An Innovative RFID Sealing Device to Enhance the Security of the Supply Chain

Francesco Rizzo[1], Marcello Barboni[1], Paolo Timossi[1], Graziano Azzalin[1] and Marco Sironi[1]

Joint Research Centre of the European Commission
Institute for the Protection and Security of the Citizen
Via E. Fermi 2749, 21020 Ispra (Va), Italy

Abstract. One of the most vulnerable elements of the supply chain, from a security point of view, is the commercial container. Due to its nature of transportation vector for goods, it can easily be exploited as a carrier for illegal and dangerous items. In this paper, while acknowledging the need for a global and comprehensive approach to supply chain security, we focus on the security of commercial containers. We discuss the technologies presently used in the field of commercial container security. In particular, we give an overview of the reasearch carried out by the Joint Research Centre (JRC) of the European Commission in the field of supply chain security. We then discuss in-depth the active RFID-based sealing systems designed at the JRC, giving a detailed technological description and presenting the experimental results of the laboratory tests.

1 Introduction

Security threats to transport infrastructures, which have dramatically increased in recent years, have given a considerable boost to the study of a secure transport system. One of the most critical elements in the transport supply chain is represented by the flow of commercial containers. Commercial containers, in fact, are made following obsolete construction rules that do not have security as a primary goal. A huge number of such containers, which are used daily in the global supply chain, are extremely vulnerable. Containers are subject daily to potential physical attacks to their integrity.

Among different proposals considered in order to avoid this security lack, two main solutions can be considered. The first one relies on the use of on-board smart systems that control the internal volume of the container by using different device sensors. These systems are able to send an alarm message to remote servers if a non-authorized door opening has been detected [1], [2], [3]. The second solution focuses on maintaining the physical integrity of the closed container doors by means of mechanical seals. Every attempt to trespass on the container should leave behind evidence on the seal. However, the possibility to physically tamper with the seal during the long journey periods in which containers are not controlled, makes this solution highly vulnerable and ineffective. Moreover, even when the tampering is detected, a mechanical seal cannot provide

Rizzo F., Barboni M., Timossi P., Azzalin G. and Sironi M. (2009).
An Innovative RFID Sealing Device to Enhance the Security of the Supply Chain.
In *Proceedings of the 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges* , pages 7-16
DOI: 10.5220/0002167700070016

information regarding the time and the place in which the infraction took place.

In order to overcome these problems, a new class of electronic seals based on Radio Frequency Identification technology (RFID) has been developed (see for example [4], [5]). The basic idea is to add new security features with respect to standard mechanical seals, by exploiting the capabilities of contactless reading, information storage and remote control distinctive of RFID systems.

The European Commission has considered the raising need of safety in supply chain and has started the analysis of the problem through its scientific and technologic reference centre, the Joint Research Centre (JRC). The JRC has focused its research work on the development of container sealing systems based on the use of passive and active RFID technologies. The main objectives are to satisfy the increasing needs of high security and, at the same time, to be extremely competitive from an economical point of view. In fact, raising the security level and the automation of check operations should bring to a general improvement in the logistic issues of the supply chain.

In the next sections an innovative electronic sealing system, completely developed at the JRC, will be shown. The system is based on the standard RFID technology. However, while current the electronic sealing systems are based on the use of only one RFID technology (passive or active RFID), our solution exploits the conjugated capabilities of both technologies. This choice has been done in order to design a new sealing system able to guarantee a greater security level at relatively low production costs.

2 Sealing Systems

A seal, by definition, is a device that can be applied to an object and that must be broken before access to the object can be obtained. The purpose of sealing an object is to guarantee the identity of the object, and to guarantee that the object has not been altered since the application of the seal.

To fulfill the definition of seal a device must therefore have the following features:

- it cannot be opened, even temporarily, without leaving behind unconcealable evidence
- it is identifiable, and its identity cannot be altered without leaving behind unconcealable evidence

Sealing is a practice that dates back thousands of years, long before the use of writing became common and widespread. Ancient seals were generally impressions on wax or clay (intaglios) obtained through the use of small bone or stone cylinders carved with geometric designs. Seals were used to secure the fastenings on jars, boxes and bags. If the seal was broken, it suggested that the item had been opened. Evidence of the use of seals in Mesopotamia, ancient Egypt, Japan and China dates as far back as 3200BC[6].

