

Electronic cargo seal for safe and secure supply chain traceability

Jung Ung Min and Minyoung Park*

Abstract

Recently, the United States government plans to introduce electronic container seals on all imported containers as a mandatory requirement. Further, containers without electronic seals may be prohibited or restricted for import based on this planned regulation. An electronic seal is a tamper-free seal with radio frequency identification (RFID) chips embedded in it. It could provide additional security information such as the tamper evidence and the history of tampering status. In this paper, a brief review of the types of container seals, the characteristics of electronic seals, and their system components are presented. International efforts for securing cargo security are also reviewed including Container Security Initiative (CSI), Customs Trade Partnership Against Terrorism (C-TPAT), and International Standards Organization (ISO) requirements. Finally, the current issues and the status of technology development are discussed with future directions as a final word

Keywords: *container; electronic cargo seals; security; supply chain.*

1. Introduction

A simple container seal fixed to the end of a door-locking device can produce high security provided the door's design is enhanced to ensure that the complete door arrangement cannot be easily removed. The International Organization for Standardization (ISO) Technical Committee (TC) 104 Freight Containers has worked on the design of the container doors, its bolts, and hinges to improve security features. This door design is now included in ISO 1496 Series 1 freight containers – specification and testing, the base standard for the technical design of all

Submission Date: 25/9/2006 Acceptance Date: 30/5/2007









*Professors Min and Park are both Assistant Professors in the Graduate School of Logistics, Inha University, Incheon, Republic of Korea. junmin@inha.ac.kr; mypark@inha.ac.kr

containers.

After the co-ordinated September 11 2001 attacks (often referred to as 9/11) by Islamist extremists on the United States, the U.S. government has been contemplating using the electronic cargo seal as a mandatory requirement for all inbound containers to enhance national security. Without this device, all incoming containers may be prohibited from entry into the US, or be under full inspection before customs clearance. An electric seal (e-Seal) is a radio frequency identification (RFID) embedded seal that is designed to enhance container security. In addition to physical security, the device can provide additional real-time information such as location, the time of intrusion while the attached container is waiting in container yards or moving on the ocean, and a history of tampering attempts.

The key aspects of this new device are the survival rate of the seal itself and the integrity of information pertaining to the history of the container’s security status (Table 1). Using electronic seals can provide tangible benefits by reducing costs on the manual checking process of container security. Since the year 1999, a specific workforce in ISO TC 104 discussed various approaches to electronic seals.

Table 1.
Security initiatives

US-Led Initiative	International Initiative
<p>Container Security Initiative (CSI) </p> <ul style="list-style-type: none"> ▪ Targeting and screening at “origin” (before loading) ▪ Use of technology – including “smart” containers 	<p>International Maritime Organization (IMO) </p> <ul style="list-style-type: none"> ▪ ISPS Code amendment to SOLAS Convention ▪ Equivalent to C-TPAT for ports and vessels
<p>Customs-Trade Partnership Against Terrorism (C-TPAT) </p> <ul style="list-style-type: none"> ▪ “Trusted” parties – secure origins and handlers 	<p>World Customs Organization (WCO) </p> <ul style="list-style-type: none"> ▪ Task Force on Security and Facilitation of the International ▪ Supply Chain (data for targeting plus C-TPAT for port hinterland)
<p>24-hour Advance Cargo Declaration (ACD) </p> <p>24-hour Advance Manifest Rule (AMR)</p> <ul style="list-style-type: none"> ▪ Trade Act of 2002 ▪ Advance information to assist targeting 	<p>ISO TC 8 (Technical Committee 8) </p> <ul style="list-style-type: none"> ▪ Establish standards for data, process and technology for marine cargo
<p>Operation Safe Commerce (OSC) </p> <ul style="list-style-type: none"> ▪ Richly-funded set of intelligent freight technology ▪ e-seal, intrusion detection, radiation and biological detection sensors, non-intrusive scanners 	<p>Strategic Council on Security Technology (SCST) </p> <ul style="list-style-type: none"> ▪ Launched Smart and Secure Tradelanes (SST)

In this paper, a brief review of worldwide security initiatives is presented. Associated with these initiatives, we discuss the types and the characteristics of existing seals that have been widely used in container transportation. Then, some of the pilot tests will be introduced with their key findings and implications. Finally, this paper describes recent efforts in terms of standardization and future directions.

