Towards an IT infrastructure for compliance management by data interoperability – the changing role of authorities

Wout Hofman*, Harrie Bastiaansen
(wout.hofman, harrie.bastiaansen@tno.nl)

Abstract

Since 9/11, the Customs Trade Partnership Against Terrorism (C-TPAT) was an initiative to increase container security. Through the Entry Summary Declaration (ENS), authorities require shipping lines to timely submit data to the first port of call in the EC.. However, an ENS contains insufficient data for proper risk analysis. This paper presents an IT infrastructure to capture so-called upstream data that allows customs to match delivery - with container data. It proposes Semantic Web technology for secure, global trade, with a gradual migration strategy of all stakeholders. In its final stage, only export and import declaration based on commercial documents is required; all other data can be captured by various authorities for risk analysis. Transport security will increase, whilst the administrative burden will decrease.

Keywords: data ownership, Linked Open Data, Semantic Web, secure trade, smart risk analysis

1. Introduction

Globalization and increased growth of international trade are two drivers for economic growth, which expose the population to new risks [1]. These risks impose information requirements on traders and logistic services providers by authorities [2] implemented by new procedures and IT systems like the Entry Summary Declaration system (ENS). Whereas in the past, a summary declaration was produced when a vessel entered a port, currently it needs to be submitted to a port of discharge 24 hours before the goods are actually loaded in a port of loading. Current logistic processes and IT systems of traders (e.g. shippers, consignees, forwarders and carriers) need to support these requirements.

Complexity of commercial transactions, logistics, and border procedures in international trade require an innovative approach to improve efficiency and effectiveness [2] [3]. The data pipeline is envisioned to address these problems, by integrating data from various parties in the supply chain and incorporate data from new tracking and monitoring technologies, which would enable real-time data management for businesses [4]. It is a conceptual view on trader networks that form logistic chains based on value propositions [5]. This conceptual view needs to be implemented. Technically, concepts from Linked Open Data [6] can be used to gather data from traders acting as resources [7], but another approach is to increase visibility based on supply chain events [8]. The latter approach introduces central components like an Aggregated Discovery Service storing events of resources [9]. These solutions all have to support various requirements, one of the most important being data ownership [10].

In global trade, still a lot of data is exchanged by paper documents or not captured in IT systems at all leading to incomplete and inconsistent data in various resources in trader networks. Exchanging paper documents means rekeying and/or copying data to other documents, leading to all types of errors and data inconsistency. Interoperability amongst traders is expected to increase completeness and consistency of data [11].

*Corresponding Author. Email: wout.hofman@tno.nl

This paper describes a number of phases for realizing an IT infrastructure based on Semantic Web technology for data capture by authorities [12], leading to improved risk analysis with a decrease in administrative burden by piggy backing on trader data [13]. First of all, the paper describes the issue of data capture by customs for risk analysis. These are requirements to the IT infrastructure described. Secondly, different options will be presented based on various technical solutions and, thirdly, a phased approach to the IT infrastructure will be described. The first phase of this IT infrastructure is already applied in trade lanes [14] as a controlled experiment [15]. Finally, we will draw conclusions and identify future work.

2. Container security data requirements

This section describes the issue of incomplete data for risk analysis by customs authorities for container security. Secondly, based on analysis of these risk analysis processes, two potential issues are derived. Thirdly, requirements to IT as a basis for solving these issues will be given.

2.1. Incomplete – and inconsistent data sets

This section identifies that the issue of incomplete data sets by customs relates to different legal procedures that have to be supported by traders. To improve risk analysis, reliable and complete trade data is required [4]. Authorities require the following data set for risk analysis purposes [2]:

- People and entities: who are involved in trade, e.g. buyer, seller, forwarder, and carrier. These people and entities compose chains in global trade networks. They can be a ‘trusted trader’ or Authorized Economic Operator (AEO) [13], which gives them a status in risk assessment.
- Goods: the actual products with their packaging shipped from a seller to a buyer or transported from one or more production sites to distribution centers or warehouses.
- Historic data: data on previous goods shipped by people and entities between different countries. Historic data comprises trade patterns.

