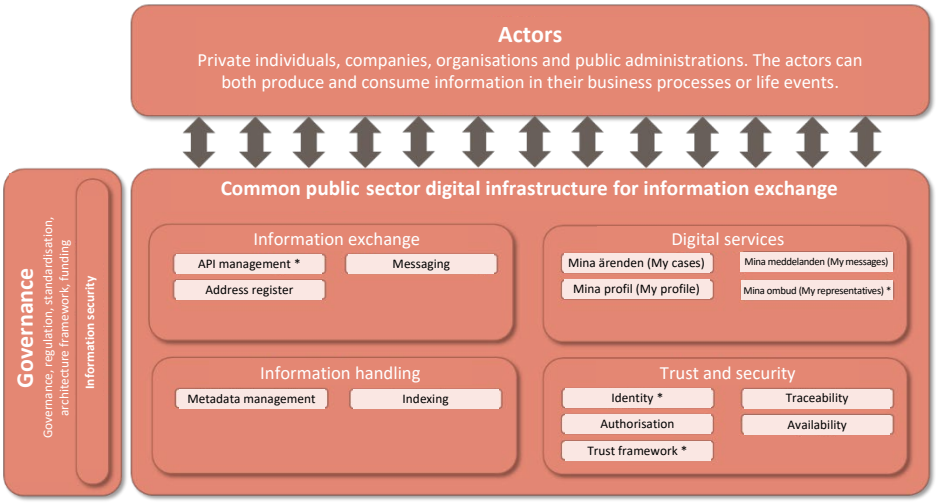


Figure B. Conceptual vision illustrating which common public-sector building blocks are needed for secure and efficient digital information exchange.

The following common public-sector building blocks are proposed to be included in each category. Building blocks that are marked with (*) are prioritised, which does not mean they are more important than the others, but that they are fundamental or essential in order to establish the ecosystem. Appendix 2 describes the prioritised building blocks in more detail. A separate in-depth security analysis must be carried out for each of the building blocks.

4.1.1 Digital services

Building block (*)	**Mina ombud (My representatives)**
Purpose	The purpose is to enable an individual to represent another individual or legal entity in a digital service. It includes the granting of permissions based on the authority to sign for the company, and the ability to monitor which permissions have been granted/received.
Existing solution	No national solution, but separate solutions exist locally in different authorities to address their own needs.
Needs/gap analysis	The result of the needs analysis cannot be achieved by any existing solution. The Swedish Companies Registration Office is running a feasibility study to achieve the result of the needs analysis.

Building block (*)	Mina ärenden (My cases)
Purpose	This building block provides an overall view of an individual's cases (person or company) in the public sector. The need is to be able to follow a wider range of cases than those of a particular authority. For example starting a business, rehabilitating from injury/illness, settling in the country.
Existing solution	No national solution, but many authorities and municipalities have their own solutions.
Needs/gap analysis	

Building block	Min profil (My profile)
Purpose	The purpose is to give users agency over the information about them held by public actors so they can see which actors have access to what and so they have some means of controlling access to the information. The building block also manages contact information and information about how an individual wants to interact with the public sector.
Existing solution	Instead of a national solution there are separate solutions for specific needs, for example at the Swedish Companies Registration Office (verksamt.se). Every authority with a Mina sidor (My pages) function has also created some of this building block.
Needs/gap analysis	Several components are missing at present or have an uncertain legal basis. 1. There is a lack of clarity as to who is the information owner for certain common data sets, e.g. contact information. 2. At present there are often no technical means of accessing the information, and there are no standardised APIs from information owners to retrieve information 3. As a user, in many cases, it is not possible to override secrecy in order to transfer information from one actor to another (data portability) 4. There are no national building blocks to give users an overview and the ability to control information flows. It is not easy for individuals to know where the

	information about them is located, who is allowed to access it and who has accessed it. 5. There are no national building blocks to follow a user's case involving multiple actors.

Building block	**Mina meddelanden (My messages)**
Purpose	To enable secure messaging to private individuals and businesses
Existing solution	Available nationally with the possibility of further development.
Needs/gap analysis	A business analysis is being planned in which the needs/gap and a repositioning of Mina meddelanden (My messages) will be studied.

4.1.2 Information exchange

Building block (*)	**API management**
Purpose	The purpose is to align functionality for publishing, using and executing APIs in the context of information exchange.
Existing solution	Instead of a national solution there are separate solutions for specific needs such as the Swedish Companies Registration Office, Lantmäteriet, the Swedish Tax Agency (Developer Portal), the Swedish eHealth Agency, the Swedish Forest Agency, etc.
Needs/gap analysis	There is no national coordination or national solutions such as prerequisites for finding and connecting to APIs.

Building block	**Address register for digital communication**
Purpose	The purpose is to safeguard digital communication on the basis of digital addresses so that messages can reach the correct addressee. This includes addresses for actors in the public sector (including private service providers), organisational functions in public actors, and companies and individuals.
Existing solution	Instead of a national solution there are separate solutions for specific needs. Example: SDK – *Säker Digital Kommunikation*

	(secure digital communication)[9], PEPPOL[10] – procurement handling including cross-border. The SDK and PEPPOL projects are both based on the eDelivery product. Other examples are HSA, a health and healthcare address register, and FAR, an address register for Mina Meddelanden (My messages).
Needs/gap analysis	No national solution.

Building block	**Messaging**
Purpose	Messaging involves defining common policies for structuring, transporting and validating digital messages, and for acknowledging receipt. Messaging also includes notification functions. An example of a need is an authority's need for notification from another authority that a particular information variable such as a decision has been made or changed.
Existing solution	Messaging is available nationally for some specific areas but requires more developed functionality. Examples include SDK and PEPPOL. In terms of notification, there is a need for an overview of the options for developing effective alert functions.
Needs/gap analysis	At present there are no national principles, rules and guidelines for generic messaging: • Encrypt, seal, and verify message transfer. • Validate message (structure and content) and transport envelopes before sending and after receiving. • Manage acknowledgements. • Trace and monitor. For notification, the legal context first needs to be reviewed but it is also necessary to examine how to create common design principles based on the needs.

[9] SDK – https://www.inera.se/aktuellt/projekt/saker-digital-kommunikation/ – read 2019-06-27
[10] PEPPOL – https://peppol.eu/ – read 2019-06-27

4.1.3 Information handling

Building block	Metadata management
Purpose	The purpose is to standardise descriptions of information and services. For example this requires uniform versioning, common descriptions of concepts and classification of information. The building block is more of a framework in nature than a service.
Existing solution	Instead of a national solution there are separate solutions, for example in the field of geodata under the act and ordinance on geographic environmental information (*lagen och förordningen om geografisk miljöinformation*). FGS – *Förvaltningsgemensamma standarder* (common public-sector standards)[11], the Swedish National Archive's standards on how information must be structured. At present, compliance is guaranteed through publication of machine readable service descriptions in a number of authorities but not all.
Needs/gap analysis	There are no national paradigms, standards and guidelines for metadata. There are also no rules on how these standards and guidelines should be described in technical protocols. Tools may also be needed to manage metadata, such as common definitions.

Building block	Indexing
Purpose	The purpose is to streamline the availability of stored information by providing an index of where information about a particular object is stored. It is therefore not necessary to search for the specific information in order to access it.
Existing solution	At present, separate sector-specific solutions exist for each information exchange. Example: NPÖ – *Nationell Patient Översikt* (national patient overview)[12] – central function indexing which provider holds a patient's medical records.
Needs/gap analysis	The needs analysis refers to the Swedish Agency for Economic and Regional Growth and work on verksamt.se. There are no sector-specific or national solutions for these needs.

[11] *Förvaltningsgemensamma specifikationer* (common public-sector specifications) – https://riksarkivet.se/fgs-earkiv

[12] *Nationell patientöversikt* (national patient overview) – https://www.vardgivarguiden.se/avtaluppdrag/it-stod-och-e-tjanster/e-tjanster-och-system-a-o/beslutsstod/nationell-patientoversikt-npo/ – read 2019-06-27

4.1.4 Trust and security

Building block (*)	Identity
Purpose	Consists of rules and processes that aim to ensure that an entity (such as legal entity or an individual) always has a unique and consistent digital identity.
Existing solution	Individuals have an obvious identifier in their co-ordination number (*samordningsnummer*) and personal identity number (*personnummer*). In the same way, organisations can be identified with their organisation number (*organisationsnummer*). However, there are no rules or processes specifying how people within an organisation can have a unique consistent identity in their communications with other actors outside their own organisation.
Needs/gap analysis	There are no national cross-cutting solutions for use for example in services linked to legal entities, IOT, machine to machine.

Building block (*)	Authorisation
Purpose	The purpose is to safeguard assigned rights to use an information asset in a specified way.[13]
Existing solution	All actors must manage authorisation in order to meet the information security requirements. There are no general national solutions.
Needs/gap analysis	There are no general national solutions.

Building block (*)	Trust rules
Purpose	The purpose is to enable cooperation and to simplify information exchange.
Existing solution	Various solutions exist but none meet the needs of a national plan. For example Swedish electronic identification, federation solution for e-health and schools, geodata collaboration.
Needs/gap analysis	There are no general national trust rules or a national solution.

[13] SIS TR-50:2015 Terminology for information security

Building block	Availability
Purpose	The purpose is to guarantee access for authorised individuals in the right situations. Access involves interaction between a user and a resource that results in the transmission of information between them or the use of resources.[14] Partly based on an SLA database (Service Level Agreement).
Existing solution	At present, separate solutions are developed for each organisation.
Needs/gap analysis	There is no nationally scalable solution.

Building block	Traceability
Purpose	The purpose is to be able to reconstruct the sequence of events after they occur.
Existing solution	At present, separate solutions are developed for each information exchange.
Needs/gap analysis	There is no nationally scalable solution.

4.1.5 The impact of the building blocks on the availability of basic data

The report on the secure and efficient access to basic data stated that this report will propose solutions regarding the availability of basic data. The examples of needs highlighted in the final report on the secure and efficient access to basic data were:

- there must be a very high level of availability, with specified response times,
- access to basic data must be provided via machine readable interfaces, and
- basic data is subject to effective change management.

The above requirements should also be applicable in a broader context to other types of data held by authorities.

The building blocks proposed in this report reflect the fact that it must be possible to handle the requirements from basic data as a natural part of the common public-sector digital infrastructure for information exchange.

[14] SIS TR-50:2015 Terminology for information security

4.2 Existing law

4.2.1 Overall assessment of building blocks

The focus of the legal assessment of the proposals in the report is to identify what is possible within the existing law in order to satisfy identified needs. The need for legal changes to strengthen governance in this area is discussed in more detail in chapter 6 on consequences.

The authorities consider that national feasibility studies, investigations and development of the national building blocks can take place on the basis of government assignments. This applies to all building blocks. However, in order to deploy technical components of a building block at *national level* or to issue binding requirements for a building block at national level, the lead authority is required to have a basis in statutes consisting of:

1. A legal basis for providing the technical component of the building block to other actors at national level.
2. A legal basis for issuing a binding requirement to use the building block at national level.
3. A legal basis for handling information in the building block.

The building blocks that are considered to have some legal basis in all the points above under existing law are those covered by the Swedish ordinance with instructions for the Agency for Digital Government (*förordningen med instruktion för myndigheten för digital förvaltning*) (DIGG), and concern the public administration's access to electronic identification and signature infrastructure and services. The proposals in this report may, however, mean that the legal basis in this part needs clarification or development, to be analysed in more detail according to proposed actions in chapter 5.

The authorities consider that the first question can at least be dealt with by adding the relevant rules to ordinances with instructions (*förordningar med instruktion*) for the authorities in question. Nevertheless, if the lead authority is to be able to issue government regulations concerning a building block, including for municipalities, the building block must be regulated by law.

The authorities consider that the building blocks may create concentrations of information that in themselves create an information exchange. These concentrations may contain personal data and be sensitive in nature. In order to create such concentrations, a specific legal basis is considered to be necessary, which does not exist today except as specified above.

One legal issue regarding the governance of each building block is that responsibility for the building block may be divided between several authorities. In addition, use of the building block can be subject to procurement rules for municipalities that need the building block, and this might make the building block counterproductive.

One general conclusion is that the existing law will have to be developed in order to guarantee a legal basis for the building blocks. Chapter 6 on consequences contains more

details on the need for legal changes. The following sections describe in more detail the legal framework for the common public-sector digital infrastructure for information exchange.

4.2.2 General description of existing law

The legal framework for common public-sector digital solutions is subsumed primarily under public IT law, which spans traditional legal fields within public law and other areas. The authorities have chosen to apply a delineation method according to this legal field as described in the eSam checklist for lawyers[15], which is a compilation of legal issues and relevant statutes governing the way organisations cooperate in development initiatives.

4.2.2.1 Competence issues in the legal evaluation of the building blocks

- *Legal area of competence of the authority*: Participation in a digital infrastructure involves the authorities performing their official functions. The activities of the authorities are governed by law and other statutes, see paragraph 1 (3) of the Instrument of Government(*regeringsformen*) and paragraph 5 (1) of the Administrative Procedure Act (*förvaltningslagen*). The activities for which the authorities have a legal basis constitute their area of competence.

  An authority's area of competence is regulated primarily through the instructions (*instruktion*) applicable to it and through special statutes governing the authority's activities. In addition, more general statutes concerning the activities of authorities, such as the Administrative Procedure Act and the Government Agencies Ordinance (*myndighetsförordningen*), describe the functions of authorities and constitute a basis for their competence. Administrative functions can be transferred to municipalities, to other legal entities and to individuals. However, administrative functions involving the exercise of official authority may be transferred only with a basis in law, see chapter 12 paragraph 4 of the Instrument of Government.

- *Handling of information on behalf of another authority:* A common public-sector digital infrastructure in which authorities cooperate by using the same technical components may cause authorities to handle information on each other's behalf. Such handling could involve storage or mediation, in other words permanent or temporary handling. The storage of information by an authority on behalf of another authority raises the question of whether information becomes a public document with the authority holding it, or whether the exclusion in chapter 2 paragraph 13 of the Freedom of the Press Ordinance (*tryckfrihetsförordningen*) is applicable.

- *Public access and secrecy in information exchange:* Information held by an authority is subject to the Public Access to Information and Secrecy Act (*offentlighets- och sekretesslagen*), and an authority that stores information is prohibited from

[15] Checklist for lawyers (*Checklista för jurister*), Report from the E-delegation 19/06/2014

disclosing it in contravention of the law. An authority may consequently only disclose information which is either not subject to secrecy or is subject to secrecy but there is a provision to override secrecy. Secrecy encompasses a prohibition both to release documents and to disclose information verbally, i.e. professional secrecy as well as confidentiality of documents. As a general rule, secrecy also applies between authorities. However, there are a number of provisions in the Public Access to Information and Secrecy Act that override secrecy between authorities, see chapter 10 of the Public Access to Information and Secrecy Act.

- *Responsibility for personal data in information exchange:* The question of who is the controller and who is the processor in the processing of personal data in the architecture must be explored. According to article 4.7 of the General Data Protection Regulation (GDPR) the controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The factor which determines who is the controller is the actual decision-making process concerning the purposes and means of the processing. Responsibility for personal data may also be defined in national law, for example in a register statute (*registerförfattning*).

  One or more controllers may also jointly determine the purposes and means of the processing. In that case they are designated as joint controllers, provided that they comply with certain provisions of article 26 of the GDPR.

  A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, see article 4.8 of the GDPR. For example, a processor may be engaged to store information that includes personal data on behalf of a third party. Where data is processed by a processor, the processing must be governed by a contract or a statute, see article 28.3 of the GDPR.

- *Agreements and requirements concerning procurement:* The Public Procurement Act (*lagen om offentlig upphandling*) governs the purchase of services by an awarding authority. An architecture solution in which an authority manages the processing of information on behalf of another authority may, in some cases, be regarded as being subject to a procurement process. It is clear from the existing law that agreements between government authorities are not covered by the Public Procurement Act, but that agreements between government authorities and municipalities may well be subject to procurement requirements.

4.2.2.2 Legal forms of governance

- *Cooperation:* Within their area of competence, authorities may choose to cooperate in order to develop information exchange solutions. An authority can and must cooperate with other authorities. According to paragraph 8 of the Administrative Procedure Act, authorities are required to cooperate with others

in the context of their own activities. The provision implies a general, but not unlimited, obligation to cooperate. An authority will always decide the extent to which its own circumstances allow resources to be allocated to support the authority requesting assistance. This provision cannot be used as a basis for cooperation projects falling *outside* the relevant authority's area of activity.[16] No new structures must be created in the form of special cooperation bodies, which, irrespective of the relevant provisions, take decisions which cannot be attributed to any of the collaborating authorities.[17]

Paragraph 6 (2) of the of the Government Agencies Ordinance states government administrative authorities must cooperate with authorities and others in an effort to capitalise on the potential benefits for individuals and for the government as a whole. The Government Agencies Ordinance does not in any way entitle an authority to act outside its area of competence as part of the cooperation. In their activities, government authorities must work towards the development of secure and efficient information exchange, see paragraph 2 of the Ordinance on information exchange by government authorities (*förordning om statliga myndigheters informationsutbyte*). However, that provision does not confer any competence to cooperate outside the authority's general area of competence.[18]

- *Mandatory governance*: The governance of an information exchange infrastructure may also be mandated by laws or other statutes, on the basis of the assignment of powers laid down in constitutional law. In this case, governance refers to obligations and rights relating to connection and to the reuse of information and the digital solutions.

