Technical Requirements of the e-Waybill Service

Shoaib Bakhtyar[1*], Johan Holmgren[1, 2], Jan A. Persson[1, 2]

[1] Department of Computer Science and Engineering, Blekinge Institute of Technology, Karlskrona, Sweden.
[2] Department of Computer Science, Malmö University, Malmö, Sweden.

* Corresponding author. Tel.: 0046734223921; email: shoaib.bakhtyar@bth.se

Abstract: An electronic waybill (e-Waybill) is a service whose purpose is to replace the paper waybill, which is a paper documents that traditionally follows a consignment during transport. An important purpose of the e-Waybill is to achieve a paperless flow of information during freight transport. In this paper, we investigate five e-Waybill solutions, that is, system design specifications for the e-Waybill, regarding their non-functional (technical) requirements. In addition, we discuss how well existing technologies are able to fulfil the identified requirements. We have identified that information storage, synchronization and conflict management, access control, and communication are important categories of technical requirements of the e-Waybill service. We argue that the identified technical requirements can be used to support the process of designing and implementing the e-Waybill service.

Key words: E-Waybill, e-Waybill service, system design, technical requirements.

1. Introduction

An electronic waybill (e-Waybill) is a service that provides the functions of a paper waybill, and which is capable of storing, at least, the information present in a paper waybill [1]. An important purpose for using an e-Waybill is to enable faster (paperless) transfer of information during freight transport (see, e.g., [2]). In addition, e-Waybills contribute towards reducing the administrative overhead typically associated with paper waybills: paper waybills need physical storage space and sometimes require (mainly in transport involving multiple carriers) the same information to be written on several waybills. Furthermore, the authors in [1] recently argued that the potential synergies between an e-Waybill and other services could lead to increased utilization of intelligent transport systems (ITS) services. In turn, this could lead to more sustainable transport, for example, by enabling more efficient use of vehicles and transport infrastructure.

There exist several examples of electronic replacements of the paper waybill. The International Air Transport Association (IATA) implemented an e-Waybill for air freight transport, which is referred to as an e-Air Waybill [3]. Mei and Dinwoodie [4] proposed an electronic version of the bill of lading, that is, the consignment document used in sea transport. For road transport, the company DHL implemented the DHL Express Waybill (see, [5]). Finally, a multi-modal e-Waybill, which is an important initiative for achieving the vision of using a single transport document during a consignment, was proposed in the e-Freight project [5]. The e-Freight project also identified a number of implementation challenges, that is, accessibility, communication, security, ownership, and authentication, which should be considered when implementing their e-Waybill. As part of their analysis of synergies between an e-Waybill and other ITS services, five e-Waybill solutions are recently suggested in [1], which can be seen as abstract system design

specifications for the e-Waybill service. The five solutions differ in where (at back-office and/or at the freight level) the e-Waybill information is stored, and where e-Waybill users are allowed to read and write e-Waybill information. A common property of the earlier e-Waybill initiatives is that they are based on storage of the e-Waybill information only at back-office (i.e., in a back-office system), whereas the solutions in [1] also considers information storage by the freight.

In this paper, which is an improved version of Chapter 2 of the Licentiate thesis by S. Bakhtyar [6], we contribute an extended analysis of the e-Waybill solutions provided in [1]. In particular, we identify and elaborate on the non-functional (technical) requirements of the solutions. We consider this to be important in order to support the implementation of an e-Waybill service that make use of storage both at back-office and by the freight. We regard the identification of the technical requirements of the e-Waybill service and the elaboration of technologies that can be used to implement the requirements as the main contribution of this paper.

The paper is organized in the following way. Our research methodology is presented in Section 2, followed in Section 3 by a discussion on the e-Waybill service and the recently proposed solutions for implementing the e-Waybill. The technical requirements for the e-Waybill solutions are identified in Section 4, followed in Section 5 by a detailed discussion on the identified technical requirements. The paper is concluded in Section 6.

