Comparing a Shipping Information Pipeline with a Thick Flow and a Thin Flow

van Engelenburg, Sélinde; Janssen, Marijn; Klievink, Bram; Tan, Yao-hua

DOI
10.1007/978-3-319-64677-0_19

Publication date
2017

Document Version
Accepted author manuscript

Published in
Electronic Government: 16th IFIP WG 8.5 International Conference, EGOV 2017, St. Petersburg, Russia, September 4-7, 2017, Proceedings

Citation (APA)
van Engelenburg, S., Janssen, M., Klievink, B., & Tan, Y. (2017). Comparing a Shipping Information Pipeline with a Thick Flow and a Thin Flow. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren, P. Parycek, H. J. Scholl, & D. Trutnev (Eds.), *Electronic Government: 16th IFIP WG 8.5 International Conference, EGOV 2017, St. Petersburg, Russia, September 4-7, 2017, Proceedings* (Vol. 10428, pp. 228-239). (Lecture notes in Computer Science). Springer. https://doi.org/10.1007/978-3-319-64677-0_19

Comparing a Shipping Information Pipeline with a Thick Flow and a Thin Flow

Sélinde van Engelenburg✉, Marijn Janssen, Bram Klievink, and Yao-Hua Tan

Delft University of Technology, Delft, The Netherlands
{S.H.vanEngelenburg, M.F.W.H.A.Janssen, A.J.Klievink, Y.Tan}@tudelft.nl

Abstract. Advanced architectures for business-to-government (B2G) information sharing can benefit both businesses and government. An essential choice in the design of such an architecture is whether information is shared using a thick or a thin information flow. In an architecture with a thick flow, all information is shared via a shared infrastructure, whereas only metadata and pointers referring to the information are shared via the shared infrastructure in a thin flow architecture. These pointers can then be used by parties to access the information directly. Yet, little is known about what their implications for design choices are. Design choices are influenced by the properties of the architecture as well as the situation in which B2G information sharing takes place. In this paper, we identify the properties of architectures with a thin and thick flow. Next, we determine what this implies for the suitability of the architectures in different situations. We will base our analysis on the case of the Shipping Information Pipeline (SIP) for container transport. While both architectures have their pros and cons, we found that architectures with a thin flow are more suitable when non-standardized, and flexible sharing of sensitive information is required. In contrast, we found that architectures with a thick flow are more suitable when in-depth integration is required.

Keywords: Business-to-government information sharing · Information sharing · Shipping information pipeline · Supply chain · Thick flow · Thin flow · Information architecture

1 Introduction

Governments require businesses and other actors to report information, for example for purposes of taxation or keeping statistics. Most Business-to-Government (B2G) reporting is highly regulated, with obligations pertaining to scope, scale, timing and format for sharing. However, more information can be shared than is formally required, which can result in advantages for companies and governments. For instance, some Customs organizations put businesses that share additional information in a trusted, green trade lane, in which there are less and more conveniently timed physical inspections of their goods [1]. Each inspection delaying the delivering of goods causes additional work. In a green late companies will have less inspections resulting in lower costs and faster delivery.

Anything beyond obligatory information sharing is more difficult to arrange and relies on collaboration between government and businesses [2]. Organizations seek control over what happens to their information and how information is being shared [3]. Any information sharing that is not required by law for B2G reporting encounters the challenge of balancing this desire for control with the autonomy of other actors in the network, i.e. those you use data of or share data with [4]. Hence, any information sharing architecture will have to accommodate this balance.

In the many possible B2G information sharing architectures all information can be shared indirectly via the architecture or some information can be shared directly between parties. The former is called a thick information flow architecture, whereas the latter is called a thin information flow architecture. In a *thick* flow, the actual information itself is shared via the architecture [4]. In a *thin* flow, information shared via the architecture is limited to metadata and pointers to the information businesses intend to share [4]. The pointers can be used to directly access the shipping information in the systems of the businesses.