4.2.2.3 Legal principles for disclosure of information

- *The authority is responsible for its own information:* One principle for disclosure of information is that each authority is responsible for its own information and for ensuring that such handling is in accordance with applicable law. It is therefore the authority itself that must ensure that it complies with applicable law (see also chapter 12 paragraph 1 of the Instrument of Government).

- *Legal basis for disclosing information:* An authority requires a legal basis on which to disclose information. The need for an authority to have a basis in law for all

[16] Govt. Bill 2016/17:180 Modern and legally certain administration – the new Administrative Procedure Act (*En modern och rättsäker förvaltning – ny förvaltningslag*), page 292 f.

[17] Govt. Bill 2016/17:180 Modern and legally certain administration – the new Administrative Procedure Act (En modern och rättsäker förvaltning – ny förvaltningslag), page 71.

[18] In this context, note that the final report of the Investigation into the effective management of national digital services (*Utredningen om effektiv styrning av nationella digitala tjänster*) proposed that state authorities should be entitled to cooperate outside their area of activity in the context of digitalisation of public administration. SOU 2017:114 reboot for digital administration (*reboot – omstart för den digitala förvaltningen*), see page 56.

actions it takes follows from the principle of legality in chapter 1 paragraph 1 (3) of the Instrument of Government and paragraph 5 of the Administrative Procedure Act, which provides that an authority may only take actions which have a basis in law. The principle of legality should be interpreted as meaning that an authority in the broadest sense must have a legal basis for the measures it undertakes.[19]

Examples of mandatory legal bases for disclosure include the authorities' duty to report to another authority, disclosure under freedom of information, communication in accordance with the Administrative Procedure Act and disclosure in accordance with chapter 6 paragraphs 4–5 of the Public Access to Information and Secrecy Act. An example of voluntary disclosure is when it takes place as a service under the Administrative Procedure Act, which does not specify what is considered to be a service, but on what basis an authority may choose, for example, to post information on its web site.

There are no common rules on disclosure in national information provision.

- *Register statutes:* Where appropriate, some personal data processing by authorities is governed by so-called register statutes (*registerförfattningar*), which regulate matters such as the purposes for which an authority uses automated processes with personal data.[20] The purposes set out in a register statute imply that the authority may not process personal data for any purpose other than these (principle of finality, article 5.1 d of the GDPR). This means that for the electronic disclosure of information, if the information is covered by a register statute, the disclosure must be in accordance with the purposes set out in the applicable register statute.

- *Information security:* The legislation in the field of information security is fragmented and consists of a number of different regulations that need to be applied alongside each other. Legislation in the field of information security can be said to apply to activities on the one hand and to information on the other.[21]

  The GDPR imposes security requirements on the processing of personal data. The Public Access to Information and Secrecy Act prohibits the disclosure of secret data, which is why general documents must be handled in a secure way. The Protective Security Act applies to anyone who carries out activities that are relevant to the security of Sweden or who is subject to an international security obligation (security-sensitive activities) which is binding for Sweden.

[19] Govt. Bill 2016/17:180 Modern and legally certain administration – the new Administrative Procedure Act (*En modern och rättsäker förvaltning – ny förvaltningslag*), pages 57–58.
[20] For an overview of Swedish register statutes, see SOU 2015:39 Official Data Act (*myndighetsdatalag*) page 94.
[21] SOU 2018:25 Law as a basis for public-sector digitalisation (*Juridik som stöd för förvaltningens digitalisering*) page 315.

Requirements concerning the information security of government authorities are contained in the Ordinance (2015:1052) on crisis preparedness and the surveillance authorities' actions at times of high alert (*förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap).* In addition, the Swedish Civil Contingencies Agency (MSB) has issued regulations on the information security of public authorities and on reporting by government authorities of IT incidents. Municipalities and county councils are not subject to the ordinance and regulations above, but are instead covered by the Act (2006:544) on municipal and county council action before and during extraordinary events during peacetime and times of heightened readiness (*lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, vilken saknas specifika bestämmelser om informationssäkerhet*), which contains no specific provisions on information security. The Act (2018:1174) on information security for vital societal functions and digital services (*lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, med krav på säkerhet för leverantörer av vissa tjänster*) has been in force since 2018 and contains security requirements for suppliers of certain services.

The list of statutes above is not exhaustive. There is a lack of legislation involving a coherent common approach for all government and municipal authorities, something that the Government Inquiry into the law relating to digitalisation (*Digitaliseringsrättsutredningen*) identified as a shortcoming from the point of view of digitalisation.[22]

4.3 Proposals concerning governance, incentives, roles and responsibilities for the common public-sector solutions

4.3.1 Legal form of governance for the building blocks

The previous section noted that a legal basis is required for authorities in order to perform official functions relating to the building blocks, for example in order to provide national technical functions. It also noted that existing law needs to be developed in order to give the building blocks the necessary legal foundation for the relevant authorities (legality). This section discusses ways in which responsibility for the building blocks can be legally regulated (legal form of governance). The authorities propose that responsibility for the building blocks should form part of the public commitment and should be explicitly stated in statutes with instructions for the relevant authorities.

The choice of legal form of governance is in many respects a matter of finding an appropriate balance. The appropriate form of governance should be selected on the basis of *arguments relating to democracy, legal certainty and efficiency*. Just because governance

[22] SOU 2018:25 Law as a basis for public-sector digitalisation (*Juridik som stöd för förvaltningens digitalisering*) page 329.

based on collaboration is possible does not necessarily mean that collaboration is the most *expedient* form.

When choosing the form of governance of an infrastructure and its components, it is important to consider the *purpose* it is intended to fulfil. If the purpose of the infrastructure is to pursue an important national interest, it may be necessary to include it in the public commitment. The public commitment is a commitment that the legislative authority has identified as a public responsibility, and it defines the boundaries of what are official functions, not only in relation to individuals, but also what is reserved for market actors. Functions not covered by the public commitment are typically the responsibility of market actors.[23]

In each individual case, what constitutes a public commitment is a political attitude and a political decision. Such a decision cannot be delegated or decentralised to government authorities. Some of the grounds normally cited for a public commitment are a more efficient economy, redistribution, stabilisation policy and accountability where citizens do not themselves have sufficient knowledge and information. The private market cannot meet all the needs that are important for the country and the citizens. Certain public goods must instead be guaranteed by means of government commitments.[24]

As a result, if the interests and needs that the infrastructure is intended to satisfy are an important *national interest*, on the typical grounds set out above, then the infrastructure itself constitutes an important national interest and may therefore have to form part of the public commitment. Since the question of what forms part of the public commitment cannot be delegated to the authorities, it must be determined by the Riksdag or the government. In itself, this implies that collaboration is an inappropriate legal form of governance for such infrastructure or building blocks.

The Reboot inquiry found that the public commitment for common public-sector digital functions should be governed by statute.[25] The inquiry defined common public-sector digital functions as services like Mina meddelanden (My messages) and electronic ID documents for example. Other examples that the inquiry believes may constitute common public-sector digital functions include systems for managing permissions and digital signatures, systems for secure communication between authorities, standards for the transfer of information between authorities and companies, and standards for open data.[26] The hallmark of common public-sector digital services is that they are common digital solutions that are infrastructural in nature and are a crucial prerequisite for public e-service development as a whole.[27] However, the inquiry found that every one of the common public-sector digital functions required further analysis to define the extent of the public commitment in relation to the role of the private actors.

---

[23] SOU 2017:114 reboot for digital administration (*reboot – omstart för den digitala förvaltningen*), see page 104.
[24] SOU 2017:114 reboot for digital administration (*reboot – omstart för den digitala förvaltningen*), see page 103.
[25] SOU 2017:114 reboot for digital administration (*reboot – omstart för den digitala förvaltningen*), see page 101.
[26] SOU 2017:114 reboot for digital administration (*reboot – omstart för den digitala förvaltningen*), see page 107 et seq.
[27] SOU 2017:114 reboot for digital administration (*reboot – omstart för den digitala förvaltningen*), see page 106 et seq.

Nevertheless, collaboration as a legal form of governance can perform a complementary role in the development and management of a building block. If an authority lacks legal competence for collaboration, the government could issue a regulation requiring a certain form of collaboration, or the authority's area of competence could be extended by modifying the authority's instructions.

In practical terms, it may be beneficial for different building blocks in an infrastructure to be regulated at different levels, so that the respective advantages and disadvantages of the legal means of governance are safeguarded, and also so that aspects of democracy, legal certainty and efficiency are taken into account. For example, a law or regulation may impose an obligation on an authority to participate in a particular infrastructure, while questions relating to the technical frameworks for services in the infrastructure may be determined by other forms of governance, for example through collaboration or through an authority's execution regulation (*verkställighetsföreskrift*). One existing example of possible governance in the corporate area is the Ordinance (2018:1264) on digital gathering of data from companies (*förordning (2018:1264) om digitalt inhämtande av uppgifter från företag*). The ordinance is intended to reduce the volume of data submitted to authorities by companies. This type of governance could be used for all or part of the public administration, either for the infrastructure as a whole or for individual building blocks/domains.

Bearing this in mind, the authorities propose that the building blocks of the conceptual architecture must form part of the public commitment relating to the common public-sector digital infrastructure for information exchange (legal governance model). This means that as a point of departure, it must form part of the official responsibility of the relevant government authorities to develop and manage building blocks that have already been identified and that will be identified in future.

4.3.2 Incentives for better progress

In the light of the analyses and proposals set out above in this report, it is clear in simplified terms that it is necessary to move from an identified current situation to a new situation as outlined in the conceptual architecture. The current situation consists of fragmented digital solutions and little incentive for national coordination. The new situation consists of tangible national building blocks with designated responsible actors. In the new situation, the building blocks will be used throughout public administration in digital information exchange, which will realise the benefits of the investments made. This transition will require an efficient and long-term form of governance that incentivises and stimulates development.

Initially, incentives can be created with *coordinated governance* based on government assignments. This should be combined with national initiatives in prioritised applications that have the potential to kickstart a self-sustaining connection to the building blocks.

It is also proposed to create incentives by *establishing collaboration between authorities* concerning the building blocks.

To incentivise the use of the building blocks proposed in this report, the authorities recommend imposing a *requirement for ongoing national initiatives* to use the building blocks of the digital solutions within these initiatives. It is felt that a requirement of this kind will ensure that the benefits are fully realised, while also driving the development of the building blocks according to the needs in the value chains and their timeframes.

Examples of national initiatives where the building blocks are needed include the government's decision of 2016 on digitalisation in a number of priority development areas in the public sector.[28] In this context, the government awarded digitalisation assignments to Lantmäteriet, the Swedish Board of Agriculture, the Swedish Environmental Protection Agency and the Swedish Agency for Economic and Regional Growth in these four value chains: the planning process, the food chain, environmental information and easier business startups.[29]

Such requirements may be included when the government assignments are drafted, guaranteeing that progress will be made during development. In the long term, however, there is a need for long-term sustainable governance that stimulates the use of the building blocks. According to the comparative international analysis, early scrutiny of legislation is an important success factor. The authorities therefore recommend that the government appoints a legal commission as proposed by the Government Inquiry into the law relating to digitalisation (*Digitaliseringsrättsutredningen*), see SOU 2018:25 page 446. In its final report on a smarter planning process, Lantmäteriet outlined a method and a concept for a phased approach linked to such a commission, which must also be taken into account.[30]

4.3.3 Responsibility for the building blocks

A building block consists of multiple aspects intended to standardise a certain activity at national level. This could be a technical component, a kind of administrative national framework for the building block, for example regarding specifications for information, or a technical description. It is the various aspects aiming to standardise something in the building block that need to be incorporated into the Swedish model of administration as an administrative responsibility.

The authorities consider that the responsibility for the building blocks can be apportioned as follows.

Legal: In this part, the responsibility is to coordinate the technical, semantic and organisational aspects of the building block, without responsibility overlapping unnecessarily with other authorities.

---

[28] Budget Bill 2016/17:1, category 22, section 4.4.2.

[29] For example see Budget Bill 2016/17:1, category 18, section 3.5.7, and the government assignment about working towards digital first – for a smarter planning process (*regeringsuppdrag att verka för digitalt först – för en smartare samhällsbyggnadsprocess*), N2016/01419/EF.

[30] Lantmäteriet, national availability of geodata in the planning process 2019-04-19 – final report of the assignment encouraging a smarter planning process, Lantmäteriet dnr 519-2018/2889, appendix 1 (*Nationellt tillgängliggörande av geodata i samhällsbyggnadsprocessen 2019-04-19 – slutrapport i uppdraget att verka för en smartare samhällsbyggnadsprocess, Lantmäteriets dnr 519-2018/2889, bilaga 1*).

Technical: In this part, the responsibility relates to the technical component of the building block, either the entire technical infrastructure or a specific digital service.

Semantic: In this part, the responsibility relates to the administrative component of the building block, specifying how information and services must be described so that the information can be exchanged fully automatically.

Organisational: In this part, the responsibility relates to the administrative component of a building block that guarantees easy (compulsory or non-compulsory) connection to the building block, for example by allowing a designated authority to decide on the connection instead of decisions being taken by each information-producing authority in the collaboration relating to the building block. It may also be about streamlining contract management as required by legislation, for example processor agreements, by giving the coordinating authority the right to issue regulations in this context.

Each building block has at least some of the semantic and organisational aspects.

However, taking responsibility for the requirements of a building block may require specialist knowledge about the properties of the information or the users' needs, for example, or an area of expertise such as data protection and security.

At present, the legal competence of authorities (and therefore also specialist knowledge) is categorised into areas of expertise defined by each authority's instructions. This suggests that the various aspects (technical, semantic and organisational) must be allocated, where appropriate, to authorities with such relevant competence.

Bearing this in mind, the authorities consider that the following types of responsibility are necessary for the building blocks.

- Responsibility for ensuring that the building blocks exist and are conceptually coherent within an architecture. This includes, for example, developing and managing a national framework for basic data[31], metadata management of information and services.
- Responsibility for realising building block solutions – centrally or locally.
- Responsibility for creating semantic order – centrally and sector/domain-specific. See also proposals for basic data domains.[32]

The authorities consider that responsibility should be shared between DIGG and authorities looking after the domains (information domains), initially the Swedish Companies Registration Office, Lantmäteriet and the Swedish Tax Agency within the

[31] Assignment concerning secure and efficient access to basic data (*Uppdrag om säker och effektiv tillgång till grunddata*) – Swedish Companies Registration Office, DIGG, Lantmäteriet and the Swedish Tax Agency Dnr 2018-31 page 50

[32] Assignment concerning secure and efficient access to basic data (*Uppdrag om säker och effektiv tillgång till grunddata*) – Swedish Companies Registration Office, DIGG, Lantmäteriet and the Swedish Tax Agency Dnr 2018-31 page 51

respective information domain. This division of responsibilities will have to be described in more detail as each building block is developed, see chapter 5 on measures.

4.3.4 Other areas of responsibility

A building block is designed to be used by other actors, and may even depend on collaboration with different actors in order to function. This means that, in addition to responsibility for the building block itself, there are also areas of responsibility for the actors which contribute to or use the building block.

The authorities have identified the following areas of responsibility, although they require further investigation before they can be framed as concrete proposals.

- Responsibility as data host: At present, public actors are not all in a position to use the possibilities of digitalisation. Even if there is a clear system of responsibility for building blocks, there may be a threshold for authorities to use them. To make the building blocks easier to use, there could be some kind of service responsibility towards government and municipal authorities. Data hosting is intended to make information easier to access through APIs. In this situation, a data host acts on behalf of another (government or municipal) authority.

- Responsibility as an information producer: The frameworks around the building blocks developed by the relevant authorities will impose requirements on information-producing actors, in other words in situations where the information handled by a building block is developed by or occurs in actors other than the authority with responsibility for the building block. One responsibility under discussion is “information responsibility” for information producers from the point of view of digitalisation. This kind of responsibility would clarify, for example, an actor's obligations in respect of a building block. Initially, however, this responsibility could be developed as part of a collaboration between producers.