2. Methodology

The requirements of a system are usually classified as functional and non-functional, where the functional requirements define what the system should do, and the non-functional requirements define how to achieve the functional requirements. Non-functional requirements can also be defined as attributes or constraints on a system [7], and they may have a significant effect on the design and implementation decisions taken during the development of a system [7]. There exist several methods that can be used to identify the functional and non-functional requirements of a system. We used the structured analysis and design technique (SADT) method in [8], which is regarded as a classical work on requirements engineering, in order to identify the functional and non-functional requirements of the e-Waybill service (see also, [9], [10]).

SADT suggests that the requirements of a system should be identified in a process involving three steps. The first step concerns identifying the context, and it should establish why the system is needed. The purpose of the second step is to identify what the system should do, by identifying what features are required in order to allow the system to operate in its context. The third step concerns identifying the non-functional (technical) requirements of the system, by determining how the system should be constructed.

The first two steps of SADT were implicitly addressed in previous work [1]. In this paper, the focus is on the third step, which we use in order to identify the technical requirements of the e-Waybill service. We derive these requirements by analyzing the implications of the functional requirements from the perspective of the five e-Waybill solutions suggested in [1]. Additionally, by studying the literature, we identify the existing technologies with potential to fulfil the technical requirements of the e-Waybill service. For each of the five e-Waybill solutions, we then elaborate on how the identified technologies are able to fulfil the technical requirements of the service. It should be mentioned that a functional requirement typically can be mapped into one or more technical requirement [11]. We argue that this justifies our approach of using the functional requirements as a starting point for identifying technical requirements.

3. E-Waybill Service and Solutions

We define an e-Waybill as a service that provides the functions of a traditional paper waybill, and which is capable of storing, at least, the information present in a paper waybill. Furthermore, we refer to an e-Waybill solution as a design specification for the e-Waybill service. As mentioned above, the five solutions suggested in [1] differ in where the e-Waybill information is stored, and where read and write access are provided to the e-Waybill information. The e-Waybill information can be stored in an information system at the back-office (i.e., at the back-office level) and/or by the freight (i.e., at the freight-level), which is often inside the vehicle. It should be noted that access to information at the freight-level typically requires physical access to the freight. The two storage locations gives, together with the three properties of storage, and read and write access, the following six properties that can be used to define e-Waybill solutions:

1) The e-Waybill information is stored at back-office.
2) The e-Waybill information is stored by the freight, for example, in a hand-held device or on RFID tags.
3) Read access is given to e-Waybill information stored at back-office.
4) Read access is given to e-Waybill information stored by the freight.
5) Write access is given to e-Waybill information stored at back-office. It should be noted that the write access includes the possibility to update already written e-Waybill information.
6) Write access is given to e-Waybill information stored by the freight.

Based on these 6 properties, the authors in [1] identified the five e-Waybill solutions that are specified in Table 1.

It is important to mention here that for e-Waybill solution 5, a copy of the e-Waybill should also be stored at the back-office; however, this copy of the e-Waybill is not synchronized with the e-Waybill stored by the freight. Hence, the up-to-date e-Waybill information is only present at the freight-level.

Table 1. The e-Waybill Solutions Identified in [1]

Solution	Back-office			Freight-level		
	Storage	Read	Write	Storage	Read	Write
1	yes	yes	yes	no	no	no
2	yes	yes	yes	yes	yes	yes
3	yes	yes	yes	yes	yes	no
4	yes	yes	no	yes	yes	yes
5	no	no	no	yes	yes	yes

4. Requirements Identification

In this section, we present the technical requirements of the e-Waybill service, which we have identified by following the SADT method (see Section 2). The first and seconds steps of the method have been mainly addressed in [1], and they are discussed in the two first subsections of this section. The third step, whose outcome is the main contribution of this paper, and in which the technical requirements are identified, is discussed in the third subsection of this section.

• Step 1: Why is an e-Waybill service needed?

