Design of a Business-to-Government Information Sharing Architecture Using Business Rules

Sélinde van Engelenburg(✉), Marijn Janssen, and Bram Klievink

Faculty of Technology, Policy and Management,
Delft University of Technology, Delft, The Netherlands
{S.H.vanEngelenburg,M.F.W.H.A.Janssen,
A.J.Klievink}@tudelft.nl

Abstract. Information sharing between businesses and government agencies is of vital importance, yet business are often reluctant to share information, e.g. as it might be misused. Taking this into account is however often overlooked in the design of software architectures. In this research we apply a design science approach to develop an software architecture that is acceptable by businesses. From a case study we derive the requirements an architecture should meet in order to contribute to increasing willingness to share information. In this paper the architecture is developed and evaluated according to the requirements. We recommend the use of different types of business rules that provide businesses with control over their data, in combination with encryption and decryption of data to provide access to parts of the data within an organization.

Keywords: Software-architecture · Information sharing · Business rules · Encryption · Decryption · Supply chain · Customs

1 Introduction

Easy and seamless information sharing can have advantages for both businesses and government agencies [1–3]. There are however some factors, such as the competitive advantage of having information that other parties do not have, that might make businesses unwilling to share their information [2]. Some research has been conducted on building trust between stakeholders and on governance and identifying gains of using architectures facilitating information sharing, in order to support the adoption of such architectures [3–5]. In this paper, the main premise is that in order for businesses to be willing to share information, businesses and government agencies first will want to make sure that the sharing and use of information does not harm their interests and that it complies with legislation [2, 6]. An architecture could very well help to ensure businesses of this, but currently, there is no knowledge about what such an architecture should look like.

In this research, we take a design science approach to develop a software architecture facilitating information sharing between businesses and government agencies. This architecture should have properties such that businesses are more willing to share information when they use the architecture, than when they share information directly.

D. Bianculli et al. (Eds.): SEFM 2015 Workshops, LNCS 9509, pp. 124–138, 2015.
DOI: 10.1007/978-3-662-49224-6_11

Usually the focus of research is on finding explanations or predictions for e.g. human or organizational behaviour. However, in design science ways of expanding the boundaries of human and organizational capabilities are looked for by creating new and innovative artefacts [7]. Central is the development and evaluation of IT-artefacts with the intention to solve organizational problems [7]. The evaluation of IT-artefacts provides feedback information that is used to improve the quality of the product [7]. The IT-artefact developed in this research is a software architecture. The organizational problem we intend to solve is that of the unwillingness of businesses to share information in cases when it could be advantageous for the them or for the government agencies. The organizational problem was studied based on literature and this resulted in requirements for the architecture. The architecture was then developed and evaluated based on these requirements. For the kernel theories of our research, we want to refer to the related research in Sect. 3.

The research in this paper is related to research from many different domains, e.g., knowledge management and research on confidentiality and trust. Some of the innovative nature of this research results from not limiting its scope to a single domain or point of view. Concerning the organizational problem, the scope is limited to the case of information sharing between companies in an international supply chain and customs. This case is appropriate for our research due to its complexity and the involvement of various types of actors, amongst others. For the architecture, the scope is limited to the flow of data and its structure. The contents and form of data and the components are outside of the scope of this paper. These would be highly complex and therefore it is important to first determine whether the structure of the architecture will result in meeting the requirements. The evaluation of the architecture is restricted to the requirements we determined. Of course there may be other requirements that are of importance as well, but they are subject to further research.

In Sect. 2 of this paper, we sketch the case of information sharing between businesses in a supply chain and customs. In addition, the requirements will be elicited from the point of view of both businesses and government agencies. In the following section, we will start by discussing related research. Subsequently, we present the aforementioned software-architecture. In Sect. 5 we make the connection between the requirements and the architecture and we evaluate the architecture.

2 Requirements to Share Information

2.1 Companies in a Supply Chain and Customs

A supply chain can be described as complex network, which consists of many different stakeholders, including shippers, deep-sea carriers, port operators, and customs organizations [8]. Mentzer et al. [9] argue that supply chains can be defined in various ways. According to Tsay et al. [10] modern usage of the term supply chain is consistent with the following: "*a supply chain is two or more parties linked by a flow of goods, information and funds*" [10]. In concurrence with this description, with companies in a supply chain, we refer to the companies that are linked by a flow of goods, information and funds. However, our main focus will be on the companies that have a role in transporting containerized goods, such as shippers, carriers and freight forwarders. These companies are especially interesting for our case, since they deal more directly with customs and the use of containers increases the need for information sharing. We will elaborate on this below. The government agency in this case is customs. The role of customs is that of a gate-keeper, excises-, duties- and tax-collector and they are responsible for monitoring the flow of goods and interfere with it if there are safety, security and other public policy reasons to do so [6].