Currently, authorities capture only data based on declarations for legal procedures [16]. For international trade, export, re- export, import, transit, bonded warehousing, and landing procedures are specified. Whereas bonded warehousing, transit, and landing procedures consider packages, containers and possibly transport means for transit and landing in a port of call, export and import procedures relate to customs regimes. Transit is required in (EU) continental logistics, whereas intercontinental requires landing procedures. Export (or re-export) and import procedures consider the actual products shipped by a seller to a buyer. Sellers have to get approval of customs authorities in the country of origin of the products; buyers have to pay VAT (Value Added Tax) for bringing these products to the market in a country of destination. For landing procedures, authorities have imposed ENS submission from a port of loading, 24 hours prior to a loading of a vessel in that port. The ENS, submitted by a carrier or his agent, is incomplete, whilst:

1. It does not specify the contents of the cargo or containers. A carrier or his agent is not aware of the actual content of a container, also from a liability perspective [17].

2. It does not list the cargo or containers that are actually loaded on a vessel in a port of loading, e.g. changes to the loading can be made at the latest stage.

Literature states [13] that authorities can piggy back on data available by traders in the earlier mentioned pipeline. As the above illustrates, different procedures lead to different data sets. A complete and consistent data set can be based on data retrieval from all traders involved in logistic chains, thus constructing a complete view of different perspectives like product, cargo, containers and transport means. Current procedures only provide partial and inconsistent data sets: not all people and entities are mentioned and not all information on transported cargo is present, which could also lead to the assumption that historic data is incomplete.

2.2. Container targeting

The objective of customs is to target only suspicious containers that require inspection based on risks analysis rules implemented by a risk engine thus providing a seamless flow of goods to traders that behave according to legislation, creating so-called green lanes [2]. In this respect, there are two solutions to improve container targeting based on complete and consistent data sets. We will explain both.

The first solution is in line with existing procedures. Export/import and landing data retrieved from traders by declarations is fed into a risk engine. The result of risk analysis is:

- ‘Green’: no further action required by customs.
- ‘Orange’: possible suspicious, incomplete data set (section 2.1).
- ‘Red’: suspicious and physical inspection required.

For so-called ‘orange’ containers additional data needs to be retrieved to improve risk analysis. Some initial figures of customs authorities indicate that 20-25% of containers have code ‘orange’. Mostly, customs officials know which trader to consult to retrieve additional data for a proper decision.

A second solution is to gather data from all potential resources to construct a complete data set as input for risk analysis without increasing the administrative burden for traders, with the objective is to reduce the percentage of containers with code ‘orange’ and customs effort for risk analysis, and support seamless logistics. We will call this ‘smart risk analysis’. An IT infrastructure needs to offer functionality to customs (1) to know all potential traders as data resources, whereas these traders act global, and (2) the ability to piggy back on trader data [13].

2.3. Requirements to an IT infrastructure

A future proof IT infrastructure for container security must fulfill as set of basic functional and non-functional requirements as described in this subsection. The main functional requirements are: (a) complete and consistent data set, (b) the support of dynamic business relationships, (c) minimization of the administrative burden for individual stakeholders (e.g. traders), and (d) data ownership [10] and liability [17]. The main non-functional requirements are: (e) scalability (also called organic growth [9]) and performance, and (f) a migration strategy. One of the main issues of a migration strategy refers to the fact that an IT infrastructure developed within the context of the Cassandra project can still be used after the

*Corresponding Author. Email: wout.hofman@tno.nl

project is completed. Each of these functional and non-functional requirements is further elaborated in the subsequent paragraphs.

