ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
University of St.Gallen

AUTO–ID LABS

# The Potential of RFID and NFC in Anti-Counterfeiting

## *Improving Customs Processes with RFID and NFC Technology to Fight Illicit Trade*

*Mikko Lehtonen, Thorsten Staake,*
*Florian Michahelles, Elgar Fleisch*

**Auto-ID Labs White Paper** WP-BIZAPP-027

**Mikko Lehtonen**
Senior Researcher
ETH Zurich

**Thorsten Staake**
Senior Researcher
University of St.Gallen

**Florian Michahelles**
Associate Director
Auto-ID Labs ETH Zurich

**Elgar Fleisch**
Research Director
Co-Chair of Auto-ID Labs
University of St.Gallen and ETH Zurich

Contact:

Auto-ID Labs ETH Zurich/St.Gallen
Swiss Federal Institute of Technology (ETH) Zurich
Department of Management, Technology and Economics
Kreuzplatz 5
8032 Zurich
Switzerland

Phone: +41 44 632 86 24
Fax: +41 44 632 10 45

E-Mail: mlehtonen@ethz.ch
Internet: www.autoidlabs.org

Business Processes & Applications

# Abstract

In this paper, we investigate how RFID and NFC could improve current customs processes to fight illicit trade. During the import process, customs officers have to evaluate which consignments are inspected and, if an inspection takes place, whether intellectual property rights have been infringed. We propose new micro processes that leverage the dual-existence of products and logistic units in order to enable easier, faster and more reliable inspection of goods and analyze the impact of the improved processes on counterfeiting.


# 1. Introduction

Counterfeit and pirate goods cause increasing economic losses to companies, industries and countries, and threaten the consumer health and safety while fostering other illegal activities [9]. The value of counterfeit trade is estimated up to EUR 500 billion annually and is escalating rapidly [20]. Taking into consideration the high growth-rate in the world container port traffic - having average annual increase of 11.8% between 2000 and 2004 [26, 25], compared to 2% average annual increase in the world GDP during the corresponding period [27] - we can conclude that an increasing number of containers with an increasing number of counterfeit and pirate goods flows to affected markets every year.

The problem of counterfeit products is no longer specific only to certain industries or brands; today, all kinds of products from fast-moving consumer goods (FMCG) to luxury items are affected. The majority of counterfeit products in the Western countries are imports and the primary sources of counterfeits are in Asia, China alone representing the source of more than 50\% of fakes stopped at the European borders [4]. The most important means of transport of counterfeit products is sea, being responsible of 70% of stopped fake products in Europe [4]. Modern technology and high level of industrialization have made it possible for illicit manufacturers to produce fake products in high volumes and to imitate the original grade and quality [9].

Fortunately, development in technology has also enabled novel countermeasures. Most notably, the emerge of radio-frequency identification (RFID) technology has opened many opportunities to fight illicit trade [22, 8]. RFID allows for automatic identification of tagged objects and establishes a link between the physical world and a virtual world. This so called *dual existence* of objects enables a number of new ways to manage the physical world, and thus RFID is being used for example to automate many supply chain processes [12]. Combined with Near Field Communication (NFC), standardized technology for short-range wireless connectivity between a reader and tag[1] [23] for hand-held devices like mobile phones [19], RFID could be effectively used to authenticate products [18]. However, even though RFID is used more and more to label logistic units as they flow through the supply chain, it is not yet realistic to assume that individual items would be tagged. Therefore RFID

[1] also peer-to-peer communication is supported, e.g. between reader devices

  

product authentication should take place inside the supply chain, while the products travel in tagged units such as pallets and cases.

As a consequence, RFID and NFC have substantial potential to improve customs countermeasures against illicit trade. Customs is very important authority in protecting societies against counterfeit products and in many cases the only gatekeeper between the manufacturer of counterfeit goods and the end customers. Due to the rapidly increasing workload and obligations concerning other interests than finding fake products, customs resources in anti-counterfeiting are very limited. Therefore increasing the efficiency of customs processes for finding counterfeit goods is important for the success in the fight against illicit trade.