We selected this case because of its complexity, amongst others, which is due to the inclusion of various types of actors, both from government and business. These parties have different roles and interests. Adding to the complexity is the international character, due to which visibility on the whole chain is limited and various legislations may play a role.

The limited visibility presents a particular problem, as in containerized transport it is not feasible to open each container to look what is inside [11]. This poses a problem for customs who try to monitor the flow of goods and try to determine whether companies comply with regulation [12]. To companies it is often also very important to know what is in containers. Just like customs, companies want to reduce security and safety risks. For instance carriers want to know the weight of goods in containers so that they can make a stowage plan that ensures the stability of the ship. Better data may also help actors in optimizing supply chains [13].

Good quality information on what is inside containers is therefore very important to the companies in the supply chain as well as to customs. The information that customs and companies need often is available in other places in the supply chain. For instance the manufacturer of the goods that are transported has a lot of details on them, such as their weight. The shipper who packed the box has information on the contents of containers [12]. However, much of the information that companies have and that could benefit customs is not provided to customs [13]. Companies often only have access to information that is altered, inaccurate and vague as well [4, 12, 14].

Governments seek to reduce the administrative burden to attract economic activity to their country. Consequently, the sharing of additional information is often voluntary, which requires that businesses are willing to do so. This is of course very important for our research, since it focusses on the willingness to share information. As this complexity and these tensions have been studied before, there is material available for use in this study.

2.2 Requirements

A way to provide both companies in a supply chain and customs with high quality information, is by making it possible and easier for them to share information that already is available. Research by Fawcett et al. [2] suggests that willingness is key to information sharing in supply chains, but is often overlooked and misunderstood. An important factor influencing the willingness to share information is the need to keep information confidential [15]. For competitive (e.g. fear of being bypassed in the chain) or security (e.g. confidentiality on high value goods) reasons, companies may be hesitant to share information with others [2, 3].

There may also be a challenge in the willingness to receive additional information. For example, according to international rules, the description of goods carriers receive from the shipper influences their liability in case of damage or loss. If a shipper does not provide the carrier with information on the value of goods and a full description, then the liability of the carriers is limited to a certain amount per package. This has as a result that carriers may not even want to have this information. [12] Therefore they cannot provide this information to customs or other companies in the supply chain that they are in direct contact with, who might benefit from this information.

The last factor influencing the willingness to share information is the confidence that the sharing of information or its use is in compliance with legislation. The legal status of information gathering and sharing is often unclear, since different legal considerations may play a role [6]. This is a barrier for companies to share information with customs. Clarity is not improved by the fact that with whom data can be shared legally, depends on the country in which the goods are moving in [16] and that different sources of law, such as national and European law, might be applicable at the same time. Moreover, legislation may change frequently [17]. Uncertainty about the legal status of information, as well as the legality of the methods for obtaining it, may lead for instance carriers to shielding their data from other parties [6].

From analysing the literature on information sharing between companies in a supply chain and customs discussed above, we can abstract three requirements that influence the willingness to share information, namely:

- Keeping information confidential when needed.
- Ensuring there is no obstruction for information sharing from the possible increase of liability when businesses receive information.
- Ensuring the sharing of information and its use is in compliance with legislation.

3 Related Background

There exists a vast amount of research related to the research in this paper. This makes it impossible to discuss the related research from all different domains in its entirety. We do want to discuss some different kinds of architectures that are related to the architecture in this paper. For a more comprehensive overview of related research we refer to the work of Sahin and Robinson [18] and Yang and Maxwell [19].

Bharosa et al. [1] present two different software architectures for information sharing. The first is called Standard Business Reporting in which a standardized data representation format and semantics are used by businesses to file official reports. It incorporates a government gateway that is used to move messages from businesses to the appropriate government agency and return a receipt. The other architecture they discuss is a Continuous Control Monitoring architecture. This architecture incorporates an intermediary platform that the business uses to push key performance data to, which are then monitored by the government agencies. While in both cases in this study monitoring compliance by government agencies and limiting administrative burden do play a role, the architectures themselves are very different, which has likely to do with the fact that they are applied in different domains, namely mainly in the financial domain and in a meat supply chain.

In the domain of our case of information sharing a notable concept that has been proposed is that of a data pipeline. The purpose of the data pipeline is to capture data at the source and to improve the coordination of border management and reduce administrative burden for businesses [12, 13, 20]. This architecture differs in structure and flow of data from the architectures described above as well.

The description of the different possible architectures above shows that architectures for facilitating information sharing can be quite different from each other. This implies that the architecture we develop should be very flexible in order to be of use in different circumstances. Our solution to this is to make the architecture such that it can be incorporated in architectures in which the flow of data itself is central (such as those described above) in order to increase the willingness to share information.