As we can see, the definition of seal has not changed much with time. In the field of container security, a seal is a device that is applied to one or both the container doors and that has to be broken in order to gain access to the inside of the container. A seal also carries evidence of its own identity, to ensure that the seal itself has not been replaced.

One very common error found in technical literature is the mix-up of the definitions of seal and lock. While the function of the latter is to deter the opening of the object to which it is applied through its mechanical strenght and robustness, the former is a device that indicates whether the object has been opened or not. The only physical strenght that a seal is required to have is one such that it does not break during normal use.

There exists a wide variety of devices that offer both the seal and lock functionalities, all or in part. For the purposes of this document these hybrid devices will be treated as seals.

Seals are designed to be tamper-evident. Normally, to determine if a seal has been tampered with, a visual inspection is required, as the tampering attempt will have altered in an evident way the physical aspect of the seal. With the use of modern technologies, though, a new family of seals has surfaced. These are seals that carry on board some class of electronics, that extends possibilities of seal inspection beyond the normal on-field visual inspection. These seals are normally referred to as eSeals or Smart Seals.

In literature today there are many different classifications of seals, based on the type technology they employ, on physical characteristics, or on the supposed level of security they offer. In this article we offer the following classification:

Mechanical Seal: a device that carries out the basic function of a seal as described at the beginning of section 2, based uniquely on its physical characteristics. These seals can be made of different materials, ranging from plastic, to thin aluminum foil, to steel in varying degrees of thickness. All these seals share the same sealing principle, e.g. the fact that they cannot be opened and closed back again without leaving evidence behind. This evidence is detected at inspection time, through manual inspection. The identity of these seals is established through the use of a unique identity number embossed on the body of the seal itself. Alteration of this number should not be possible without leaving evidence behind. If a seal is made of two detachable parts, the identity number should be embossed on both parts, to avoid malicious mixing of parts from different seals.

Smart Seals: the definition of this family of seals is very generic, they include any seal that has a form of intelligence built in that extends the functionality of mechanical seals. They are usually able to give more information regarding their status, and allow a number of additional ways of carrying out inspection. For example, a steel seal could be molded with a technique that introduces random imperfections in its internal structure that renders each seal unique, thus giving each seal a unique ”signature”[7]. This signature can then be verified through the use of ultrasonic inspection. These seals are usually designed to alter their signature in a known way when removed. This way they fulfill the definition of seal in that they carry evidence of tampering attempts and a unique identity. Other smart seals include devices that use different technologies to assess their status. These technologies include, but are not limited to, pressure sensors, thermocouples, Speckle signatures [8], holograms, radio frequency identification (RFID).

eSeals: this is a particular category of Smart Seal that deserves a special definition due to their unique characteristics and potentialities. For the purposes of this article and the definition of seal given here, eSeals are seals based on active, passive or mixed

RFID technology. The presence of one or more RFID device embedded in the seal can be exploited for different purposes. For example, the internal memory of the RFID chips can be used to save a log of events, and it is possible to assess the correct closure of the seal to avoid maliciuos ”fake intallations”. An eSeal, in fact, features the possibility to certify that it has been closed correctly and can save in the internal memory the time of closure and identity of the operator who performed the installation. Furthermore, with RFID technology a new way of inspecting the seal becomes possible: in fact, in many applications it is the seal itself that performs a self-diagnosis and communicates its state to the inspector. This way the possibility of human error is greatly reduced, and the quality of inspections depend less on the inspector’s skills and experience than before. When active RFID technology is employed, the seals can be inspected at a distance and on-the-fly (i.e. without physically stopping the cargo). Active seals depend on the presence of an on-board battery for their operation, and this limits the maximum lenght of a single journey.

