3.3 SCS Technologies for Container Integrity: Container security devices and seals

Container Security Devices (CSD) play a crucial role in ensuring the integrity of the container along the supply chain and facilitating trade and Customs processes. Cargo security can be enhanced through the use of both mechanical and electronic seals. Both mechanical cargo seals and e-Seals act as barriers against pilferage, smuggling, and sabotage of cargo within containers and trailers en route to their destination. If either type of seal is found to be broken or if its identification (ID) number is different from the one on the cargo document, this is an indication that the container or trailer door might have been opened by an unauthorized person at some point in the transportation route. The unique ID numbers on both mechanical and e-seals provide tracking information. It is expected that the ID number on either type of seal will be recorded at each handoff in the chain of custody to provide information about when and where the container or trailer was handed over and the seal status at that time.

Ideally, seals should only be placed on containers by the party directly responsible for stuffing and/or visually verifying the contents of the container. In this respect, it should be stressed that the party responsible for stuffing and sealing the container is the first, and most important, link in a “secure” container transport chain. One must however remember that even high-security mechanical seals are only as good as the procedures in place to affix, monitor and document them at each transfer of responsibility.

3.3.1 Mechanical Seals

For the purposes of this document, the following terms and definitions from ISO 17712 apply. The classifications and types are outlined below.

A mechanical seal is a device marked with a unique identifier and is often marked by the seal owner’s or issuer’s stamp and/or color. It is externally affixed to the container doors and designed to evidence tampering or intrusion through the doors of a container and to secure closed doors of a container. In addition, depending on its construction, the seal provides varying degrees of resistance to an intentional or unintentional attempt to open it or to enter the freight container through the container doors. Even if a tampered seal were to be replaced with a similar unit after entry, the seal’s unique identification number might not match with the one that was recorded when the original seal was affixed. The sealing process for security seals is as important if not more important than the seal itself.

Proper sealing protocols are comprised of a number of elements including the following:

- Purchasing/sourcing and shipping procedures for seals
- Training in seal use and verification
- Tracking of seal inventories and safe storage/release procedures
- Correct application of seals
- Recording seal numbers
- Managing and transmitting seal numbers
- Recording seal operations and identification of people involved and time and date
- Recording seal anomalies
End-of-use and end-of-life disposal of seals.

Without proper sealing and checking protocols, the use of seals can be counter-productive as they can instill a false sense of security as to the status of the container handle/door. In theory, security seals should prove effective in detecting any attempt to tamper with the container.

In reality, however, simple security seals are relatively easy to defeat. The reasons are numerous but include the ease with which they can be cut, the possible lack of proper seal documentation, the possibility of poor security management in the container transport chain and the relative ease of replicating certain seals and their numbers. As with simple indicative seals, verifying the seal is both a manual and time-consuming process and thus many seals are only summarily checked, if checked at all, while in transit. Finally, and this is not a problem unique to security seals, experienced thieves have devised ways to bypass the handle or the container doors entirely when gaining entry to the container.

One must however always remember that even high-security mechanical seals are only as good as the procedures in place to affix, monitor and document them every time the container changes hands (at each transfer of responsibility).

In addition, once illegitimate cargo stealthily finds its way into a container prior to affixing the seal, the sealed container will be as good as a legitimate passport all the way to destination. This is why upstream supply chain security procedures must include the company, personnel and facilities that produce, pack and stuff the cargo into the container.

3.3.1.1 Types of mechanical seals

High security seals

This is a seal that is constructed and manufactured of material, such as metal or metal cable, with the intent to delay intrusion. High security seals generally must be removed with quality bolt cutters or cable cutters. They require inspection to indicate whether tampering has occurred or entry has been attempted. According to the 9/11 Commission Act of 2007, effective October 15, 2008 all containers in transit to the United States shall be required to be sealed with a seal meeting the International Organization for Standardization Publicly Available Specification 17712 (ISO/PAS17712) standard for sealing containers. It is crucial that companies are aware that all cargo arriving by vessel at any port of entry in the United States are required to be sealed with a seal meeting the ISO/PAS 17712 standard for High Security seals. The WCO has also endorsed the ISO 17712 standard for seals.