As discussed in Section 1, the e-Waybill service, as an electronic replacement of the paper waybill, has potential to contribute to a paperless flow of information in freight transport and faster flow of freight information Additionally, the e-Waybill service may reduce the administrative costs that are typically associated with paper waybills, for example, since paper waybills need physical storage space, and since there are situations (mainly in transport involving multiple carriers) that require that the same information is written on several waybills. By utilizing on synergies between ITS services, the e-Waybill service, if implemented with storage of the e-Waybill information both at back-office and at the freight-level, also has the potential to contribute to increased use of ITS services.

- Step 2: What are the functional requirements of the e-Waybill service?

As an electronic replacement of the paper waybill, the e-Waybill service should provide the same functions as the paper waybill:

1) It should be able to prove that there exists a contract for transport, which is important since there should exist an agreement specifying the conditions for transport.
2) It should be able to show which actors have been in control of the consignment, who is currently in control, and who will be in control in the future.
3) It should be able to store the essential consignment information.

We also consider authorized read and write access to the e-Waybill information as a functional requirement (requirement four) of the e-Waybill service, even though this is not directly implied from the functions of a paper waybill. The reason is that an e-Waybill, in particular when back-office storage is used, has the potential to be accessed by users without physical access to the storage medium, which is not the case for a paper waybill. Bakhtyar *et al.* [1] argue that the five considered e-Waybill solutions, which specify the locations for storage, and read and write access to the waybill information, are capable of providing the identified functions of the e-Waybill service. We have therefore chosen to use the five e-Waybill solutions provided in [1] as input to the technical requirement specifications step (step 3 of SADT), which is presented in the next subsection.

- Step 3: What are the technical requirements of the e-Waybill service?

As mentioned above, we based the technical requirement identification process on the identified functional requirements of the e-Waybill service and the three properties of storage, and read and write access, which are central in the considered e-Waybill solutions. The identified technical requirements are further discussed in Section 5.

There are several technical requirements concerning the third functional requirement, that is, that the e-Waybill should be able to store the essential e-Waybill information. Each of the five e-Waybill solutions specifies whether the e-Waybill information should be stored at back-office, by the freight, or at both of these locations. The types of storage medium needs to be chosen in a way that it allows read and write access to the e-Waybill information at the location(s) where read and write access should be provided, respectively. In addition, the storage medium needs to be large enough to store all relevant e-Waybill information, as well as any other information that is considered relevant to store. To address the functional requirement of read and write access (the fourth requirement), the e-Waybill information may be read and written only by authorized actors, and there should exist some type of mechanism to enable authorized read and write access. Hence, we regard access control, including authentication control, as an important technical requirement of the e-Waybill. It might also be relevant to store the e-Waybill information in an encrypted form, which is important, for example, in situations where it is impossible to prevent physical access to the storage medium.

To address the first and second functional requirements of the e-Waybill, that is, it should be able to prove that there exists a contract for transport and it should be to show which actors been (currently is and will be) in control of the consignment, we also consider communication as an important category of technical requirements. In order to enable read and write access to the e-Waybill information, there needs to exist fast and reliable communication links between the e-Waybill information storage locations and the actors with access rights. The communication links may be permanently active, or active only when an actor or a system needs to access the information. When the e-Waybill information is stored both at back-office and by the freight, there also needs to exist communication links between the two e-Waybill information storage locations. Finally, it is important to emphasize that the communication links need to be secure enough to ensure that only authorized users are able access the e-Waybill information in clear text,

that is, in an unencrypted form.

For the e-Waybill solutions 2, 3, and 4 (where the e-Waybill information is stored, and can be read, both at the back-office and by the freight) there is a need for synchronization in order to make sure that an up-to-date version of the e-Waybill information is available for read access at both of the storage locations: the updates made at one location need to be made also at the other location. Conflict management is needed in solution 2, where write access is provided at both of the storage locations, in order to deal with conflicts that may occur due to simultaneous updates. In summary, we have identified four categories of technical requirements, which we further elaborate on in the next section, that is, 1) information storage, 2) access control, 3) communication, and 4) synchronization and conflict management.