3 Electronic Active Seal

The electronic active seal developed at the JRC is an integrated sealing system designed and realized with the aim of increasing supply chain security. In particular, this seal has been studied to minimize the tampering possibility of a standard container, by sealing both its doors at the same time, as shown in Fig. 1.

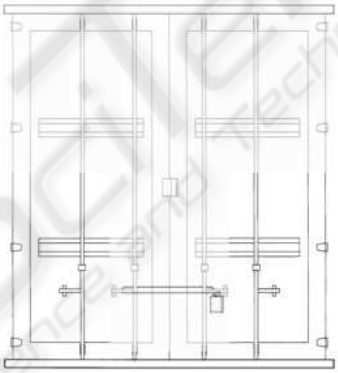

Fig. 1. Schema of a standard container with closed and sealed doors. The electronic seal guarantees the container locking by wrapping both the two bars of the doors.

Fig. 2 shows the external appearance of the electronic seal and its internal structure. The seal is composed by a main plastic body linked to an external cable by two connections. One end of the cable is fixed to the body and cannot be taken out, otherwise the seal would break and the unauthorized opening detected. The other cable end can be inserted in the main body, secured by a ring nut and can be opened.

The electronic components of the system are embedded into both the main body and the external cable. The active RFID circuit is placed in the seal body, together with

a passive low frequency (LF) transponder reader, working at the frequency of 125 KHz. A passive RFID chip is installed in the removable end of the external cable. The passive transponder is used to guarantee the proper closure of the seal: when the end of the external cable is inserted and the seal is closed, the passive system reads the unique identifier (UID) of the passive tag and transmits it to the active transponder. Every active circuit is linked to the UID of a specific passive transponder. Such pairing mechanism is set during the seal production process and ensures that the seal is correctly closed with the right cable (the pairing is signaled through a buzzer at seal closure). Once the seal is closed every attempt of opening it will be detected from the passive RFID system components and signaled to the active circuit logic. The external cable represents another critical component of the system: possible attacks to the system could be done cutting the shielded cable and re-closing it after the container opening. The solution adopted to avoid this problem is the use of a conductive wire inside the external cable. This wire gives an electrical connection to the electronic circuit placed in the main body, which is continuously monitored by the electronics. Any attempt of cutting the cable would result in a loss of electrical continuity for the electronic seal, and thus an alarm would be triggered.

Fig. 2. Left picture: a closed electronic seal with main body, external cable and closure ring nut highlighted. Right picture: internal structure of the electronic seal.

Every tampering attempt will result in a change of the seal state and will be automatically recorded in a memory section of the electronic card. In general, the seal memory will contain information on any possible operation (authorized opening, unauthorized opening or cable cutting) done on the seal during its working time and after its correct closure (i.e. after that the correct pairing between the passive tag and the active seal electronics has been performed). When the seal memory becomes full it is necessary to reset it by using the portable reading system, as explained in the next subsection.

3.1 Interrogation System: Activator and Receiver

The active seal is essentially based on an active RFID transponder equipped with an internal power source. The power source is used to activate the integrated circuits and

to broadcast the response signal to the reader. The transponder is in a sleeping communication state until the reception of an appropriate signal sent by an activation unit (data uplink). This unit sends a microwave electromagnetic carrier radiation, at a frequency of 2.45 GHz. Once the active transponder has been woken, it inquires its memory and sends an appropriate electromagnetic reply at a frequency of 433.92 Mhz. A receiving unit collects the transponder reply (its 32-bit ID code, followed by other data - downlink).

In RFID applications and, in general, in systems based on wireless communication protocols, a relevant topic is the security related to the data transmission. The active RFID seal can be easily exsposed to security attacks such as eavesdropping of the radio communications between the transponder and the reader and cloning attempts [9]. In order to overcome these security risks it is necessary to consider cryptological procedures, in which transmitted data can be encrypted prior of the transmission disallowing a potential external attack.