There are many types of seals on the market that meet or exceed the ISO 17712 standard and many seal manufacturers. Businesses are responsible for acquiring seals from legitimate manufacturers. Companies purchasing seals should be backed by the seal manufacturer’s test report issued by an independent ISO17025 certified testing laboratory. Businesses should maintain this documentation for future reference. While this guide does not endorse any particular seal manufacturer or product, there are organizations, such as the International Seal Manufacturers Association (ISMA) that can provide information on seal manufacturers offering ISO PAS 17712 high security seals.
A variety of High security Seals is shown below:

**Padlock seal**: Locking body with a bail attached: either wire shackle padlock (metal or plastic body), or plastic padlock and keyless padlock seals.

**Cable seal**: Cable and a locking mechanism. On a one-piece seal, the locking or seizing mechanism is permanently attached to one end of the cable. A two-piece cable seal has a separate locking mechanism which slips onto the cable or prefabricated cable end.

**Bolt seal**: Metal rod, threaded or unthreaded, flexible or rigid, with a formed head, secured with a separate locking mechanism

**Barrier seals**: Designed to provide a significant barrier to container entry. A barrier seal may, for example, enclose a portion of the inner locking rods on a container. Barrier seals may be designed to be reusable.

**Security seals**

Seal that is constructed and manufactured of material that provides limited resistance to intrusion and requires lightweight tools for removal. Security seals require inspection to indicate whether tampering has occurred or entry has been attempted.

**Wire seal**: length of wire secured in a
Some examples are crimp wire, fold wire and cup wire seals.

Strap seal: metal or plastic strap secured in a loop by inserting one end into or through a protected (covered) locking mechanism on the other end

**Indicative seals**

Seal that is constructed and manufactured of material that can easily be broken by hand or by using a simple snipping tool or shear. Indicative seals require inspection to indicate whether tampering has occurred or entry has been attempted.

Cinch or pull-up seal: indicative seal consisting of a thin strip of material, serrated or non-serrated, with a locking mechanism attached to one end. The free end is pulled through a hole in the locking mechanism and drawn up to the necessary tightness. Cinch or pull-up type seals may have multiple lock positions. These seals are generally made of synthetic materials such as nylon or plastic. They should not be compared to simple electrical ties

Twist seal: steel rod or heavy-gauge wire of various diameters, which is inserted through the locking fixture and twisted around itself by use of a special tool.

Label or Tape seal: These seals are self-adhesive and self-voiding seals. They are used as an adjunct security protocol on doors for any container. They are hand applied by removing the protective paper backer and sticking them to the container over or under the keeper bars. They are used to visually indicate tampering or opening of the doors while unattended. These seals work as a silent sentry to monitor doors where bolt seals, plastic seals or other conventions seals cannot. Bolts or any seals placed in a normal right hand seal hole are easy to circumvent. Tape door seals are manufactured with barcode, coated with anti counterfeiting components. This application procedure will indicate if the doors had been removed. These seals are easy to visually interrogate and they provide a formidable barrier to thieves against surreptitious entry. As a chain of custody tool, anyone seeing them violated will immediately know with little or no training.

**3.3.2 Electronic Seals**

The need to further secure containers containing high value goods has led to the development of several types of so-called “smart” seals. These types of seals have integrated physical security and information management capabilities. It is the latter functionality that sets these aside from their mechanical
counterparts since they can transmit data regarding their status as well as the information regarding the contents of the container. At a minimum, an electronic seal system combines a physical sealing device with a data chip capable of recording and restituting basic information regarding the container contents, such as an electronic cargo manifest, and a mechanism for reading the information recorded on the chip. A higher level of functionality is added by systems capable of electronically communicating whether the seal has been broken or otherwise tampered with. These seals use radio frequency (RF), infra-red (IR) or fiber optics to transmit data. In their most advanced iterations, electronic seals can be coupled with a variety of sensors (e.g., radioactive, radiological, chemical, biological, light, CO2, etc.) that can record and communicate data regarding the in-container environment. In combination with a global positioning system (GPS) transceiver, alerts or status messages regarding the container can be transmitted in real time to a central processing system that can pinpoint the container’s location. The following section on e-seals is outlined in the Organization for Economic Co-operation and Development and European Conference of Ministers of Transport *Container transport security across modes* (2005).

**What do e-seals monitor?**

E-seals only monitor the seal’s status and that of any sensors connected to the seal – they do not monitor the condition inside the container. This nuance is important. As pointed out earlier, a container’s integrity can be compromised without compromising the integrity of the seal. Even when sensors are attached, the seal records sensor events which may or may not reflect what is actually happening within the container environment. “False-positive” readings from sensors are a particular concern but one should not overlook the possibility that sensors can be defeated by more or less sophisticated means.