- Responsibility for users of the building blocks: The purpose of the building blocks is to create benefits for the actors (users), which need secure and efficient access to information in digital form. This means that if users do not see any reason to use the building blocks, it will be impossible to achieve the goal of more efficient and secure information exchange. In order to incentivise use, user responsibility could be developed according to something called “the once only principle” (TOOP), see the European Commission's eGovernment Action Plan. Several European countries have begun to incorporate TOOP into their legislation. In Belgium, Estonia and the Netherlands, binding legislation has already been passed.[33] Development of this kind could be considered in connection with the legal governance of the building blocks in Sweden.

[33] EU-wide digital Once-Only principle for citizens and businesses – policy options and their impact, EU 2014

5 Proposed measures

Proposal: The authorities propose that the government should:

- Enable a form of governance similar to the national programmes created in the analysed countries, in order to make decisions over time about activities to develop and realise a common public-sector digital infrastructure for information exchange within and with the public sector.
- Make decisions about government assignments and the necessary funding for the short-term proposals described below, which can be regarded as a feasibility study for the next item, resulting in a roadmap for the development of the common public-sector infrastructure to be coordinated by DIGG.
- Make decisions – over time and in consultation with DIGG – about government assignments and the necessary funding for the development of the building blocks, for the authorities that are expected to have a national administrative responsibility for the building blocks in question, as well as initiatives that promote national implementation.
- Set up a legal commission to ensure that the necessary long-term legal basis is established for the building blocks and information exchange.

Initially (2019-2020) the proposed government assignments are as follows:

1. A roadmap (DIGG, Swedish Companies Registration Office, Swedish Social Insurance Agency, Lantmäteriet, Swedish Tax Agency, Swedish eHealth Agency and Swedish National Courts Administration)
2. API management (DIGG, Swedish Companies Registration Office, Lantmäteriet, Swedish Tax Agency, Swedish Environmental Protection Agency and Swedish eHealth Agency)
3. Identity (DIGG in collaboration with the Swedish Association of Local Authorities and Regions, Swedish Social Insurance Agency and Swedish eHealth Agency)
4. Mina ombud (My representatives) (Swedish Companies Registration Office and Swedish Tax Agency)

5.1 Starting points and challenges

The assignment states that for the solutions judged to be appropriate, the authorities must submit proposals for measures allowing them to be used more intensively over the long term in the public sector.

One challenge for development towards efficient and secure information exchange is to balance

- standardisation, uniformity, governance with
- flexibility, innovation and non-compulsion.

Further measures and choices are necessary in the light of a proportionality assessment based on these conflicting needs. In-depth security analyses are required for all measures linked to building blocks.

One important motivation when choosing measures was to develop existing architectures and solutions and not necessarily to replace them with new solutions. This means that the proposed starting point for further development is to move towards a more advanced common public-sector digital infrastructure for information exchange, permitting authorities to retain their solutions while allowing a more modern user interface to be introduced.

Legislation, governance and funding are considered to be crucial success factors for development. As a starting point, practical implementation should be assigned to authorities with greater digital maturity and capacity. In addition to legal instruments, other incentives are also required to boost progress in development.

Another starting point in choosing a technical solution consists of principles for reusing existing solutions that should be applied:

- Is there a functioning publicly-owned solution that can be reused to meet common needs?
- Is there a publicly-owned solution that can be reused and further developed to create a common solution?
- Is there a solution available in the EU or beyond that can be reused and further developed into a solution for Sweden?
- Is there a commercial standard solution that can be procured and used for all actors?
- Develop a new common solution for use in the public sector.

5.2 Measures

The authorities propose that the government should take the following measures:

- Enable a form of governance similar to the national programmes created in the analysed countries, in order to make decisions over time about activities to develop and *realise* a common public-sector digital infrastructure for information exchange within and with the public sector.
- Make decisions about government assignments and the necessary funding for the short-term proposals described below, which can be regarded as a feasibility study for the next item, resulting in a roadmap for the *development* of the common public-sector infrastructure to be coordinated by DIGG.
- Make decisions – over time and in consultation with DIGG – about government assignments and the necessary funding for the development of the building blocks, for the authorities that are expected to have a national administrative responsibility for the building blocks in question, as well as initiatives that promote national implementation.

- Set up a legal commission to ensure that the necessary long-term legal basis is established for the building blocks.

As a basis for relevant government assignments, the authorities would like to highlight the following input:

- *Coordination.* It is proposed to instruct DIGG to prepare, plan and coordinate initiatives and assignments together with authorities involved in the development of relevant building blocks, and to draft relevant guidelines and standards.

- *Roadmap.* It is proposed to instruct DIGG to formulate a roadmap for development, in collaboration with the Swedish Companies Registration Office, Lantmäteriet, the Swedish Social Insurance Agency, the Swedish Tax Agency, the Swedish National Courts Administration and the Swedish eHealth Agency. The roadmap must describe:
  - Details of infrastructural building blocks and architecture for the common public-sector digital infrastructure for information exchange.
  - Governance, collaboration, responsibility and management model
  - Cost calculation
  - Funding solution
  - Collective simplified contract model

  It is proposed to launch the assignment in late 2019 and to run it until the end of September 2020 with an interim report in January 2020. It is proposed to pay DIGG SEK 1.5 million in order to take the lead. It is proposed to pay other authorities SEK 500,000 each. (Total SEK 6 million)

- *API management.* It is proposed to instruct DIGG to prepare for and realise the API management building block, in collaboration with the Swedish Companies Registration Office, Lantmäteriet, the Swedish Environmental Protection Agency and the Swedish eHealth Agency. This includes the following:
  - Formulating proposals for standardisation of descriptions of legal rules, operating rules and technology
  - Administrative model of the above descriptions
  - Establishing the ability to search for a service
  - Establishing the ability to address a service
  - Roadmap for ongoing development work for the building block (as set out in the above assignment)
  - Establishing development support for developers
  - Formulating a standardised process for API life cycle management
  - Addressing issues linked to central (common) components alongside the governance assignment

  It is proposed to launch the assignment in late 2019 and complete it at the end of September 2020. DIGG will be paid SEK 2 million in order to take the lead. The other participating authorities will receive SEK 750,000 each. This brings the total cost of the assignment to SEK 5.75 million. DIGG's assignment includes coordinating the API management assignment with the in-depth governance assignment.

- *Identity*. It is proposed to instruct DIGG, in collaboration with the Swedish Association of Local Authorities and Regions, Swedish Social Insurance Agency and Swedish eHealth Agency, to investigate national identification solutions that support the common public-sector digital infrastructure for information exchange. The work includes the following:
  - National solution for electronic identification in the service, supporting the use of electronic identification in the service across different areas of activity.
  - Identifying the scope for applying the identification solution to organisations and units.
  - A national solution for e-signatures that will also include private service providers.

  It is proposed to launch the assignment in late 2019 and complete it at the end of January 2020. It is proposed to pay DIGG SEK 1.5 million, the Swedish Social Insurance Agency SEK 0.5 million and the Swedish eHealth Agency SEK 0.5 million for the assignment.

- *Mina ombud (My representatives)* – it is proposed to task the Swedish Companies Registration Office and the Swedish Tax Agency with the following assignment. Based on the outcome of the work done in 2020, subsequent assignments may need to be adjusted in terms of their content.

  - *Permissions at national level – pilot in the corporate area,* (Swedish Companies Registration Office)
    Time period: 2020-01 -- 2020-12
    Cost: SEK 7 million
    Partners: DIGG, the Swedish Tax Agency
    Objective: To develop a first version of a national permission solution in which a natural person is able to represent a company (registered with the Swedish Companies Registration Office) in a digital service. This also includes a service to make it easier for consumers to manage the authority to sign for a company.

  - *Permissions at national level – expansion/further development in the corporate area,* (Swedish Companies Registration Office)
    Time period: 2021-01 -- 2021-12
    Cost: SEK 7 million
    Partners: DIGG, Swedish Tax Agency and other public actors.
    Objective: To establish the solution and scale up usage based on the ascertained need, and to include more services in which natural persons need to represent companies. To investigate the requirements for representing legal entities other than companies/natural persons, see proposed assignment for 2022.

- *Permissions at national level – representing natural persons*
  (Swedish Tax Agency)
  Time period: 2021-01--2021-12
  Cost: SEK 7 million
  Partners: DIGG, Swedish Companies Registration Office
  Objective: To expand usage of the proposed solution to situations in which natural persons need to represent other natural persons.

- *Permissions at national level – expansion/further development to cover more legal entities,* (Swedish Companies Registration Office)
  Time period: 2022-01 -- 2022-12
  Cost: SEK 3 million
  Partners: DIGG, the Swedish Tax Agency and other authorities able to assign organisation numbers
  Objective: To refine the developed solution so it covers types of legal persons registered with authorities able to issue organisation numbers other than the Swedish Companies Registration Office.

6 Consequences

Summary:
At present, there are a range of problems with information exchange within and with the public sector, resulting in various negative consequences. The proposals put forward by the authorities aim to address these problems. The consequences of the proposals include stronger governance and coordination through the creation of common public-sector building blocks.

The proposals will have different consequences depending on how it is decided to handle common costs and the funding of common public-sector building blocks. However, the consequences are small in relation to the potential benefits and positive socio-economic impacts potentially resulting from improved access to public data.

6.1 Overall consequences

The purpose of the proposal for common public-sector building blocks is to strengthen the governance and coordination of the public sector with regard to secure and efficient information exchange. Under the proposal, the government will be responsible for ensuring that the building blocks exist and are used. What alternative solutions are there and what will be the impact if the proposal is not implemented?

The alternative to the proposal is that the development and administration of the building blocks is driven by market actors in the field of digitalisation. Businesses are already offering digital solutions in which a company undertakes to store and make the actors' information available. But the state has overall responsibility for the fundamental information infrastructure of society.[34] The state is also responsible for formulating basic principles on how public information should be made available to society. The authorities therefore consider that the alternative in which the development is driven by market actors is not conducive to efficient and secure information exchange.

If the proposal is not implemented, it is considered that there will be greater fragmentation and duplication in public administration around digital solutions, counteracting the objective of a more efficient and secure information exchange.

6.2 Costs and funding

The assignment discusses three funding options for the development and management of the necessary solutions, all of which are neutral in terms of the government budget:

1. Voluntary funding by one or more authorities
2. Funding from usage charges, or
3. Funding from a redistribution of appropriations.

[34] SOU 2003:111 pages 216, 221 and 318 and Govt. Bill 1995/96:125 page 19.

A combination of several of the above could also be an option. Voluntary funding from collaboration between authorities has been tried, for example, in the development of verksamt.se and Mina meddelanden (My messages). Although it worked initially in these cases, such funding involves a great deal of uncertainty. The agreements are often short-term and funding has to be secured annually for the following year. This means that it is difficult to manage the long-term development of the components, and there is considerable uncertainty for the users. There is no incentive to create reusable components. Is it worth investing in this component? How long will it be available for, will charges be imposed in future? Even if voluntary funding is combined with an assignment for the provider, which will be necessary in most cases, there will be considerable uncertainty.

Funding based on usage charges (transaction-based charges) risks diluting the benefits of the common components, especially if the charges are transaction-based. As a result, the costs will be difficult for the users to budget for. The cost increase for the user of a common component is unlikely to be in proportion with the provider's cost increase as the marginal cost is normally very low for providing the component (it increases instead incrementally when different capacity thresholds are reached).

If the cost price is used instead, early adopters will bear the brunt. To prevent unreasonably high unit costs for the first authorities to connect, additional funding will be necessary, at least for a transitional period, even if the charge-based model is selected.

Central funding by means of appropriations is the solution most likely to support the digitalisation of public administration. This is mainly because appropriations must be combined with an assignment for the authority, thereby signalling a long-term vision and stability, but there are other advantages too.

Advantages of funding by means of appropriations:

- Compatible with the idea of open data, that information should be free to download for those who need it.
- There is no need to establish an infrastructure for invoicing and invoice management, i.e. a customer service that can answer invoicing questions and possible customisation of the technical solution.
- There will be no risk of a difficult annual settlement in order to avoid subsidisation between the authorities.

The funding would be through a redistribution of appropriations from the state authorities to a common pot for the development and management of shared capabilities/components/building blocks. This kind of structure is budget-neutral, which is the starting point in the design of state reforms. Further investigation is needed to determine how the authorities that are funded by charges will contribute to the funding.

In the next step, a model could be explored in which government grants to municipalities and county councils are reduced and redirected.

6.3 Benefits

Time constraints made it impossible to carry out cost/benefit analyses of the proposals and measures in the context of this assignment. In the forthcoming work to realise proposed measures, it is proposed to make each participating actor responsible for its own cost/benefit analyses. This is because the benefits that are calculated must be realistic and each organisation has a responsibility to realise the benefits. These calculations can then be aggregated and applied in a larger context.

The comparative international analysis[35] clearly shows that there are major socio-economic impacts and benefits arising from the provision and use of public data. There are also direct operational benefits in terms of time savings and reduced administrative costs as well as efficiency aspects in the form of greater reuse of common public-sector building blocks.

In terms of operating benefits specifically, the operating costs of public administration[36], principally IT costs[37], are estimated to fall because of reduced working hours and more efficient use of resources as a result of reuse of common public-sector building blocks for information exchange. Information gathered from participating authorities supports the view that the costs of information exchange burden different parts of the organisation. Mostly, however, they are IT costs in the form of costs for system development, operation and architecture, but also other operating costs such as legal, contracts and business development. A general estimate is that between 60% and 80% of the costs of information exchange are IT costs and the rest are other operating costs.

Operating benefits may arise from benefits with a direct impact on the budget, in the form of reduced operating costs. For example cheaper/free use of central components, lower charges for postage and paper due to electronic information exchange and reduced working hours.

Potentially there are also indirect benefits in the form of efficiency gains resulting from changed work processes and qualitative benefits that are difficult to quantify, in the form of improved access to services, better decision-making and greater user satisfaction.

[35] See appendix 1, section 7.4.3.2 Socio-economic impacts and benefits

[36] In this report, operating costs are defined as the cost that consists of the total cost of operation including depreciation. They usually correspond to the "Operating expenses" line in the income statement of the authorities.

[37] In this report IT costs are defined as the costs that can be attributed to IT functions, but are not limited to the IT organisation. The costs consist of costs including depreciation for the operation, management and development of IT systems and equipment.

6.3.1 Worked example of impact on operating benefits

The IT costs[38] for the authorities included in the assignment are as follows:

Authority	**IT cost 2017**
Swedish Tax Agency	SEK 2,081,084,000
Swedish Social Insurance Agency	SEK 2,050,000,000
Lantmäteriet	SEK 397,735,000
Swedish Companies Registration Office	SEK 222,188,000
Swedish eHealth Agency	SEK 186,707,000
Swedish National Courts Administration	SEK 259,948,000
Total:	SEK 5,197,662,000

Assuming, on the basis of the different scenarios, that the proposed measures in this assignment will lead to efficiencies and reduced IT costs amounting to annual beneficial impacts equivalent to 0.5/1/2 per cent[39] per year of the IT cost, the resulting savings are considerable. The scenarios are thought to range from restrictive to optimistic, and it should be added that there may be difficulties in directly realising and quantifying impacts of this kind on an annual basis.

0.5% lower IT costs is equivalent to an SEK 25,988,310 annual saving for the authorities.
1% lower IT costs is equivalent to an SEK 51,976,620 annual saving for the authorities.
2% lower IT costs is equivalent to an SEK 103,953,240 annual saving for the authorities.
This only corresponds to the estimated operating benefit in terms of reduced IT costs for the parties involved in the assignment, and other public sector actors are expected to enjoy similar efficiency gains.

6.3.2 Worked example of impact on social benefit

In 2017 Ramböll[40] conducted a meta-analysis of existing literature with the aim of estimating the potential of a national digital infrastructure in Sweden. In the meta-analysis, the identified socio-economic impacts from the various countries under investigation were extrapolated to Swedish circumstances.

The results of the meta-analysis show that all in all, a reform of the national digital infrastructure can be expected to have very positive net impacts for Sweden.

[38] Authorities' strategic IT projects, IT costs and digital maturity (*Myndigheters strategiska it-projekt, it-kostnader och digital mognad*), DIGG 2019. The information relates to the IT cost for 2017 except for the Swedish National Courts Administration (2016).

[39] Compare this estimate with the estimated benefit of E-arkiv and E-diarium calculated by the Swedish National Archives in 2011, corresponding to a 5% reduction in annual IT costs due to lower costs for storage and system management.

[40] Potential analysis of NDI (*Potentialanalysis av NDI*), Ramböll, assignment from the Ministry of Finance 20170324

A drive to improve the infrastructure for information provision is expected to create an annual net positive value for society of SEK 1.2 billion, with a lower bound of SEK 906 million and an upper bound of SEK 1.3 billion.

The benefits of the reforms are expected to exceed the costs after 3 to 5 years. A combined distribution analysis indicates that about 40% of the impacts of the reform are expected to accrue to public actors with the remaining 60% going to private actors in the form of companies and individuals.