Which architecture is best for which circumstances is not known. There are only limited insights in the implications for design choices of these two types of architectures. The objective of this paper is twofold: we inventory the essential properties of these two types of architecture, and based on them, we analyse their implications. To this end, we focus on the case of container supplying in which the Shipping Information Pipeline (SIP) is used to share information with Customs.

In the next section, we will describe the SIP with a thick and a thin flow. Subsequently, we present a list of properties relevant to making a choice in design for the architectures. Section 4 contains the actual comparison of the thin flow and the thick flow using this list. In section 5 we discuss what this implies for design choices for the SIP in different situations.

2 A Shipping Information Pipeline

The sharing of shipping information in supply chains can benefit businesses as well as Customs [5–7]. Reliable shipping information allows businesses to work together more effectively and efficiently and for synchro-modality to optimize the goods flow [7, 8]. Customs is tasked with monitoring the flow of goods and interfering with it if necessary for security, safety or public policy [5]. It is not feasible to physically inspect all goods they need to monitor and they thus have to rely on the shipping information of businesses in the supply chain to fulfil their responsibilities [9, 10].

In the current situation, the shipping information shared is often not timely, not originating from the source, filtered and altered, which might result into inaccurate information [6, 10, 11]. Yet, the information that businesses in the supply chain gather is of high quality, since their own commercial operations depend on it [5]. Customs often is expected to make it attractive for companies to trade in their country. For this reason, they reward businesses who do share information voluntarily (see e.g., [1]).

2.1 The Shipping Information Pipeline

The idea of a SIP was first proposed by UK and Dutch Customs [12, 13]. It was developed to allow original information to be captured in real-time at the source to increase reliability [6]. The data that are made available in the SIP are the raw and original data that companies have in their systems to base their own operations on [6]. When this data are made available in the SIP, they could be reused for other purposes than that they were gathered for, according to the piggy-backing principle [14, 15]. According to Hesketh [10], the information that is shared between the parties describes the transactional data that is captured by the parties in the supply chain, the physical data that is captured by tracing, tracking and monitoring devices and relevant commercial risk management data such as quality and technical compliancy tests. In the pipeline, data on goods and people are distinguished from data on different modes of transport (e.g. ship, rail, truck etc.) [8].

The SIP is based on a Service-Oriented Architecture (SOA), in which resources are made available as independent artefacts that can be accessed in a standardized way [6, 16]. SOAs are the de facto standard for data integration [8]. In the SIP, each subsequent party in the supply chain makes their source data accessible as soon as it becomes available [6]; for example a seller starts with a purchase order, then sends an invoice, and when his goods are received by the buyer a payment transfer is made. With each step, the data is enriched with new data [6]. By linking the data that becomes available in this manner, an integrated data view is created, providing a full view of the trade lane [6]. The SIP is therefore referred to as an integrated data pipeline or seamless integrated data pipeline as well [8, 10].

The main differences between the SIP and other kinds of data pipelines are that in the SIP data is shared between parties in a supply chain and with Customs and that it only supports the sharing of shipping information. Furthermore, it allows for a transition from the current data push approach in which businesses push documents to Customs, to a data pull approach in which Customs pulls the data they require [6]. Naturally, the access to data in the SIP is only allowed for parties that are authorized to do so by the owners of the data [6].

Whether the SIP supports thick or thin information flows highly influences the properties of the architecture. In the literature on its more practical design, usually the SIP involves a single or limited number of central components that the information goes through [11, 17]. Such a central component can be a port community system or business community system acting as a central hub, or an event repository [11, 17]. Considering the emphasis on more centralized versions of the SIP, it makes sense to compare a centralized SIP with a thick flow with a centralized SIP with a thin flow in this paper. It is important to note that technical centralization not necessarily means centralized control [18].

2.2 A Thick and a Thin Flow

In a B2G information sharing architecture with a thick flow, the messages sent between services contains the actual information that a party wants to share [4]. The information flowing in our case of the SIP thus includes the shipping information (hence, the name “thick flow”). In the case of a SIP with a thick flow, the systems of the businesses containing the shipping information are linked to the SIP using a standardized interface. When new shipping information becomes available, it is pushed or pulled from them to the central component (step 1 thick flow, fig. 1) where it is linked to the data already available. Other parties can then pull the information from the SIP (step 2 thick flow, fig. 1).