Complete and consistent data set. As stated in section 2.1, customs currently has incomplete data and is therefore not fully equipped to perform risk analysis compliant with authority guidelines [18]. In essence, customs are lacking data of packaging of products stuffed in containers. Furthermore, they do not have a complete view of all people and entities involved in shipment of goods from a country of origin to a country of destination (section 2.1). From a container targeting perspective (section 2.2), customs has to be able to complete the data set or perform smart risk analysis.

Dynamic business relationships. Continuous product - and service innovations lead to dynamic collaboration between the various stakeholders resulting in changing logistic chains [5]. There are various ways of building up such dynamic logistics chains. In most cases, there is not a single party that defines the entire chain. Instead, there is a hierarchical structure in a chain based on commercial relations: a seller requires a 'transport service' to deliver products to a buyer. To implement this 'transport service', one might need other services (e.g. dispatching, forwarding, shipping, etc.). These lower level services are not known to a buyer or seller. Depending on logistic - and commercial optimizations, different organizations can be involved (e.g. a different carrier or shipping line, depending on the time of delivery). Following such a layered approach, the chain is built up and evolves dynamically.

An IT infrastructure should not limit organizations in their choice to perform business. The support of dynamic business relations has consequences for interoperability when it comes to data sharing. It needs to support ever changing links between parties and there is no overall chain coordinator. Each organization controls its part of a chain. Based on organizational autonomy, each organization must be able to deliver its particular services. Those services must not be restricted to particular (pre-defined) roles. For instance, organizations do not conform to a standard 'forwarder' service template, each has its particular services. Moreover, an IT infrastructure should support improved data sharing as a competitive advantage, lowering the barriers to trade for some.

Administrative burden. Stakeholders in logistics chains already face an administrative burden, in one country more than another. As such, an IT infrastructure should at least not increase but at most minimize the administrative burden. Moreover, a potential decrease in the administrative burden may for many stakeholders provide the incentive to adopt a proposed IT infrastructure.

Data ownership and liability. Data ownership is considered to be a major issue for business to not participate in collaboration and providing data to third parties. IT security measures have to be implemented for Identification, Authentication, and Authorization (IAA) for authorized data access. Another issue is that traders do not always want to have all data, because it increases their liability and thus the assurance premium for transport [17]. Instead, they just require data for their value proposition [5]. An IT infrastructure should deal with data ownership and liability to increase its acceptance by both traders and authorities, whilst still providing the complete data set to authorities based on the piggy backing principle [13].

Scalability and performance. By their distributed nature supported by many traders, logistic chains are currently scalable, available, and performance is given by availability and performance of physical processes and resources like vessels, road infrastructure, etc. Scalability of an IT infrastructure implies that new stakeholders can easily connect to the infrastructure to support new logistic chains, others than the ones validated by the Cassandra project, which is also known as seamless interoperability or – integration [19]. It also implies low entry barriers for new stakeholders, especially Small and Medium-sized Enterprises (SMEs) with a relatively low IT maturity [20]. Performance of supply chains relates to logistic services offered by individual actors. An IT infrastructure should not impose any limitations on business in terms of this business wise specified and implemented availability, scalability and performance.

Migration. An IT infrastructure has to be implemented in a sector of the society that is very dynamic, has a great many stakeholders with a large population of SMEs, operations continuity is of large economic importance, (large) enterprises already have legacy IT, and a number of service providers is active as Business Community Systems (BCS) operating in ports (e.g. Port Community Systems (PCSs) like Portbase for the Rotterdam - and Portic for the Barcelona port), within a country (e.g. Eastport Technology in China or tradeXchange in Singapore) and across country boundaries (e.g. Descartes). These BCSs are privately owned (Descartes), others are installed by customs to increase data quality (e.g. Eastport Technology) or owned by a trader community (e.g. PCSs). Supply chain visibility platforms are a last category of available IT solutions, e.g. the ones based on EPCIS of GS1 [9] or SICIS developed by the EU FP7 SEC Integrity project for terminal milestone. Hence, for a successful introduction of an IT infrastructure, a smooth migration should be enabled and stipulated that should not only support the as-is situation, but also the to-be ('keep the shop open') with optimal re-use of existing functionality. This is approach is both applicable to traders and to customs authorities, implying for instance that a number of customs procedures will exist alongside the proposed IT infrastructure.