Our research is related to some research on the use of business rules to capture legal knowledge, which is relevant as in our architecture business rules are used to capture legal knowledge as well. Gong and Janssen [17] propose a framework that can be used to automatically derive business processes from such business rules.

4 Towards a Software Architecture

The Software Engineering Standards Committee [21] defines an architecture as *"The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution"*. The architecture we developed, consists of a decision component and a component that allows access to data according to the decision. Metadata, business rules, global rules and context information on the requester of access to data is used as input for the decision component to reach a decision. Access to data is prevented or granted by respectively encrypting parts of data and decrypting parts of data using decryption keys.

In this section we will describe the architecture we developed. Section 5 contains an overview of the requirements and the solutions in the architecture.

4.1 The Decision Component and Providing of Decryption Keys

The decision component can be used by businesses or government agencies that have received encrypted data to request a key to decrypt the parts of the data that they are allowed to see according to the decision. A decision in this case should not be viewed as a simple yes or no, but contains a specification on which parts of the data the requester is allowed to access and which not. Based on the decision of the decision component, a key is provided to the requester which they can use to decrypt the parts of the data they are allowed access to according to the decision.

The decision of the decision component is based on business rules that are provided by the owners and by the senders of the data. When a decision is requested, these business rules are requested by the decision component from the owners and senders of the data. In addition to the business rules, the decisions are based on global rules as well. The global rules play a role in all decisions and are element of the decision component itself. Furthermore, the requesters of access provide context information on themselves and their intention to use the data as input to the decision component. They also provide metadata on the data they want to receive a decryption key for.

After the decision component has received all required rules, metadata and context information and has reached a decision using these, there are two possibilities. The first is that according to the decision the requester is not allowed access to any part of the data, in which case the requester is informed of this. The second possibility is that according to the decision the requester is allowed access to parts of the data. In that case the decision and other needed information is send to a component that generates a decryption key that can be used only by the requester of the information to decrypt exactly the parts of the information they are allowed access to according to the decision. This key is then send to the business or government agency that has requested access and they can use this key to get access to the appropriate parts of the data.

4.2 Business Rules

In order to make a decision on whether a business or government agency can have access to parts of data, the decision component needs the business rules that are specified by the owners and previous senders of the data. The decision component obtains these business rules by requesting them from these owners and senders. In order for the decision component to do this, the metadata that the requesters send the decision component with their request, should contain information for each part of the data on who the owners and previous senders are. If the business rules are requested each time a decision has to be made, it is possible for owners and senders of data to change their business rules and thereby influencing all decisions subsequent to this adaptation.

A business rule can be defined in various ways. Graham [22] defines business rules with an emphasis on the form and expressive power as follows: *“A business rule is a compact, atomic, well-formed, declarative statement about an aspect of a business that can be expressed in terms that can be directly related to the business and its collaborators, using simple unambiguous language that is accessible to all interested parties: business owner, business analyst, technical architect, customer, and so on. This simple language may include domain-specific jargon.”*. However, since the focus of this paper is more on the function of the business rules in the architecture, the definition of Ross [23] fits our purposes better. He defines business rules as a directive intended to influence or guide business process behaviour.

Business rules in the described architecture can be used by owners and senders of information to specify who does and does not have access to which parts of the data they own or send and in what cases. Since they are used by the decision component to reach a decision, they can control access to their data by specifying these rules.

Business rules can be general, e.g. specifying that all information can be used by anyone if they have a certain goal. They could also be very specific and e.g. specify that only a certain company gets access to a specific part of the data. To illustrate some ways in which business rules could be used, we provided some examples. It is important to mention that the use of first order logic (FOL) in the example is not meant as a recommendation to use FOL to express the rules in the architecture since their form is outside of the scope of this paper. FOL was chosen to make the example intelligible to most readers. In the example, symbols have their usual meaning and arguments that are capitalized denote variables.

$$\begin{gathered} \mathit{HasRole}(X, \mathit{customer}) \wedge \mathit{Has\_Role}(Z, \mathit{manufacturer}) \wedge \\ \mathit{InformationOn}(Y, Z) \rightarrow \neg \mathit{Access}(X, Y) \end{gathered} \tag{1}$$

$$\mathit{Goal}(X, Y, \mathit{security\_check}) \rightarrow \mathit{Acces}(X, Y) \tag{2}$$

Example (1) shows a business rule that might be specified by a seller who does not want customers to access information on the manufacturer of goods. In example (2), there is a business rule that could be used to express that if the goal of the requester of access to part of the data is to perform a security check, access to that part of the data is allowed.

