ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20160916124618
Original scientific paper

Automated Authentication and Authorisation of Consignors and their Consignments within Secure Supply Chains

Roman GUMZEJ, Bojan ROSI

Abstract: In cross-border transport, in particular in air-transport, since 2010 there is the notion of a known consignor. This term is used in connection with an airfreight distribution company, which has introduced appropriate safety and security measures into its business process. Hence, its transport units are considered "safe" and can be handled with fewer overheads and more quickly. Due to the ever-increasing airfreight traffic, the notion of efficient security in airfreight is becoming increasingly pressing and requires information technical support to be able to handle shipments in time. In order to sustain security throughout entire supply chains all consignors should adhere to the same security standards – build a secure supply chain. This article presents methods and mechanisms for automated authentication and authorisation of known consignors and their transport units that enables swift identification and secure handover of shipments among known consignors and distribution centres. In their application they are not bound to air-transport and can be used to secure supply chains in general.

Keywords: authentication; authorisation; known consignor; secure supply chain; transport unit

1 INTRODUCTION

Attempted bomb attacks by express package delivery service in 2010 triggered an extensive debate on security measures in mail and goods delivery, especially in air-traffic. Weaknesses in transport security were investigated with the goal to effectively protect a supply chain. It was discovered that they could be lead to cargo handling procedures and cargo data access, as well as training of personnel [1]. Consequently, by the Commission Regulation (EU) No. 185/2010 [2] a set of measures and mechanisms have been defined, which have led to the improvement of air transport security.

Due to increasing risk, transport units must be subjected to appropriate security checks, especially before loading them to planes or ships. This process introduces additional overhead, resulting in increasing transport costs and slowing down logistics processes. Due to cross docking, handovers of cargo within supply chains may occur multiple times. In supply chain management there is a notion of a cold chain, representing a temperature-controlled supply chain, i.e. an uninterrupted series of storage and distribution activities, which maintain a given temperature range. Here, a notion of a secure supply chain is introduced, representing a series of storage and distribution activities, which maintain a given security standard.

Directive (EU) No. 185/2010 with its amendments describes the terms that any trusted consignor or distribution centre needs to fulfil in air-transport in order to be recognised as such. It also describes the methods and measures it needs to apply in order to protect its own and transit transport units. Upon arrival of a transport unit, the distributor (air-carrier) needs to check the consignor's status and handle the transport unit accordingly. Inquiries about consignor status are made to the EU database, holding data on the current status of all known consignors' locations. In case the transport unit does not originate from a trusted consignor, the transport unit is treated as unknown in concordance with all prescribed security measures. In case the transport unit originates from a trusted consignor, however, most security checks can be omitted and such transport units may progress faster. While the inquiries to the EU database of known (trusted) consignors are performed through secure information channels, the data about and on shipments remain unprotected, as printed one- (bar) or two-dimensional (QR) identification codes can easily be counterfeited and/or switched.

In this article an original approach is presented to securing the transport units and their data as well as the data on their consignors in conformance with the Directive (EU) 195/2010 by secure automated authentication and authorisation methods and mechanisms.

1.1 Directive (EU) No. 185/2010

According to the regulation, the EU distinguishes between three types of entities in a secure supply chain:

Regulated agent: An agent, freight forwarder or any other entity that handles cargo and ensures security controls in respect of cargo and mail.

Known consignor: A consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of cargo or mail on any aircraft.

Account consignor: A consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow carriage of that cargo or mail on all-cargo or all-mail aircraft only.

According to the Information for cargo handling entities in non-EU countries [3] air carriers that fly cargo or mail from a non-EU airport to an EU airport (ACC3s) must ensure that all cargo and mail carried to the EU is physically screened or comes from a secure supply chain, which is validated according to the EU regulations.

Any entity that is not one of the above described entities is an unknown entity and may not be part of a secure supply chain. All cargo or mail coming from an unknown entity needs to be screened by or on behalf of an ACC3 or by a third country regulated agent before being loaded on board an aircraft bound for the EU.