2. Security initiatives

Multiple types of responses to security have been initiated by different government organizations, international organizations, and businesses to enhance global supply chain security (Gutierrez and Hintsä 2006). These reactions can be subdivided into US-led and international ones that are summarized in Table 1.

CSI, short for 'Container Security Initiative', is a program that was started by the U.S. Customs Service in early 2002. The main objective of CSI is to ensure security in international supply chains, particularly those ocean cargo transportation. CSI puts teams of Customs professionals in ports around the world to target containers that may pose a risk for terrorism.¹ Minimum standards for CSI are:²

- Checking of all cargo exiting, in transit, or arriving at a port;
- Non-intrusive equipment such as gamma, x-ray or radiation detection equipment available near ports;
- Established automatic risk management system;
- Sharing of information by ports with U.S. Customs and Border Protection (CBP);
- Thorough inspection of ports to resolve infrastructure vulnerabilities.

In addition, the U.S. government has implemented a 24-Hour Rule based on the Trade Act of 2002. This rule requires information on cargo destined for the U.S. to be submitted to CBP 24 hours prior to loading at a foreign port via CBP's Automated Manifest System (AMS). This helps agents analyze container content information and failure to comply this rule would stop the cargo from leaving the port.

The Customs-Trade Partnership Against Terrorism (C-TPAT)³ is a voluntary program that has been jointly established between the government and private sectors to build cooperative relationships for supply chain and border security. Currently, only importers, carriers, brokers, warehouse operators based in the U.S. are eligible to participate in this program, but in the case of manufacturers, no restriction is applied to joining the program. C-TPAT participants can apply for the Free and Secure Trade (FAST) program to expedite goods from Canada to the U.S. (Hu *et al.*, 2005). In C-TPAT, it is required that a high security seal must be affixed to all loaded containers bound for the U.S. More specifically, C-TPAT demands all seals used or distributed by the sea carrier must meet or exceed the current ISO/Publicly Available Specifications (PAS) 17712 standards for high security seals.

Operation Safe Commerce (OSC) was established in 2002 to fund business initiatives aiming to enhance cargo security from packaging to delivery. It started by the U.S. Department

¹http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml

²http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/minimum_standards.ctt/minimum_standards.doc

³http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_criteria/

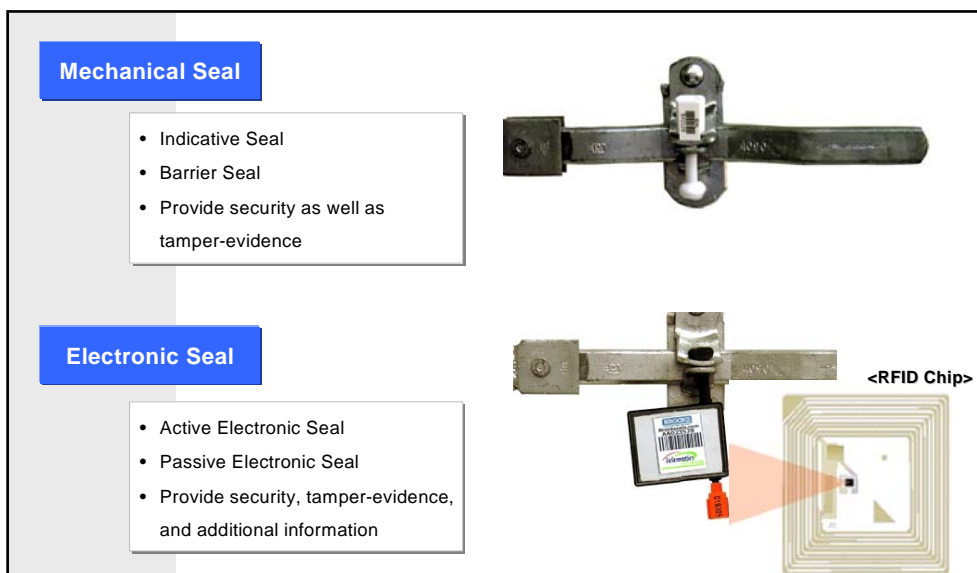
of Transportation (DOT) and CBP. The U.S. government worked collaboratively with industry leaders through OSC and in its second stage, it distributed about US\$28 million in grants to seaports in the Los Angeles/Long Beach, California; Seattle/Tacoma, Washington; and New York/New Jersey regions to develop and implement safe shipping methods.