Global businesses rules are basic rules that the decision component includes for each decision and that are not organization specific. They could be used to incorporate some general common sense in the decision process and to make sure that access to data is allowed only in accordance with legislation. We provided some examples below. It is important to note that they are not meant as a proposal for a specific design as well. The global rules are expressed in FOL, symbols have their usual meaning and arguments that are capitalized denote variables.

$$\mathit{GoalGathered}(X, Y) \wedge \mathit{GoalUse}(Z, X, Q) \wedge Y \neq Q \rightarrow \neg \mathit{Access}(Z, X) \tag{3}$$

$$\mathit{SecurityStatus}(\mathit{emergency}) \wedge \mathit{HasRole}(X, \mathit{customs}) \rightarrow \mathit{Access}(X, \mathit{all}) \tag{4}$$

The global rule in (3) expresses that access to data is not allowed for a requester if their goal for using the data is different from the goal for which it was gathered. In (4) a global rule is expressed that is used to grant customs access to all information in case of an emergency situation.

Since global rules are the same for all data, they all could be saved in the same location and be retrieved when needed in the decision process. If they are changed, e.g. because of changes in regulation, this change influences all subsequent decisions.

4.3 Metadata and Context Information

In order to make decisions based on the rules, metadata and context information are needed to determine which rules are applicable. Ma [24] provides a comparison of twenty-seven definitions of metadata. Zuiderwijk et al. [25] defines metadata as *"structured, encoded data that describes characteristics of information bearing entities to aid in the identification, discovery, assessment, and management of the described entities"*. Often, metadata is simply defined as "data about data" [26, 27]. Examples of metadata that could be sent with the encrypted data, is information on the owners and previous senders of the encrypted data or the goals for which parts of the data initially was gathered. It also could be important to incorporate for instance information on the way in which different parts of data are linked.

The metadata should be send with the encrypted data itself. There are several reasons for this. The receivers of encrypted data probably would like to receive at least some basic information on the data that they have received and it is easiest to send this together with the data itself. Furthermore, information on the owners and previous senders of the data is metadata as well and is needed for the decision component in order to determine from who business rules should be requested. Of course there might be cases in which it is not desirable for receivers of information to have access to all metadata. In that case, parts of the metadata could be encrypted. The decision component should receive the metadata, together with the request for access to data itself from the business or government agency that is the requester.

The last input that is needed for a decision by the decision component is context information on the requester of access to the data and their intent to use the data. Such context information of course is available with the requesters of access to data themselves. Businesses and government agencies making a request should send this context information together with their request to the decision component. Some sort of authentication could be send as part of the context information as well.

4.4 Regulating Access via Encryption and Decryption of Parts of Data

In many cases, access to data is regulated by sending or not sending data to others or by allowing or not allowing others access to a database. This differs for the architecture we developed. Namely, in this architecture, encryption and decryption of parts of data is used to regulate access to data. This means that it is possible for businesses to send encrypted data to each other and to government agencies directly without thereby automatically granting them access to all the data they are sending. As a result, the access to data and the location where the data is saved are not linked. In other words, physical access to information does not imply logical access in this case.

Because of the use of encryption and decryption to regulate access to data, the flow of encrypted data itself can be very flexible and can be adapted to specific needs and circumstances. There is no obvious obstruction to using any kind of flow of information between businesses and government agencies. It is for instance possible that there is a direct data flow between the users of the architecture. In that case, businesses and government agencies could announce that they have data and send it upon request or they can take the initiative to send data when they think it is necessary. Another possible example is using a physical shared data space.

The fact that access and location are no longer linked, means that it is possible for businesses and government agencies to share the information that they have received with others as well, without automatically granting them access. This allows for the possibility for organizations to enrich data or combine the data that they have received in useful ways and to share it with others. In order for this to work, the enriched data or combined data should be encrypted as well before sending and the rules of the owners of the original data, previous senders and the new sender should be applicable on the new data that is based on them. An example of the enrichment of data could be if a company added the weight of containers to the data, based on received information on the weight of goods and their own information on in which containers goods are. If they would send the enriched data, the business rules of the owner of the information on the weight of the goods, as well as the previous senders of this information would be applicable, in addition to of course the business rules of the company itself.

5 Evaluation of the Architecture

5.1 An Illustration

To illustrate the way in which the architecture we developed works and how the components and users relate to each other, we have provided an example related to our case study. Figure 1 shows the flow of information in the architecture, while Fig. 2 is an UML sequence diagram. In the figures, there are two businesses and a government agency. Other ways of sharing information than shown in the example are possible, but sending information directly is the most simple and thus the clearest way to illustrate the structure of our architecture. The flow of the encrypted data follows the physical flow of goods in the supply chain. Business 1 sends encrypted information to business 2. Business 2 enriches the information with their own and sends the enriched information to the government agency. Of course, usually, business 2 would in this case request access to the information as well. This request is left out of the diagrams to guard their intelligibility, as is the encryption of the data and generation of rules and such. After the government agency has received the encrypted data, it uses the decision component to obtain a decision. Then a key is generated and shared with customs based on the decision. Note that the decision process pulls the business rules from the businesses and that this happens after the data is requested.