The basic security requirements for cargo and mail from non-EU countries may be found in the Annex to

Regulation (EU) No. 1082/2012 [4], Regulation (EU) No. 654/2013 [5]. In their Attachments 6-C2, 6-C3 and 6-C4 they contain the checklists, which EU aviation security validators use to assess an entities' compliance with the EU security objectives. Depending on the entities' business and its current security measures, the entity may need to update its security programme, enhance its security measures or provide for the necessary screening equipment. The entities' security measures need to be in accordance with at least ICAO (International Civil Aviation Organization) standards. In the event an entity carries out screening, its screening methods need to be in accordance with EU requirements.

EU aviation security validations may only be carried out by approved EU aviation security validators. All approved validators an entity may engage are included in an EU database [6].

If an entity is not validated and approved according to the EU requirements, it may not form part of the secure supply chain of an ACC3. As a consequence, all the cargo or mail the entity forwards will need to be screened by or on behalf of the ACC3 or a third country regulated agent before being loaded on board an aircraft bound for the EU.

1.2 Obtaining and Sustaining Known Consignor Status

According to the Commission Regulation (EU) No. 185/2010, which speaks of defining detailed measures for the implementation of common standards in air-transport security, a known consignor can be confirmed by the appropriate authority. The approval itself is bound to a location.

The competent authority of each member state determines the responsibilities for the endorsement process of a known consignor. An applicant shall seek for the approval from the competent authority of a member state, from which it receives guidelines for known consignors, according to its location. The authority carries out the verification of the listed consignor's location in order to assess the fulfilment of the requirements by the applicant. By doing so, it also considers the fact, whether the applicant is already the holder of an Authorised Economic Operator (AEO) certificate (according to Regulation (EC) 648/2005 [7]). It uses the official validation list for known consignors (Annex to Regulation (EU) No. 1082/2012 [4], Regulation (EU) No. 654/2013 [5]). This control list contains a declaration of obligations and is signed by the legal representative of the applicant or the person that is responsible for security at a given location. Once the validation control list is filled out, the data it contains is treated as classified information that is kept by the competent authority. If the authority is satisfied with the validation, it makes sure that on the following business day the necessary information about the consignor is entered in the database of the European Union (e.g. Tab. 1). Herewith, the competent authority attributes each approved known consignor location a single alphanumeric code UAI (Uniform Alphanumeric Identifier) in the standard format.

A known consignor at any location assigns at least one person, responsible for the implementation and control of the security measures, at the location. This person must successfully pass a background check in advance.

The known consignor is reaffirmed at regular time intervals that are not more than five years apart. This includes on-site verification to assess if a known consignor still complies with the requirements. If the competent authority is no longer satisfied with the fulfilment of requirements by the known consignor, it cancels its status for the specific location and makes sure that the change is visible in the EU database. Any known consignor shall be recognised as such in all Member States (according to Commission Regulation (EU) No. 185/2010, pp. 30, 31 [2]).

In order to become a known consignor, a candidate should at the first stage introduce certain security measures against unauthorised accesses to or tampering of transport units. They address details about the production process, product packaging, storage and dispatch. In its application, the company must also provide the details about the organization (name, company's address, number of employees, contact information, the nature of its business, etc.), details of its recruitment procedures (permanent, temporary, etc.) and security training of all employees that have access to its shipments. The candidate needs to demonstrate the security of the cargo location (physical fence, barriers, alarms, doors, windows...). It is also essential that appropriate access control procedures be in place. The known consignor candidate needs to demonstrate that the access to the storage and dispatch facilities is controlled and secured. The known consignor candidate needs to provide details of the packaging process to demonstrate that all finished goods are checked prior to packaging and to describe the outer packaging, if the latter is required.

A known consignor (candidate) needs to provide all details concerning the method of transportation to the regulated agent, evidence of qualifications of contractors and cargo insurance. In case the company uses its own transport, its drivers have to go through appropriate training. If the company uses external contractors, they are only allowed to contain the cargo in consignments. The consignments must be protected by seals or some other appropriate method. Assembled explosive and incendiary devices may be carried in consigned transport units, if the requirements of all safety rules are fully met. Explosive and incendiary devices, whether assembled or not, shall not be carried in consignments of mail. (Commission Regulation (EU) No 185/2010, p. 31 [2]) A known consignor may pass consignments, which it has not packaged itself, to a regulated agent, provided that they are separated from its native consignments and that their origin is clearly indicated on the consignments or the accompanying documentation (Aviation authority, [8]).