All of the above mentioned initiatives are not specifically describing specific seal requirements other than C-TPAT. However, C-TPAT's requirements are confined to mechanical seals only, not to electronic seals.

3. Container seals

In general, container seals are more common in international trade than for domestic transportation. For domestic shipments, locks are more common (Wolfe, 2002). Seals themselves have been parts of good security devices that can be traced back to ancient China and Mesopotamia around BC 5000. Using a seal in a container provides information pertaining to the integrity of the container moving through a supply chain.

In a broad sense, two types of security seals are generally available as shown in Figure 1: mechanical seals and electronic seals. The mechanical seals and the electronic seals can be further classified into barrier seals and indicative seals, active seals and passive seals respectively.



Source: photo from EJ Brooks

Fig 1. Type of container seals



Barrier seals are adding physical protection to the traditional tamper indication feature. To remove a barrier seal, it is necessary to have special devices such as bolt cutter. Barrier seals have many variations, from a simple cable type (steel cable) to the bullet-type bolt seals.

An indicative seal is designed to leave evidence of any attempted removal. The seal’s low most subtle attempts at tampering.

Electronics can improve the seal process by improving the completeness, richness, and value of information; and the quality of physical protection (Wolfe, 2002). The basic function of electronic seals is to provide complete and thorough tracking of a container’s status with information on the timing of any tamper attempts.

The classification of electronic seals depends upon the type of RFID chips embedded in security seals. An active electronic seal contains an active RFID chip that initiates automatic communication using its own battery. Since a passive RFID chip does not have its own power source, the electronic seal can only react to interrogating signals from RFID readers. Detailed comparisons between the two electronic seals are shown in Table 2.

Table 2
Comparison of active and passive seals

Classification	Types	Features
Electronic Seal (e-Seal)	Active Seals	<ul style="list-style-type: none"> ▪ Initiate transmissions and response to reader ▪ On board power (battery) ▪ Long range ▪ Omni-directional ▪ More expensive than passive seals ▪ Disposable, Reusable ▪ 433MHz (ISO 18000-7, RFID Standard] 
	Passive Seals	<ul style="list-style-type: none"> ▪ Activated and interrogated by a reader ▪ Battery-free (Semi-passive or batter-assisted passive) ▪ Simple, inexpensive ▪ Short range ▪ Directional for maximizing antenna exposure ▪ 860 – 960Mhz (ISO 18000-6, RFID Standard) 

The core benefit of electronic seals is to increase the traceability of the container’s security status while containers are moving throughout the entire supply chain. As mentioned earlier, electronic seals provide accurate audit trails by detecting any breach or tamper attempts and offering a richer data set such as location, environmental conditions, and even radiation information. In addition, the electronic seals have the capability of immediately reporting any security related events so that authorities can interrupt any criminal intent (Wolfe, 2002). When electronic seals

mount RFID chips on traditional mechanical seals, they also provide the same physical protection as barrier seals.

4. ISO standards on seals

Containers, by nature, are transported in an open system where heterogeneous stakeholders and operators are working collaboratively. Therefore, standardization is an essential prerequisite to realize an efficient international transportation system.

The International Organization for Standardization has published ISO 17712, Freight Containers – Mechanical Seals. It describes standards on high security seal, security seal, and indicative seal. Currently, this standard is adopted by U.S. government: more specifically, it is a mandatory requirement on C-TPAT.

As for electronic seals, a specific workforce in ISO TC 104 has discussed various approaches to electronic seals. ISO 18185, Freight Containers – Electronic Seals describes basic principles on the configuration of attachment of RFID chip and stored data set (identification number, time sealed and opened, and tampering event information. These principles are specifically addressed in the following sections of ISO 18185:

- Part 1, Communication protocol;
- Part 2, Application requirements;
- Part 3, Environmental characteristics;
- Part 4, Data protection;
- Part 6, Messages sets for transferring between seal reader and host computer;
- Part 7, Physical layer.

Since ISO 18185 is using a read-only tag, Part 5, Sensor interface has been withdrawn from its original version.