In an architecture with a *thin* flow, the messages that parties send via the architecture only contain metadata and pointers to the actual information. The pointers that are sent via the architecture can be used to access the information in the systems of the businesses directly via another data exchange platform (e.g. Internet, VPN etc.). In the case of the SIP, the information flowing through the architecture, thus does not include the shipping information itself (hence, the name “thin flow”). In a SIP with a thin flow, only the systems containing the metadata need to be connected to the SIP via a standardized interface.

For the thin flow, when new data becomes available, its metadata and a pointer is added to a reference index (step 1 thin flow, fig. 1), where the new data is linked to the data already available. This reference index is the central component of the SIP. Parties that are in need of information consult the reference index (step 2 thin flow, fig. 1) and use the pointers to pull data directly from the system where it is stored (step 3 and 4, fig. 1), without intermediation of the SIP. They could even be kept up-to-date using a publish/subscribe mechanism [19]. The sharing of the actual information in the thin flow is thus distributed and arranged between two parties.

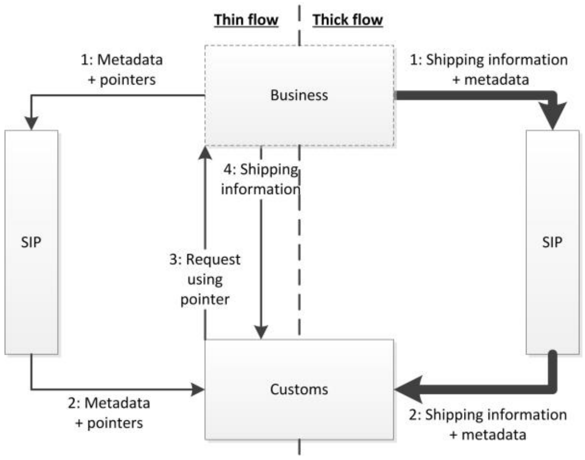

Fig. 1. A SIP with a thin flow and a SIP with a thick flow

3 Properties to Compare the Architectures

In this section, to select the relevant properties of thin and thick flow architectures, we first discuss some factors impacting the choice for a design of a B2G information sharing architecture. Then, we will discuss the properties of the architecture these factors are influenced by. In the next section, we will use these properties to compare the architectures with a thick and a thin flow. Based on this comparison, we will describe what they imply for design choices in different situations.

The voluntary sharing of information in addition to the information that businesses are obligated to share can be valuable to businesses as well as governments. However, this voluntariness makes the willingness of businesses to participate vital. Therefore, this willingness will very likely affect the design choices made for the architecture.

The willingness of businesses to participate in B2G information sharing is influenced by their need to keep information confidential and their confidence that the sharing is compliant with laws and legislation [20, 21]. Businesses might for instance require information to be kept confidential for competitive reasons (e.g., fear of being bypassed in the supply chain), or for reasons of security (e.g., fear of high-value goods getting stolen) [7, 22]. This makes the *security* of the architecture an important property to compare the different architectures on.

The sharing of information is governed by laws and regulations that require the *protection of privacy*. According to article 8, of the European Convention on Human Rights everyone has the right to respect for their private life [23]. According to jurisprudence, "everyone", in this case, also includes legal entities such as businesses [24]. Furthermore, it includes the right to protection of professional reputation [24].

Another factor is the *costs* associated with information sharing. If these are too high compared to the possible benefits, businesses will not to be willing to participate. We expect the initial investment and the resources required over time to play a role.

For businesses to be willing to share their information, they might want to have some form of control and influence on the way in which decisions about the architecture are made. The *governance* of the architecture might be as important as its infrastructure [22]. Therefore, businesses could require that the architecture is governed in a certain way. Whether a SIP with a thin or a thick flow allows for such governance thus might be an important property for making a decision as well.