The business entities from third countries who wish to attain known consignor status can achieve this in two stages. The first is by the introduction of a security programme that provides the certification authority with details on security controls of cargo or mail they deliver to the EU. The second stage is reaffirmation of the certification by validation that appropriate cargo-handling activities are in place at intervals not exceeding five years. In addition, they need to submit a copy of the report on their validation (Commission Regulation (EU) No.

185/2010, p. 37, 38 [2]). All carriers that are non-members of the EU and deliver cargo or mail to EU Member States have to comply with the mentioned security requirements. In accordance with the Regulation (EU) No. 185/2010, carriers must ensure that the cargo or mail destined to the EU were checked or that they come from a secure supply chain. In order to do this, a carrier must be confirmed as carrier from a third country, delivering cargo or mail to the Member States of the EU (ACC3-operations in the European Union from third countries) [9].

1.3 Current State in Slovenia

An insight into the database of regulated agents and known consignors in Slovenia currently reveals only three regulated agents (RA), all located at the international airport of Ljubljana, and two known consignors (KC) (see Tab. 1).

While collecting information on the known consignors and regulated agents in Slovenia, the listed pharmaceutical companies Krka, d.d. and Lek, d.d., were consulted. In their experience the main advantage of this type of transport management in air transport is faster handling of goods on the dispatch airport, because, when the goods are sent by a known consignor, there is no need for additional security controls, e.g. X-rays of goods. So far their status did not bring them any direct financial benefit. On the other hand, the fulfilment of the requirements according to Directive (EU) No. 185/2010 required substantial organisational changes, e.g. in some parts of the internal logistics chain it was necessary to add new security mechanisms in the form of complete technical control over the goods, ready for dispatch, separate flow of goods under the status of a known consignor and provision for flight control access to shipping zones. Furthermore, it was necessary to check impunity and provide for appropriate training of personnel, who are in contact with the dispatched goods, and need to obtain special security certificates. Hence, we may conclude that, in their experience, additional security did bring them benefits, but with a cost of the internal organisational changes.

Table 1 List of known consignors [10]

DHL Ekspress (Slovenija), d.o.o	Zgornji Brnik 130U, SI-4210 Brnik	10.05.2018 (RA)
Aerodrom Ljubljana, d.d.	Zgornji Brnik 130a, SI-4210 Brnik	21.10.2018
UPS Adria (S) Ekspres, kurirske storitve, d.o.o.	Zgornji Brnik 130, SI-4210 Brnik	31.03.2019 (RA)
KRKA, d.d., Novo mesto	Šmarješka cesta 6, SI-8501 Novo mesto	31.05.2016 (KC)
LEK farmacevtska družba, d.d.,	Verovškova 57, SI-1526 Ljubljana	03.04.2018 (KC)

1.4 Related work

Since air-traffic security is a broad and complex topic, in [11] there is an overview on all aspects of aviation security, from security related policies and regulations over passenger and baggage as well as cargo security. Finally, the methods and mechanisms for aviation security are summed up as security operations. To be effective a combination of policies and regulations resulting in appropriate methods and mechanisms with associated technical solutions are necessary.

A partial solution to the implementation of air-cargo tracking solution with security elements has been presented in the case study [12]. It employed RFID technology to ensure tracking and secure handling of ULDs in air traffic. However, the associated information flow among consignors and distribution centres has been left out, hence rendering a technically sound, but, from supply chain security point of view, incomplete solution.

Other partial solutions also used RFID technology to provide for tracking of aerospace spare parts [13, 14] to secure airlines. They mainly emphasize the importance of traceability of airline spare parts and the positioning of RFID readers within an aircraft to effectively monitor the state of installed spare parts.

Some related works [15, 16, 17] on supply chain security are mainly focused on providing standards and regulations to ensure a maintained level of quality of service along supply chains, including security, based on lessons learned in total quality management.

This article focuses on methods and mechanisms to support security while sustaining efficiency throughout supply chains. They are not limited to airline cargo transport, although they rely on standards on transport security that have been primarily introduced in air-transport, in particular Commission Regulation (EU) No. 185/2010 and associated regulations. In order to provide a complete solution to air-cargo security, the World Cargo Symposium (WCS) has been identified by the IATA Cargo Strategy [18] as a unifying decision making forum where all supporting regulations and solutions would come together to provide for coherent and consistent security solutions.