In this paper, we propose ways how RFID and NFC could be used to improve existing customs processes to fight illicit trade. Illicit trade is a roof term for trade with goods that infringe Intellectual Property Rights (IPRs) and for a number of grey market activities and contract breaches. Infringing goods can be either counterfeit-or pirate goods, depending on whether they infringe a trademark or a copyright, respectively. We will use the term *counterfeit* in the rest of this paper to cover both counterfeit and pirate goods. Besides infringing goods, illicit trade also covers a number of activities that are treated as counterfeiting by trademark owners but not by enforcement agencies, such as parallel trading and factory over-runs. In these cases, the goods itself do not differ from originals but they are transported or manufactured without the consent of the right holder.

This paper is organized as follows. Section 2 introduces the customs' role in anti-counterfeiting, how RFID is used in customs today and the import process in the European Union. In section 3 we propose ways to improve the current process by making use of RFID and NFC technologies. Section 4 analyzes the impact of the proposed improvements and we finish with conclusions.

# 2. Customs

Customs is a critical institution for protecting the interests of a society and its citizens. It manages the physical movement of goods and people across borders and is responsible of collecting customs duties at import. National customs administrations cooperate with industries and with each other and their work is governed by the World Customs Organization (WCO). The role of WCO is to increase the efficiency and effectiveness of customs administrations and, in order to achieve this goal it provides guidelines [14] for modern customs principles.

## 2.1. Customs and Counterfeiting

Customs are responsible for about 70% of all seizures of counterfeit products in the world [2]. The role of customs is especially important in protecting the European Union and the U.S. because the vast majority of counterfeit products in those markets are imports [4] and, after entering the market, subject to free circulation within the community. However, in anti-counterfeiting customs role is more supportive than proactive, which means that customs mostly provide help to trademark owners to protect their IPRs when this is requested.

Customs authorities fail to seize large amounts of counterfeits either because they do not know how to recognize the fakes or because the process of gathering statements from trademark owners is too time-consuming. Proper labelling, overt anti-counterfeiting technologies and training in recognizing counterfeits would, for example, assist officials in enforcing the IPRs of affected trademark owners. Furthermore, the lack of information sharing is often perceived to be one of the main obstacles in the fight against counterfeiters [9].

Finding counterfeit products is one part of customs responsibility to control the trade. Other control objectives include finding various kinds of dangerous materials. While controlling the trade, however, customs also work to facilitate the trade in order not to disturb import and export. These two objectives conflict and thus customs always have to balance the trade-off between control and facilitation. Taking into account also the fact that the vast majority of goods that pass through customs are legal and thus should not be disturbed, it can be seen that finding counterfeit goods is not among customs' top priorities.

## 2.2. RFID in Customs Today

Customs are using RFID in many ways today. In the busy Shenzhen customs in Hong-Kong, RFID has been used to speed and facilitate the flow of low-risk traffic since 2002 [11]. The Shenzhen customs use passive RFID tags to identify vehicles and their drivers in the traffic lanes. Vehicle ID, driver ID and weight of the consignment are compared to the information that is sent in pre-hand into the customs department's computer system. If any discrepancies occur, the consignment is subject to closer inspection.

Customs use RFID also to strengthen the security of consignments. To guarantee the integrity of cargo, shippers install electronic seals, or *e-seals*, into their containers. The e-seal consists of an active tag and a mechanism that can detect if a container's door has been opened without authorization, so that it can communicate whether the container's integrity has been guarded or not. E-seals are used to secure cargo arriving to the U.S. from many foreign ports [10, 14]. The concept of an *e-container* was set forth in [29] as a risk mitigation technology against the risks associated with global container transport. The suggested e-container uses real-time monitoring of a container’s physical status acquired from an array of

embedded RFID-enabled sensors. It is shown that by selecting a suitable set of sensors (e.g. those measuring ambient temperature, light, air humidity, radioactivity etc.), a number of container transport threats can be mitigated, such as smuggling of drugs, weapons or humans and theft during inspections. The role of RFID in the e-container is to provide connectivity and real-time telemetry.

Also tracking of tagged containers increases cargo security, and it has been used for example in automated border program of the U.S. customs [10]. During the recent years, the movement of international cargo has become more and more regulated. Though these regulations do not demand the use of RFID, they oblige companies to provide more accurate and timely data on shipments [15]. One consequence of this trend is the emerging of *green lane* programs where shipping companies gain lighter inspections when they conform to certain additional regulations, such as in the Smart & Secure Tradelanes (SST) initiative [13] or the Customs-Trade Partnership Against Terrorism (C-TPAT) [28]. In addition to the control of the flow of goods, RFID chips in electronic passports allow for biometric identification of travellers [17].