The degree to which the architecture can adequately support the sharing of reliable information, is also important for the decision-making process. In fact, it is vital for the usefulness of the architecture. There are two important properties of the architecture that affect the reliability of information sharing.

When information is transferred it might be corrupted or lost. When this happens, the architecture cannot deliver its intended functionality, namely providing access to reliable information. The chances for and possible extent of issues with *data integrity* can therefore be important for design choices in architecture.

In a similar fashion, the way in which the architecture deals with faults and errors is vital for the reliability of information sharing. The *fault tolerance* of the architecture determines its coping with errors [25]. It determines to what extent data can still be shared in the architecture when something goes wrong and components fail.

The design of the architecture influences for how long it will be able to support information sharing in the future. Therefore, anticipation of future changes in the situation in which B2G information sharing needs to be supported will be an important factor influencing design choices.

Not all businesses that are a source of information might immediately be willing or able to connect to the architecture. This might change in time and the load on the architecture might grow. The architecture should then accommodate a growing number of connections and a larger volume of data. This makes its *scalability* an important property. Furthermore, in time more and unforeseen types of data might become available for sharing. For the architecture to accommodate this, it should be scalable on this dimension as well.

Other kinds of foreseen and unforeseen future changes might occur, changing the way in which the SIP should support information sharing. Examples are changes in the laws on data protection or the evolvement of new types of security attacks. Its *flexibility* is therefore another important property.

Table 1 shows the factors impacting design choices we focus on and the properties of the architecture that they in turn are affected by, based on our discussion. We will use this list of properties for comparing a SIP with a thick flow and a SIP with a thin flow. The number of each property corresponds with a subsection of section 4.

Table 1. List of properties for comparing the architectures

Main Factors	**Properties**
Willingness of businesses to participate	1. Security and privacy protection
	2. Costs
	3. Possibilities for governance
Reliability of the information sharing process	4. Data integrity and fault tolerance
Flexibility for anticipating future changes	5. Scalability
	6. Flexibility

4 Comparing the Thin and Thick Flow Architectures

In this section, we will describe the properties of a SIP with a thin flow and with a thick flow. In the next section, we will discuss how these influence the suitability of the thin and thick flow in different situations.

4.1 Security and Privacy Protection

In a technically centralized SIP with a thick flow, the shipping information and metadata goes through some kind of central component in the SIP. A security failure in this component would mean that the security and privacy of all shipping information and metadata is compromised. Encryption of the messages and sending and storing metadata and shipping information separately are possible solutions [26].

Since metadata is already shared via the reference index in the thin flow, there is no need to send it again with the follow-up message containing the shipping information; a reference number should be sufficient. As a result metadata and shipping information cannot be accessed at the same time.

In the thick flow, there is central accessibility to detailed shipping information. When the information is stored in the central component it could be immediately accessed. If it is not stored, or only temporarily stored in the central component, then the information sharing through this component might still be monitored. This is a concern for some stakeholders in the SIP [13]. In the thin flow, there is also central access to metadata. It depends on the content of the metadata in the thin flow whether similar big brother issues or global security and privacy issues could occur there. Security problems with shipping information will only be local.

In the thick flow, access will have to be controlled centrally. The more information and parties are involved, the more complex the rules for controlling access may become. In the thin flow, the reference index is a central component and will also require some central access control. However, for the shipping information itself, businesses can locally define roles and access rules. This might lead to less complex rules and provides businesses with more direct control.

In the thick flow security measures and access control can be developed and maintained centrally. In the thin flow there are a lot more connections between parties that need protection using local security measures. In a thin flow, security measures thus are as strong as the weakest link.

4.2 Costs

The SIP with a thick flow allows parties to combine forces and share part of the maintenance and keeping up to date of the central component of the SIP and its connections. This might lead to lower costs for individual parties. For the thin flow such possibilities are more limited. Additionally, sharing costs for e.g., developing security measures could lead to problems on a global scale that are avoided otherwise.

The interface of the systems of the businesses in a thick flow needs to contain many data elements, in other words, it is a ‘thick’ interface [4]. This requires initial investments to make it conform with an extensive standard. In the thin flow, the interface with the central component can be thin. Such a thin interface seems less costly to implement at first sight. However, the metadata still requires standardization.