1.5 IATA Cargo Strategy 2015-2020

According to IATA Cargo Strategy, the ten industry key priorities by 2020 are:

1) Enhancing safety
2) Improving security
3) Pushing for smarter regulations
4) Strengthening the value proposition of air cargo
5) Driving efficiency through global standards
6) Modernizing air cargo
7) Improving quality
8) Protecting cash
9) Strengthening partnerships
10) Building sustainability

Although they pertain to air transport that typically represents less than 1 % of world trade by volume, but on the other hand a 35 % of world trade by value, with higher value shipments and their increased security they should pertain to most of the world trade to build sustainability. Due to accelerated urbanisation, increasing the number of mega-cities, their mega-regions are expected to create agglomeration of GDP and population and are expected to drive the world trade.

According to [18] safety remains the first priority. Some commodities may endanger the safety of the carrier,

its passengers and/or crew, if not shipped in accordance with stipulated regulations. In this respect growing attention is directed also towards design and use of fire resistant unit load devices (ULDs) used also to maintain the cargo in a specified temperature range. Equally critical the security measures need to be both efficient and effective. To be efficient the regulations need to be managed by the industry, or else they will substantially slow down transit times. In order to prove effective, they need to provide shippers with greater transparency, reliability and predictability. To drive efficiency, global standards are needed (e.g. to ensure 48 hours end-to-end shipping time, where the customer so demands). The vision is to have a paperless industry and be able to rely on high-quality data available on demand by all relevant stakeholders. To improve quality, the transportation industry needs to maintain reliability and consistency of its services. Governed by the Cargo Agency Conference (CAC) the Cargo Account Settlement System (CASS) enables the swift, reliable, and cost-efficient movement of founds among airlines and their cargo partners, and could serve as a model to developing equal systems to accommodate a worldwide distribution network of accredited cargo agents. This would also strengthen partnerships among carriers.

In order to increase safety and security the focus of measures and mechanisms introduced is directed towards partnerships, information sharing and global standards. Besides dangerous goods, also live animals, perishables and pharmaceuticals require regulations and standards for documentation, handling and training. In order for security measures to be effective, information support mechanisms are being introduced (e.g. e-CSD, Cargo-XML, ACI) to improve air cargo security in compliance with the EU ACC3 regulation without disrupting the flow of cargo.

With this in mind in this article an original approach to securing supply chains is presented by providing them with appropriate information support to enable automated authentication and authorisation of consignors and their shipments and an undisrupted flow of information along secure supply chains. At the same time, it introduces mechanisms to protect transport units and their data also while in transit.

2 AUTOMATED AUTHENTICATION AND AUTHORISATION IN SECURE SUPPLY CHAINS

The core problem of known consignors' transport units' authentication and authorisation is the ability to recognise and pass them on with minimum overhead. At the same time, maintaining or increasing transport security is required. With the goal of speeding up logistics processes and reducing costs, the procedure of automated authentication and authorisation of transport units and their consignors is introduced, as described in the sequel.

In the previous section the regulatory requirements that a secure supply chain entity needs to comply with according to Commission Regulation (EU) No. 185/2010 have been described. In addition to implementing an appropriate security policy it needs to obtain and maintain its status as described. While maintaining its status it is enlisted in the EU database of known consignors and regulated agents to be recognised as such and its shipments to be treated accordingly.

In response to the core problem of reducing overhead while identifying the transport units and determining the status of their consignors, the proposed automated authentication and authorisation procedure for known consignors' transport units is being described in the sequel.

2.1 Authentication and Authorisation Procedure

The procedure to authenticate and authorise transport units of known consignors is designed in a way that guarantees transport unit's safety and confidentiality of data transmitted between a regulated agent (distribution centre) and the unit, the distribution centre and the authorisation authority of known consignors as well as between the distribution centre (regulated agent) and known consignors in the sense of Directive (EU) No. 185/2010, dated 4 March 2010.