5. Discussion on the Technical Requirements

In this section, we provide a detailed discussion on the identified technical requirements of the e-Waybill service. In addition, we elaborate on existing technologies, which might be used to fulfil the identified requirements.

5.1. Information Storage

The type of e-Waybill information is necessary to take into account, when choosing the type of storage media to use, because different types of information puts different requirements on the storage media. Some of the e-Waybill information remains static throughout a transport, for example, goods id and type, as well as specification of the consigner and the consignee. The e-Waybill also includes dynamic information, for example, the information about who is currently in control of the consignment, which is updated whenever a new actor (e.g., a carrier) takes over the responsibility for consignment. Barcode labels would work for static e-Waybill information; however, the limited storage capabilities of barcode labels typically make it impossible to use them for storing all of the e-Waybill information. An option would be to use a barcode label to store only the e-Waybill identifier, while the remaining information could be stored in a handheld device. For dynamic information, a possible choice is to use RFID tags, which have larger storage capabilities than barcode labels. The e-Waybill information may be also stored, potentially in combination with other storage medias, in handheld devices, and in the On Board Unit (OBU) of a vehicle or in similar systems, for example, in terminals. A handheld device with barcode or RFID tag reading capabilities can be used to scan the goods, and transmit information to other storage medias, such as an OBU. At back-office, for example, a customer order system or an Electronic Data Interchange (EDI) system (see, e.g., [12]), is capable of storing the e-Waybill information. In addition, the storage media should have the capability to allow read and write access to the e-Waybill information. For the e-Waybill information stored at back-office, this can be achieved via an Internet connection. At the freight-level, there are different options for storing the e-Waybill information. For example, actors with physical access to the freight may connect to the e-Waybill using a handheld device with capabilities to read barcode labels or RFID tags. As mentioned above, information can also be stored in OBUs or in similar systems, which may be accessed using short distance wireless communication.

The storage media should have the capability to allow only legitimate actors to access the e-Waybill information. This can be achieved by using some kind of authentication control mechanism, for example, including an electronic signature. Access control mechanisms are further discussed in the next section. In order to further protect the e-Waybill information, there are situations where the information needs to be stored in an encrypted form. There exist several algorithms that can be used to encrypt and decrypt the e-Waybill information, for example, symmetric-key and asymmetric-key cipher techniques. At the back-office level, as well as in OBU's and handheld devices, any type of state-of-the-art cryptographic techniques (see, e.g., [2]) can be used. An example of a technique that can be used to together with RFID

tags is public-key cryptography, which was suggested in [13].

As mentioned above, the e-Waybill information may be stored by the freight using barcode labels, but their limited storage capabilities and non-line-of-sight, as well as the impossibility for multiple-tag simultaneous-reading from a short distance, make RFID more efficient than barcode labels [14]. RFID tags are a possible alternative because of their storing, updating, communication, and information security capabilities. An e-Waybill contains sensitive information about a consignment, and RFID tags have been earlier used to store sensitive information, such as biometric data and electronic signatures, for example, in passports [15]. Additionally, RFID tags have the capability to incorporate sensor readings, which makes it possible to use them in applications that require monitoring, asset management, and tracking [16]. Examples from the literature show that the integration of RFID and the Internet may enable supply chain management systems with capabilities such as inventory monitoring, and track and trace of goods [14], [17], [18].

5.2. Access Control

There exist several mechanisms that can be used in order to control who should be allowed to access what resources, for example, role-based access control, task-based authorization control, and the fine-grained object approach (see, [19]). For each of the e-Waybill solutions specified in Table 1, there needs to be proper authentication and authorization mechanisms at each of the locations where the e-Waybill information is available for read and/or write access. For example, in e-Waybill solution 2, which allows read and write access at both the back-office and by the freight, authentication and authorization access control needs to be implemented at both locations.