In the thin flow, the shipping information itself needs to be shared as well. Since this is arranged between two parties, it might be the case that parties need to share or receive information according to different standards. Investments are needed by companies to work with these different standards.

Costs for implementation might be affected by how easy it is to use existing connections between parties for information sharing. For the thick flow, this might be easier with existing “thick” connections, such as those using a port community system. In the thin flow existing peer-to-peer connections for the sharing of the shipping information might be used as a basis.

4.3 Possibilities for Governance

In the thick flow, a lot of agreements are required initially, since once the system is setup everything has to work. Realizing such agreements is extremely difficult, especially in international settings such as that of the SIP. In the case of a thick flow, a large group with a great variety in parties, have to give up some of their autonomy to a system they do not have control over.

The governance in the case of the thin flow has to focus on agreements on the sharing of metadata, but not on the sharing of the shipping information, as that remains under control of the parties. As a result, without a clear incentive, the sharing of the shipping information might be perceived as contributing to a vulnerability or might result in opportunistic behaviour of other parties (e.g., inappropriately using the information) [27]. The thin data flow is therefore likely to start with low depth of integration ([28] in [27]). Only gaining a sufficient level of trust between parties will lead to higher levels of integration and more benefits of the information sharing. The paradox is that it also requires governance to create a situation that warrants against opportunism or at least bilateral agreements. This results in a fragmented system, where parties cannot rely on (all) shipping information actually being shared via the SIP.

4.4 Data Integrity and Fault Tolerance

In the thick flow, if shipping information is corrupted during sharing from the source to the central element, then all other parties with which the data is shared, receive the corrupt data. In the thin flow, issues with corrupt shipping information are only local. However, for the metadata central problems with data integrity might occur.

The centralized sharing of shipping information in the SIP with a thick flow, introduces a single point of failure. The reference index is a central element of the SIP with a thin flow and also constitutes a single point of failure. If the reference index cannot be used, parties might not know where to find shipping information and this will make sharing harder.

4.5 Scalability

For both architectures, scaling up the number of users would in general mean a higher volume of information that is shared via the SIP. The increase of volume of information per user is higher in the thick flow, since the shipping information itself is shared via the SIP. Therefore, it will require better scalability than a thin flow SIP.

In the thick flow, parties can use a standardized interface to link to the SIP and then they can exchange information with all other parties. For the thin flow, there is a possibility that all parties agree on such an interface as well. If not, adding a new party means that new arrangements about interfaces need to be made. This might involve a lot of work if it is a regular occurrence. At the local level there might be more heterogeneity and even manual work required without agreements on standards.

An effect of sharing new types of data is that new elements need to be added to the interfaces involved in the sharing of the shipping information. For the thick flow, depending on the design of the interface, this might be difficult to arrange since it involves adding an element to the interfaces of all parties in the SIP. The thin flow might have the same problem, depending on whether changes to the interfaces for metadata need to be made as well. However, for making additions or changes to the interfaces required to share the shipping information, less parties are involved.

4.6 Flexibility

A thick flow entails that the shipping information is shared via the architecture. This means that no large changes can be made to the route of information while still being a SIP with a thick centralized flow. Such a change might also be difficult to realize due to the changes in agreements and adaptations required by a lot of parties involved. For the thin flow, the route the information takes could be changed simply by changing the pointer so that the information is pulled from a different system.

In the thick flow, a component (e.g., for anonymization) can be added centrally, affecting the sharing of all shipping information such that it e.g., conforms with new legislation. In the thin flow, when a lot of parties are sharing their shipping information using the same newly added component, it is questionable whether we can still talk about a thin flow. It might be useful to switch to a different kind of architecture when adaptations are needed that require highly complex components that are hard to implement and develop for individual parties. However, in that case there are similar problems as in the thick flow, since a lot of parties need to agree.