It is defined as a protocol (see Fig. 1) and is composed of the following steps:

1) While preparing a transport unit for shipment, a known consignor seals the unit and places a tag on its opening (see Fig. 2) in a way which prevents it from being opened without removing the tag. In the RFID tag's chip (see Fig. 3) the transport unit's identification (ID), declaration and authorisation bit string (ABN) are stored.
2) Before a known consignor deploys a transport unit, it announces this to a distribution centre by transmitting the transport unit's identification (ID) and declaration to the centre.
3) Upon arrival of the transport unit at a distribution centre, it is authenticated: it is weighed, its identification and declaration are read out from the unit's tag; the transport unit is sorted out as unknown in case it was not announced or its declaration data are inconsistent with its previously collected data.
4) In case the authentication of the transport unit and its consignor were successful, the distribution centre generates two integers, random numbers $p < q$ from the interval (0: length), where "length" matches the number of bits, constituting the ABN, and sends an authorisation request to all its known and accredited consignors, encrypted with the one-time key for its communication with the known consignor who announced the transport unit. Hereby, this consignor is solely enabled to decipher this message correctly.
5) As response this known consignor sends the transport unit's ID and the part of the ABN_TOBE authorisation bit string from the p^{th} to the q^{th} bit, which is compared to the same part of the ABN_ASIS authorisation bit string read out of the transport unit's tag. In case the two sequences match, the transport unit is authorised as known. Otherwise, it is assumed that the transport unit was manipulated and, hence, it is sorted out as unknown.

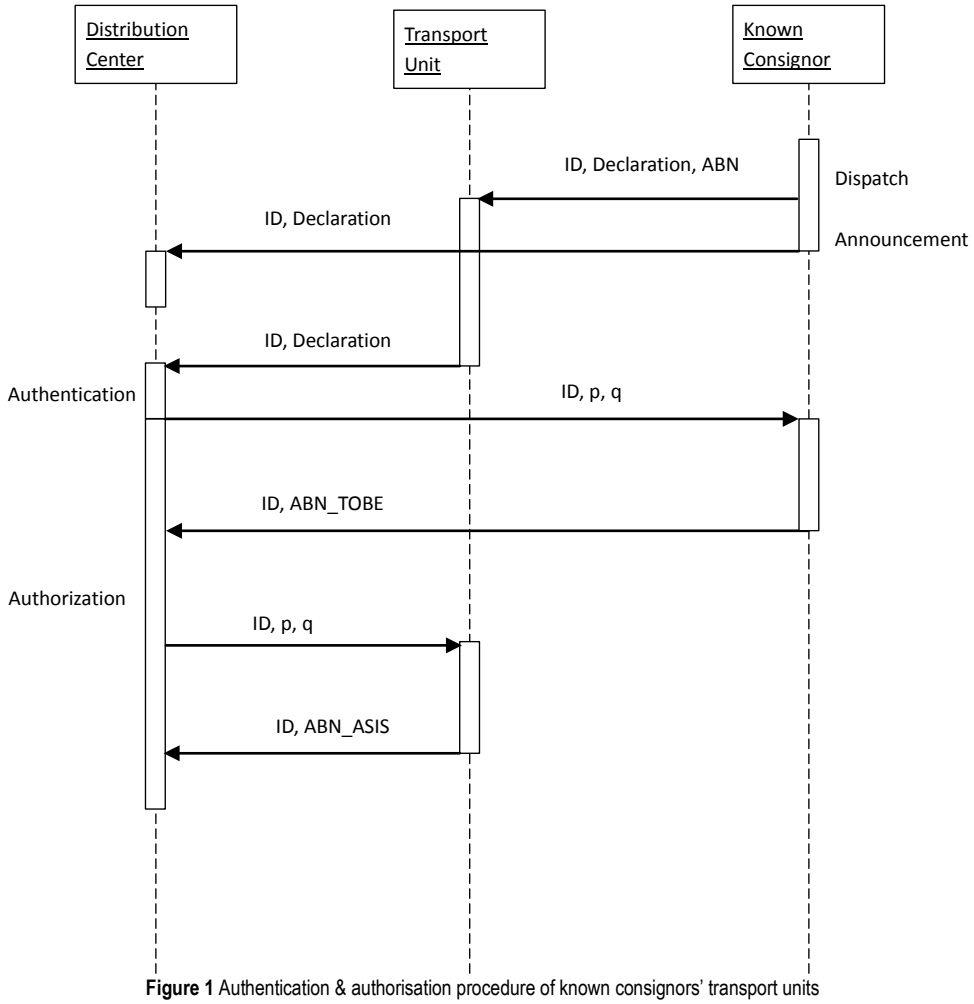

Figure 1 Authentication & authorisation procedure of known consignors' transport units