Authentication concerns proving that a user is the person who he or she claims to be. For the e-Waybill, the access control mechanism must ensure that only legitimate actors or systems should be able to use the service. In addition, a particular actor or system should only be given access to read and write e-Waybill information based on what they are authorized to do. Traditionally, username and password are used to authenticate actors who want to access a system. Another way to ensure that only authorized users are given access to the e-Waybill information is to use an electronic signature, which can be used in order to guarantee that only genuine actors are able to write e-Waybill information. There should be a mechanism to prove the integrity of an electronic signature, in order to validate that a particular signature is associated with a genuine actor or system. A private-public key encryption mechanism can be used to implement an electronic signature, where the signature is encrypted using the private key of the signer and decrypted using a public key by the verifier. A certification authority (CA) could be responsible for handling the public keys of an actor or system, and in that way verify that a particular actor or system is the owner of a particular public key [16].

For authorization control, there exist several models, which are all based on two authorization models, that is, mandatory and discretionary access control (see, e.g., [20]-[23]). We believe that a customized authorization mechanism should be developed primarily based on the preferences of the organizations using a particular e-Waybill system. The organization's preferences are important to consider, because different organizations may have different policies for accessing the e-Waybill information. It should be up to the involved organizations to decide which e-Waybill information to be accessible by a particular actor.

5.3. Communication

For enabling the users to access the e-Waybill, there should exist communication links between the storage locations (where access is provided) and the actors with access rights. As will be discussed in the next subsection, for the e-Waybill solutions that store the e-Waybill information both at the back-office and by the freight, there also needs to exist a communication link for synchronization between the two storage

locations. The communication links need to be active only when the e-Waybill information is accessed or synchronized.

The distance over which communication needs to occur may have implications on the type of communication link that could be used. The e-Waybill information stored at back-office may typically be accessed using an Internet connection. In this case the communication distance does not really matter, since the Internet is accessible worldwide. For actors with physical access to the freight, communication could occur directly using a handheld device or short-distance wireless communication, for example, Bluetooth and Wi-Fi. Short-distance communication can also be used for communication in case multiple types of storage medias are used at the freight level, for example, both RFID tags and an OBU. Remote communication, which is important for synchronization purposes, requires that the e-Waybill information is stored in a device with an Internet connection.

In order to prevent unauthorized access to the e-Waybill information, the communication links need to be secured. For short distance communication, there exist networking techniques that enable secure communication, including Wi-Fi, Bluetooth, and ZigBee (see, e.g., [24], [25]). For communication over the Internet, there is typically a need to secure the information using cryptographic techniques.

5.4. Synchronization and Conflict Management

As mentioned in the previous subsection, there is a need for a communication link, for synchronization, between back-office and the freight-level, for those e-Waybill solutions that store e-Waybill information at both of the locations. Synchronization is important in order to make sure that up-to-date e-Waybill information is available at both storage locations.

In solutions 3 and 4, where the e-Waybill information may be written at only one location, at back-office in solution 3 and at the freight-level in solution 4, synchronization only requires replicating the up-to-date information from the location where write access is provided to the other location. In solution 2, write access is given both at back-office and at the freight-level, and simultaneous updates of the e-Waybill information may result in update conflicts. Therefore, there is a need for a conflict management mechanism.

Defining access rights (authorization) for different actors may be helpful in order to prevent conflicts, because limiting the access rights of the users as much as possible reduces the possibility of conflicts. As mentioned in Section 5.2, we believe that there is a need for a customized access control mechanism, since organizations typically have different actors with different roles. It should be up to the organizations involved in a consignment to define which parts of the e-Waybill information should be accessible, for read and write respectively, for a particular actor at a particular location. For example, a consigner may have access to the e-Waybill information only at the back-office, whereas a driver may only have access at the freight-level.

Another approach is to completely avoid update conflicts, for example, by using sessions (see, [26]) when updating the e-Waybill information. In this type of mechanism, only one actor (or system) is allowed to update (write) the e-Waybill information at the same time. Once an actor requests to update the e-Waybill information, a session manager locks the e-Waybill service for updates by other actors. If more than one actor wants to update the e-Waybill information at the same time, the session manager has a choice to use either a time-based or role-based access policy. In a time-based policy, the actors that request to update the e-Waybill information are placed in a queue, and in a role-based policy, importance is given to the role of an actor. In the latter case, a priority needs to be defined for each of a number of organizational roles.