**What do shipping-related information e-seals provide?**

E-seals cannot provide detailed information on the contents of a container. What they do provide is information regarding what the party responsible for sealing the container said was in the container. If that party was an originating shipper, one might assume that the information is more or less correct. However, if that party is once or twice removed from the originating shipper like in the case of a carrier placing an e-seal on a container that arrived at the terminal with a non-conforming mechanical seal, then the shipping documents loaded into the seal’s memory only reflect the e-seal-affixing party’s best available information as to the contents of the container. In a worst case scenario, a conforming e-seal on a container containing illegitimate cargo might actually facilitate the transport of that cargo, rather than prevent it. Non-declaration or mis-declaration of goods is not an unknown phenomenon in international transport, and the catastrophic outcomes of certain incidents such as mislabeled calcium hypochlorite or fireworks-containing containers, highlights both the reality and the risk of such situations. Any sense of security instilled by the presence of an e-seal on an intentionally mis-manifested container containing a WMD would have dramatic consequences.

**E-seal infrastructure**

For e-seals to be an effective part of a global container security strategy, they must be accompanied by a host of reading devices/scanners, computer hardware and a suite of underlying information
management software systems capable of properly processing the seal data. Today, these requirements are far from being met, and their fulfillment throughout the container transport chain is not at all assured in the near future. It is likely that major terminal operators will be the first to place e-seal readers at strategic locations within their container terminals and to use such systems to monitor and track the status of such seals. Some of the major maritime carriers might start to deploy e-seal readers as well. However, it is not at all sure that smaller ports will be able to deploy and effectively manage such systems in the medium term. Furthermore, while it is feasible that major railroads and barge operators might also be able to deploy the underlying infrastructure and hardware necessary to support e-seals, it is highly unlikely that small road carriers and smaller barge/rail operators will be in a position to do so any time soon – if ever. What is likely to emerge is uneven support for e-seals across the container transport chain with certain high security nodes capable of processing e-seal data punctuated by areas of low or no e-seal functionality. Properly identifying the boundaries of these zones and developing appropriate container transfer protocols among these zones are necessary components of a comprehensive container security plan.

**Types of E-seals**

There are four types of e-seals, classified by the four different communication systems used between the seal and its "reader:"

- Radio frequency identification (RFID)
- Infrared (IR)
- Direct contact, and
- Mobile GSM or satellite.

The following data is provided by the US Department of Transportation office of Freight Management and Operations:

**1- RFID Seals**

RFID technologies are most common among electronic seals. Fundamentally, they marry RFID transponders or their components with manual seal components. There are two main types of RFID tags and seals, passive and active.

Passive seals do not initiate transmissions—they respond only when prompted by the device used by a reader. A passive seal can identify itself by reporting its ID similar to a standard bar code. The tag can also perform processes, such as testing the integrity of a seal. A battery-free passive seal is simple, inexpensive, and disposable. Passive seals tend to be short range and directional to maximize antenna exposure to reader signal strength. Maximum read range for electronic seals without battery-assisted communications tends to be two-three meters, with some debate in the industry about efficacy beyond two meters.

Active seals can initiate transmissions as well as respond to interrogation. All active tags and seals require on-board power, which generally means a battery. A major attraction of active tags
and seals is the potential for longer-range and Omni directional communications—up to 100 meters. Expressed user needs for greater range and the ability of signals to wrap around obstructions in terminal operating environments prompted the international standards group working on electronic seal and read/write container RFID standards to add active RFID protocol(s).

Theoretically, the only difference between passive and active tags and seals is the ability to initiate communications from the tag—a distinction that means passive RFID tags could not initiate mayday calls. However, a designer could add on-board power to a passive tag, match other functionality and, setting aside regulatory, safety, and cost issues, increase read range and directional flexibility by increasing power and adding antennas. This perspective seems most appropriate to laboratory R&D discussions.

2-Infrared Seals

IR is a less common choice than RFID. It does not appear to be any standards issues about IR, but there are unresolved disagreements about its technical merits. Reported industry concerns include short range, slow data rates, effects of fog and rain, and susceptibility of some designs to generate false positive tampering signals. In addition, infrared systems are directional, offering line-of-sight performance without an ability to wrap around corners.

3-Contact Seals

These seals work in most harsh weather environments. Contact and near-contact technologies include contact memory buttons, PDA and electronic key plug-ins, low frequency RFID, and short range IR. Proponents of contact and near-contact solutions argue that it is important to have a human being visually observe the seal, and their solutions provide that added benefit. Proponents of longer-range solutions criticize the missed opportunity for labor and process timesaving.