The power consumption of the active seal depends on the operational state. In the transmission mode, the maximum value of the power consumption is $P_{Max} = 75mW$. However, this value reduces to $P_{Max} = 12mW$ in the receiving state and to $P_{Max} = 4.5\mu W$ in the sleeping mode. Therefore, we have evaluated that using as internal power source a standard lithium battery, the medium life of the active transponder in standard environmental conditions is greater than one year. The transmission logic is shown in Fig. 3.

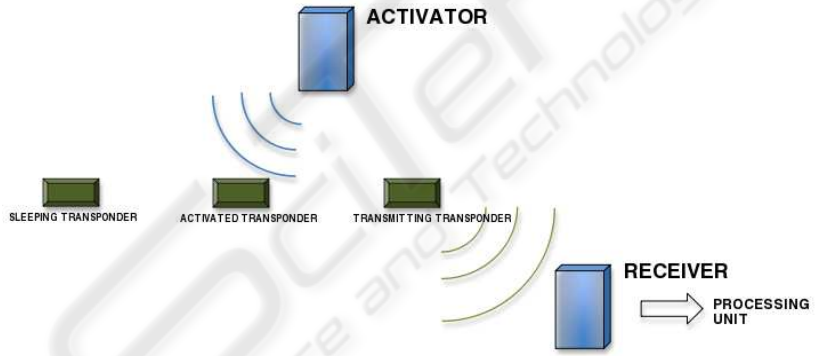

Fig. 3. Schema of the system operation logic. In particular, only transponders that go through the activation field (blue lines) transmit their information status through a 433 MHz electromagnetic radiation (green lines) to the receiver. Finally, the information is sent to a processing unit.

There are two different reading systems for our active seal: a fixed reader composed by two different parts (activator and receiver) and a portable reader, which has the activation and receiving units integrated into one. In Fig. 4 are shown both the reading system solutions.

The portable system is a handheld RFID reader in which the activator and reader units are integrated. This device has the possibility to scan and operate on different seals at the same time. Moreover, due to the small dimensions of the integrated antennas, the reader has a spatially reduced capability of operating on the seals when compared to

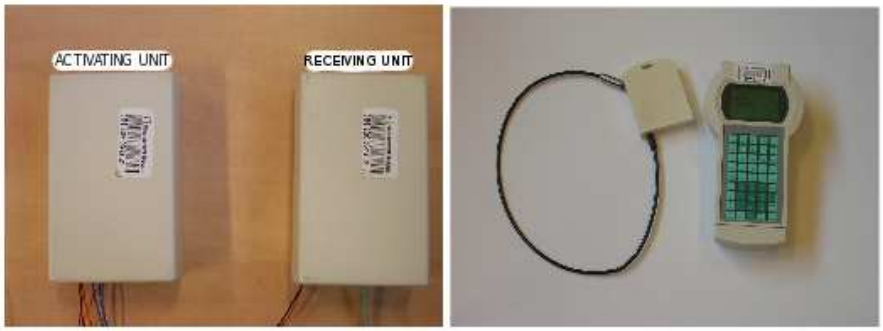

Fig. 4. Left picture: fixed reader solution with separated activator and receiver. Right picture: handheld reader with a closed electronic seal.

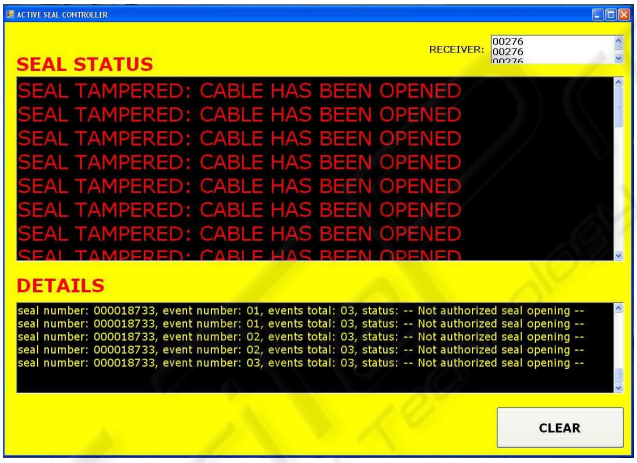

Fig. 5. Screenshot of the application program that manages and shows the operations the status of the electronic seal.