From the practical perspective of the industry, the World Shipping Council, the International Mass Retail Association, the National Industrial Transportation League, and their member companies have suggested the following requirements for electronic seals (WSC, 2003):

- Have a unique seal number that can be both electronically read and can be read visually, as it is wholly impractical to have electronic readers at all relevant points;
- Record the date and time when the seal was activated or sealed;
- Record the date and time when the seal was opened or breached;
- If a RF device, operate within a single radio frequency bandwidth approved and publicly available in all trading nations;
- Must be able to be read by a universal reader capable of interrogating seals from different manufacturers;
- Must perform reliably in all operating environments with an insignificant number of false

- readings; and
- Meet the minimum physical security standards of the ISO high security seal standard.

Even with the above suggestions, however, it seems that ship owner concern on electronic seals is focused upon the economic aspects, not upon security. Due to this reason, industry practitioners believe that electronic seals are only warranted in the case of very valuable and sensitive cargo such as nuclear waste (Wolfe, 2002).

5. Pilot tests on e-Seals

The Smart and Secure Tradelane (SST) initiative is a private/public initiative to help secure the global supply chain, initiated by the Strategic Council of Security Technology. SST Phase One was completed in 2003 with the secured supply chain networks comprising fixed and mobile RFID readers in 64 nodes across 18 trade lanes (SST 2003). A total of 818 containers were affixed with electronic active seals that included intrusion/tamper detection sensors. In this project all electronic seals automatically reported their identification and security status to fixed or handheld RFID readers at each critical node. This allows integrating the physical supply chain with the virtual information chain. The security process with electronic seals is depicted in Figure 2.

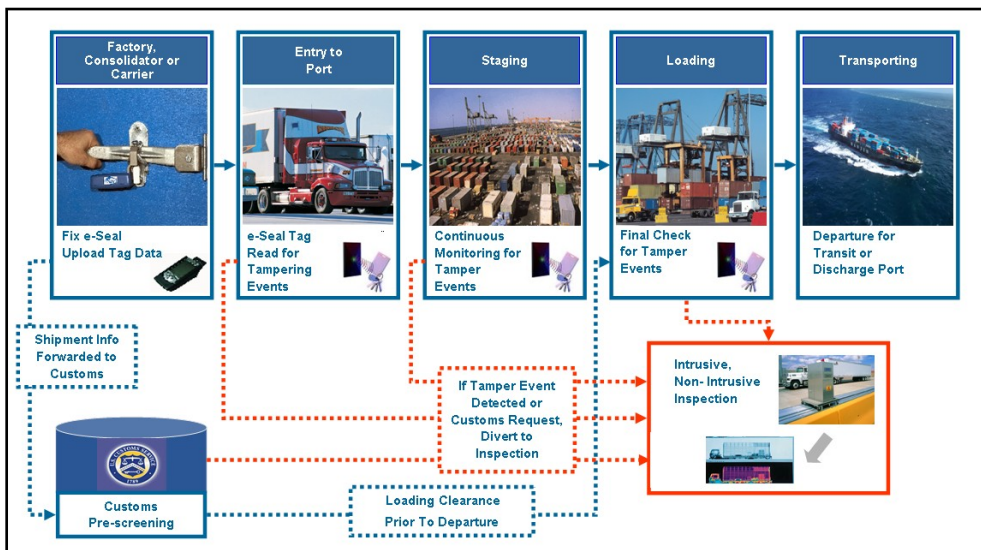


Fig 2. Security process with electronics seals in SST

The estimated potential benefits from the implementation of SST Phase One ranged between US\$378 and US\$462 per container after subtracting the operating and variable costs (SST, 2003). The majority of the estimated benefits of the SST are derived from reducing the safety stock and pipeline inventory; only between US\$28 and US\$34 was regarded as the benefit from increased security. However, it is noteworthy that about 11% of the entire tested container gave a tamper alert to the port authority. Since SST aims to facilitate the use of electronic seals based on their demonstrated success, attention has been focused up on the benefits of having transparent secured supply chain, and not on the technical pros and cons of electronic seals.

As a technology-oriented pilot test, an intensive evaluation of electronic seals was undertaken by the Washington State Department of Transportation (WSDOT) in 2002 (Jensen *et al.*, 2002). In this test, electronic seals were tested and evaluated in two different scenarios: in-bond shipments of containerized produce shipments by truck across the international border, and in-bond auto parts shipments via container ships from Japan.