3. Technical options for a complete data set in logistic chains

An IT infrastructure is all about authorities retrieving a complete data set for risk analysis. Data can be retrieved using different technical solutions. Quite a number of these solutions are based on an Event Driven Architecture (EDA) [21] supported by supply chain visibility platforms [7]. Other solutions combine an EDA solution based on EPCIS [9] with a Service Oriented Architecture (SOA) [21] or Resource Oriented Architecture (ROA) [22] to retrieve additional data [12]. The SOA solution has already been experimented [23] and not scalable to include additional trade lanes. It showed, however, that procedures could be simplified with increased data visibility.

There are two issues identified in an EDA solution [9] relevant to data retrieval by customs. The first issue is the discovery of events: which traders need to be queried on additional data for specific cargo data? Two potential solutions are proposed, one of which is the preferred one. The first solution is a Directory Service (DS) registering systems of traders as resources. This solution implies that a query for additional needs to be submitted to all registered systems leading to potentially a large number of queries to assess additional data for targeting (section 2.2). By mentioning the trader to be queried as known to customs (section 2.2), a DS only identifies the system of that trader for querying. The second solution is a so-called Aggregated Discovery Service (ADS). An ADS stores basically all events on objects generated by a trader in a central store as well as a local EPCIS store [9]. A query for additional container data is evaluated by the ADS to submit that query only to only those traders that have actually events registered for that container. Security mechanisms can be

*Corresponding Author. Email: wout.hofman@tno.nl

implemented in the ADS to prevent unauthorized access to data (see the issue of data ownership in section 2.3).

The ADS solution is the preferred one by Lorenz [9], since it optimizes the number of queries. It can also support events for a great variety of objects, including business documents like purchase orders. However, this solution implies that an ADS stores all sources that have a particular event on an object, thus is potentially a (global) supply chain visibility platform. Data ownership might become an issue, depending on a governance model of such a solution. The second issue identified by Lorenz [9] states that there will not be one ADS, but federated ADSs are required. This subject is identified for future research [9]. An EDA solution combined with SOA for retrieving additional data can be a good basis for retrieving additional data of so-called 'orange' containers (section 2.2).

A smart risk analysis solution as proposed in section 2.2 requires that all data like specified in section 2.1 is available to a risk engine for risk analysis. Events are not required, since data needs to be retrieved from all available trader systems by for instance SOA [13] or ROA [22]. A DS for identifying relevant data sources is required, but an ADS not.

SOA or ROA are technical solutions to support smart risk analysis. Another solution is given by Linked Open Data (LOD) [12]. LOD assumes that sources publish their data to be retrieved by others. Like in SOA solutions, LOD considers also the semantics and syntax of published data. Berners-Lee [24] distinguishes four stages to publish data, ranging from publishing resource identifiers in for instance a DS to RDFs (Resource Description Framework schema) according to agreed semantics specified by an ontology (Ontology Web Language - OWL) with (RDF) links to other sources. In our case, these links would relate to other traders, with whom business documents are exchanged, e.g. from a seller/shipper to a forwarder. There are three approaches to evaluate these links [12]:

- Crawling: data is captured at regular time intervals from resources registered in a DS. This approach is comparable to a search engine, but needs to be applied to semantics known to customs. There are platforms like CKAN that offer this type of functionality and provide an Application Programming Interface (API) that could be used by a risk engine.
- On the fly dereferencing: links in data captured from a resource lead to capturing data from resources identified by these links. This approach can be used to capture additional data of containers with code 'orange' (section 2.2).
- Query Federation: a data source receiving a query initiates a query to another data source based on a link. In terms of container targeting, it implies that a customs query received by a trader initiates new queries to other traders participating in the same logistic chain.