## 2.3. The Import Process

Due to limited resources and size of the workload, it is impossible to search every consignment entering the country; in practice, only about 1-4 percent of imported goods are inspected. Therefore customs success in anti-counterfeiting depends on how the scarce resources are allocated, which in practice means deciding which consignments are inspected. Customs conduct *risk analysis* to identify high-risk consignments in pre-hand [5]. The risks are estimated by combining the likelihood and consequence of an event [5] and the analysis is based on information in the {\it freight papers} that are used in processing the flow of imported and exported goods. Freight papers like the {\it air waybill} specify, for example, the shipping route and the cargo manifest of a consignment and they can exist both in physical and electronic form. Though the risk-analysis can be partially automated, interviews with customs officers reveal that the experience of the officers plays a very important role in recognizing suspecting consignments. Regarding counterfeiting, the country of origin is the most important criteria in the risk-analysis and, consequently, often attempted to be disguised by the carriers of counterfeit goods [9]. Careful selection of inspected containers can provably provide considerable improvements in the detection rates of counterfeit products [3].

Our focus is on how counterfeit goods are seized in the European customs import process, illustrated in Figure 1. The legal aspects of this process are defined by the European Council regulation 1383/2003 [1]. To protect their IPRs, the right holders have to lodge an *application for action* where they provide the customs with the information to authenticate original products. The application for action is an important form of cooperation between customs and industry and the customs rarely seek for counterfeit goods without an application in place.

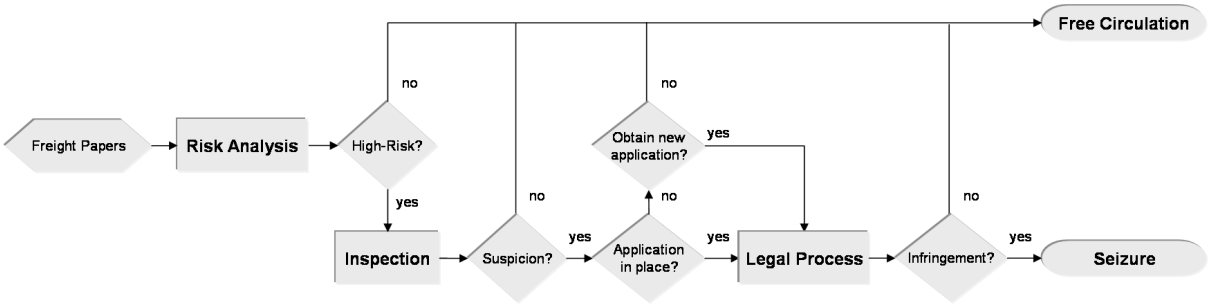


***Figure 1. Simplified diagram of the European customs import control process for seizing counterfeit goods***

# 3. The Improved Processes

In this section, we describe new micro processes that can be used to improve the existing customs import process to find and seize more counterfeit goods. The enabling technologies of the proposed processes are RFID and NFC (e.g. an NFC enabled Personal Digital Assistant (PDA) with internet connection), allowing the customs officers to scan all tagged items in their field work. We take into account that in a modern customs process, the flow of information and the flow of goods are separated and therefore the customs officers need to move to the warehouse to conduct the physical inspections. In a very lean and automated import process, the time that the products spend in the customs warehouse can be very small and measured in tens of minutes, which sets additional time-constraints for the inspections.

## 3.1. Facilitated Manual Authentication

Inserting RFID tags on logistic units allows for novel ways to obtain information for manual authentication[2] of goods during the inspection. This facilitates the inspection by making product authentication faster and more reliable by providing the inspectors with accurate and timely data. The process steps are following:

1. Obtain the product-class identification (ID) number (i.e. two first fields of standard structure *company prefix.item reference.serial number*) of the product under inspection. Three different scenarios are distinguished:
    a. Read the product tag to obtain the product-class ID (item-level tagging).

[2] In this work, authentication is defined as answering whether something original or not

b. Read the consignment (e.g. pallet or case) tag to access a data structure of product ID numbers (e.g. electronic freight papers) where the product-class ID can be found (Figure 2).

c. Search the product-class ID from a database that links product classes with their ID numbers. This approach is made feasible by the relatively small amount of product classes that would have information for manual authentication in a database.