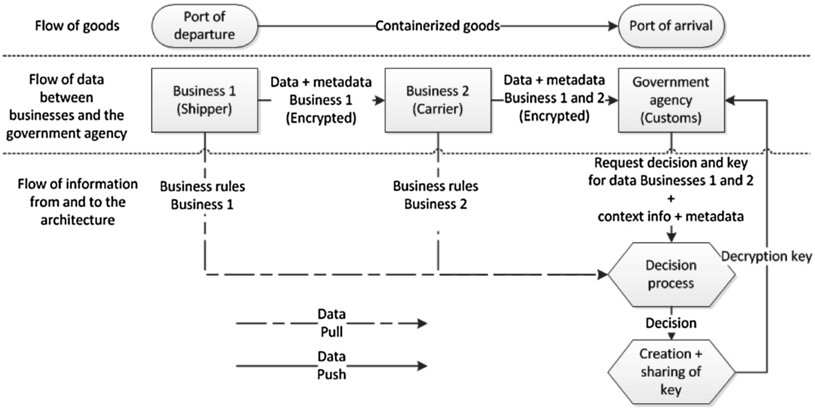
Flow of goods
Port of departure
Containerized goods
Port of arrival
Flow of data between businesses and the government agency
Business 1 (Shipper)
Data + metadata Business 1 (Encrypted)
Business 2 (Carrier)
Data + metadata Business 1 and 2 (Encrypted)
Government agency (Customs)
Flow of information from and to the architecture
Business rules Business 1
Business rules Business 2
Request decision and key for data Businesses 1 and 2 + context info + metadata
Decision process
Decryption key
Decision
Creation + sharing of key
Data Pull
Data Push

Fig. 1. The flow of information in an example for the described architecture

In Fig. 2 the procedures that are executed by the architecture and its users can be observed as well as what happens in case access to data is not allowed according to the decision process. To guard the intelligibility of the diagram, the components of the architecture itself are not shown separately as is done in Fig. 1.

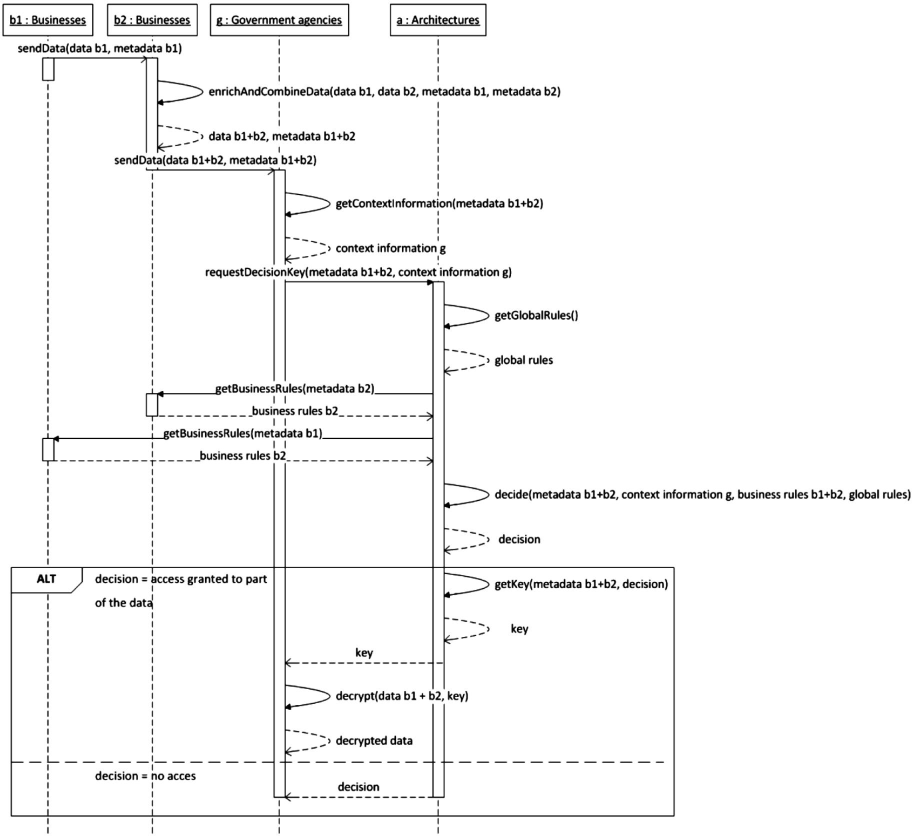
b1 : Businesses
b2 : Businesses
g : Government agencies
a : Architectures
sendData(data b1, metadata b1)
enrichAndCombineData(data b1, data b2, metadata b1, metadata b2)
data b1+b2, metadata b1+b2
sendData(data b1+b2, metadata b1+b2)
getContextInformation(metadata b1+b2)
context information g
requestDecisionKey(metadata b1+b2, context information g)
getGlobalRules()
global rules
getBusinessRules(metadata b2)
business rules b2
getBusinessRules(metadata b1)
business rules b2
decide(metadata b1+b2, context information g, business rules b1+b2, global rules)
decision
ALT
decision = access granted to part of the data
getKey(metadata b1+b2, decision)
key
key
decrypt(data b1 + b2, key)
decrypted data
decision = no acces
decision