2.2 Cargo Protection Mechanisms

Automated authentication and authorisation of known consignors' transport units relies on relatively long bit strings that uniquely identify the transport units (ABN) and can be used for the authorisation of known consignors and their transport units. They are stored on sealed RFID tags (see Figs. 2 and 3), readable from the outside of transport units.

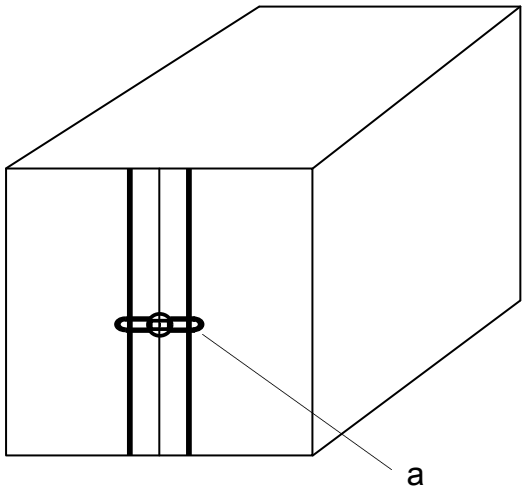

Figure 2 Sealed transport unit with an RFID tracking device

A sealed RFID chip (Fig. 3c) is connected with three sensors (Fig. 3c, 3b and 3d), triggering an alarm in the unit's tag upon electronic tampering, forced removal of the tag or forced opening of the transport unit. An alarm in the unit's tag results in the re-initialisation of its authorisation bit string (ABN), hereby disabling the unit's authorisation and rendering it unknown.

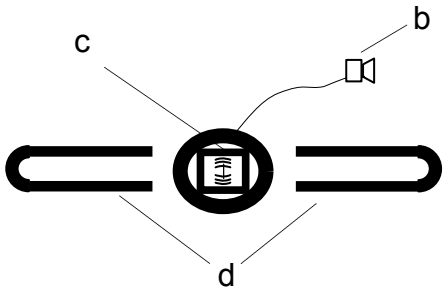

Figure 3 Sealed RFID chip of the transport unit's tracking device with sensors

In addition, any non-protocolled reading and re-writing of the data in the tag's RFID chip would also trigger the alarm.

To protect data transfer among a regulated agent (distribution centre) and a known consignor, one-time key encryption is used, based on keys of message length. A synchronous data transfer protocol (see Figure 1) among pairs of communicating parties ensures that every key is used just once and there is always a new key available.

2.3 Data Protection Mechanisms

The procedure for the authentication and authorisation of known consignor's transport units utilises one-time keys to encrypt the transferred messages, since this is the only way to ensure their complete safety and confidentiality. This is only possible if during encryption all possible encoded messages are equally possible, which makes any conclusions on the original message, made based on an intercepted encoded message, impossible.

Corresponding with the Shannon's theorem on coding data sources [19], an encryption system is completely secure, if and only if the number of possible keys is at least as great as the number of possible messages. This is achieved by equal lengths of messages and keys. Encryption algorithms usually utilise the same key over a longer period of time. Only encryption algorithms, for which holds that the available computing power is not sufficient to test all possible encryption keys for decrypting an intercepted encrypted message, are considered secure. Consequently, in the long run only encryption algorithms, which use one-time keys, are completely secure, considering the Shannon's theorem. Hence, our procedure is based on one-time keys. In the sequel several examples of their generation are presented.

The first example of one-time keys generation is based on sources of non-deterministic noise for every key-bit, e.g. sampling thermic noise of resistors, Zener-diods or transistors and discretisation of the input signal. The sampled values can be stored on ordinary storage media in exactly two samples, one of which goes to the distribution centre and the other to a certain known consignor.