2. Find the network address of an authorized server for the product class using an address resolution system (e.g. EPC Object Naming Service [6]).
3. Establish a secure connection with the authorized server (e.g. EPC Information Service [7]).
4. Download the data for manual authentication.

Customs officers would benefit from the described process by having an automated way to obtain information for authentication of tagged, as well as not-tagged products. This information could contain technical descriptions and pictures of the original product class and descriptions of common counterfeit features. In practice, the product-class ID database could be gathered from applications for action (subsection 2.3) to enable authentication of certain non-tagged goods, though the described process would above all decrease the effort of authenticating tagged original products.

This micro process relies on right-holders upkeeping the authentication data on online servers and letting the customs to access it. Having the authentication data on the right-holder's server guarantees the timeliness of the data and allows it to be updated and published to all stakeholders without delays. In addition, the technology allows the customs officers to take pictures of counterfeit consignments and upload them, and other data, to right-holder's server to share information of actions of counterfeit players.

## 3.2. Automated Authentication

Although RFID is primarily an identification technology, it also supports for many ways of authenticating physical entities. The starting point of RFID product authentication[3] is to insert a tag on the product and to authenticate the tag or use it to collect data for authentication. Even low-cost tags can be used for product authentication (e.g. track and trace based plausibility check [22]), though achieving higher levels of security can substantially increase the price of the tag. A comprehensive review on RFID product authentication techniques can be found from [18]. Currently there are no standardized RFID product authentication protocols and, furthermore, multiple protocols are needed to balance the trade-off between cost and security. For these reasons, it is necessary to establish which authentication

[3] This applies also to other logistic units

protocol, if any, the inspected product (tag) supports, before the authentication can take place. The process steps are following:

1. Identify the product by reading the product tag.
2. Obtain the network address of the authorized server.
3. Establish a secure connection with the authorized server.
4. Establish which authentication protocol, if any, the inspected product supports.
5. Automatically authenticate the product (tag) using the supported protocol.

The presented process facilitates the inspection of tagged original goods by making it faster and more reliable than a manual check. Support for multiple authentication protocols does not pose specific hardware requirements because authentication protocols can be made transparent for the interrogator. In particular, the authentication can be processed on the back-end server so that the reader device only needs to be informed about the result. It should be kept in mind that usually it is actually the tag that is authenticated and not the product itself. Therefore a verification is required to make sure that the authenticated identity really matches the physical product. Omitting this verification makes the system vulnerable to simple attacks where fake goods are equipped with any authentic tags.

For cases where no network connection is available (e.g. inside a container or a vessel), an offline authentication protocol is required. Feasible solutions for offline authentication, however, have not yet been proposed [18]. In some cases the problem can be overcome through *batch mode* authentication [24] where the reader device initiates the authentication in offline mode, for example during inspection inside the steel container, and finishes the authentication when a network connection becomes available.

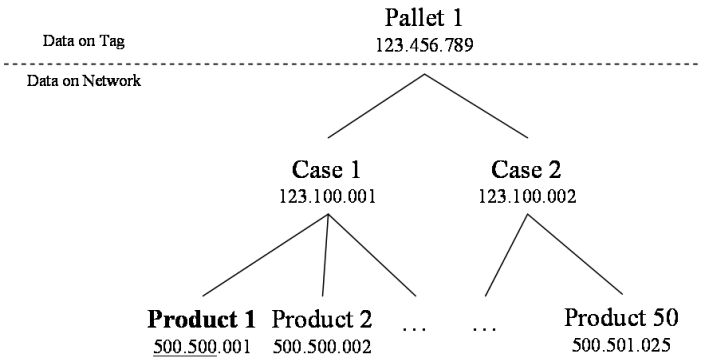


***Figure 2. An example of how the aggregated data structure of a logistic unit can be used to obtain the product-class ID number (500.500) of one specific product (Product 1). The pallet ID number acts as a link to data on network.***

## 3.3. Machine-Readable Freight Papers

RFID enables also automatic identification and authentication of tagged freight papers. The carrier company could insert RFID tags with consignment identifier numbers into the physical freight papers to allow for automated document handling process at customs. Making use of the dual existence, the tag could provide a link to electronic freight papers or to an aggregated consignment data structure as illustrated in Figure 2, for example, to enable customs officers to access all data of a consignment by scanning the freight papers. The main motivation to use RFID with freight papers is to have the same infrastructure to identify containers, pallets, cases, and freight papers. Even though RFID is not the only nor always the optimal technology to make documents machine-readable [16], the benefits of having only one infrastructure would outweigh the privacy- and cost-related shortcomings. Furthermore, the RFID tag could be used to strengthen the security of the physical documents.