The crawling mechanism, also known as pull in trade [13], seems a good solution for smart risk analysis. On the fly dereferencing could be a solution of a customs authority to retrieve additional data in the current procedures, whereas combined with query federation it might support a federated ADS [9]. A SOA, ROA, or LOD approach for data retrieval by customs requires additional security mechanism [25].

4. A proposed IT infrastructure for compliance management

This section describes a phased implementation of an IT infrastructure meeting requirements given in section 2 and technology evaluation in section 3. Table 1 presents an overview of the phases that will be described in more detail in this section. Issues like harmonization of interfaces for Business to Business integration (B2Bi) are part of this discussion. The basic innovation is in phase 3 of the infrastructure where seamless interoperability [19] based on value propositions [5] is under development, and phase 4 where authorities crawl logistics value webs [12] for compliance management and risk analysis.

Table 1. Overview of the phases for the IT infrastructure.

Phase	Name	Description
Phase 1	Experiments	A basic infrastructure to support controlled experiments
Phase 2	Backbone Infrastructure	Upstream data retrieval to support new controlled experiments
Phase 3	Trader Interoperability	Piggy backing on trader data with improved quality and completeness by interoperability in dynamic chain configurations
Phase 4	Secure Trade Based on Smart Risk Analysis	Seamless logistics based on customs risk analysis with complete and high quality data

4.1. Phase 1: experiments

The first phase supports controlled experiments in Living Labs (LLs) for retrieval of additional container targeting data in a so-called customs dashboard (section 2.2). Besides testing different technical solutions and configurations, the main objective is to discover (a) whether it leads to improved data quality for customs and (b) has additional value for business resulting in a business case for an infrastructure. The technical solutions for interfacing to customs will be evaluated in a trade lane (1) based on EDA with EPCIS solution(s), (2) with a push mechanism to share data via BCSs in different countries, and (3) a combination of both. Customs authorities participating in the experiment can access data via a web service (SOA), independent of the underlying technical solution. In the third experimental setting, the BCSs also have to act as EPCIS systems. First results of these experiments indicate only a positive business case for one of the experiments, i.e. a UK based trader with additional data entry by a container stuffing operator in China, whereas the results of the other experiments are not (yet) satisfactory. The experiments are the basis for a Backbone Infrastructure.

4.2. Phase 2: Backbone Infrastructure

The second phase offers an infrastructure that can be easily extended with new experiments, e.g. (1) new trade lanes and (2) new customs authorities. It should be easy for traders to link into the Backbone and provide additional data to customs authorities via this backbone. However, it also should be easy for new BCSs to become part of the Backbone, based on interface specifications resulting from the experiment that enable organic growth of the backbone.

*Corresponding Author. Email: wout.hofman@tno.nl

Constructing the Backbone Infrastructure requires a number of issues to be solved. One of these issues relates to customs access of the backbone. The following solutions are feasible that need to be evaluated after completing the experimental phase:

1. One (or more) DS(s) governed by authorities registering available backbone systems. The number of queries for additional data might increase leading to decreased performance. In case each authority has a DS, backbone systems need to register in each DS. Traders either register with one of the backbone system or participate as a backbone system themselves.
2. One (or more) DS(s) governed by backbone systems and each customs authority interfacing with only one backbone system. The backbone systems must have a query federation mechanism (section 3) to retrieve additional data from systems in other countries or may already have the data available based on a push mechanism implemented by the backbone systems.
3. One (or more) ADS(s) governed by authorities to query only those backbone systems that can provide data. It implies that an ADS has to receive events triggered by a trader linked to one of the backbone systems. An alternative is to implement one (or more) ADS(s) governed by backbone systems. Each authority links to one ADS.
4. Use on the fly dereferencing of links between traders in combination with a DS for identifying backbone systems (section 3). In this case, the links need to be stored by the backbone systems. Outcome of the evaluation of the Living Lab Backbone might be that the backbone systems already have all required data and this solution is not required.