One of their key findings is that an electronic seal system is acceptable and feasible from a technological perspective, but the system cannot fulfill security requirements on its own. This is because the tested electronic seal does not provide 'real' real-time information. The developed system can help reduce acts of pilferage on containers by being able to track when the container was opened, but it does nothing to stop the potential corruption of a container during shipment. Therefore, the security related data from electronic seal should be integrated with other systemic data to provide for enhanced security against worst-case scenarios such as the smuggling of weapons of mass destruction (WMD). The evaluation team recommended that a national border enforcement procedure should be defined and developed to address an electronic seal which turned out to be 'tampered with' upon reaching a border entry station. Also, they posed a concern because of the reliance upon a single system that has no duplication for secondary security checks, and is not part of any integrated security system. Any technology that is implemented to increase security has to be fully supported and dovetailed with other systems to ensure that the integrity of shipments is verified by multiple checks.

6. Conclusion

Currently, the remaining issues on electronic seals seem to be cost, standardization, and security of electronic seals. From a technological viewpoint, the electronic seal system can be developed in a more sophisticated way should the need arise. But as ship owners have communicated in the World Shipping Council report (WSC, 2003), all if these additional functions are costly and justified only in case of very valuable and sensitive cargo such as nuclear waste. Characteristically, the freight industry operates on thin margins. Seal manufacturers tell of carriers arguing over cents in the costs of seals, but at least all the electronic seals cost much more than traditional seals. Important trade-offs seem to be reflected in whether one chooses to emphasize the purchase cost or the amortized per shipment costs (Wolfe, 2002).

There are also major concerns over the allocation of costs – whether they will be absorbed by

carriers, passed on to shippers, or underwritten by governments – and whether carriers and shippers can offset them with operating efficiencies or insurance benefits. Many carriers emphasize the importance of applying increased costs uniformly to prevent some firms getting an economic advantage.

As shown in World Shipping Council's report in 2003, standardization needs to be adopted in the industry so that a universal reader can interrogate any respective of manufacturer. Without global standard, the current technique includes shortcomings that might become a severe problem in any future practical application. Therefore, standardization work should continue to define technical solutions for the electronic seal for the day-after-tomorrow.

Finally, more attention needs to be given to the security of electronic seals. Definitely, the commercial availability of these devices and their readers, at reasonable and competitive prices, will be a significant factor to carriers, shippers, and terminal operators in their decision regarding whether to use manual or electronic seals as an indicator of in-transit tampering. However, as Johnston (2003) highlighted, it is important to recognize that e-seals are not necessarily a solution to containerized cargo security concerns. Furthermore, even the current ISO proposal (18185) has been attacked for its poorly defined security functions. More specifically, the current proposal does not provide data integrity function and if 'digital signature security scheme' is used, the communication time will be extended by between 40 % and 100 % (Barlas, 2005).

Even with these concerns, however, electronic seals have the potential to make positive impacts upon both security and operational efficiency. If we can resolve the issues outlined above, electronic seals can not only enhance supply chain traceability but also in a safer and more secure manner.

References

- Barlas, S. 2005. ISO reconsidering e-seal specification. *RFID Journal*. <http://www.rfidjournal.com/article/articleview/1696/1/1/>
- Gutierrez, X., and J. Hints. 2006. Voluntary supply chain security programs: A systematic comparison. Paper presented at the International Conference on Information Systems, Logistics and Supply Chain, Lyon, France.
- Hu, Y., Z. Khan, and M. Young. 2005. Balancing security and efficiency: An assessment of approaches utilized in containerized cargo security. Paper presented at the 11th Annual GTTL (Global Trade, Transportation and Logistics) Conference, Seattle, WA.
- Jensen, M., N. Williamson, R. Sanchez, A. Newton, and C. Mitchell. 2002. WSDOT intermodal data linkages freight ITS operational test evaluation final report. Washington, D.C.: U.S. Department of Transportation.
- Johnston, R. G. 2003. Tamper-indicating seals: Practices, problems and standards, Los Alamos, NM: Los Alamos National Laboratory.

- SST. 2003. Network visibility: Leveraging security and efficiency in today's global supply chains. Smart & Secure Tradelanes (SST).
- Wolfe, M. 2002. Electronic cargo seals: Context, technologies, and marketplace. North Mansfield, MA: North River Consulting Group.
- WSC. 2003. In-transit container security enhancement. Washington, DC: World Shipping Council.