the fixed reading system. For this reason, in order to avoid possible ambiguities when more than one seal falls within the operating range of the fixed reader, only the portable reading system can reset the memory or authorize the seal opening. In addition, after the initial scan of the transponders in the reading region, the handheld device has the possibility of selecting a specific seal and of operating only on its memory. The portable reading system can authorize the opening for a container check. Once the system has sent the authorization signal, the operator has a fixed time window in which the seal can be opened without triggering an alarm. After this time interval, any seal opening will be considered as an illegal tampering operation and recorded in the memory.

An activator and a receiver compose the fixed reading system. Both the components are powered by a 12V (2A) DC current. In order to visualize the transponder data, the receiving unit has an Ethernet module that permits the connection with a processing unit. Once the network connection has been established, the application program will permit the visualization of the data. The application program automatically connects to

the receiver and shows on the screen the memory content of the seals that are in the reading field. In particular, as shown in Fig. 5, the program has two main windows. In the window at the top the seal status is shown. The window at the bottom displays all the details: the seal number, the number of operation read, the total number of operations stored in the memory and the operations made on the seal.

A log file, containing all the information sent by the seals to the processing unit, is automatically opened in the same directory of the application program. If the log file is already present in this directory, the program will append the new data to the existing file.

4 Reading Performance: Experimental Results

In this section we show the main experimental results of the reading capabilities tests carried out on the active RFID sealing system. We have conducted a series of static readings in different conditions by considering both different activation powers and various reader-seal geometrical configurations.

The aim of static reading tests were to determine the performances of the system by considering fixed positions between the active transponder and the reading system. In particular, we focused on the determination of the physical parameters which define the communication region between the active seal and the reading system. We assumed a set up configuration in which the activator was placed next to the receiver, about two meters above the ground, and the seal in front of the two devices. No obstacles were put between the system components.

The planar antenna of the activator generates a microwave carrier radiation with a circular conic lobe. The cone has a planar opening angle of about 90^0. In Fig. 6 we plot the experimental shape of the regions in which the seal is activated by the transmitter and the resulting reply is received by the reading unit, for two different values of the attenuation $Att_i = 10\log(\frac{W_{Max}}{W_i})$, where W_i is the radiation power of the activating unit. The figure shows that the communication region has the conic shape similar to the activation region only near the reader. As the distance between the seal and the reader increases, the size of cone progressively reduces and, at large distances, secondary lobes appear.

Another important parameter is the system reading distance d, defined as the maximum communicating distance along the cone axis. We have evaluated this parameter considering the mean behaviour of a number of seals. In fact, due to unavoidable manufacturing differences, every seal has characteristic activating and transmitting thresholds. Table 1 summarizes the measures conducted at the maximum power emitted by the reader. In particular, we have found the following mean value $\bar{d} = (21.9 \pm 3.6)m$. $\bar{d}$ and its error σ_d were evaluated through the standard statistical analysis:

$$\bar{d} = \frac{\sum_{i=1}^{N} x_i}{N} \tag{1}$$

$$\sigma_d = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \bar{x})^2}{N-1}} \tag{2}$$

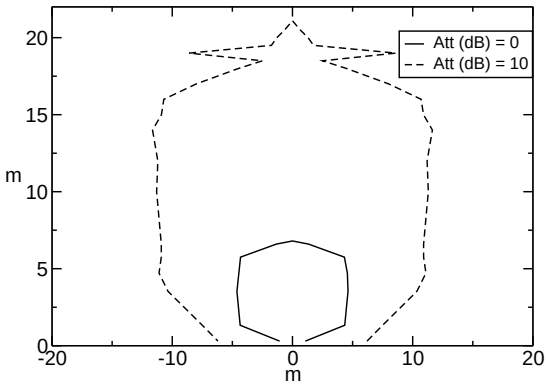

Fig. 6. Shape of the communication region for the system reader-seal. The two regions refer to full activating power W_{MAX} (dashed line) and a tenth of this power $W_{MAX}/10$ (solid line).