Fig. 2. UML sequence diagram for the example for the described architecture

Next we will evaluate the architecture presented in the previous subsection by analysing the way the requirements are met by the architecture. In addition, we discuss some other advantages and disadvantages of the architecture described.

5.2 Keeping Information Confidential When Needed

In the architecture businesses and government agencies can control who does and does not have access to their information by specifying business rules. The responsibility to specify these rules so that their interests are not hurt, lie with the parties themselves. If they think that certain information for instance will be of competitive advantage, they can specify business rules which deny their competitors access to this information. Since each time a decision is made by the decision component, the appropriate business rules are pulled from the systems of the owners and senders of data, businesses can modify, add or remove them if this is needed and this will result in changes on who gets access to information. Businesses are thus provided with a means to control their data and to make sure it is kept confidential when needed.

At first sight, the level of control businesses can exert over access to their data in the architecture is not much unlike other situations in which businesses or government agencies for instance choose to send data that is not encrypted to some parties and not to others. There are however some important differences. The first is that in the described architecture, the rules for who gets access to what parts of data and who does not are explicit and applied in a consistent manner. Making a refined specification, might make businesses and government agencies realize more clearly what parts of their data actually needs to be kept confidential and for whom. A consequence of this is a more refined distinction between data that other parties can and cannot have access to, which in turn results in increased willingness to share data. A problem with the fact that businesses and government agencies have to specify business rules is that it could be a lot of work and they might not want to make such an investment if it is not clear how they could benefit from it.

The second difference is that parties sending received data to others, do not need to be afraid of breaking confidentiality or damaging trust between parties, if the data that they send is encrypted. When access to data and the location where data is saved are no longer linked, sending data to others does not automatically mean granting them access. Even if data is received from other sources, access to data is still controlled by the owners of data and the previous senders because their business rules stay applicable. This makes it easier for parties to send data that they have received and enriched or combined with their own data, since it no longer has the consequence of breaking confidentiality. As access to data is no longer needed to make sure that resending it does not break confidentiality, businesses that cannot access data themselves can resend it easier as well. For these reasons, it is expected that willingness to share information will increase.

To the original owners of information, it might be reassuring to know that wherever their data is, their business rules are applicable and access is only granted following these rules. Furthermore, they might be reassured by the fact that these rules are as well applicable on enriched or combined data that is based on their data, eliminating the risk that their data can be abstracted from this by parties from who the data should be kept confidential. This might increase their willingness to share their information. Of course there is still a possibility that other parties might send decrypted information to others and breaking confidentiality in that way. The risks of this are not higher than parties sharing data illicitly when businesses or government agencies granted them access to data directly themselves. In the case of the described architecture, there clearly is the option of sending information encrypted and thereby respecting the rules that are specified by the owners and senders of the data. Therefore, when information is send decrypted, the attempt to circumnavigate the control of the owners and senders of information on their data is much more clear.

5.3 Ensuring There is No Obstruction for Information Sharing from the Possible Increase of Liability When Businesses Receive Information

For the second requirement, it is not completely clear how liability is influenced by the use of the architecture. When businesses or government agencies receive certain information, it could increase their liability. In the case of the architecture, they could receive and store such information, but not have access to it, or even know that it exists and that that they have it stored. While it is not completely clear from a legal point of view whether they are still liable, we could look at what is reasonable. One could say in this case that in a sense they did not receive or do not possess the information that is in the data. It is reasonable that in that case the receiving and storage of the encrypted data should not make them liable. In consequence, the willingness to store this information and subsequently share it with others would probably improve. A decision by the decision component could serve as proof that data indeed cannot be accessed if needed. There of course is a difference between cases in which encrypted data cannot be accessed and cases in which the business or government agency chooses not to access the data. In the second case, the position that receiving and storing this data should not increase liability is harder to defend.