5 Impact on the Design of B2G Information Sharing Architectures

The properties of the thick and the thin flow are important for several factors that impact the design choices for a B2G information sharing architecture. The way in which they impact the design choices depend on the situation in which B2G information sharing takes place. It is very hard, if not impossible, to say something in general about which choice for a design is more suitable, without taking the situation into account. Therefore, to say something about the impact on design choices, we have to say something about the situations in which a thick or thin flow is suitable.

In the previous section we discussed different properties of the architectures with a thick and a thin flow. Based on these, we present an overview in the tables below of the suitability of the architectures in different situations, with respect to these properties. Based on the factors, a thick or thin flow is considered suitable in a situation if in that situation the architecture: improves or not decreases willingness of businesses to participate, supports a sufficient level of reliability of information sharing, or is flexible enough to adequately adapt to anticipated future changes.

Table 2. Thick and thin flow suitability: willingness of businesses to participate

Property	Thick flow suitable when:	Thin flow suitable when:
1. Security and privacy protection	No serious consequences of (global) security issues	Serious consequence of (global) security issues
	No concerns for big brother is-	Concerns for big brother issues

	sues	with information, but not metadata
	Simple access rules sufficient	Complex rules required
	Parties do not need to control access directly	Parties need to control access directly
	Parties do not trust others to take sufficient security measures	Parties trust others to take sufficient security measures
2. Costs	Low costs required for development, maintenance etc.	Higher costs for development, maintenance etc. permitted
	High short-term costs for implementing thick interface permitted	Low short-term costs for implementing thin interface required
	Low long-term costs for connecting to new parties required	High long-term costs for many different connections permitted
	Existing connections are “thick”	Existing connections are “thin”
3. Possibilities for governance	Easy to get agreements between parties	Hard to get agreements between parties
	Actually sharing is important	Commitment to share not required

Table 3. Thick and thin flow suitability: reliability of information sharing

Property	**Thick flow suitable when:**	**Thin flow suitable when:**
4. Data integrity and fault tolerance	Incorrect data has no serious consequences	Incorrect data can have serious consequences
	Not being able to share has no serious consequences	Not being able to share has serious consequences

Table 4. Thick and thin flow suitability: flexibility for anticipating future changes

Property	**Thick flow suitable when:**	**Thin flow suitable when:**
5. Scalability	Not expecting to add a high number of parties in the future	Expecting to add a high number of parties in the future
	Not expecting to share many new data elements in the future	Expecting to share many new data elements in the future
6. Flexibility	Low need for a flexible route of information	High need for a flexible route of information
	Expecting to make changes that affect all information sharing	Not expecting to make changes that affect all information sharing

6 Conclusions and Suggestions for Further Research

In this paper we compared a B2G information sharing architecture with a thick flow and with a thin flow. We found that the choice for a thick flow or a thin flow causes properties of architectures to be quite different. The main cause for this is that in a thick flow more information is shared over an central infrastructure. Design choices for an architecture are not only influenced by the properties of the architecture, but also the situation in which B2G information sharing takes place. In every specific case in which a design choice is made, advantages and disadvantages of design choices need to be weighted carefully. However, in our case we found that an architecture with a thin flow would be more suitable when sensitive information is shared, it is hard to get parties to agree or commit, there is a need for high scalability and reliability and sharing between individual parties should be flexible. In contrast, we found an architecture with a thick flow to be more suitable when information is not sensitive, it is easy to get parties to agree, commitment to actually share information is important, the architecture does not need to be scalable or very reliable and future changes affecting all information sharing are expected.

There are some limitations to this research. We only compared a centralized SIP with a thick flow with a centralized SIP with a thin flow in a case of information sharing for container supply chain. Distributed variants of thick and thin flow architectures should be subject to further research. Furthermore, the comparison in this research is purely analytical. Evaluating thick and thin flow architectures in practice might provide further insight. Additionally, there might be other properties and factors that are important herein other cases. This can be investigated in future research as well.