6.4 Consequences of the proposals for municipal autonomy

The authorities consider that the proposal to establish common public-sector building blocks in a digital information exchange infrastructure does not alter the fundamentals of the decision-making powers of municipalities under existing law. However, the proposal does affect information management when these decision-making powers are exercised. Municipalities will need to comply with national rules before connecting to and using the building blocks.

One effect of the proposal is considered to be to give individuals more influence over their own information and their own cases. Such influence depends on standardised information that is easy to access and use.

The proposal is also deemed to have a positive impact on processes that require secure and efficient information exchange, for example the planning process, as it will be possible to automate them to a greater extent. Process automation increases transparency and equal treatment in cases.

These impacts are considered to be mainly positive in terms of the interests that municipal autonomy is intended to protect, and this supports the proposal.

The consequences for municipal autonomy means that governance must be based on legislation. In other words, it is not sufficient to regulate the building blocks by means of ordinances. Regulating the digital information exchange infrastructure by means of ordinances alone would mean that the infrastructure is not common public-sector infrastructure, in other words common to state and municipal organisations.

6.5 Other consequences

6.5.1 Consequences for the public commitment

The authorities consider that the proposal concerning building blocks in a common digital infrastructure for information exchange entails more responsibility for the state. The responsibility concerns the creation and management of proposed building blocks. The responsibility also includes the development of regulations and standards for each building block and, where relevant, technical components in a building block.

The relevant authorities whose current remit would have to be clarified or developed in a first step are DIGG and basic data authorities such as the Swedish Companies Registration Office, Lantmäteriet and The Swedish Tax Agency. In the long term, the responsibilities of other so-called staff authorities will also need to be clarified regarding the building blocks, for example the role of the Swedish Civil Contingencies Agency.

6.5.2 Consequences for existing law

Introducing necessary new legislation to support the broader public commitment and to create a common public-sector framework for the state and the municipalities is a major project that may be difficult to achieve in the near term. However, the authorities consider it to be a critical success factor for digitalisation and for the investments that must be made in the development of proposed building blocks.

As a proposed first step, the authorities should perform a detailed analysis of the legal basis required for each building block according to the proposed measures in chapter 5. The authorities also propose that the necessary legal changes should be coordinated by a legal commission, in other words a committee set up by the government.

6.5.3 Consequences for competition between companies

The proposals submitted are considered to have a positive impact on companies over the long term because there will be new opportunities to create needs-oriented products based on the services that will be available in the common public-sector digital information exchange infrastructure. From the point of view of companies, it is important to know early in the process what the public sector will deliver, especially in the case of technical components. In the shorter term, the proposals may have a negative impact on some companies as existing private services are replaced by public solutions.

6.5.4 Compliance with EU legislation

The proposal is fundamental to implementation of the relevant EU directives, including Regulation (EU) 2018/1724 of the European Parliament and of the Council establishing a single digital gateway. The proposal is also in line with the EU's objectives driving the development of EU legislation in this area, including the Digital Agenda for Europe.

1 Appendix 1 – Comparative international analysis

1.1 National solutions and initiatives

A number of different information exchange solutions exist in different sectors and domains in Sweden at present, and there are several exciting initiatives underway in this area. In the context of this report, we have not been able to describe all of them in detail, but have focused instead on solutions and initiatives that have a broadly-based/common public-sector approach.

1.1.1 SHS dissemination and retrieval system (*Spridnings och hämtningssystemet*)

SHS is a communication and transmission protocol aimed at increasing the security of communication over the Internet and SGSI. Asynchronous as well as synchronous information flows are supported.[41]

In this context, a protocol is an agreement between two or more parties regarding the rules for communicating between computers or programs or between nodes in a network. These rules guarantee that communication is technically possible by ensuring that all parties use the same language.

SHS was developed on the initiative of Swedish authorities, but the protocol is now used not only in authorities but also in municipalities and county councils.

At present, SHS is used to[42]:

- send electronic documents
- retrieve information from other authorities' data systems
- subscribe to information from other authorities
- send questions to another authority, to be answered on another day
- provide information such as receipts

No new technology was developed for SHS – established standards with widespread vendor support were used instead, such as http/SSL and SOAP.

SHS offers a message-oriented service architecture and forms an important part of the infrastructure providing coherent administration and the opportunity to develop e-government e-services. SHS is not proprietary so it is open for everyone to use.

SHS is currently the most well-established and widespread system managing communication between authorities via the Internet. SHS is in use today as a technical

[41] In-depth analysis of SHS (*SHS Fördjupad analys*) by MSB SOES, October 2014

[42] SHS information web site of the Swedish Social Insurance Agency: https://www.forsakringskassan.se/myndigheter/e-tjanster/shs – read 2019-06-27

protocol in a variety of domains and authority-specific solutions such as SSBTEK (information exchange complex for economic assistance), RIF (judicial system), Lefi Online (benefit information), etc. These solutions were created to meet specific needs within a defined target group.

SHS 2.0 was finalised in 2013 and uses the same standards and regulatory frameworks for technical interoperability as Inera's National Service Platform (based on RIV-TA). This means that municipalities, county councils and authorities can communicate technically with each other.[43]

SHS provides a component in the form of a global SHS directory that acts as a directory service which publishes information about which actors use SHS and their addresses (communication identifiers). The directory also publishes information about the types of products that can be accessed.

In an analysis from Ramböll[44], the Swedish Association of Local Authorities and Regions found that SHS works well for the larger national authorities with large volumes of data, but that smaller actors such as municipalities and regions considered that the technical solution was too costly and incompatible with the need for synchronous information transfer.

By itself, SHS cannot be regarded as a comprehensive solution to a country's information transfer needs, and lacks a number of components that exist in comparable national solutions abroad. SHS is essentially just a technical protocol (comparable to eDelivery's AS4 protocol). It is therefore unfair to make direct comparisons between SHS and the other solutions in the context of this comparative international analysis.

The Swedish Social Insurance Agency has a coordinating role in the administration and operation of SHS. At present, SHS is officially managed by an SHS council headed by the Swedish Social Insurance Agency, which is responsible for the regulatory framework and the specifications. The SHS council provides leadership and oversight in the development of the SHS specification, and adapts it to new trends and technologies.

1.1.2 National Service Platform (*Nationella tjänsteplattformen*)

The National Service Platform[45] is a technical platform that simplifies, secures and streamlines information exchange between different IT systems in health care and social care. The platform is the hub between systems and e-services that need to communicate with each other, and allows information exchange to take place securely and cost-effectively.

The National Service Platform supports loose coupling by acting as a switchboard for all systems that want to communicate with each other. Organisations can connect their

[43] RIV Instructions: http://www.rivta.se/ – read 2019-06-27

[44] Analysis of Estonian-Finnish cooperation in the X-Road digital infrastructure (*Analys av det estnisk-finska samarbetet kring den digitala infrastrukturen X-road*), Ramböll 2016-01-29

[45] National Service Platform: https://www.inera.se/digitalisering/infrastruktur/nationella-tjansteplattformen-och-tjanstekontrakt/ – read 2019-06-27

systems to the National Service Platform and exchange information that way without connecting to each other directly. A system wanting to contact another system makes a call to the service platform, which forwards the message to the correct system.

For information exchange via the National Service platform to work properly, all actors must agree on how to communicate. Inera is responsible for developing and managing technical specifications – known as service contracts – describing how the requesting system should structure its question message, and how the responding system should structure its reply message. The service contracts are designed for specific functions or business processes, for example for registrations or reservations.

There are also regional service platforms in different regions such as Dalarna and Stockholm. A regional service platform facilitates integration between local systems, which communicate with each other through RIVTA compliant service contracts. In addition, a regional service platform facilitates connections to the National Service Platform. Once a connection between a regional service platform and the National Service Platform has been reliably established, it can be reused for all new connections to the National Service Platform.[46]

The main purpose of the service platform is to provide a national web service for each type of service. IT support in the care system is seldom a national service for a particular function. Responsibility for the organisation's operational IT support is regional. The same function therefore exists in multiple places. Sometimes the same system is copied, and sometimes the systems are different. The diverse flora of systems is an impediment for consumers of services such as citizen portals. Without the service platform, each service consumer would need to keep track of which service belongs to which care provider and also understand the different technical dialects used in communication.

The service platform supports technical and semantic interoperability in a technology-independent way, and forms the basis for services such as *Nationell patientöversikt* (national patient overview), *Elektronisk remiss* (electronic referral) and *Journalen via nätet* (web-based medical records).

Over 500 care systems are connected, communicating with each other via the service platform, and the number of calls via the platform is increasing. On average more than 70 million producer calls are made every month.[47]

Inera is responsible for the National Service Platform, developing and managing national digital services in e-health and digitalisation on behalf of regions and municipalities. Inera is also responsible for the common infrastructure and IT architecture on which the services are based. Inera is a company owned by SKL Företag AB, regions and municipalities.

---

[46] The service platform in confluence (*Tjänsteplattformen i confluence*): https://skl-tp.atlassian.net/wiki/spaces/SKLTP/overview – read 2019-06-27

[47] Number of calls and response times: https://www.inera.se/aktuellt/statistik/tjansteplattformen/ – read 2019-06-27

1.1.3 Secure Digital Communication (the SDK project)

The Secure Digital Communication (*Säker digital kommunikation*) project[48], or SDK for short, aims to equip Sweden with a standardised capability for secure digital communication between public actors, including private service providers delivering public assignments. This involves defining a common method of transferring sensitive information in a uniform, efficient, secure and agreed way. In the long term, it must also be possible to convey information to individuals and other stakeholders through existing communication channels by adapting to the same standards. Secure digital communication must also be possible beyond Sweden's borders.

The project is being run with Inera as the project owner with the Swedish Association of Local Authorities and Regions, Kommentus, and in collaboration with regions, municipalities and government authorities.

Secure digital communication is based on eDelivery. Basing the development of the SDK solution on eDelivery means that the project uses the EU's eDelivery specifications to configure components such as access points, metadata service, address registers and links to eDelivery components at national level and within the EU. The project adds parts that are currently missing in eDelivery but are needed for SDK, for example an SDK address book which as well as supporting addressing between organisations as in eDelivery, also supports addressing between functions within organisations. The project is also developing a message specification setting out the structure of the secure message.

The main motivations for using eDelivery for SDK are to reuse established standards for secure messages, to avoid isolated solutions and to enable communication even beyond Sweden's borders. In Sweden, DIGG, the Swedish Agency for Digital Government, is responsible for eDelivery.

In 2018 a proof of concept was created to verify the SDK concept including the strategy of building on the EU's eDelivery framework for secure messaging. The result was that the standards and specifications underpinning the SDK project work well for sending, receiving, notifying and acknowledging secure messages and attachments between different theoretical actors.

1.1.4 Swedish Government Secure Intranet (SGSI)

SGSI[49] is a communication service for secure communication between organisations in Sweden and Europe, funded by charges. SGSI has its own infrastructure that is separate from the Internet and is therefore not exposed to Internet disruption such as denial-of-service attacks. Traffic is carried between connected organisations in so-called VPN tunnels which are encrypted.

[48] SDK Inera: https://www.inera.se/aktuellt/projekt/saker-digital-kommunikation/ – read 2019-06-27

[49] SGSI MSB: https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyhetsarkiv/Nyhetsarkiv-2017/Sa-fungerar-SGSI-natet2/ read 2019-06-27

SGSI can be used to access the databases of other connected authorities, to send secure e-mail and to run secure video conferencing over the connection. SGSI, being linked to the secure TESTA network, also allows Swedish authorities to access sector-specific EU services or to exchange information with other EU member states.[50]

Connected organisations use SGSI as an infrastructure for exchanging sensitive information. This reduces the risks associated with sending sensitive information. Connected organisations decide for themselves who to communicate with over SGSI and what to send. To communicate over SGSI, senders and receivers must agree to establish a connection and decide on what kind of communication it will be used for.

An authority can only join if it is SGSI accredited. This is in order to establish trust and confidence in how the authority handles issues relating to information security and in particular SGSI security. To achieve this, the authority is transparent about its information security activities, especially about the security of the connection to SGSI.[51]

1.2 European Union initiatives and solutions

1.2.1 EU objectives and strategies

Europe 2020 – the EU's common strategy for growth and jobs – and the Digital Agenda for the same period clearly identify the Digital Single Market[52] (DSM) as a key objective. This objective reflects the substantial need for greater digital mobility across European borders. To achieve this objective, efficient information exchange is a crucial prerequisite. Without the complete, secure and efficient exchange of fundamental data, there is no guarantee of timeliness and quality in information exchange between the member states.

There are a number of initiatives to establish DSM – Horizon 2020, the EU's research and innovation funding programme, and the supporting programmes Interoperability Solutions for European Public Administration (ISA²) and Connecting Europe Facility (CEF).

Implementation plans such as the European eGovernment Action Plan as well as agreements between the member states, for example the Tallinn Declaration[53], further boost the objective by highlighting important activities such as cross-border and stable eID systems (eIDAS) and cross-border information exchange based on the "Once Only Principle"[54]. The 20 actions in the action plan aim to make public administrations and public institutions within the EU transparent, efficient and inclusive by providing cross-border and user-friendly digital public services to all EU citizens and businesses.

[50] Isa2: https://ec.europa.eu/isa2/solutions/testa_en – read 2019-06-27
[51] SGSI factsheet (*Faktablad SGSI*) MSB 180817
[52] Digital Single Market: https://ec.europa.eu/digital-single-market/en
[53] Ministerial Declaration on eGovernment – the Tallinn Declaration October 2017
[54] The Once Only Principle: http://www.toop.eu/

In the publicity for the plan, the European Commission states that it is up to the member states to choose their own technical platform and system support and also decentralised or centralised infrastructure. This is subject to adherence to agreed principles.

All actions in the eGovernment Action Plan and the seven principles are relevant to the government assignment concerning secure and efficient electronic information exchange in the public sector. We should pay particular attention to the "interoperability by default" principle in the part of the assignment which relates to secure and efficient electronic information exchange in the public sector. The principle is explained in the Action Plan with the text "public services should be designed to work seamlessly across the Single Market and across organisational silos, relying on the free movement of data and digital services in the European Union".

The wording implies a likely aim to coordinate and interconnect the member states' information exchange infrastructures. As previously stated, such interconnection presupposes a universal Swedish infrastructure. Otherwise, multiple costs will be incurred, for example where isolated domains connect separately to an EU infrastructure.

The actions in the eGovernment Action Plan that are most relevant to this assignment include action 18 "Assess the possibility of applying the once-only principle for citizens in a cross-border context". In addition, the somewhat clearer, ongoing actions 7 "Submit a proposal for a Single Digital Gateway" and 9 "Set up in cooperation with the Member States, the mandatory interconnection of all Member States' business registers" will have a significant impact on Swedish infrastructure if they are implemented.

1.2.2 Interoperability solutions and common frameworks for European Public Administrations (ISA²)

The ISA² programme[55] is intended to help member states provide digital interoperability services. The help includes methods for interoperability, standardisation, semantics, architecture and data sharing. The aim is to encourage European public administrations to communicate electronically and seamlessly with each other and with citizens and businesses.

ISA², working with the member states, has developed the European Interoperability Framework (EIF). The framework provides specific guidance on how to develop and introduce interoperable digital public services. The programme also supports the introduction of interoperable services with the European Interoperability Reference Architecture (EIRA).

1.2.3 Connecting Europe Facility (CEF)

The Connecting Europe Facility (CEF)[56] is a key EU funding instrument to facilitate cross-border collaboration between public administrations, companies, citizens and others by distributing digital service infrastructures (DSIs). The projects funded and

[55] ISA2: https://ec.europa.eu/isa2/home_en – read 2019-06-27

[56] CEF Telecom: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom – read 2019-06-27

supported are expected to help create a European ecosystem of interoperable and interlinked digital services that keep the digital single market working.

CEF Building Blocks are a set of services (including software, documentation, training and support) provided by the European Commission and supported by the member states. The purpose of the building blocks is to support the development of DSM by providing reusable functions and support for cross-border digital services. The European Commission is currently focusing on the eID, eSignature, eDelivery, eTranslation and eInvoicing building blocks.

The building blocks with accompanying backup and support are free to use for all European projects related to digital public services. Each building block consists of

- a service platform with technical specifications and standards that must be complied with,
- a layer of sample software meant for reuse to facilitate implementation of the technical specifications and standards,
- a layer of services, e.g. software, test features, help desk, depending on the building block.

Member states can receive EU funding to implement projects using the building blocks.

1.2.4 eDelivery

eDelivery[57] consists of reusable specifications, software and services that form a digital service infrastructure in a variety of domains.

The main purpose of eDelivery is to ensure that public actors can exchange data and documents across EU borders in a secure, interoperable and reliable way. eDelivery also supports information exchange with companies and citizens.

eDelivery is based on a distributed model where every participant becomes a node in the network by using standard transport protocols and security policies. eDelivery allows direct communication between participants without the need to set up bilateral channels.

eDelivery contains a number of different components and tools, for example transport protocols, addressing functions, enveloping and certificate management, that can be used and adapted/developed according to a specific need. The solution is therefore customisable, and an organisation's own components and specifications can also be added.

eDelivery is designed to support a model called a four-corner model but can also be used in other configurations. eDelivery applies technical specifications and can be used in domains of all kinds to guarantee the secure and reliable transmission of structured, unstructured and binary data and documents. The transfer does not have to take place across EU borders, but can also take place within a sector or domestic domain.