# 4. Discussion

In this section, we analyze the impact of the proposed micro processes on the existing customs import process and on anti-counterfeiting. First, the use of RFID and NFC supports the modern customs principles given by WCO [21], which include continuous development of control techniques and maximum use of information technology. Second, RFID enables new means of communication between the right-holder of goods and customs. Currently customs receive the information of the content of a merchandised consignment only from the carrier company's freight papers. Tagging cargo would enable the customs officer to access the manufacturer's online server that maintains data about the tagged products, which could make the customs process less dependent on the data provided by the carrier company. Most notably, this link could provide means to inform the right-holder about grey market activities such as parallel trade. However, this could need changes in legislation because currently customs do not have legal basis to interfere in these kinds of activities.

We have shown how RFID and NFC can improve information sharing and help customs officers to recognize fakes, given that right-holders tag their consignments. This helps customs to seize bigger amounts of counterfeit products, which provides economic benefits for the affected right-holders. In addition, RFID brings value also in other supply chain applications and so the cost of tagging the cargo doesn't need to be justified only by the increased supply chain security.

The proposed processes contribute primarily to faster, easier and more reliable authentication of tagged consignments, while the product-class ID number database (subsection 3.1) would also facilitate manual authentication of non-tagged products. We have shown how also the case or pallet level tags, together with an aggregated data structure of

the logistic unit, can be used to facilitate the authentication of single products inside the unit. However, RFID-enabled authentication per se does not considerably increase the number of counterfeit products customs find, if only a small ratio of cargo supports it. Furthermore, it can be assumed that counterfeit products usually are not tagged. Therefore the underlying problem is how technology that can authenticate some of the original products can be used to distinguish the fake ones. This is illustrated with the following example.

## Example

Let's consider the import process described in subsection 2.3. and concentrate on counterfeit goods only. Assuming that customs ability to select suspicious shipments cancels out the chance of not detecting counterfeit goods even though they have been inspected, we can estimate that the probability to find counterfeit goods in an inspection equals the percentage of all imported goods that are counterfeits, denoted by $P_1$. In practice this assumption means that by inspecting *y*% of cargo, customs find *y*% of counterfeits. Let's further assume that *x* percent of imported consignments are tagged and thus support for authentication as described in subsections 3.1 and 3.2. Assuming that counterfeit consignments are never tagged, the customs can direct the tagged *x* percent of imported goods into a green lane program where they are not inspected (e.g. the upper path in Figure 1). Doing so, the counterfeit goods can be searched among smaller amount of consignments and, if other factors remain unchanged, the probability to find counterfeit goods in one inspection increases to:

$$P_2 = \frac{P_1}{100 - x}$$

In accordance with the underlying assumptions, also the total number of found counterfeits increases by the same factor than the probability of finding counterfeits in a single inspection. This is demonstrated in Figure 3 which illustrates the effect of RFID penetration *x* to seizure rate.

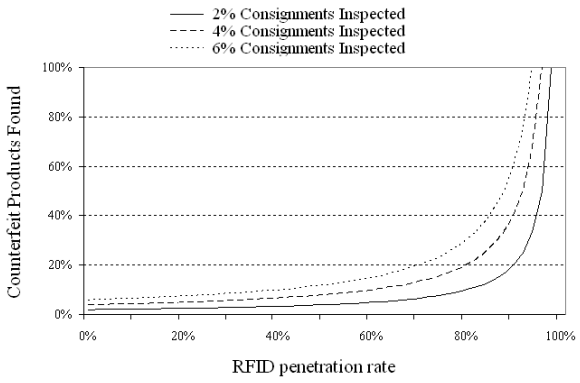


***Figure 3. An evaluation of how theinspection rate and RFID penetration rate of imported goods affect the number of found counterfeit products.***

## Analysis

The example illustrates how high RFID penetration in the imported cargo can help customs to find increasing number of counterfeit products without increasing the number of inspections. In the optimal case, the lack of RFID tags in a consignment would act as an indicator of counterfeit origin. In practice, however, also tagged cargo needs to be inspected because also counterfeit goods can be tagged. Therefore the role of automated authentication process (subsection 3.2) is to find the non-authentic, forged tags. Ultimately, this could lead to a situation where the lack of tags indicates counterfeit origin while the forged tags can be easily found.