5.4 Ensuring the Sharing of Information and Its Use is in Compliance with Legislation

The last requirement has to do with the confidence that the sharing of information and its use is in compliance with legislation. The global rules that the decision component uses, could be used to make sure that access is only granted to parts of data if this complies with legislation. These rules could be adapted in case legislation changes, without users having to keep track of such changes in legislation and their influence on whether they can or cannot share information themselves. At the moment, it is unclear whether the same legislation that is applicable to data that is directly accessible is applicable to data that is encrypted and cannot directly be accessed. However, for the same reasons as in the situation with the increase of liability, it might be reasonable to say that this should not be the case. If encrypted data could be shared freely and access is only granted to parts of data when this is in compliance with legislation, it is reasonable for users of the architecture to be confident that they comply with legislation if they only send encrypted information and only access information according to the decisions of the decision component. This in turn might lead to an increase in their willingness to share information.

While at first sight this would be an ideal situation for the users of the architecture, there might be some problems as well. The responsibility to be compliant in a sense shifts from the users of the architecture to the organization that specifies the global rules, resulting in some ethical and legal difficulties. Furthermore, the organization specifying the global rules, has a lot of power, since they have an influence on all requests for access and this may not be desirable. A solution could be to let the decision component be governed by the users themselves, solving some of the ethical difficulties with responsibility and distribute the power between the users.

5.5 Other Properties of the Architecture

The described architecture has some other interesting properties worth discussing. The first is the security of the data in the architecture. If encrypted data falls in the wrong hands, someone can attempt to decrypt it themselves illegally. Since in our architecture they can have the encrypted data stored in their own systems, they could go about their business uninterruptedly. The data should thus be encrypted well enough to make it not worth attempting to decrypt it illegally or so that this takes such a long time that by the time they succeed, the data has lost its worth. Hence, the quality of encryption is vital. There are some advantages of the described architecture considering security as well. If someone decrypts data illegally, they can only access that data and e.g., not a full database. Furthermore, there does not need to be a single component through which all data passes, which would have possessed its own risks.

Another property of the described architecture is that it is very flexible. There is no clear obstacle for the architecture to be part of any information sharing architecture, since the way information is send to others is and does not need to be specified. Furthermore, it allows for the constant adaptation of business rules and global rules to new (legal) circumstances, and changes of interests and needs.

6 Conclusion and Suggestions for Further Research

The architecture we developed empowers business by providing them control of their information sharing. The fact that business rules can be specified by the owners and senders of information and that these are applicable even when information is not received directly from its original source or when it is combined or enriched, gives owners the control to keep their data confidential when needed. In addition, in the architecture the sharing of data that is received by others, that is enriched or combined, is especially made easier by using the combination of business rules and encryption. Furthermore, it seems that using global rules to make sure that data access complies with legislation, is an option for increasing willingness to share information.

Overall, an architecture incorporating business rules, global rules, a decision component and encrypted data has enough potential to merit further investigation. Especially since the proposed architecture is very flexible and could be combined with other architectures, combining their advantages as well. We do recommend that this is coupled with investigating the legal framework such an architecture would exist in.

The subject of control management and especially role based access and attribute based access such as described in [28, 29] seems very relevant for future research, in particular when working out what the different kinds of business rules and global rules should look like. Metadata and context information plays an important role in the architecture as well, making it an important topic for further research. Research on knowledge representation as well as existing formats and standards for metadata are relevant for this. In order to reason with the rules and information, theories from the domain of automated reasoning and decision support are significant as well and should be taken into account. Generating and distributing keys and encryption of data is vital for the architecture, but far from trivial. Research on encryption and computer security should therefore have an important part in future research. Other ways of increasing security, e.g., by using authentication or signing of data, for this architecture should be investigated as well.