[57] eDelivery: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery – read 2019-06-27

eDelivery is already being used today in several different domains and large-scale projects at EU level, for example in the system interlinking business registers, the eJustice portal, PEPPOL, etc. The European Commission is clear in its strategy of using the digital service infrastructure building blocks to create a single digital market within the EU. It provides funding for technical development, support and administration of key components and grants are also available for implementation.

At present, the use of eDelivery is mainly domain-specific, although the solution is technically not limited to that purpose. The main purpose of the existing implementations is to facilitate cross-border interoperability and guarantee exchange between countries in different sectors and domains.

1.2.5 Single digital gateway (SDGR)

In October 2018, the European Parliament and the Council adopted Regulation (EU) 2018/1724 establishing a single digital gateway. The Regulation aims primarily to provide citizens and businesses in the EU with access to information, to procedures and to problem-solving services.

The Regulation has been published and the implementing acts are being drafted. They will have an implementation period of 3-5 years. One implementation will be a shift to a European top-level domain where information and e-services will be made searchable and usable for all EU citizens. The Regulation will apply to most areas of the public sector. In addition, the SDGR means that certain data, including basic data, must be searchable and accessible across borders in the same way.

1.2.6 The Once Only Principle (TOOP)

The EU's TOOP project is a sub-project of Horizon and is one of the 20 priority actions in the European Commission's eGovernment Action Plan for the period 2016–2020. TOOP is based on the principle that a piece of information should only have to be provided once, to one authority/instance. The project focuses on the cross-border digital information exchange of company information between authorities within the EU. The overall aim is to demonstrate the feasibility of the “Once Only Principle” by developing a proposal for a federated European digital information exchange infrastructure. The proposal will be based on pilot developments in several areas, all focusing on the exchange of company information. Despite this focus, it will be possible to develop the result so it can handle digital information exchange in other areas too.

After being extended for nine months, the project is expected to finish in March 2020. One of the reasons for the extension was that TOOP was given the extra task of being the technical system that carries information under the Single Digital Gateway Regulation.

Several European countries have begun to incorporate TOOP into their legislation and regulations. In Belgium, Estonia and the Netherlands, binding legislation has already been passed.[58]

1.3 International solutions

1.3.1 Estonia – X-Road (X-tee)

X-Road[59] is a centrally managed distributed data exchange layer between information systems. X-Road enables the secure transmission and exchange of data between information systems over the Internet. X-Road acts as an intermediate layer and makes it less complex for members to communicate securely between parties.

X-Road consist of two key components. Central Server, which is a register of X-Road members and their security servers. The security server is the gateway to the network and is required in order to both produce and consume services via X-Road. The servers carry requests between information systems.

In addition, the solution is based on a range of trust services such as certification, validation and logging of messages and transmissions. These may be provided by third parties or centrally.

X-Road technology is currently in use in Estonia (where it is called X-tee), Finland (suomi.fi Data Exchange Layer) and about ten other countries such as the Faroe Islands, Kyrgyzstan and others. Iceland is also in the process of implementing the solution.

X-tee is described as a fully distributed and secure platform for information exchange[60]. The platform was initially only available to the public sector but was later also extended to private actors for greater efficiency and convenience. People also call the solution the backbone of the Estonian government because the vast majority of their registers and databases are made public through the platform. With X-tee's logic and architecture, there is no central storage of information. Instead, all data between actors is received and sent as needed.[61]

The technology behind the X-tee is not unique – the system is based on international standards and protocols and since 2016[62] its source code has been open and accessible for anyone to use.

The aim in Estonia is for each type of data, for example the addresses of citizens, to be stored only in one place – and for everyone to have access to the information via X-tee without the need to save their own copies. Estonia also has legislation prohibiting an

[58] EU-wide digital Once-Only principle for citizens and businesses – policy options and their impact, EU 2014
[59] X-Road e-Estonia: https://e-estonia.com/solutions/interoperability-services/x-road/ – read 2019-06-27
[60] Introduction to X-tee: https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html – read 2019-06-27
[61] Report on X-Road (*Rapport om X-road*) – Ramböll 2016-01-29
[62] Open source code: https://github.com/ria-ee/X-Road – 2019-06-27

authority from asking a citizen or company for information already held by another authority – instead they must use X-tee to obtain this information.

The use of X-tee in Estonia is very widespread. In 2018 nearly a billion requests were handled by X-tee[63].

The Estonian Information System Authority (RIA) is responsible for coordinating and implementing Estonia's digitalisation policy. The authority's job is to coordinate the development and administration of information systems so that Estonian citizens get the best possible service. The RIA is responsible for all public infrastructure relating to information technology such as X-tee, the government e-portal[64] etc. The authority reports to the Estonian Ministry of Economic Affairs and Communication, which is responsible for the development of the country's information policy. Within the ministry, there is a department called the Government CIO Office which plays an important role in the information policy of the country. This department is responsible for the government's IT budget, coordination of IT, standardisation, etc. The department is divided into six different teams (Legal, Financing, ICT Skills, Cybersecurity Policy, Govtech, International Affairs).

Estonia has joined with Finland to establish the "Nordic Institute for Interoperability Solutions (NIIS)" which is a common network and a collaboration platform for the development of X-Road technology. The NIIS is responsible for managing and revising X-Road's source code, licensing and distribution principles, development and support, etc.

1.3.2 Finland – eSuomi.fi Data Exchange Layer

Suomi.fi Data Exchange Layer[65] is a standardised, uniform, coordinated, interoperable and secure data exchange layer that enables the exchange of data and access to information sources in a simple and cost-effective way.

Suomi.fi Data Exchange Layer is Finland's national implementation of the X-Road technology. In contrast to Estonia, X-Road is not the only technology in use in the country, where some sector/domain-specific solutions still exist. Suomi.fi Data Exchange Layer also contains other components, e.g. a directory of services and certain components relating to monitoring of the services.

Existing services connected to the data exchange layer allow all integrated information sources and service components to be used, improving cost-effectiveness and enabling more efficient development through reuse.

Suomi.fi Data Exchange Layer uses the same code base as X-tee in Estonia in all core components. All the differences between Suomi.fi Data Exchange Layer and X-tee relate to local configuration

[63] X-tee factsheet: https://www.x-tee.ee/factsheets/EE/#eng – read 2019-06-27
[64] Eesti.ee gateway: https://www.eesti.ee/en/ – read 2019-06-27
[65] eSuomi.fi Data Exchange Layer: https://esuomi.fi/suomi-fi-tjanster/suomi-fi-informationsled/?lang=sv – read 2019-06-27

The API Catalogue[66] in Finland is a directory of APIs in the national data exchange layer. The purpose of the directory is to help producers and consumers develop more efficient electronic services and to encourage reuse of the information. Service providers can choose to use only the API Catalogue.

Public sector organisations are either required or entitled to use the data exchange layer under Finnish legislation. The same legislation also entitles private sector organisations to use the data exchange layer to transfer information.

Connecting and using the service is free for everyone, including the private sector. Each actor covers its own implementation costs, but the Ministry of Finance may in some cases grant funding to public organisations.

The information provided via the data exchange layer is either transferred between users and providers on a contractual basis, or is freely available by everyone connecting.

In Finland, the Population Register Centre is responsible for the operation and management of the national service architecture for e-services, and the Finnish Ministry of Finance performs governance functions.

1.3.3 Denmark – Datafordeler

Datafordeler[67] (data distributor) in Denmark provides authorities, businesses and citizens with secure and easy access to basic data from public registers. The purpose of the data distributor is to make basic data available and to facilitate transfer with a common data model[68]. The solution constitutes the digital infrastructure for the distribution of basic data in Denmark and has gradually replaced a number of previously distributed solutions.

The data distributor ensures that authorities and organisations have easy and secure access to basic data in a single system, instead of isolated systems and interfaces.

The data distributor is restricted to and designed for information exchange concerning basic data, but can also be used to distribute other relevant data. The solution carries information in the public and private sectors.

The data distributor was developed within the framework of Denmark's basic data programme called "*Gode grunddata till alle*" (good basic data for all), a national initiative working to standardise and make the country's basic registers available. The programme started in 2012 and has gradually modernised basic data in a number of sub-programmes.

The Danish Agency for Data Supply and Efficiency (SFDE) has operational responsibility for the data distributor. SFDE is part of the Danish Ministry of Climate, Energy and Utilities.

[66] API Catalogue in Finland: https://liityntakatalogi.suomi.fi/sv/ – read 2019-06-27
[67] About Datafordeleren: https://datafordeler.dk/vejledning/om-datafordeeren/ – read 2019-06-27
[68] Data model: https://datafordeler.dk/vejledning/datamodel/ – read 2019-06-27

1.3.4 Singapore – APEX

The Government Technology Agency of Singapore (GovTech) develops and is responsible for Singapore's API exchange (APEX)[69]. APEX is a centralised information exchange platform where public actors can exchange data in an efficient and secure way using APIs. The platform supports central monitoring and security management for the APIs. APEX is Singapore's tool connecting different types of systems and is used by various authorities and ministries, which in many respects have various existing domain-specific and sector-specific solutions.

APEX is based on a self-service model in which the calling authority can obtain various kinds of data and information directly from other authorities by using pre-configured checks of rights and access. The APIs published on APEX can either be open to the public, or private (for internal use by the public sector).

The APIs are reusable for integration with other services and applications, or for statistics. This allows existing infrastructure to be used, which saves costs because authorities do not need to create new services from scratch. It also shortens the time taken to develop new services.

Public actors can use APEX to manage and evaluate/monitor their APIs and real-time data consumption and obtain an overview of how their information is being accessed.

APEX currently has about a hundred connected APIs and more are being added all the time. GovTech uses APEX for its "MyInfo" service, a platform in which users only need to provide their personal data to the government once, instead of for each transaction.

APEX is part of a common national digital infrastructure called the "Singapore Government Technology Stack (SGTS)"[70], which consists of a number of technical building blocks providing common software services and shared infrastructure services that authorities and other public actors can reuse to build and test new services and applications quickly and efficiently. The main aim is to create a common platform for back-end services so that the authorities can focus on content and customer-facing services without having to create infrastructure, storage and information exchange systems from scratch.

SGTS consists of a number of different standardised layers, a fundamental infrastructure layer consisting of container-based hosting and cloud solutions. An application layer (intermediate layer) consisting of a collection of developer tools or components. It includes components such as APEX, platform-as-a-service (NECTAR) and common security and analysis components. The microservice layer manages various reusable common public-sector services such as payments, authentication and identification solutions. The top layer consists of front-end applications for consumer-facing digital services.

[69] Apex and Nectar: https://www.tech.gov.sg/media/technews/getting-to-know-nectar-and-apex – read 2019-06-27
[70] Singapore Tech Stack: https://www.tech.gov.sg/products-and-services/singapore-government-tech-stack/ – read 2019-06-27

GovTech is an authority (statutory board) forming part of the "Smart Nation and Digital Government Group" (SNDGG) which answers directly to the Prime Minister's Office (PMO). The PMO consists of a number of authorities and agencies that provide support and advice on strategically important issues. GovTech works with public actors to develop and deliver secure digital services and applications to individuals and companies in Singapore. GovTech is responsible for the infrastructure and solutions needed to realise the country's strategies.

1.3.5 Belgium – Federal Service Bus

Belgium is considered to be in the vanguard of information exchange between authorities – their Federal Service Bus (FSB) platform and the regional solution Maximum Data Sharing Between Agencies (MAGDA) are highlighted as examples to follow.[71] In 2017, the Magda platform won the award for best IT solution for the public sector in a competition organised by the European Commission.[72]

Belgium does not have a single solution for the supply and transfer of information in the country, but rather a network consisting of several different "service integrators" in various sectors. Efforts are being made to connect them with each other. There are two regional service integrators, one for Flanders and one for Wallonia, there is a federal service integrator and there are service integrators for the welfare sector and the e-health sector. These integrators interconnect and provide access to different data sources within the network.

The country has identified and defined what it calls authoritative data[73] and sources, which correspond to data sources in which basic data is stored. This data is sent on within the ecosystem through a common data exchange layer based on the service integrators using web-based services.

In Belgium, ministries are called Federal Public Services (FPS), and each FPS has one or more responsible ministers. The FPS Policy and Support is responsible for federal IT, budget, organisation, support, etc. Within this organisation, a department called "Directorate General Digital Transformation"[74] (formerly FEDICT, now BOSA) is responsible for digitalisation in the country, and supports the government in the process. The Digital Transformation Office (BOSA) is responsible for the national infrastructure and develops components such as the common information exchange solution (Federal Service Bus, FSB). It is responsible for implementing and developing government policy and is the driving force in the country.

1.3.6 Netherlands – Digikoppeling

Digikoppeling[75] (Digilink) is a set of standards for electronic information exchange between public actors. Digikoppeling supports the exchange of data between public actors

[71] Access to base registries report 2016 – European Commission
[72] Sharing and Reuse Awards Contest 2017: https://ec.europa.eu/isa2/awards_en – read 2019-06-27
[73] Information exchange in Belgium: https://dt.bosa.be/en/gegevensuitwisseling – read 2019-06-27
[74] DG DT: https://dt.bosa.be/en – read 2019-06-27
[75] Digikoppeling: https://www.logius.nl/diensten/digikoppeling – read 2019-06-27

and links to other building blocks within the Dutch digital infrastructure. Digikoppeling does not regulate the content of the transfer, but only the logistics.

In order to exchange data between IT systems, organisations must agree about formats, transport methods and packaging. Digikoppeling is a specification of two international standards for electronic transfer, WUS and ebMS2. The different standards are used to meet different types of needs and solution paradigms.

Logius is responsible for the management, development and promotion of national digital infrastructure components in the Netherlands. Logius is a department of the Ministry of the Interior and Kingdom Relations.

1.3.7 Norway – Altinn

Altinn[76] is a common public-sector solution and interface for developing and maintaining forms and processes, combined with a solution for reporting and information exchange primarily between the private sector and authorities. Companies and individuals can report their information through Altinn either through an Internet portal or through their own internal information systems or software solutions. Altinn acts as Norway's point of single contact[77]. Altinn, which translates as “all in”, is a comprehensive solution and platform for digital services rather than a solution for information exchange.

Altinn offers a number of different types of functionality, for example the solution can be used to send documents or large quantities of data between public actors and the private sector. Information from the actors' registers can be sent to one or more recipients. The information is sent either from machine to machine or via the inbox/messaging service. Altinn only acts as an intermediary and does not concern itself with the content, but it does guarantee delivery and traceability. Altinn provides a common technical infrastructure that ensures secure transport between the actors. Altinn has its own administrative organisation that manages maintenance, operation and backup of the technical solution.

Altinn also allows users to access information that public actors have saved in their systems. This makes it easy for users to access their own data and retrieve it directly from the database. This could be a way of obtaining customer information, permits, licences, etc.

Altinn also offers a consent service allowing access to data about people or organisations that the public sector already has, for example tax information. The consent service is used when a public actor is not legally entitled to acquire the information without permission. The user can see what information they are sharing and who with, for how long and for what purposes. The service simplifies data collection from users and allows previously collected data to be used for more purposes after consent has been obtained. It also enables private actors to use public data in a secure and efficient way.

[76] What is Altinn: https://www.altinn.no/om-altinn/hva-er-altinn/ – read 2019-06-27

[77] Points of single contact EUGO: https://ec.europa.eu/growth/single-market/services/services-directive/in-practice/contact_en – read 2019-06-27

Altinn also has a permission service that controls who can use a digital service. The users log on via the Norwegian ID-porten[78]which is the Norwegian common public-sector portal for logging into public services on the Internet. They are then able to access the service via the ID-porten. If someone intends to use a service on behalf of a company, a lookup is performed in Norway's Central Coordinating Register for Legal Entities to confirm that the person is authorised to act on behalf of the company.

This is a product that lets you control who can use a digital service. Users log on via the ID-porten and are then passed onto the service. If someone intends to use a service on behalf of a company, a lookup is performed in Norway's Central Coordinating Register for Legal Entities[79] to confirm that the person has a role on behalf of the company.

Altinn is provided and managed by the Brønnøysund Register Centre, which is tasked with developing and operating digital services and registers. The Brønnøysund Register Centre is an authority forming part of the Norwegian Ministry of Trade, Industry and Fisheries.