6. Conclusion

We have identified and elaborated on the technical requirements for different system designs of the

e-Waybill service, based on the properties of storing and accessing the e-Waybill information at the back-office and at the freight-level. The identified technical requirements are derived from the functional requirements of the e-Waybill service and they concern aspects related to information storage, access control, communication, and synchronization and conflict management. In addition, we have discussed existing technologies regarding how they are able to fulfil the identified requirements.

We have considered five e-Waybill solutions, which can be seen as abstract system design specifications for the e-Waybill service (see Table 1). These solutions are of three types: solution 1 is a back-office solution, solution 5 is a freight-level solution, and solutions 2, 3, and 4 are both back-office and freight-level solutions, which differ only in where write access is given to the e-Waybill information. We conclude that there are technical requirements, which are common for all of the solutions, for example, the need to protect the e-Waybill information using cryptographic techniques and authorization control. There are also requirements that only concern some of the solutions, mainly synchronization and conflict management. For solutions 2, 3, and 4, where the e-Waybill information is stored (and read access is provided) both at back-office and by the freight, there is a need for synchronization in order to maintain up-to-date versions of the e-Waybill information at both locations. Solution 2 also requires a mechanism for resolving conflicts that may occur as a consequence of simultaneous updates. The reason is that solution 2 provides write access at both of the locations. For solutions 1 and 5, where the e-Waybill information is stored only at one location, there is no need for synchronization and conflict management. At back-office, where the e-Waybill information is typically stored in an information system, the identified technical requirements can be fulfilled using standard technologies. For example, access may be provided and controlled using an Internet connection and standard access control mechanisms. For information stored by the freight, there are typically more options regarding how to fulfil the technical requirements. The e-Waybill information may be stored, for example, directly on the freight (using barcode labels or RFID tags), in handheld devices, or in the OBUs of the vehicles that carry the freight. It is also possible to use multiple storage medias, where electronic communication needs to occur in between. For example, barcode labels could be used to store static information about a consignment, and other storage medias could be used to store dynamic information. Short distance communication may be based on technologies, such as Bluetooth and Wi-Fi. Long distance communications links using the Internet need to exist in order to enable synchronization and conflict management and to allow remote actors to access the e-Waybill information. It is important to secure these communication links using cryptographic techniques, in order to prevent unauthorized access to the e-Waybill information. In Table 2, we summarize the identified technical requirements for each of the five e-Waybill solutions.

Table 2. Technical Requirements of the e-Waybill Service

Technical requirements	e-Waybill solutions				
	1	2	3	4	5
Encrypted information storage	yes	yes	yes	yes	yes
Static and dynamic information storage	yes	yes	yes	yes	yes
Information storage by the freight	no	yes	yes	yes	yes
Information storage at back-office	yes	yes	yes	yes	no
Read access control by the freight	no	yes	yes	yes	yes
Write access control by the freight	no	yes	no	yes	yes
Read access control at back-office	yes	yes	yes	yes	no
Write access control at back-office	yes	yes	yes	no	no
Synchronization	no	yes	yes	yes	no
Conflict management	no	yes	no	no	no
Long distance communication links	yes	yes	yes	yes	no
Short distance communication links	no	yes	yes	yes	yes