References

1. Bharosa, N., Janssen, M., van Wijk, R., de Winne, N., van der Voort, H., Hulstijn, J., Tan, Y.-H: Tapping into existing information flows: The transformation to compliance by design in business-to-government information exchange. Gov. Inf. Q. **30**, S9–S18 (2013)
2. Fawcett, S.E., Osterhaus, P., Magnan, G.M., Brau, J.C., McCarter, M.W.: Information sharing and supply chain performance: the role of connectivity and willingness. Supply Chain Manag. Int. J. **12**, 358–368 (2007)
3. Klievink, B., Janssen, M., Tan, Y.-H.: A stakeholder analysis of business-to-government information sharing: the governance of a public-private platform. Int. J. Electron. Gov. Res. **8**, 54 (2012)
4. Klievink, B., Lucassen, I.: Facilitating adoption of international information infrastructures: a living labs approach. In: Wimmer, M.A., Janssen, M., Scholl, H.J. (eds.) EGOV 2013. LNCS, vol. 8074, pp. 250–261. Springer, Heidelberg (2013)
5. Overbeek, S., Klievink, B., Hesketh, D., Heijmann, F., Tan, Y.-H.: A Web-based data pipeline for compliance in international trade. In: Proceedings of the CEUR Workshop, vol. 769, pp. 32–48 (2011)
6. Janssen, M., Smeele, F.: JUridical and context-aware Sharing of informaTion for ensuring compliance (JUST) (2013)
7. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Q. **28**, 75–105 (2004)
8. Van Baalen, P., Zuidwijk, R., van Nunen, J.: Port inter-organizational information systems: capabilities to service global supply chains. Found. Trends® Technol. Inf. Oper. Manag. **2**, 81–241 (2009)
9. Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D., Zacharia, Z.G.: Defining supply chain management. J. Bus. Logist. **22**, 1–25 (2001)
10. Tsay, A.A., Nahmias, S., Agrawal, N.: Modeling supply chain contracts: a review. In: Tayur, S., Ganeshan, R., Magazine, M. (eds.) Quantitative Models for Supply Chain Management, pp. 299–336. Springer, New York (1999)
11. Levinson, M.: The world the box made. In: The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger. Princeton University Press, Princeton (2010)
12. Hesketh, D.: Weaknesses in the supply chain: who packed the box. World Cust. J. **4**, 3–20 (2010)
13. Klievink, B., van Stijn, E., Hesketh, D., Aldewereld, H., Overbeek, S., Heijmann, F., Tan, Y.-H.: Enhancing visibility in international supply chains: the data pipeline concept. Int. J. Electron. Gov. Res. **8**, 14–33 (2012)
14. Lee, H.L.H., Whang, S.: Information sharing in a supply chain. Int. J. Manuf. Technol. **1**, 79–93 (2000)

15. Urciuoli, L., Hintsa, J., Ahokas, J.: Drivers and barriers affecting usage of e-Customs — a global survey with customs administrations using multivariate analysis techniques. Gov. Inf. Q. **30**, 473–485 (2013)
16. van Stijn, E., Hesketh, D., Tan, Y.-H., Klievink, B., Overbeek, S., Heijmann, F., Pikart, M., Butterly, T.: Annex 3: The Data Pipeline. Connecting International Trade?: Single Windows and Supply Chains in the Next Decade, pp. 158–183. United Nations Economic Commission for Europe (2011)
17. Gong, Y., Janssen, M.: A framework for translating legal knowledge into administrative processes: dynamic adaption of business processes. In: Cerone, A., Persico, D., Fernandes, S., Garcia-Perez, A., Katsaros, P., Ahmed Shaikh, S., Stamelos, I. (eds.) SEFM 2012 Satellite Events. LNCS, vol. 7991, pp. 204–211. Springer, Heidelberg (2014)
18. Sahin, F., Robinson, E.P.: Flow coordination and information sharing in supply chains: review. Implications Dir. Future Res. **33**, 1–32 (2002)
19. Yang, T.-M., Maxwell, T.A.: Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. Gov. Inf. Q. **28**, 164–175 (2011)
20. Stijn, E. Van, Klievink, B., Janssen, M., Tan, Y.-H..: Enhancing business and government interactions in global trade. In: Third International Engineering Systems Symposium CESUN 2012. pp. 18–20 (2012)
21. Software Engineering Standards Committee: IEEE Recommended Practice for Architectural Description of Software-Intensive Systems (2000)
22. Graham, I.: Business Rules Management & Service Oriented Architecture. Wiley, Chichester (2006)
23. Ross, R.G.: Principles of the Business Rule Approach. Addison-Wesley Longman Publishing Co., Inc., Boston (2003)
24. Ma, J.: Managing metadata for digital projects. Libr. Collect. Acquis. Tech. Serv. **30**, 3–17 (2006)
25. Zuiderwijk, A., Jeffery, K.G., Janssen, M.: The potential of metadata for linked open data and its value for users and publishers. JeDEM-e-J. e-Democracy Open Gov. **4**, 2012 (2012)
26. Jeffery, K.G.: Metadata: the future of information systems. In: Brinkkemper, J., Lindencrona, E., Sølvberg, A. (eds.) Information Systems Engineering: State of the art and research themes. Springer, London (2000)
27. Schuurman, N., Deshpande, A., Allen, D.M.: Data integration across borders: a case study of the Abbotsford-Sumas aquifer (British Columbia/Washington State) 1. JAWRA J. Am. Water Resour. Assoc. **44**, 921–934 (2008)
28. Sandhu, R.R.S., Coynek, E., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Comput. (Long. Beach. Calif) **29**, 38–47 (1996)
29. Hu, V.C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K.: Guide to attribute based access control (ABAC) definition and considerations. NIST Spec. Publ. **800**, 162 (2014)