The issues of data ownership and liability also need to be solved. IT security mechanisms must be in place to prevent unauthorized access to trader data stored by a backbone system. These IT security mechanisms can be agreed between the backbone systems and authorities that would like to access these systems [25]. Furthermore, the experimental phase must provide clear business cases for traders and customs authorities to participate and BCSs to develop a business model.

4.3. Phase 3: Trader Interoperability

In the previous phases, traders can also participate in the backbone or can use a backbone system to act on their behalf. Trader interoperability is not a prerequisite. Since there are many traders that need to become interoperable, a Backbone Infrastructure will address the adoption of interoperability for those traders. However, traders may also have their own B2Bi profiles. In most cases, these B2Bi profiles each have their particular semantics, although they may use the same syntax [26] and are able to share data electronically. The focus of this phase is achieve full interoperability amongst traders; they have to be seamless interoperable and offer their logistic service for dynamic supply chain configurations [5]. There have been various approaches to solve this issue, e.g. electronic business XML is one of the proposed solutions [27]. One of the approaches of ebXML is to standardize the earlier mentioned B2Bi profiles at process level, but they did not consider data semantics. Although it is feasible to model a process between two organizations, ebXML was never widely applied by business. Another approach is to apply the so-called Common Framework [28]. This framework is not yet taken up by business and supported by an IT infrastructure for traders to become interoperable.

An alternative solution to seamless interoperability is based on modeling value propositions [5], relate these to a B2Bi profile and thus construct a Logistic Service Profile (LSP) of a trader. These LSPs can be published by a trader at his website or in a Business Service Registry (BSR). Data ownership and liability requirements will be dealt with in Business Communities (BC). The proposed solutions are currently investigated and will be developed as a Proof of Concept for testing in descriptive scenario's [15]. Based on the results, the IT infrastructure for seamless interoperability is expected to become available by 2015.

Customs access to the IT infrastructure is based on LOD concepts [12] (section 3) by accessing business events of traders that have registered their services in a BSR [29] with access control mechanisms specified by a (national) Customs Business Community [25]. Traders can register in this community, which is similar to so-called Trusted Trader or EORI databases currently maintained by customs. Governance of BSRs and BCs is yet to be investigated. Each customs authority is able to access those traders that have registered themselves in the Customs-BC. In case a trader is registered in a Customs-BC governed by another customs authority, federation mechanisms will have to be implemented [25].

A trader can register by one Customs-BC. In case that trader needs provide data for goods movements to other authorities than the one governing that BC, those authorities need to receive an event of that trader. Currently, an ENS is such an event, that also carries data. A customs authority can use this event to launch an on the fly dereferencing query (section 3) with the particular trader generating the event. The latter query allows the authority to gather details of the supply chain in another country. It requires that two (or more) Customs-BCs form a chain of trust [25].

4.4. Phase 4: Secure Trade with Smart Risk Analysis

Secure Trade based on trader interoperability provides high quality data to authorities for Smart Risk Analysis (section 2.1) of all logistics chains stemming from, going to or passing its area. This is in fact the to-be situation, in which each authority crawls data of traders registered with its Customs-BC, receiving events of foreign traders, and cross-validating chain data with external sources representing people and entities and historic data (section 2.1). Each customs authority has a complete data set of all goods movements in its area, crawling other customs authorities or using events with on the fly dereferencing (section 4.3) to complete this data set with incoming or outgoing goods.

In this to-be situation, only export, re-export, import, and possibly bonded warehousing procedures need to be implemented. These procedures reflect the start, end and relevant intermediate events for an authority. It is expected that, although a lot of research needs to be done, customs IT systems will greatly simplify and the administrative burden of traders will reduce drastically. If a particular customs authority also implements System Based Auditing with periodic reporting like already feasible in current customs legislation (MCC: Modernized Customs Code), administrative burden would be minimized for traders.