The identified technical requirements may, to a large extent, solve the implementation challenges identified in the e-Freight project (see, [5]) for implementing the e-Freight multimodal e-Waybill. Cane et al. [5] identified accessibility, communication, interoperability, security, ownership, and authentication as the main implementation challenges for their multimodal e-Waybill solution, which is also based on storage of e-Waybill information at different locations. Accessibility concerns having access to the e-Waybill information at the right time and place. The technical requirements, identified in this paper, regarding information storage have the potential to solve the challenge of accessibility by ensuring that the e-Waybill information is accessible where it is stored. The communication challenge concerns the capability to exchange e-Waybill information between all the actors. This challenge is addressed by the technical requirements that concern access control and communication. The challenge of security is about authentication and authorization, and can be addressed by the technical requirements for read and write access control. The ownership of business data is about users having control of their own business data and it can be ensured by considering the technical requirements for encrypting the e-Waybill information and synchronization between the different e-Waybill information storage locations. It is our belief that the identified technical requirements can be used to support the process of designing and implementing the e-Waybill service. We argue that the organizational preferences also need to be considered in the design process, in particular concerning the choice of a proper access control mechanisms. However, in order to achieve acceptance of an e-Waybill service, we suggest that it, at least in its early versions, should allow the users to work in a similar way as they are used to work with a paper waybill. Therefore, the e-Waybill service should not require significant organizational changes for the involved actors. In addition, an organization interested in implementing the e-Waybill service could consider the technical requirements discussed in this paper in order to support the process of choosing which of the five e-Waybill solutions to use, as well as to choose which technologies to use when implementing the chosen e-Waybill solution. extensions.

References

[1] Bakhtyar, S., Holmgren, J., & Persson, J. A. (2013). Analysis of information synergy between e-waybill solutions and intelligent transport system services. *World Review of Intermodal Transportation Research, 4(2/3),* 123–139.

[2] Pedersen, J. T., Gyngell, J., & Katsoulakos, T. (2010). *The e-Freight Project: European e-Freight Capabilities for Co-modal Transport.* e-Freight Consortium.

[3] IATA. (2009). IATA cargo shipment record (e-AWB): Functional specifications. Retrieved January 3, 2015, from http://www.iata.org/whatwedo/cargo/e/Documents/e-awb-functional-specifications.pdf

[4] Mei, Z., & Dinwoodie, J. (2005). Electronic shipping documentation in china's international supply chains. *Supply Chain Management: An International Journal, 10(3)*, 198–205.

[5] Cane, T., Mattheis, S., Tsoukos, G., Focas, C., & Koliousis, I. (2012). The e-Freight multimodal e-Waybill. Presented at the e-Freight conference, Delft, Netherlands.

[6] Bakhtyar, S. (2013). *On the Synergies between an Electronic Waybill and Intelligent Transport Systems Services.* Licentiate dissertation, Department of Computer Science and Engineering, Blekinge Institute of Technology, Karlskrona, Sweden.

[7] Glinz, M. (2007). On non-functional requirements. *Proceedings of 15th IEEE International Requirements Engineering Conference* (pp. 21–26). Delhi, India: IEEE.

[8] Ross, D. T., & Schoman Jr, K. E. (1977). Structured analysis for requirements definition. *IEEE Transactions on Software Engineering, SE-3(1),* 6–15.

[9] Hansen, S., & Lyytinen, K. (2010). Challenges in contemporary requirements practice. *Proceedings of*

2010 43rd Hawaii International Conference on System Sciences (pp. 1–11). Honolulu, HI: IEEE.

[10] Kedad, Z., & Loucopoulos, P. (2011). Considering quality factors for business processes during requirement engineering. *Proceedings of 2011 Fifth International Conference on Research Challenges in Information Science* (pp. 1–9). Gosier, France: IEEE.

[11] Chung, L., & Prado Leite, J. C. S. do (2009). On non-functional requirements in software engineering. In A. Borgida, V. Chaudhri, P. Giorgini, & E. Yu (Eds.), *Conceptual Modeling: Foundations and Applications* (pp. 363-379). Springer Berlin Heidelberg.

[12] Lankford, W. M., & Johnson, J. E. (2000). Edi via the internet. *Information Management & Computer Security, 8(1),* 27–30.

[13] Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007). Public-key cryptography for RFID-tags. *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 217–222). White Plains, NY: IEEE.

[14] Wu, N., Nystrom, M., Lin, T., & Yu, H. (2006). Challenges to global RFID adoption. *The International Journal of Technological Innovation, Entrepreneurship and Technology Management, 26(12),* 1317–1323.