# 5. Conclusions

Though RFID is used in customs logistics in different ways today, it has unused potential to help customs in the fight against illicit trade. In this paper, we have proposed new micro processes that make inspection of tagged cargo faster and more reliable making use of mobile devices with RFID and NFC technologies. The impact of our contribution is evaluated in an example analysis which demonstrates how the benefits of RFID-enabled product authentication depend on the RFID penetration of imported cargo. Providing customs with the required infrastructure would allow right holders to use state-of-the-art RFID technologies to protect their products, contributing towards safer supply chains.

  

# References

[1] European Commission. Regulation (EC) no. 1383/2003. Official Journal of 2 March 2003, L 196, page 7, 2003.

[2] European Commission. Counterfeiting & piracy: Frequently asked questions. MEMO/05/364, Brussels, 11 October, 2005.

[3] European Commission. International customs operation ”FAKE”. IP/05/1383. Brussels, 8 November, 2005.

[4] European Commission. Community-wide counterfeit statistics for 2004, 2006.

[5] European Commission. Standardized framework for risk management in the customs administrations of the EU, 2006.

[6] EPCglobal. Object naming service (ONS) specification version 1.0. EPCglobal public document, October 4, 2005.

[7] EPCglobal. EPCglobal architecture framework version 1.0. EPCglobal public document, July 1st, 2005.

[8] U.S. Food and Drug Administration. Combating counterfeit drugs - a report of the food and drug administration. February 2004.

[9] Organization for Economic Co-operation and Development (OECD). The economic impact of counterfeiting, 1998.

[10] RFID Journal. E-Seals smooth border crossings. News Article, September 3, 2002.

[11] RFID Journal. RFID speeds border crossings. News Article, October 15, 2002.

[12] RFID Journal. Wal-Mart draws line in the sand. News Article, June 11, 2003.

[13] RFID Journal. Interest grows for tagging cargo. News Article, February 2, 2005.

[14] RFID Journal. Colombian shipper to use RFID. News Article, May 15, 2006.

[15] RFID Journal. Coping with regulations. Perspective Article, 2006.

[16] RFID Journal. DHS subcommittee advises against RFID. News Article, May 22, 2006.

[17] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in E-passports. In Conference on Security and Privacy for Emerging Areas in Communication Networks SecureComm, (to appear), September 2005, Athens, Greece, 2006. IEEE.

[18] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch. From identification to authentication – a review of RFID product authentication techniques. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[19] Nokia. Nokia unveils the world’s first NFC product - Nokia NFC shell for Nokia 3220 phone. Available at http://press.nokia.com (29.6.2006), 2004.

  

[20] International Chamber of Commerce (ICC). The fight against piracy and counterfeiting of intellectual property. Policy Statement. Submitted to the 35th ICC World Congress, Marrakesh, 7 June 2004.

[21] World Customs Organization. The Kyoto convention: Customs contributing to the development of international trade. Fact Sheet, 2006.

[22] T. Staake, F. Thiesse, and E. Fleisch. Extending the EPC network - the potential of RFID in anti-counterfeiting. In 2005 ACM symposium on Applied computing, pages 1607–1612, New York (NY), 2005. ACM Press.

[23] NFC Forum. http://www.nfc-forum.org/home, 2006.

[24] G. Tsudik. YA-TRAP: Yet another trivial RFID authentication protocol. In International Conference on Pervasive Computing and Communications PerCom 2006, March 2006., Pisa, Italy, 2006. IEEE, IEEE Computer Society Press.

[25] The Review of Maritime Transport, 2003. United Nations Publication UNCTAD/RMT/2003, 2003. ISBN 92-1-112582-0.

[26] The Review of Maritime Transport, 2005. United Nations Publication UNCTAD/RMT/2005, 2005. ISBN 92-1-112674-6.

[27] International Trade Statistics 2004. World Trade Organization (WTO), 2004.

[28] U.S. Customs and Border Protection. Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan. November 2004. Available at http://www.customs.gov/linkhandler/cgov/import/commercial_enforcement/ ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf (29.8.2006).

[29] A. Schlesinger. Mitigating Container Security Using Real-Time Monitoring with Active Radio Frequency Identification and Sensors. Master's Thesis, Massachusetts Institute of Technology, June 2005.