References

1. Customs Administration of the Netherlands: Pushing boundaries: The Customs Administration of The Netherlands' Point on the Horizon for the Enforcement on Continuously Increasing Flows of Goods, (2014).
2. Klievink, B., Bharosa, N., Tan, Y.H.: The collaborative realization of public values and business goals: Governance and infrastructure of public-private information platforms. Gov. Inf. Q. 33, 67–79 (2016).
3. Homburg, V.M.F.: The political economy of information exchange politics and property rights in the development and use of interorganizational information systems. Knowledge, Technol. Policy. 13, 49–66 (2000).
4. Klievink, B.: Unravelling Interdependence: Coordinating Public-Private Service Networks. Delft University of Technology, Delft (2011).
5. 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).
6. 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).
7. 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. An Int. J. 12, 358–368 (2007).
8. Overbeek, S., Klievink, B., Hesketh, D., Heijmann, F., Tan, Y.-H.: A Web-based data pipeline for compliance in international trade. Witn. 2011. 32–48 (2011).
9. Levinson, M.: The World the Box Made. The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger. pp. 1–15. Princeton University Press (2010).
10. Hesketh, D.: Weaknesses in the supply chain: who packed the box. World Cust. J. 4, 3–20 (2010).

11. Klievink, B., Aldewereld, H., Tan, Y.-H.: Establishing Information Infrastructures for International Trade: Discussing the Role and Governance of Port-Community Systems. 5th International Conference on Information Systems, Logistics and Supply Chain (ILS2014). pp. 1–10. Dinalog (2014).
12. Pruksasri, P., van den Berg, J., Hofman, W.: Global Monitoring of Dynamic Information Systems A Case Study in the International Supply Chain. Computer Science and Engineering Conference (ICSEC) (2014).
13. Jensen, T., Tan, Y.-H.: Key Design Properties for Shipping Information Pipeline. In: Janssen, M., Mäntymäki, M., Hidders, J., Klievink, B., and Hutchison, D. (eds.) Open and Big Data Management and Innovation. pp. 491–502. Springer International Publishing (2015).
14. Tan, Y.-H., Bjørn-Andersen, N., Klein, S., Rukanova, B.: Accelerating Global Supply Chains with IT-Innovation. (2011).
15. Hofman, W.: Supply chain visibility with linked open data for supply chain risk analysis. WITNESS 2011. pp. 20–31 (2011).
16. Graham, I.: Business Rules Management & Service Oriented Architecture. John Wiley & Sons, Ltd (2006).
17. Lucassen, I., Klievink, B., Griffioen, H., Commission, E.: Cassandra – WP400 – Asia-NL/UK trade lane Living Lab report. (2010).
18. Janssen, M.: Insights from the introduction of a supply chain co-ordinator. Bus. Process Manag. J. 10, 300–310 (2004).
19. Papazoglou, M.P., Van Den Heuvel, W.J.: Service oriented architectures: Approaches, technologies and research issues. VLDB J. 16, 389–415 (2007).
20. 20. 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).
21. van Engelenburg, S., Janssen, M., Klievink, B.: Design of a Business-to-Government Information Sharing Architecture Using Business Rules. Software Engineering and Formal Methods. pp. 124–138. Springer (2015).
22. Klievink, B., Janssen, M., Tan, Y.-H.: A Stakeholder Analysis of Business-to-Government Information Sharing. Int. J. Electron. Gov. Res. 8, 54–64 (2012).
23. European Court of Human Rights: European Convention on Human Rights. (2010).
24. Karampetsou, A.: Container Information & Privacy Concerns: Opening the ``Pandora’s" box? Legal challenges of a Business-to-Customs Information Sharing with regard to Containerized Cargo. Current Issues in Maritime & Transport Law. pp. 1–17. Bonomo Editore, Bologna (2016).
25. Lee, P.A., Anderson, T.: Fault tolerance: principles and practice. Springer Science & Business Media (2012).
26. O’Brien, L., Bass, L., Merson, P.F.: Quality attributes for service-oriented architectures. (2005).
27. Hart, P., Saunders, C.: Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange. Organ. Sci. 8, 23–42 (1997).
28. Massetti, B.L.: The Effects of Electronic Data Interchange on Corporate Organization, (1991).