1.4 Comparative international analysis based on specific aspects

1.4.1 Technical prerequisites

On the whole, from a technical point of view, there is no great difference between the solutions we studied in detail in the outside world and the solutions that already exist in Sweden. The solutions are usually built on similar topologies in the form of three or four corners models. They are often based on similar technologies or standards – XML, SOAP or REST being the most prevalent. SHS and the Service Platform (SHS) both have a number of similarities with X-Road and eDelivery, as they are all based on distributed architectures without central storage, transport via the Internet and authentication through certificates.

Several countries have published the source code for their solutions under open licences. There is generally a great deal of transparency around the technical solutions, primarily in order to promote development and use.

What distinguishes the solutions is usually the kind of key components created and how the use of the solution is controlled. Key components of the solutions are often found in the form of addressing/address registers, certificate management, transport protocols and various kinds of security and trust services.

Compared with the private sector and the corresponding information provision solutions, it is clear that some of the countries' solutions are based on apparently outdated thinking and technology.

[78] ID-porten: https://eid.difi.no/nb/id-porten – read 2019-06-27

[79] Entity Registry: https://data.norge.no/data/registerenheten-i-br%C3%B8nn%C3%B8ysund/enhetsregisteret – read 2019-06-27

It is usual to find multiple technical solutions in the analysed countries, and sector/domain-specific solutions or region-specific solutions remain in place even though a common digital infrastructure for information provision has been introduced. Usually the common digital infrastructure consists of standards, regulatory frameworks and common central reusable components, rather than a common technical platform or solution that can meet all needs.

Countries such as Finland, Belgium and Singapore preserve region-specific, sector-specific and/or domain-specific solutions that are then linked by national standards or common public-sector solutions and components. Denmark has restricted its common information exchange solution to providing basic data alone.

The primary purpose of a common public-sector solution in these countries is therefore to enable cross-sectoral/cross-domain exchange and to make important data sources available in a standardised way. The solution in most countries also encompasses integration and exchange with the private sector and citizens.

Example from Belgium – regional solutions that work together

Belgium does not have a single solution for the supply and transfer of information in the country, but rather a network consisting of several different "service integrators" in various sectors. Efforts are being made to connect them with each other.

There are two regional service integrators, one for Flanders and one for Wallonia, there is a federal service integrator and there are service integrators for the welfare sector and the e-health sector. These integrators interconnect and provide access to different data sources within the network. All integrators use the same types of standards and regulations to guarantee interoperability.

1.4.1.1 API management

Several countries highlight the growth of APIs and the transition from traditional solutions to API solutions based on REST/JSON. Singapore uses a fully API-based solution as the basis for its information exchange. Finland has an API database to supplement its data exchange layer, and future versions of X-Road[80] will support REST, allowing REST API to be produced and consumed over X-Road. The Netherlands, too, emphasises the growth of API-based solutions as a challenge and a major opportunity going forward. The development is also illustrated in a quotation[81] by the Estonian Government's CIO Sim Sikkut as follows:

"...we have to change how we procure and architect things. For example, we have to be much more micro-service and API-based as opposed to [deploying] monolith systems."

APIs and API Gateways are no longer new technologies or particularly innovative solutions, but rather private sector practices. The innovation and benefits flow from making these technologies more accessible and increasing their use in the public sector.

[80] X-Road REST support: https://www.niis.org/blog/2019/3/25/two-steps-from-the-x-road-rest-support – read 2019-06-27

[81] Interview in IDG: https://www.idgconnect.com/idgconnect/news/1023053/creating-digital-society-learn-estonia – read 2019-06-27

In a report[82] on the topic, Gartner highlights the concept of "Full Life Cycle API Management" with the following definition:

"Full life cycle API management involves the planning, design, implementation, testing, publication, operation, consumption, versioning and retirement of APIs. It includes a developer's portal to target, market to and govern an ecosystem of developers to use APIs, as well as API gateways for runtime management, security and gathering of usage data."

The report describes how a technology passes through different phases and how technologies are expected to mature and deliver value in the public sector.

The conclusions that can be drawn from the report are that full life cycle API management is a technology that is about to mature and that has great potential to deliver value within public administration.

Another report[83] from Gartner sets out challenges, recommendations, and the introduction of APIs by public administrations.

In the report, Gartner identifies the following key challenges:

- *The versatility of APIs can be a disadvantage, causing confusion when trying to communicate API strategies to government executives. The potential of APIs, along with the challenges associated with using them, is not well-understood.*
- *APIs are key to empowering ecosystem partners and promoting service innovation. But ad hoc API initiatives without focus can result in a scattered array of APIs that are not linked to government or community outcomes.*
- *Maintaining funding or support for an API program can be difficult if the value the program produces cannot be translated to business outcomes and measured.*

Gartner also identifies the following recommendations:

- *Instill a business outcome focus into your API program by using key business leaders as API product managers. Add API product manager responsibilities to the current roles of key business-focused champions that are passionate about alternate service delivery channels and business models.*
- *Focus on API programs that represent value to internal and external stakeholders by co-creating a multifaceted strategy that supports the development, delivery and curation of API products.*
- *Deliver APIs that have clear, measurable benefits, or that are considered strategic investments, by establishing critical evaluation criteria for potential API products as part of your API framework. These criteria should categorise and prioritise API development, but should not be so restrictive that they stifle transparency or innovation.*

The report recommends a result-focused strategy to identify the best method for API applications in public administration.

The report also describes how APIs are used in public administration.

[82] Gartner – Hype Cycle for Digital Government Technology, 2018

[83] Gartner – Government APIs Are About Delivering Outcomes, Not Technology

- *Many government organisations are largely ignoring APIs, not positioning them within their business or technology strategies.*
    - *in these organisations, APIs are integration tools and only used for point-to-point solutions to unlock data in legacy systems or on an ad hoc basis.*
- *Others are tacking them onto open data programs by wrapping static government datasets as APIs.*
- *Other government organisations and central information and communication technology (ICT) bodies have established API standards, guidelines, reference architectures and supporting governance models*
- *More API-centric government ICT departments are working to establish an "API first" culture, creating APIs for all government services, building internal and external development communities, and implementing full life cycle management*

1.4.1.2 Interoperability and compatibility

Interoperability between the various analysed solutions occurs only in a few cases. Interoperability is defined here as systems that are capable of working together and communicating with each other. For example, this can be achieved by using the same type of technical protocols.

SHS 2.0 is interoperable with the Service Platform.[84]

Inera has developed a regulatory framework for interoperability that has been used in Swedish e-health since 2009. The regulatory framework contains guiding principles and detailed instructions about how to design systems and technical solutions to lay the foundation for cooperation between regions and municipalities. It also contains documentation and auditing templates for systems developed according to the technical reference architecture.

The regulatory framework is based on a number of standards, specifications and recommendations from recognised standardisation bodies.

The same set of standards and regulations for technical interoperability are contained in the authorities' specifications known as SHS 2.0 (dissemination and retrieval system). This means that municipalities, regions and authorities can communicate technically with each other if the systems of both parties adhere to these regulations.

X-tee is interoperable with soumi.fi Data Exchange Layer.

The Population Register Centre of Finland and the Estonian Information System Authority (RIA) agreed in September 2016 to federate their data exchange layers, in other words to establish confidence between the Finnish and Estonian data exchange layers. The agreement enables the technical mediation of information from a service connected to the Suomi.fi data exchange layer to the Estonian data exchange layer and vice versa.

Under the agreement, organisations exchanging information must conclude individual agreements. Once the data exchange layers have been coordinated in the production environment, it becomes possible to exchange data such as population register data between the countries.

[84] Inera about interoperability: https://www.inera.se/digitalisering/interoperabilitet/teknisk-interoperabilitet/ – read 2019-06-27

Compatibility of international solutions with existing Swedish solutions

Although in many respects there are technical similarities between national solutions and the analysed solutions in terms of the choice of programming language, solution paradigms and components, they are not directly compatible with each other. Interoperability would require a major effort to reconfigure connections to provide service switches and bridges.

1.4.2 Governance, organisation and funding

1.4.2.1 Governance and organisation

Several countries have made much more progress than Sweden on the management of basic data and information exchange. In most cases, there are formulated national strategies and a designated actor or organisational model for the management and administration of common infrastructure. The designated actor is usually a central authority or department within a ministry in charge of digitalisation. In many cases, these actors have considerable capacity, competence and powers in the field.

In both Norway and Finland, there is political pressure favouring comprehensive digitalisation strategies – an example of strong management by results. "*Lösningar för Finland*" (Solutions for Finland)[85] and Norway's "*En digital offentlig sektor*" (A digital public sector)[86] describe objectives for 2025 in which common public-sector solutions and infrastructure play an important role.

Regarding methods of governance, there are differences between countries. Several have chosen governance through legislation, while others use political directives and contractual solutions within and across different sectors. In the absence of legislation, strong alternative incentives are needed which in practice culminate in the compulsory use of infrastructure developed in common. The experience of Finland in particular demonstrates the importance of clear, direction-setting policies and close cooperation between implementing actors.

The importance of cooperation is highlighted as a success factor in countries like Finland and Belgium, where the joint development of multiple technical solutions meant the benefits could be realised more quickly while ensuring interoperability between the solutions.

With regard to coordination issues, examples of other types of collaborative models – in the form of joint councils, committees or networks – are considered to have been successful in several countries such as SKATE (governance and coordination of services in e-government) in Norway and the Coordination Committee of Service Integrators in Belgium.

In terms of governance at European level, the EU aims to establish the Digital Single Market (DSM), which means in practice that governance in digitalisation is based on the

[85] *Lösningar för Finland* (Solutions for Finland) – Strategic programme for Prime Minister Juha Sipilä's government 2015-05-29
[86] *En digital offentlig sektor* (A digital public sector) – Digitalisation strategy for the public sector 2019-2025, 2019-06-11

need for clarity and order in basic data and cross-border exchange between authorities and between member states.

Example from Finland – governing legislation

With regard to the digitalisation of society, Finland has strongly emphasised centralisation, in terms of public sector organisation as well as legislation. Finland has actively worked on framework legislation for the digitalisation of society. One example is the law (24.1.2003/13) on electronic communication in government activities that was passed as long ago as 2003 and has been continuously updated since then. The law is broadly applicable to authorities and defines concepts such as electronic documents, allows decision-making documents to be signed electronically[87] and states that electronic documents generally meet the written form requirement. The law also imposes a number of obligations on authorities. For example if they have the capacity, they are responsible for creating systems to receive, send and process electronic documents.

Regarding the governance of information management[88] in public administration, there is a specific law[89] which states that the Ministry of Finance must oversee the general governance of information management within the authorities involved in public administration. This implies planning of the overall IT architecture. The law also requires authorities to endeavour to arrange their activities so that they use certain designated register data[90] for their operational needs. Such data could be referred to as basic data, for example data from the Population Information System and the Register of Associations. However, there is no statutory definition of basic data in Finland.[91]

According to the Finnish representatives contacted for the study, the above has simplified the implementation and use of the Finnish platform for electronic information exchange, because previously there was a habit of using the same services and there is a clarity in the governance.[92]

Example from Denmark – state governance

There are examples of detailed requirements in the legislation concerning standards, etc., for example for electronic invoices to the state[93], but these are limited in number. In November 2017 a strategy paper was published outlining how IT should be used in government[94]. The issues highlighted include the need for coherent IT in government, increased data sharing, closer cooperation in fundamental IT operations, common solutions and development. It is evident that public actors must keep their own house in order in terms of IT, but also join with other authorities and share

[87] In accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[88] Defined in paragraph 3 of the law (10.6.2011/634) on information management governance in public administration as follows: *information management in public administration is a support function that safeguards the delivery of public administration functions by means of information and communication technology methods and procedures.*

[89] Law on information management governance in public administration (10.6.2011/634) (*Lag om styrning av informationsförvaltningen inom den offentliga förvaltningen*).

[90] See paragraph 10 of the above law.

[91] But see page 45 RP 59/2016 rd which contains a description of basic register and basic register information.

[92] See also page 11 Programme for implementation of a national service architecture (KaPA) 2014 – 2017 Final report, Ministry of Finance, Helsinki 2018.

[93] *Bekendtgørelse om information i og transport af OIOUBL elektronisk regning til brug for elektronisk afregning med offentlige myndigheder* (Order on information and transport of OIOUBL electronic invoice used for electronic settlement with public authorities).

[94] IT governance in Denmark: https://digst.dk/strategier/strategi-for-it-styring-i-staten/ – read 2019-06-27

data with them.[95] There is also a push towards more common solutions and integrated IT operations, as well as more standardised processes.[96] So the ambition is clear, but it is not obvious whether the intention is to achieve it through legislation or otherwise. IT and information exchange in the authorities is currently constrained by legislation, so it is reasonable to assume that the intention is to achieve the ambition by means other than legislation.

With regard to the Danish solution for information exchange (Datafordeler), governance is divided into two parts. There is an overall coordination and development organisation, which is responsible for contacts and relations with other areas that rely on basic data. The other part is an implementing organisation with active responsibility for operations, management and change.

1.4.2.2 Funding

Several of the analysed countries have made major investments to create a common infrastructure, with most of them deciding to do so within the framework of national programmes. There are examples of the opposite approach – starting on a smaller, limited scale (for example basic data only) and allowing the common infrastructure to grow alongside technological developments and the public sector's requirements and needs.

Many countries highlight the importance of central funding and stress that the technical solutions should be provided free of charge, initially at least, to facilitate and justify implementation and to reach a critical mass of users. A central funding model for implementation, operation and management is considered to be an important success factor.

There are also examples of charge-based funding in the analysed countries. Generally speaking, the funding models vary considerably and there is usually no general paradigm or principles for the funding of digital infrastructure.

Example from Denmark – funding the basic data programme

In Denmark, the basic data programme was funded by means of general cuts in the appropriations paid by public sector actors. Organisations choosing to connect were then allowed to retain the benefits in the form of savings without affecting their future appropriations. This solution could work as a further incentive to implement the system and connect.

Denmark lacks universal funding principles for the digital infrastructure, and several different types of funding models are in existence depending on the context. The two main approaches are charge-based funding in which each actor pays a charge whenever it uses the services, and appropriation-based funding to operate services or provide data.[97]

Example from Singapore – Central funding models

Singapore stated that there should initially be a central funding model based on appropriations to achieve a critical mass of users. Thereafter, the situation can be reviewed with the option of

[95] *Et solidt it-fundament – Strategi för it-styrning i staten* (A solid IT foundation – Strategy for IT governance in the state) 2017-11-21, page 19

[96] Aas page 20.

[97] *Modeller för fördelning av nyttor och kostnader för digital infrastruktur (*Models for allocating benefits and costs for digital infrastructure) – Agency for Public Management Dnr 2018/40-5

switching to other types of funding, such as charges. The investment cost could otherwise become an obstacle to creating new and efficient solutions.

Example from Norway – funding principles for common public-sector digital functions

The Norwegian government has developed a number of funding principles[98]:

1. The funding models must be simple and predictable, and involve as little administration as possible.

2. Fixed costs for development and management must be covered by appropriation-based funding for the managing authority.

3. The managing authority must be transparent with its costs so it is clear what is used for management and what is used for development.

4. The managing authority must not impose charges to provide access to basic data from registers forming part of the digital infrastructure.

5. For the common public-sector digital functions that are not registers, the managing authority must receive payment from the accessing authorities to cover its costs, i.e. the variable costs incurred when the function is used. The accessing authorities pay a proportional share of the managing authority's costs.

6. As a general rule, payments between authorities must be based on charges.

7. One or more accessing authorities can together request a custom function from the managing authority, in which case they must fund development of the function. This can be done subject to the capacity and other commitments of the managing authority.

1.4.3 Costs, benefits and economic impacts

1.4.3.1 Costs

The costs for implementation in the different countries vary somewhat and have been difficult to tease out – the investments are often linked to a national programme that has a greater impact than basic data and information exchange alone, usually focusing on the entire digital infrastructure within the country. The cost of the technical solution is usually negligible in the wider context, and most of the costs in Finland, say, are instead allocated to implementation (in the form of grants), adaptation and development of key components.

We also cannot ignore the fact that, in most cases, the investments have been cost-intensive initially, primarily due to high implementation and adaptation costs. However, when contrasted with other infrastructure projects (such as roads) the costs seem rather low, so it is a matter of perspective.

[98] Ibid – government source (Norway), What are common components?

Example from Denmark – cost of the basic data programme

Denmark's total cost for its basic data programme (*Grunddataprogram*) is estimated at around DKK 673 million[99]. The programme has been delayed and expanded, so the original timetable has not been kept. Despite the delays, there is still substantial support for the programme, and it is important to emphasise that a large number of milestones and targets have been achieved.[100]

Example from Finland – cost of the KaPa program

At the start of the Finnish KaPa programme, EUR 120 million was allocated[101]. The total final cost in Finland ended up being about EUR 70 million, and the left-over funds have since been used to refine the Suomi.fi services and encourage more use. The programme is considered to be a success, having been completed on time and within budget, and this is attributed to an agile development model combined with motivated and competent staffing in both governance and implementation.[102]

Example from Norway – cost of Altinn 2

Norway's investment in Altinn 2 is estimated at NOK 939 million.[103] The investment includes several different services and components that are not directly attributable to information exchange.