To determine the sequence of using individual keys there are multiple options. It can be determined by the communication protocol or by the order in which they are stored. On the other hand, they can be chosen based on the iTAN-procedure of internet banking, by which for example a distribution centre generates a random number and sends it – unencrypted – to a known consignor, which chooses the current one-time key based on this index.

The second example of generating one-time keys is based on recursive algorithms for generating pseudo-random numbers, where the same algorithms run concurrently at a distribution centre and a known consignor location. They are based on two strictly separate bit-vectors – stable and unstable – and an endogenous signal for switching among the two. By applying appropriate rules for this switching, even very basic time-hybrid systems expose chaotic behaviour. Pseudo-random numbers generators need starting values, which can be acquired, as already elaborated by the first example.

Frequent re-initialisation of recursive algorithms with new starting values at irregular time intervals greatly increases the statistical quality of the generated keys. This can be achieved by means of a distribution centre, choosing the time of re-initialisation and index to choose the next starting value from, by the list of keys, which a distribution centre and a known consignor interchanged at certain point in time on a secure connection and is known only to them.

According to the described solution, every RFID tag is sealed and equipped with a permanent storage. The reason for not accessing it by bytes, but rather considering its whole content as one unique ABN is to increase the number of possible bit-strings for authorisation. Considering a known ABN-length, 2^{length} is the number of all possible ABN combinations. Since its parts, which can start at any random position within this bit-string (random number p), can be used for authorisation, and they are randomly long (random number q), this means that we may have (length×length) possible ABN-parts and a total of ($length^2 \times 2^{length}$) possible combinations. The probability of guessing the position, length and value of a specific ABN is hence ($length^{-2} \times 2^{-length}$), which means that with a realistic ABN-length of 14 bits, this probability would be approximately 3×10^{-7}.

3 ADVANTAGES OF SECURE SUPPLY CHAIN AUTOMATION

To summarize, the key advantages of automatic authentication and authorisation of known consignors' transport units are:

1) The transport units can undeniably and justifiably be associated with known consignors.
2) The transport units' security throughout supply chains is ensured.
3) Falsifications of transport units are recognised automatically.
4) Due to automated procedures for authentication and authorisation of transport units less or even no personnel, who might manipulate the units, may be permitted in their surroundings.
5) Confidentiality and safety of the data flow associated with transport units is guaranteed.
6) In conformance with the procedure for automated authentication and authorisation of known consignors' transport units all telecommunications concerning the transport units and their transport processes fulfil the general goals of security:
   a) confidentiality, i.e. security of access,
   b) data integrity, i.e. protection from unauthorised data manipulation,
   c) authenticity, i.e. protection from forgery, as well as
   d) responsibility, i.e. indisputability.

The combined use of such transport units' tags and the described procedure for automated authentication and authorisation of known consignors and their shipments can guarantee the safety of transport units and the security of their associated data flows in conformance with the Directive (EU) No. 185/2010, dated 4. March 2010. In addition, the overhead associated with the handling of transport units is minimised.

4 CONCLUSION

The described approach to automated authentication and authorisation of consignors and their consignments within secure supply chains reduces the number of persons, involved in goods manipulation and hence also the cost of their training and certification as well as the

risk of tampering. At the same time, it provides for automatic authentication and authorisation of transport units and their consignors and secures the information flow accompanying the shipments, which has already proven beneficial in maritime transport. Along with these benefits it introduces only a minor overhead concerning the implementation of the tags and information interchange protocols.

The suggested authentication and authorisation procedure for known consignors and their transport units shall, hence, minimise the associated overhead and ensure the confidentiality of the information flow among known consignors and regulated agents with high reliability. In the long run its implementation should result in a spread of secure supply chains including also cross-docking options with other types of transport (e.g.: ship, train, road). Considering its information technical support this solution is also suitable for securing the arising intelligent transport units travelling on the physical internet.

Last but not least, according to IATA Cargo Strategy, it combines regulations with actions to proactively support the functional areas of the future IATA Cargo Delivery Model [18]: Safety, Special Cargo, Border Management, e-Cargo & Quality, Operations and Industry Management.