Table 1. Main results of the static reading tests.

Attenuation (dB)	Seal Number	Reading Distance [m]
0	1	23.45
	2	17.30
	3	21.10
	4	14.55
	5	21.70
	6	21.60
	7	18.40
	8	18.90
	9	21.20
	10	19.30

5 Conclusions

Aim of this work has been to investigate and design a new sealing system for commercial containers, able to significantly increase the security of the supply chain. A fundamental role in the realization of this new electronic sealing device has been played by RFID technology. In particular, the possibility of information recording, remote control and contact less reading, typical of active RFIDs, has given the possibility to develop a new device with a higher security level than standard mechanical seals.

The main security features studied for the sealing system are:

- possibility to check the proper seal closure by using an internal passive RFID system, and to save operator identity and time of closure in the internal memory.
- possibility to record of every authorized and unauthorized operation made on the seal, with time and date.

– possibility to check the seal status, by remote interrogation of the electronic card memory (2.4 GHz-433 MHz active RFID communication protocol).

Experimental tests were conducted in order to determine the working performances of the system. The results have emphasized that at full power the communication between the system components becomes active and efficient at a mean distance of $\bar{d} = 21.9m$. We have also experimentally found that the shape of the communication region is a cone in proximity of the activator, which narrows as the distance seal-reader increases.

Dynamic reading trials, necessary to define the effective operating distance between the seals and the reading system when transponders are moving with respect to the reader, were not yet performed and will be further investigated. In fact, in this configuration we should consider some additional parameters affecting system perfomance. In particular, every reading data should depend on the relative speed between the seal and the reader.

Finally, the low production cost of the seal (a rough estimate for industrial production is less than 50 euros) makes it highly suitable for large scale use on commercial containers. The system is patent pending.

References

1. Satish T.S. Bukkapatnam and E. Moore and R. Komanduri: Container Integrity and Condition Monitoring using RF Vibration Sensor Tags. Proceedings of the 3rd Annual IEEE Conference on Automation Science and Engineering, (2007) Page(s) 585-590
2. R.J. Craddock and E.V. Stansfield: Sensor Fusion for Smart Containers. The IEE Seminar on Signal Processing Solutions for Homeland Security, (2005) p. 5
3. J. Whiffen and M. Naylor: Acoustic Signal Processing Techiniques for Container Security. IEE Seminar on Signal Processing Solutions for Homeland Security, (2005) p. 7
4. TJoo-Sang Park, Sewon Oh, Taesu Cheong, Yongjoon Lee: Freight Container Yard Management System with Electronic Seal Technology. Proceedings of the IEEE International Conference on Industrial Informatics, Volume , Issue , 16-18 Aug. 2006 Page(s):67-72
5. Won-ju Yoong, Sang-Hwa Chung, Hyun-Pil Kim, Seong-Joon Lee: Implementation of a 433 MHz Active RFID System for U-Port. Proceedings of the 9th International Conference on Advanced Communication Technology, Volume: 1, On page(s): 106-109
6. Encarta Encyclopedia, online version. $http://encarta.msn.com/encyclopedia_761564981/Seal_(art).html$
7. M. Sironi, A. Poucet, F. Littmann, M. Chiaramello,M. Heppleston, G. Weeks: New Ultrasonic Sealing Systems for CANDU spent fuel bundles. Proceedings of the 29th ESARDA Annual Meeting, Symposium on Safeguards and Nuclear Material Management, Aix en Provence, May 22-24, 2007
8. B. C. d'Agraives, M. Chiaramello, E. Mascetti, P. Tebaldi: Identification by Speckle Interferometry. Proceedings of the 29th ESARDA Annual Meeting, Symposium on Safeguards and Nuclear Material Management, Bruges, May 8-10, 2001 Page(s):606-609
9. Nicolas Sklavos, and Xinmiao Zhang, Wireless Security and Cryptography: Specifications and Implementations, CRC-Press, A Taylor and Francis Group, ISBN: 084938771X, 2007.