1.4.3.2 Socio-economic impacts and benefits

The main driving force for reforms and initiatives in the analysed countries usually concerned financial incentives in the form of a desire to streamline and reduce costs for the public sector. This is illustrated by the fact that the initiatives and projects are often launched and in some cases driven by the country's ministry of finance or by departments and authorities linked to it.

Calculations from several of the analysed countries show that major positive socio-economic impacts mostly depend on basic data being made available and being free to use, and on efficient information exchange. The benefits are realised primarily in the form of savings in terms of reducing the administrative burden, reducing IT costs, time savings and indirect impacts such as improved quality and secured access.

The analyses also indicate that most of the socio-economic impact (social benefits) accrues in the private sector.

Social benefits are defined as the sum of operational benefits and external benefits[104]

[99] Change in funding: https://en.digst.dk/news/news-archive/2018/march/new-timetable-for-the-basic-data-programme-approved-by-the-finance-committee-of-the-danish-parliament/ – read 2019-06-27

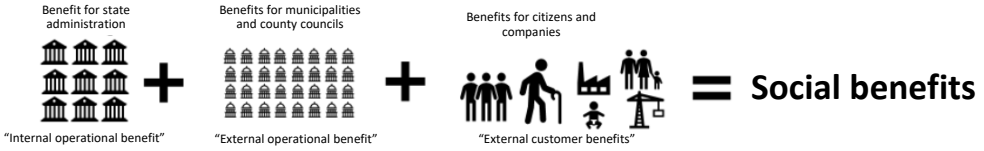
[100] Modified timetable: https://digst.dk/nyheder/nyhedsarkiv/2017/november/grunddataregistre-paa-ejendomsomraadet-udskydes-til-2019/ – read 2019-06-27

[101] Programme for implementation of a national service architecture (KaPA) 2014-2017 Final report

[102] KaPa programme finished under budget: https://vm.fi/en/article/-/asset_publisher/kapa-ohjelman-palvelut-ovat-valmistuneet-aikataulussa-ja-alle-budjetin – read 2019-06-27

[103] Revised cost benefit analysis Norway 2010 E.Fossum & E.Pedersen

[104] Figure from *Modeller för fördelning av nyttor och kostnader för digital infrastruktur* (Models for allocating benefits and costs for digital infrastructure) Dnr 2018/40-5



Example from Norway – cost/benefit calculations

In Norway, a number of cost/benefit calculations have been performed concerning the national digital infrastructure. In 2015 a calculation[105] of socio-economic impacts (cost/benefit analysis) was carried out with different options for common public-sector concepts for information management, by DNV Global on behalf of the Brønnøysund Register Centre. The analysis was based on three different scenarios, a zero option which was based on the current situation and decisions already taken. Option 1, which proposes common public-sector standards and descriptions for information management. Option 2, which proposes common public-sector standards and descriptions, as well as common services and technical infrastructure for information management.

Compared to the zero option, both options help to coordinate information management across the public sector. Option 2 is an extension of the first option – in addition to defining a common public-sector standard, it also makes available and uses the information in common web portals and services. Option 2 helps to show who in the public sector holds what data, and includes directory services describing concepts and information models.

Over an analysis period of 15 years, the efficiency gains and savings indicate a potential for option 1 of approximately NOK 13 billion with a corresponding potential for option 2 of NOK 30 billion. The calculations are based on efficiency improvements from reduced working hours and less/more efficient use of resources as a result of common public-sector information management.

The report states that it is important not only to look at cost savings when examining common public-sector solutions for information management – there are also gains to be had from a reduction in the reporting burden for companies, for example, or the opportunity to create new services. It also raises concerns about some issues that could prevent the benefits from being fully realised, such as coordination problems in the public sector and the fact that the result depends on the option being used by the major actors and the solutions being promoted.

Example from Denmark – cost/benefit calculations

In 2010 the Danish Business Authority (formerly the Danish Enterprise and Construction Authority) conducted a study into the value of the Danish address database, which was made free to use in 2002. Their calculations indicate that the financial benefits attributable to the improved access are DKK 471 million for the period 2005-2009. The costs were estimated to be about EUR 2 million over the same period. For 2010, it was estimated that the impacts would correspond to savings of EUR 14 million, of which 30% was attributable to the public sector and the remaining 70% attributable to benefits in the private sector.[106]

The estimates were based on a method that calculates the economic value of free and universal access to the addresses according to what was paid for the corresponding data before. In addition, a number of other benefits and economic impacts are listed that have not been estimated in

[105] Profit potential in a common concept for information management in the public sector. DNV GL 2015-02-27
[106] Danish Enterprise and Construction Authority, The value of Danish address data 2010.

monetary terms. These are benefits that are realised further down the value chain and consist of a number of indirect impacts such as reduced use of internal databases, greater confidence that emergency services have access to the same, accurate data, a simpler process to correct inaccuracies as only one source needs to be changed, reduced costs to update databases and higher quality of data in a common standardised format.

In 2012 it was estimated that from 2020, with the basic data strategy fully implemented, the economic impacts on society would amount to DKK 800 million annually, of which DKK 500 million would accrue to the private sector.[107]

Example from Estonia – economic impacts

The biggest economic impact of X-tee is described as time and money savings for citizens, the public sector and businesses. For example, it takes only about 18 minutes to start a company in Estonia[108], 98% of all companies are started online, 95% of all tax returns are submitted online, taking an average of about 3 minutes to complete[109]. The impact of Estonian digital signatures has also been estimated, indicating time savings of 5 days per year per person[110].

There are no official cost/benefit calculations or estimates by the Estonian state of the socio-economic benefits of the impacts of X-Road. In 2016, the World Bank published a report[111] entitled "Digital Dividends" and in its background material there is a study[112] attempting to quantify some of the economic impacts of X-Road.

The study estimated the time savings for citizens and public sector interactions. Interactions that would ordinarily have taken place in person but could now be done digitally using X-tee. The time saving was conservatively estimated at 15 minutes per interaction, which corresponds to an overall saving of 2.8 million hours up to 2014. The productivity gain of the X-tee platform is equivalent to 3,225 people working 24/7 for an entire year. These calculations are by their nature difficult to judge in terms of reliability because they are estimates. The economic benefits are not directly attributable to the platform but instead depend on the services that are enabled.

Estonia carries out similar calculations on an ongoing basis and estimates that 5% of requests made via X-tee are initiated by a natural person. And assuming that just these requests save 15 minutes compared to the time needed to process a letter, time savings equivalent to 1,264 working years were saved during 2017 alone[113].

Example from Belgium – administrative savings

Belgium has an authority (Dienst Administratieve Vereenvoudiging, DAV) which is responsible for measuring administrative simplification and monitoring the use of e-services. DAV follows up on e-government initiatives by measuring economic outcomes in terms of reduced administrative burden for a number of e-services. It measures the reduction in administrative burden from the

[107] Good basic data for everyone – a driver for growth and efficiency
[108] e-Estonia: https://estonia.ee/enter/ – read 2019-06-27
[109] e-Estonia e-tax: https://e-estonia.com/solutions/business-and-finance/e-tax – read 2019-06-27
[110] e-Estonia e-identity: https://e-estonia.com/solutions/e-identity/ – read 2019-06-27
[111] World Development Report 2016: Digital Dividends
[112] Estonian e-Governance Ecosystem: Foundation, Applications, Outcomes 2016 – Kristjan Vassil University of Tartu
[113] X-tee factsheet: https://www.x-tee.ee/factsheets/EE/#eng – read 2019-06-27

perspective of citizens, businesses and authorities. Examples of administrative burden relate to time savings or reductions in charges and transfers.

For 2017[114], DAV calculates that the 16 e-services (Tax-on-web, MyEnterprise, eBirth, etc.) examined accounted for savings of EUR 7,017,477. Most of the reduced administrative burden is thought to represent benefits for the citizens of the country (59%).

Cumulatively for these services since they started, the savings have been estimated at EUR 100,847,174 in reduced administrative burden. The services have been running for different periods, so the starting point for the measurements was 2008.

The economic impact is therefore not directly attributable to their information exchange solution (FSB), but instead to the services that are enabled through access to data from various authentic sources.

1.4.4 Legal prerequisites

1.4.4.1 Legal framework for basic data

In most countries there is no comprehensive legal framework for the management of basic data, meaning that the various data sources are subject to register legislation. Some countries have chosen to identify a number of sources as basic data in legislation, while others use contracts and agreements to regulate use, supported by clear political governance.

The countries differ in their approach to defining basic data – some have not legislated or defined basic data, whereas others have specific legislation. However, many countries use the concept or versions of it, even if it is not defined in the legislation. There, it is often used in a broader sense with the aim of identifying authentic or unique sources of data that are of great importance to society.

Example from Denmark – agreements instead of legislation

The basic data programme (*Grunddataprogrammet*) has been running for several years now, and aims to improve the quality of basic data and make it accessible to authorities, private organisations and citizens. The programme relates to certain categories of data (e.g. personal data (CPR), business data and geodata), which is available in various registers. The programme is a political initiative and is based on an agreement[115] between the government, Local Government Denmark (KL) and Danish Regions. The agreement sets out the purpose, the different categories of data covered, and the governance organisation. It also contains a section establishing a common public-sector infrastructure component (Datafordeler) for the joint distribution of basic data. One of the related sub-agreements[116] shows that all basic data is distributed via the data distributor.

[114] 2017 Les Autorites, Catalyseurs de La Simplification, Evaluation des charges administratives federales.

[115] *Aftale om gode grunddata til alle* (Agreement on good basic data for all): https://digst.dk/media/12881/grunddata-aftaletekst.pdf

[116] Sub-agreement 7: *Fælles distributionsløsning til grunddata* (Common distribution solution for basic data) (Datafordeler) 2012-05-10

The concept of basic data is not used in Danish legislation and is therefore not defined there. The term is nevertheless used in the agreements above. On the other hand, the registers containing the data in question are governed by law, such as the CPR[117] and the CVR[118].

Example from Belgium – authoritative data

In Belgium, legislation lays down what is authoritative data and authoritative sources for basic data.[119] The authoritative data held by the authoritative source is by definition unique, and this is the data that organisations must obtain[120] when they need to use data about an individual, as it is not permitted to ask for data that already exists.

Example from Norway – basic data

The concept of basic data (*grunndata*) does not exist in Norwegian laws or regulations. The concept is nevertheless widely used by authorities when they refer to certain categories of data. The concept also occurs in legal commentaries. However, it seems that there is no single definition. The type of data known as basic data is the data contained in various public registers, such as the Entity Registry which contains information about legal entities (company name, address, etc.). Another example is *Det sentrale folkeregisteret*, which corresponds to the Swedish civil registry. The legislation governing these registers also provides for the disclosure of data from them.

1.4.4.2 One piece of information, one time

Some of the analysed countries have implemented legislation that applies, and in some cases directly refers to, the "Once-Only" principles. [121]

Example from Norway – one task, one time

In Norway it is a requirement that the government's public services use digital as their first choice and that information must only need to be obtained once. Data can be obtained from another organisation if there is a legal basis for doing so (see paragraph 7 of the law on freedom of information (*offentleglova)*[122]). When the government's public organisations develop new services or update existing services, they must ensure that machine readable data from the services can be shared and used by others.

Example from Estonia – once-only principles in legislation

Estonian legislation contains references to the once-only principles in article 43 of the Public Information Act[123] which prohibits the establishment of separate databases to collect the same data. The effect of the law is to encourage public actors to make use of data that has already been collected instead of creating copies and duplicates.

[117] *Lov om Det Centrale Personregister* (Law on the CPR) (LBK nr 646 of 02/06/2017)
[118] *Lov om Det Centrale Virksomhedsregister* (Law on the CVR) (LBK nr 653 of 15/06/2006)
[119] Law establishing and organising a federal services integrator, 15 August 2012, Art. 2
[120] Only-Once Act, 5 May 2014, Art. 2.
[121] EU-wide digital Once-Only principle for citizens and businesses – policy options and their impact, EU 2014
[122] Act relating to public access to documents in the public administration (*offentleglova*)
[123] Estonian Public Information Act: https://www.riigiteataja.ee/en/eli/514112013001/consolide – read 2019-06-27

Example from the Netherlands – mandatory use of basic registers

The Netherlands has formulated requirements for use of their basic registers (basic data) that include a compulsion to use this data for public services of different kinds. The Netherlands has separate legislation for 12 of its basic registers.

1.4.4.3 Legal framework for information exchange

Most of the analysed countries lack an overall or general legal framework for information exchange. Nevertheless, there are several examples of legislation governing the management of common public-sector services which form the basis of digitalisation.

Example from Finland – KaPa legislation

Finland is one country that stands apart from the others. It has the KaPa law (30.12.2013/1226) on the organisation of the state's common information and communication technology services, which provides that most state authorities are essentially required to use common information and communication services. According to paragraph 4 of the law, the Ministry of Finance is tasked with organising the services, guaranteeing their quality and providing interoperability with the overall IT architecture. An actor which has particular reasons why it must use other services must obtain permission to do so. The final decision lies with the Finnish Government[124].

The KaPa law[125] was passed specifically to regulate electronic information exchange. The law applies to public administration and aims to improve access to and the quality of public services, to improve information security, interoperability and governance of the services, and to enhance efficiency and productivity in the activities of public administration. The law gives the Ministry of Finance responsibility for general governance of the support services. It contains definitions of support services and also states which support services, e.g. a service catalogue and a service view, must be provided, and which authorities are service providers for which support services. The legislation determines certain responsibilities at general level, such as the processing of personal data in the production of services, but specific data and permissions are provided for separately per authority.[126] No one technical solution is specified in laws or regulations – Finland uses multiple platforms and X-Road is one of them.

In the KaPa law, the Finnish legislature lays down how the support services are to be used. The legislation requires most organisations in public administration, including municipal organisations that perform statutory functions, to use the support services. Other organisations in public administration that perform statutory functions are entitled to use all support services. Private actors are entitled to use some of the support services, possibly depending on whether the actor has an agreement with an authority to perform a public function.

Example from Estonia – legal regulations for information exchange

In Estonia, too, there are legal regulations governing information exchange. The relevant legislation is the Public Information Act[127] which lays down the conditions, procedures and methods for accessing and re-using public information. The law provides for data exchange

[124] The Finnish Government is called the *Statsrådet.*

[125] *Lagen (29.6.2016/571) om förvaltningens gemensamma stödtjänster för e-tjänster* (Law on the common public-sector support services for e-services).

[126] Page 4 of Government Bill RP 59/2016 rd.

[127] Public Information Act (RT I 2000, 92, 597).

between databases belonging to the state information system. Estonia also has a regulation[128] concerning information systems for the information exchange layer, which lays down requirements for the data exchange layer, its use and the management of information systems.

Example from Norway – regulations on use in the public sector

In Norway, there is a requirement to use certain common solutions such as ID-porten which enables digital login and authentication. Public organisations must in principle use the Altinn infrastructure and service platform for the production of relevant services. Some provisions on the use of standards are contained in the Regulation on IT standards in public administration.[129] They are mainly mandatory standards for text documents on public web sites, multimedia content on these web sites, and character sets for information exchange between public organisation and with individuals and businesses.

Example from Denmark – mandatory connection

Denmark does not have a comprehensive or general legal framework for information exchange between authorities. There are nevertheless several examples of legislation governing certain common (cross-sectoral) services that underpin digitalisation. The services can be thought of as fundamental infrastructure components. In addition, there are a number of examples of laws introducing mandatory connection for citizens or the mandatory use of certain services.

Examples of fundamental components that are governed by law include Digital Post, a service that enables communication between the public sector (government authorities, municipalities, etc.) and citizens and businesses.[130] The service is comparable to Mina meddelande (My messages) in Sweden. It is mandatory for citizens to connect to the service[131] in order to receive digital mail. However, the law does not currently mandate public actors such as authorities to send the mail in digital form.

Another example of a fundamental component governed by law is NemID[132], which is the eID and signature solution provided by the government and is the official log-in service for public services.[133] The service enables citizens and employees of legal entities to identify themselves and create digital signatures in services offered by the public sector as well as by private companies. Some matters including the legal status of users are addressed in the law concerning the issuing of NemID. Many others, however, are dealt with in the agreement between Nets DanID, the provider, and the user. For example, the agreement states that information is collected from the Danish Central Person Register (CPR).[134] In some cases, there is a legal requirement to use the employee function in NemID, for example when statistics must be reported to Statistics Denmark.

What these services have in common is that they are provided centrally and that public actors (and private actors) can connect and use them.

[128] Information Systems Data Exchange Layer (27.09.2016, 4)

[129] Regulation on IT standards in the public sector (*forskrift om IT-standarder i offentlig forvaltning*) 2013-03-15-285

[130] Law on Digital Post (*Lov om Offentlig Digital Post*).