*Corresponding Author. Email: wout.hofman@tno.nl

5. Conclusions and further research

This paper presents an innovative IT infrastructure for compliance management based on applying semantic web concepts [7]. It reduces the administrative burden and yet provides secure trade. Phase 1 is currently performed [14] as a controlled experiment [15] with a limited number of traders. A proof of concept is developed for phase 3 and can be tested by 2014 supporting descriptive scenario's [15]. The last phase, Secure Trade with Smart Risk Analysis, is for future research and is expected to change collaboration of customs and trade leading to simplified trade procedures for secure trade [30]. A first description of a compliance management monitor based on business event monitoring is already available [29].

Based on the current (intermediate) results of the experiments, it will be difficult to evolve to the backbone. Possibly other solutions need to be evaluated by which customs authorities have easy access to additional data required for risk analysis, e.g. evaluating links retrieved from an ENS and requesting additional data of for instance forwarders or shippers. Possibly, each authority has to set up a community of based on international agreed interfaces and links of participating traders. According to EU legislation (MCC), customs is able to request this additional data; they do it currently by using traditional communication means like telephone.

6. Acknowledgement

This paper results from the CASSANDRA project, which is supported by funding from the 7th Framework Programme of the European Commission (FP7; SEC-2010.3.2-1) under grant agreement no. 261795. Ideas and opinions expressed by the authors do not necessarily represent those of all partners.

7. References

[1] J. Hintsa, J. Ahokas, K. Zaghbour, T. Mannisto, A. Hameri and H. J., "Conceptual model for assessing cost of security in global supply chains," in *17th International Annual EuroOMA Conference*, Porto, 2010.

[2] D. Heshket, "Weakness in the supply chain: who packed the box?," *World Customs Journal,* vol. 4, no. 2, 2010.

[3] E. v. Stijn, D. Hesketh, Y.-H. Tan, B. Klievink, S. Overbeek, F. Heijmann, M. Pikart and T. Butterly, "The Data Pipeline - discussion paper," in *Global Trade Facilitation Conference 2011 - Connecting International Trad: Single Windows and Supply Chains in the Next Decade*, 2011.

[4] S. Overbeek, B. Klievink, D. Heskeht, F. Heijman and Y.-H. Tan, "A Web-based data pipeline for compliance in International Trade," in *WITNESS workshop*, Delft, 2011.

[5] J. K. S. Spohrer, "Service Science, Management, Engineering, and Design (SSMED) - An emerging discipline - Outline and References," *International Journal on Information Systems in the Service Sector*, May 2009.

[6] W. J. Hofman, "Supply chain risk analysis based on Linked Open Data," in *eGov2011-WITNESS*, Delft, 2011.

[7] T. Berners-Lee, J. Hendler and O. Lassila, "The Semantic Web," *Scientific American,* pp. 28-37, 2001.

[8] P. Diessner and M. Rosemann, "Supply Chain event management managing risk by creating visibility," Solutions Management SCM, SAP AG, Walldorg, Germany, 2008.

[9] M. Lorenz, J. Muller, M.-P. Schapranow, A. Zeier and H. Plattner, "Discovery services in the EPC network," *Designing an Deploying RFID Applications, Intech,* pp. 109-130, 2011.

[10] C. Kuerschner, C. Condea, O. Kasten and T. F, "Discovery Service Design in EPC global Netowrk: towards full supply chain visibility," in *International Conference, IOT2008*, 2008.

[11] Berre'A-J, B. Elvesaeter, N. Fiay, C. Guglielmina, J. S.G., D. Karlsen, T. Knothe and L. S., "The ATHENA

Interoperability Framework," in *IESA2007*, Berlin/Heidelberg, 2007.

[12] T. Heath and C. Bizer, Linked Data - evolving the Web into a Global Data Space, Synthesis lectures on the Semantic Web: Theory and Technology, Morgan & Claypool Publishers, 2011.

[13] B. Rukanova, N. Bjorn-Andersen, F. v. Ipenburg, S. Klein, G. Smit and Y.-H. Tan, "Introduction," in *Accelerating Global Supply Chains with IT-innovation*, Springer, 2011.