[15] Monnerat, J., Vaudenay, S., & Vuagnoux, M. (2007). About machine-readable travel documents. *Proceedings of the International Conference on RFID Security 2007.* Malaga, Spain: Springer.

[16] Li, M., Fung, C., Sampigethaya, K., Robinson, R., Poovendran, R., Falk, R., *et al.* (2008). Public key based authentication for secure integration of sensor data and RFID. *Proceedings of the 1st ACM international Workshop on Heterogeneous Sensor and Actor Networks* (pp. 61–66). NY, USA: ACM.

[17] Delen, D., Hardgrave, B. C., & Sharda, R. (2007). RFID for better supply-chain management through enhanced information visibility. *Production and Operations Management, 16(5),* 613–624.

[18] Zhou, S., Ling, W., & Peng, Z. (2007). An RFID-based remote monitoring system for enterprise internal production management. *The International Journal of Advanced Manufacturing Technology, 33(7-8),* 837–844.

[19] Kang, M. H., Park, J. S., & Froscher, J. N. (2001). Access control mechanisms for inter-organizational workflow. *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies* (pp. 66–74). NY, USA: ACM.

[20] McCune, J., Jaeger, T., Berger, S., Caceres, R., & Sailer, R. (2006). Shamon: A system for distributed mandatory access control. *Proceedings of 22nd Annual Computer Security Applications Conference* (pp. 23–32). Miami, FL: IEEE.

[21] Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security, 3(2),* 85–106.

[22] Ray, I., & Kumar, M. (2006). Towards a location-based mandatory access control model. *Computers and Security, 25(1),* 36–44.

[23] Yuan, E., & Tong, J. (2005). Attributed based access control (ABAC) for web services. *Proceedings of IEEE International Conference on Web Services* (p. 569). Orlando, FL: IEEE.

[24] Bakhache, B., Ghazal, J. M., & Assad, S. E. (2013). Improvement of the security of ZigBee by a new chaotic algorithm. *IEEE Systems Journal, 99,* 1.

[25] Saponara, S., Solanas, A., Avoine, G., & Neri, B. (2013). Privacy and security in wireless sensor networks: Protocols, algorithms, and efficient architectures. *Journal of Computer Networks and Communications.*

[26] Lee, Y., Kim, Y., & Choi, H. (2004). Conflict resolution of data synchronization in mobile environment. In A. Laganá, M. Gavrilova, V. Kumar, Y. Mun, C. Tan, & O. Gervasi (Eds.), *Computational Science and Its Applications – ICCSA 2004, Lecture Notes in Computer Science* (pp. 196–205). Springer.

Shoaib Bakhtyar is a PhD candidate at the Department of Computer Science and Engineering, Blekinge Institute of Technology, Karlskrona, Sweden.

He was born in Kheshgi, KPK, Pakistan in 1985. He completed his undergraduate degree in information technology (BS-IT) at COMSATS Institute of Information Technology in 2006 and then received the master degree (MSc) in computer science at Blekinge Institute of Technology in 2008.

His research interests include CMR documents, electronic waybill, intelligent transportation systems, and data mining.

Johan Holmgren was born in Sweden in 1978. He graduated from Linköping University with a master of science degree in mathematics in 2004, and received his PhD degree in computer science at Blekinge Institute of Technology in 2010.

Currently, he is employed as an assistant professor at the Faculty of Computing at Blekinge Institute of Technology and at the Department of Computer Science at Malmö University, both in Sweden.

His research interests include agent–based simulation and modeling, mathematical optimization, and data mining, which he applies in the areas of freight transport and traffic modeling, health-care management, and intelligent transportation systems.

Jan A. Persson is an associated professor of computer science at Malmö University, Sweden. He received his PhD degree in optimization in 2002 from Linköping University, Sweden.

He is the head of the Computer Science Department at the Faculty of Technology and Society, Malmö University, Sweden.

He researches in optimization and simulation methods for decision support. Application areas include traffic and transport systems, ITS-service architectures, logistics and supply chain management, and healthcare management.