[131] Paragraph 3 of the Law on Digital Post (*Lov om Offentlig Digital Post*).

[132] Law on the issuing of NemID with public digital signature to physical persons and employees of legal entities (*lov om udstedelse af NemID med offentlig digital signatur til fysiske personer og til medarbejdere i juridiske enheder*).

[133] eID in Denmark: https://en.digst.dk/digitisation/eid/ – read 2019-06-27

[134] Rules for the use of NemID: https://digst.dk/it-loesninger/nemid/lovgivning/regler-for-brug-af-nemid/ – read 2019-06-27

1.4.5 Security, secrecy and privacy aspects

1.4.5.1 Security functions and building blocks

Regarding security aspects for information exchange solutions, there are a number of different requirements and needs.

Public administration needs to ensure that the infrastructure and building blocks are designed to take security into account. The services must not be vulnerable to attacks that may interrupt and disrupt operation and diminish the confidentiality or privacy of information.

The security group identified a number of key components/building blocks that are crucial to secure and efficient information exchange, but note that this is not a full analysis and more work is needed.

Two of the prioritised building blocks are identity and authentication, meaning that the producer and the consumer both need to be verified and identified. In the analysed countries, this does not form part of the technical solution for information exchange, but is usually a stand-alone central component which is considered by many to be a fundamental prerequisite.

Most of the analysed countries have national identification and signature solutions provided by the state. They include Norway (ID-porten), Singapore (Singpass), Estonia (Digi-ID) and Denmark (NemID). Many of the analysed countries also have eIDs that are approved for the highest levels of security. They often have an authentication solution that also encompasses legal entities and roles.

In principle, all solutions in the analysed countries have traceability functions in the form of message logging and message signing. The scope of logging varies depending on different circumstances in the various countries. Some solutions log the entire message (including the payload) while others only log the metadata about the transaction. Often this is due to the local legal situation and legal requirements rather than technical constraints.

Example from X-Road – security aspects

A number of design choices were made in the X-Road architecture in order to enhance security. X-Road is decentralised and the exchange takes place directly between producers and consumers. There are no intermediaries and once a secure connection is established, it is up to the actors and the network to determine availability.

X-Road does not change the ownership of data, and the data owner (producer) controls who is able to access its services and data.

All messages sent through X-Road are logged and can be used as digital evidence.

The security server, which is a core component, downloads and retains a cache copy of the global configuration and validity of certificates, allowing the solution to keep working (for a limited period) even if the core components cannot be accessed.

X-Road's distributed architecture means that the platform is scalable and able to withstand cyber attacks. It creates a trust network where messages are always exchanged between two trusted parties whose identity is verified by certificates. Although these factors offer major advantages, there is sometimes a weakness because new parties wishing to connect and become certified need first to undergo registration and verification.[135]

Example from Denmark – secrecy assessments

All secrecy assessments are carried out by the individual authorities, in other words not by the data distributor (*Datafordeler*). Secret information must not be made available via the data distributor. If secret information needs to be provided digitally, for example to another authority, the data distributor forwards the request to the authority holding the information and instructs it to use a different method not involving the data distributor.

The data distributor has three different permission levels for information consumers – Open, Known Users, and Individual Identification. Open information is completely open and no information is needed about the user. Examples of data that can be made available as Open include addresses. Known Users must identify themselves. The purpose is to allow the data distributor and the basic data authorities to find out more about the users so they can make improvements, for example to make the data more usable. Individual Identification is necessary where there are limitations of any kind on how the data can be disclosed, for example if the information is classified as secret. In this case, the data is not routed through the data distributor but the information exchange takes place directly between the source of the data and the user.

Example from eDelivery – design choices for security

Security-related design choices were also made in eDelivery, guaranteeing that data and documents cannot be improperly modified, that data is encrypted during transport and that the origin and destination of data and documents are genuine.

1.4.5.2 General Data Protection Regulation

The General Data Protection Regulation (GDPR) took effect on 25 May 2018 and contains the general provisions relating to the processing of personal data within the EU. An EU regulation is binding and directly applicable in each member state by individuals, authorities and organisations. Because the GDPR is a regulation, as opposed to a directive, member states have limited scope for their own national data protection provisions. Authorities are classed as controllers in all processing of personal data that takes place as part of the authority's activities. When an authority processes personal data, it must comply with the GDPR and the supplementary data protection law, as well as its own special register statutes.

The requirements of the GDPR are linked to an authority's security responsibility on several levels. It is important for information to be classified to determine the level of protection required and whether the GDPR applies to it. Built-in security (or privacy) must be provided, which affects the entire life cycle of a system from the feasibility study and specification phase, through design and development, to implementation and

[135] X-Road security server: https://www.niis.org/blog/2018/10/15/standalone-security-server – read 2019-06-27

decommissioning. This applies to purchasers and customers who are responsible for the processing of personal data as well as the supplier of the products and services used. Concepts such as responsibility for personal data, purpose limitation, information ownership, legal basis, rights of data subjects, task minimisation, permission administration, archiving and traceability must be handled within the regulatory framework of the GDPR.

It is important not to underestimate the need to guarantee the protection of privacy in government assignments relating to secure and efficient access to basic data and secure and efficient information exchange in the public sector. If an authority does not feel confident to share information in light of its responsibility for personal data, the consequence may be that a national consensus is not reached. This prevents the national system becoming a robust whole, in turn jeopardising the EU's objective of free movement of data and cross-border information exchange.

From a legal perspective, the conclusion is that the above should be done within existing law, but the challenge is to identify processes, methods and security measures that cater to all needs at all stages. Another dilemma is that certain disclosed information can be considered lawful from a legal perspective, but from the point of view of security it may not be appropriate for the information to be included.

The comparative international observations make it clear that Swedish national and cross-border information exchange must be secure, which means that as a first step, Sweden needs to create a secure national environment that is also efficient, so that in the next step, it can meet the requirements allowing the information to be transferred across borders.

2 Appendix 2 – Details of prioritised building blocks

The following is a more detailed description of the prioritised building blocks mentioned briefly in chapter 4.

2.1.1 Mina ombud (My representatives)

2.1.1.1 Description of the building block

There is a need for a national, common infrastructure for the management of representatives in digital services. Representatives are sometimes also called proxies or agents. The need applies to natural persons and legal entities.

Examples of applications include permission management in order to:

- Log onto Mina sidor företag (My business pages) (and access company information)
- Act on behalf of a company.
- Act on behalf of a natural person.
- Represent other legal entities such as municipalities and authorities.

2.1.1.2 Challenges

Sweden does not have a national solution for handling representatives in digital services.

- Representatives in e-services sometimes require a written power of attorney in a bureaucratic and unwieldy process.
- There is a need for representation of legal entities, natural persons and other types of organisations in digital services.
- There is a need to be able to view which permissions/powers of attorney a company has granted as well as what agents a natural person has appointed.

2.1.1.3 Motivation view

The building block is fundamental and is used to control who can represent who in digital services (authorisation). It is essential for current and future digitalisation of municipalities, authorities and private actors. The building block can also make life easier for employers, so that they can be supported by employees or external representatives.

2.1.1.4 Organisation

There is a need to represent natural persons and legal entities and other types of organisations. There is also a need for the service to be widespread/national. It is therefore considered best if it is introduced jointly by the Swedish Companies Registration Office, the Swedish Tax Agency and DIGG. It is probably appropriate to start with the capability of representing companies and then scaling up in stages.

2.1.1.5 Law

The Swedish Companies Registration Office has undertaken an initial legal study for a conceptual solution. It states that no authority is entitled to store powers of attorney on a third party's behalf, and the technical concept that has been developed takes this into account, see technology below.

In addition, there is likely to be a need for two types of representative. One type receives information and another type acts on someone else's behalf.

There needs to be an in-depth legal investigation.

2.1.1.6 Technology

The Swedish Companies Registration Office has developed a conceptual architecture based on a composite basic service that carries information about representatives from different sources. The concept can also be used to view all the representatives assigned to a person or granted by a company in a central location. It also allows representatives to be specified in an API as a step in a process or e-service. The concept also includes support to simplify the way consumers use the authority to sign for a company.

2.1.1.7 Dependencies

The building block has dependencies with several other building blocks, e.g. Identity, Authorisation and Trust Rules.

2.1.2 API Management

2.1.2.1 Description of the building block

API Management provides functionality to manage APIs throughout their entire life cycle from design, development and testing to publishing, operation, administration and decommissioning. In the digital ecosystem used for external information exchange, APIs provide well-defined interfaces that must often meet high standards in terms of quality (non-functional requirements). These interfaces can be completely open or open and secure. The building block is not concerned with what information is exchanged, but with the functionality needed to exchange information from the technical point of view. A number of public administrations have already embarked upon the journey of implementing API management. Responsibility will largely be distributed, although certain parts will be shared. The authorities consider that more work needs to be done to analyse which parts it would be better to manage and organise jointly.

There are strategic decisions within API Management regarding which parts can or should be realised as common components and which parts can or should be realised as actor-specific. The building block must handle and support:

- Developer portal/service directory
- API gateway
- Life cycle management

- Design and development
- API security
- Publishing
- Execution
- Analysis and monitoring

2.1.2.2 In-depth description of the developer portal/service directory part

The developer portal is a standardised way of describing and documenting interfaces and contracts that are made available publicly for consumption within the digital ecosystem. For example, descriptions include usage, interfaces, and underlying data models.

There are other types of descriptions too such as sample code for calls, connection rules, constraints, costs, availability, expected performance, and prerequisites and support for developers to conduct tests using the interfaces.

Challenges

How do potential consumers locate the interfaces of the public service, how are the interfaces documented, what support is available to develop solutions that consume these services as well as the current regulatory framework for connection.

Differences in processes and descriptions for connecting and consuming a public interface within the digital ecosystem are among the challenges that affect the speed, efficiency and quality of development of new solutions.

Contractual models for the connection and use of APIs are another factor limiting the options for secure and efficient information exchange.

Motivation view

The developer portal is a very important element in building a common digital ecosystem. It is the public face of the producers in the digital ecosystem. A common public-sector method of describing and publishing interfaces and for the consumer to locate these descriptions is one of the first steps in the process of accelerating the exchange of information.

Organisation

The need is wide-ranging and involves going further in creating a national structure for information exchange – an ecosystem. This includes analysing which parts of the process are common and then setting up a management organisation focused on developing and managing common standards with related technical assistance.

Semantics

Common standards for describing information models of the public services, and their technical descriptions and operational rules for connection and use.

Technology

The technical assistance required to establish the service directory/developer portal needs to be analysed in future assignments.

2.1.3 Identity

It is vitally important that organisations, individuals and entities have an unique global identity in information exchange. In particular, this is to allow operations to be traced across multiple systems and, in some cases, over several stages. However, there are quite distinct needs in terms of how these identities are managed across different entities:

- *Natural persons*: for communication between natural persons and other entities, the personal identity number (personnumret)/co-ordination number (samordningsnummer) is the obvious form of identity in Sweden today. Not everyone approves of the spread of personal identity numbers, but it has become a de facto standard used by most eID providers today.
- *Organisations*: organisations also have an obvious form of identity with the organisation number (organisationsnummer) in Sweden. For people within an organisation, however, things get more complicated. As a rule, they have unique identities but can be very different in appearance and thus be difficult to manage. In addition, they generally prefer not to reveal these identities outside their own organisation for security reasons. For communication between organisations, federations should therefore be created in which the internal identity is converted into a global identity using a format that is standardised within the federation. This global identity is then communicated within the federation using the relevant identity token.
- *Devices*: this category consists of physical devices. They can usually be identified with MAC addresses for example. More sophisticated mechanisms can be used, but hardware support is normally required (e.g. TPM) to achieve a significant increase in security.

2.1.3.1 Challenges

Asylum seekers in Sweden have no personal identity number or co-ordination number. This in turn means that eIDs cannot be issued to this group, resulting in digital exclusion. With no personal identity number or co-ordination number, this category is difficult for schools, health/social care services, employment services, etc. to process. This category is an example where identification is not currently working properly.

2.1.3.2 Motivation view

A unique and consistent identity is the basis on which an entity can use digital services that do not allow anonymous access because of the need to protect the information contained.

2.1.3.3 Technology

The creation of unique consistent identities is not fundamentally a technology issue – instead it has the characteristics of a standardisation and process problem.

2.1.3.4 Organisation

At present, DIGG is responsible for Swedish eID, but there is no explicit responsibility for broader identity initiatives encompassing hardware as well as individuals and organisations.

There is therefore a need for standardisation and a regulatory framework specifying how these identities are created and maintained over time, creating traceability and legal responsibility if necessary in the different communication patterns.

2.1.4 Authorisation

2.1.4.1 Description of the building block

Authorisation is necessary in many cases in order to access various information resources. This can be done in several different ways depending on communication patterns, resource type and protection needs.

Communication patterns of different kinds are described below with their potential impact on the authorisation mechanisms:

- *Private person to organisation*: individuals who access an e-service generally do so in order to manage information related to themselves or a person/organisation they are connected to in some way. In these cases, it is usually the resource manager who defines how access is provided, based on a number of rules that are established either from a business perspective or in other ways such as by law. However this is done, it is up to the resource manager to authorise the user, either granting or denying access to the resource, in other words the administration of authorisation is centralised in the resource manager (for example a service provider).
- *Organisation to organisation*: for this communication pattern, a federation is expected to be the most common solution. This allows the authentication taking place via the federation to be supplemented with authorisation (the token used to convey the identity is given attributes that are agreed in advance). In this way, access rights can be administered by the organisation that uses the service, meaning that the administration of authorisation can be distributed. This makes administration more scalable. This presupposes that there is trust between the organisations.
- *Representatives*: the needs analysis we carried out indicates a need to handle representatives. This can be implemented in both cases above and means in brief that one entity can act for another entity.

2.1.4.2 Challenges

An increasing number of frauds committed by means of forged identity documents, in which a front organisation is used to act as an entity, which are then resold and misused in various ways.

Organisations will become part of large federations. A large number of participants in federations also increases the risks associated with them as the number of attack vectors increases.

2.1.4.3 Motivation view

Without authorisation, only information not requiring protection can be shared. This would drastically reduce the social benefits of the infrastructure.

2.1.4.4 Technology

The technology to implement the scenarios described above is already well established. The federation solutions we see should be based on the now well established SAML 2.0 standard. The choice of technology for centralised authorisation is largely up to the affected organisation. The distributed model is more complex and requires collaboration, standards and common rules before it can be applied effectively on a larger scale.

2.1.5 Trust rules

2.1.5.1 Description of the building block

There is no technical solution to achieve trust – instead, a combination of technology, processes/working methods and culture is required that is common and accepted by the actors involved.

It is often advisable to create several levels of trust for situations in which a specific information exchange does not entail the kind of risk that would justify a certain resource allocation.

In this report, we use the term "trust rules" for a set of technical measures, processes and common cultural values.

Trust is something that affects the whole system, and technology, processes/working methods and culture can be made tangible in four parts: technical solutions, collaboration types, processes and models. This is a large and wide-ranging area, so only examples of different types of solutions are given below:

- *Technical solutions*: Different authentication strengths (e.g. passwords versus smart cards) mean that different levels of trust are created concerning the identity of a particular entity, and in some cases it may be justified to have no trust at all.
- *Collaborative approach*: A contractual agreement between two parties creates more trust than spontaneous information access on a single occasion for example.
- *Processes*: Applying a process such as ISO27001[136] should result in greater trust than using a non-established process (or no process at all). Processes also assume that there are mechanisms verifying that the actors involved are actually applying the processes.

[136] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

- Models: The ability to communicate different levels in technical solutions, collaborative methods, processes and working methods presupposes that there are common models to describe them in a clear and widely-accepted way. One fundamental model is an information classification model that describes the protection needs of various information sets.

2.1.5.2 Challenges

Trust rules can be wide-ranging and must be accepted by the parties involved. They also need to be developed and managed over time as needs change. Here, the structure of the ecosystem can contribute to a solution.

2.1.5.3 Motivation view

It is a prerequisite for establishing secure and efficient information exchange that all the actors trust the other actors and the infrastructure enough that they can accept the risk associated with information exchange.

2.1.5.4 Organisation

In all the building block descriptions above, it is obvious that collaboration and coordination are needed. The basic structure of this coordination is contained in the trust rules which in turn affect all the other building blocks. Coordination and governance will also need to be supplemented within the other building blocks.

The Swedish Civil Contingencies Agency (MSB) already has coordinating responsibility for information security and publishes comprehensive documentation including regulations and guidance documents. MSB is regarded as the obvious actor to manage the trust rules that establish the framework for coordination elsewhere. DIGG is the obvious actor to coordinate the more technologically-oriented parts of the infrastructure (e.g. standards for identities and attributes for authorisation).

The work effort required from MSB and DIGG should not be underestimated, and so resources are expected to have to increase to allow them to manage the process satisfactorily.