[14] E. v. Stijn, B. Klievink, M. Janssen and Y.-H. Tan, "Enhancing business and government interactions in global trade," in *Third International Engineering Systems Symposium - CESUN 2012*, Delft, 2012.

[15] A. Hevner, S. March, J. Park and S. Ram, "Design Science in Information Systems," *MIS Quarterly*, pp. 75-105, 2004.

[16] World Customs Organization, "WCO Data model - cross border transactions on the fast track," World Customs Organization, 2010.

[17] United Nations, "Rotterdam Rules," 2008. [Online]. Available: http://www.uncitral.org/pdf/english/texts/transport/rotterdam_rules. [Accessed 2012].

[18] U.S. Customs and Borde Protection Agency, "Container Security Initiative - 2006-2011 Strategic Plan," U.S. Customs and Borde Protection Agency, 2006.

[19] C.-M. Chituc, A. Azevedo and C. Toscano, "A framework proposal for seamless interoperability in a collaborative networked environment," *Computers in industry*, vol. 60, pp. 317-338, 2009.

[20] Consultrans, "ICT and e-Business Impact in the Transport & Logistics Industry - a sectoral e-Business watch study," European Commission, DG Enterprise & Industry, Brussels, 2008.

[21] T. Erl, Service Oriented Architecture - concepts, technology and design, Prentice-Hall, 2005.

[22] B. Sletten, "Resource-Oriented Architectures: being "in the Web"," in *Beatiful Architectures-Leading thinkers reveal the hidden beauty in software design*, O'Reilly Media, 2009, pp. 89-110.

[23] Y.-H. Tan, W. Hofman, J. Gordijn and J. Hulstijn, "A framework for the design of service systems," in *Implementing Service Science*, Springer-Verlag, 2011.

[24] T. Berners-Lee, "Linked Data - four rules," 18 June 2009. [Online]. Available: www.w3.org.DesignIssues/LinkedData.

[25] J. v. d. Berg, P. Pruksasri and W. J. Hofman, "Three protocols for securing the data pipeline for the International Supply Chain," in *International Conference e-Commerce*, Lisbon, 2012.

[26] W. J. Hofman, "Applying semantic web technology to interoperability in freight logistics," in *e-Freight2011*, Munich, 2011.

[27] A. Kotok and D. Webber, ebXML - the new global standard for doing business over the Internet, New Riders, 2002.

[28] EURIDICE, "Integrated Cargo Framework version 1.0," EURIDICE, 2010.

[29] W. Hofman, "Compliance management by business event mining in supply chain networks," in *VMBO2013*, Delft, 2013.

[30] A. Naber, W. Hofman, B. Enserink and B. Kotterink, "Rethinking the Digital-Era governance: the case of e-customs in the EU," *Journal of Public Administration Research and Theory.*

*Corresponding Author. Email: wout.hofman@tno.nl

Authors

Wout Hofman:

Wout J. Hofman is a senior research scientist with TNO since 2006 in the area of semantic interoperability. Before joining TNO, Wout has been fulltime consultant (1984-2006) in development and implementation of large scale national and international projects in for instance customs and logistics. Within TNO, Wout is actively involved in open data -, government – and EU funded logistics projects like Cassandra and iCargo. Wout received a Ph.D. in informatics (1994) on the subject of transaction management systems in logistics.

Harrie Bastiaansen:

Harrie J.M. Bastiaansen received his M.Sc. degree in mathematics, (cum laude), in 1988 and his Ph.D. degree for his dissertation on guided wave simulation in 1994. From 1993 until 2003 he worked for KPN Research and KPN Telecom on high-speed, public telecommunication data networks. Currently, he works for TNO with specialization on large scale IT-infrastructures, Enterprise Application Integration and IT-governance. Since 2011 he is actively involved in interoperability architectures for large scale logistics ecosystems., working in EU funded logistics projects like Cassandra and iCargo.