5 REFERENCES

[1] DHL Global Forwarding. Air freight security > German Federal Ministry tightens controls on the supply chain for air freight. Cargo update. (2010). http://www.dhl.de/content/dam/dhlde/logistik/pdf/dhl-logistik-cargo-update-luftfrachtsicherheit-10122010-en.pdf. (27.10.2016)

[2] European Commission. Commission regulation (EU) No. 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the basic standards on aviation security (Text with EEA relevance). (2010). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:055:0001:0055:EN:PDF. (27.10.2016)

[3] European Commission. Information for cargo handling entities in non-EU countries. (2016). http://ec.europa.eu/transport/modes/air/security/cargo-mail/entities_en.htm. (27.10.2016)

[4] European Commission. Commission Implementing Regulation (EU) No 1082/2012 of 9 November 2012 amending Regulation (EU) No 185/2010 in respect of EU aviation security validation (Text with EEA relevance). Official Journal of the European Union. (2012). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:324:0025:0049:EN:PDF. (27.10.2016)

[5] European Commission. Commission Implementing Regulation (EU) No 654/2013 of 10 July 2013 amending Regulation (EU) No 185/2010 in respect of EU aviation security validation checklists for third country entities (Text with EEA relevance). (2013). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:190:0001:0030:EN:PDF. (27.10.2016)

[6] European Commission. ACC3/RA3/KC3 EU AVSEC Validator Information List. (2016). https://webgate.ec.europa.eu/ksda/openAccess.htm. (27.10.2016)

[7] Taxation and customs union (EC). Authorised economic operator. (2016). http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm. (27.10.2016)

[8] Aviation authority. Guidance for known consignors. (2013). https://www.iaa.ie/docs/default-source/misc/guidance-for-known-consignors.pdf. (27.10.2016)

[9] Air Cargo World. Security regulation affects the world, remains relatively unknown. (2014). http://aircargoworld.com/security-regulation-affects-the-world-remains-relatively-unknown-9550/. (29.01.2018)

[10] Republika Slovenija, Agencija za civilno letalstvo, CAA. Seznam reguliranih agentov. (2014). http://www.caa.si/index.php?id=458. (27.10.2016)

[11] Price, J. (2012). Practical Aviation Security: Predicting and Preventing Future Threats, Elsevier Science.

[12] Chang, Y. S., Son, M. G. & Oh, C. H. (2011). Design and implementation of RFID based air-cargo monitoring system. *Advanced Engineering Informatics, 25*(1), 41-52. https://doi.org/10.1016/j.aei.2010.05.004

[13] Jimenez, C., Dauzère-Pérès, S., Feuillebois, C. & Pauly, E. (2013). Optimizing the positioning and technological choices of RFID elements for aircraft part identification. *European Journal of Operational Research, 227*(2), 350-357. https://doi.org/10.1016/j.ejor.2012.10.034

[14] Ngai, E. W. T., Cheung, B. K. S., Lam, S. S. & Ng, C. T. (2014). RFID value in aircraft parts supply chains: A case study. I*nternational Journal of Production Economics, 147*(B), 330-339. https://doi.org/10.1016/j.ijpe.2012.09.017

[15] Lee, H. L. & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics, 96*(3), 289-300. https://doi.org/10.1016/j.ijpe.2003.06.003

[16] Christopher, M. & Peck, H. (2004). Building the Resilient Supply Chain. *The International Journal of Logistics Management, 15*(2), 1-14. https://doi.org/10.1108/09574090410700275

[17] Jüttner, U., Peck, H. & Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. International *Journal of Logistics Research and Applications, 6*(4), 197-210. https://doi.org/10.1080/1367556031000162701 6

[18] IATA. IATA Cargo Strategy. (2015). https://www.iata.org/whatwedo/cargo/Documents/cargo-strategy.pdf. (27.10.2016)

[19] Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal, 27*, 379-423, 623-656. https://doi.org/10.1002/j.1538-7305.1948.tb00917.x

Contact information:

Roman GUMZEJ, PhD, Associate Professor
University of Maribor, Faculty of Logistics
Mariborska cesta 7, 3000 Celje, Slovenia
E-mail: roman.gumzej@um.si

Bojan ROSI, PhD, Full Professor
University of Maribor, Faculty of Logistics
Mariborska cesta 7, 3000 Celje, Slovenia
E-mail: bojan.rosi@um.si