4-Remote Reporting Seals

Remote reporting uses satellite or cellular communications. The great advantage is the ability to maintain visibility en route and to obtain near real-time event reports. It is a high-end capability, usually at high cost. As costs drop, it will become increasingly attractive for security and management applications, especially for high-value and hazardous cargo.

**Box 3-1 Comparison of E-seal technologies**

<table>
<thead>
<tr>
<th>Type</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| RFID | Broad array of capabilities  
Passive can be very low cost  
Active can be high capability and moderate cost | Lack of standards, but this is being addressed  
Lack of global frequencies, especially in regard to active RFID |
<table>
<thead>
<tr>
<th>Category</th>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR</td>
<td>Clearly effective at short ranges</td>
<td>Lack of clarity on strengths and shortcomings—contradictory information</td>
</tr>
<tr>
<td>Contact</td>
<td>Some are highly reliable in harsh environments</td>
<td>Contact &quot;keys&quot; subject to loss and misuse</td>
</tr>
<tr>
<td>Remote</td>
<td>Potential for immediate identification of problems Potential global coverage</td>
<td>High cost Usually requires significant outbound power</td>
</tr>
<tr>
<td>All</td>
<td>Potential to improve efficiency along with security</td>
<td>Risks of increasing complexity, opening new avenues of attack, and generating false confidence Need for independent assessment of vendor claims Need to assess operational impacts as well as technical performance Requirement to manage and sift increased data flow, identify false positives, and act on true positives</td>
</tr>
</tbody>
</table>

Source: US Department of Transportation
How do they work?

Before its installation on the container the e-seal must be programmed with a handheld device by validating the container number, container type and eventually the content. The RFID bolt seal is then read at each check point using the same readers as the Container tag.

Once the RFID is installed on the container and the data is loaded it will signify if the door has been tampered with.

E-seal standards

For e-seals to be effective in helping to secure international trade, they must be useable throughout the global container transport system. This means that any e-seal affixed to a container must be readable in any transport node equipped with e-seal readers, and, conversely, reading/scanning equipment in any transport node worldwide should be capable of reading any e-seal passing through. This is not the case today as many competing vendors have proposed numerous and sometimes incompatible systems. However, many administrations and the trading community in general now agree that broadly accepted standards are necessary if e-seals are going to be effectively deployed throughout the supply chain. At a minimum, these standards should separate proprietary hardware solutions from information transmission protocols and codes.

3.3.3 Conclusion: seals

Ensuring container integrity is fundamental to ensuring container security. However, past experience with anti-theft devices and container door/handle seals have revealed the inadequacy of these devices to fully protect containers from and/or reveal unauthorized access by determined criminals. Clearly, better seals must be deployed if the container is to be targeted by terrorists. However, it would be incorrect to believe that a technological fix in the form of an advanced mechanical or electronic seal alone would be sufficient to ensure that containers are not tampered with during their voyages. Any container seal is only as good as the container stuffing and sealing process in which it is involved. This process must include controlled stuffing procedures by the shipper, seal identification and management throughout the seal’s lifespan (and not just during the container voyage).

Distinction should be made between the data recorded and managed by an e-seal system that has particular security relevance such as seal status and container number, and the data that could potentially be recorded and managed by e-seal systems that have more utility from a supply chain management perspective.

Adoption of RFID in supply chain and security applications is hampered by a lack of standards and by what some call “the frequency wars.” The two issues are interrelated. RFID has no global protocols or standards. For instance, RFID on which the data ride in the US will not work anywhere else. In short, RFID for container security is applicable only to those areas of the world that have agreed on the same
frequency. Therefore, only a combination of RFID and satellite communication integrally linked to a human agent provides both security and logistics value in a global supply chain, and by its nature becomes the “smart container.” The technologies that would make the container smart are RFID, satellite, and cellular.

However, there is still a long way to go before the “smart container” can be considered a candidate for generalized use in the supply chain. To start with, the question of specifications and interoperability needs to be solved:

“Specifications must address issues such as:

- what specifically the device would be required to do and its security value
- what acceptable false positive and false negative reading rates would be
- what radio frequency would be used
- the requirements for the installation and operation of the necessary device reader infrastructure
- the requirements applicable to the necessary communications interface and protocols with Customs
- the security vulnerabilities of such devices
- the necessity of interoperability of various vendors’ devices and systems
- the data to be captured and transmitted by the device
- identification of who will have access to the data in the device
- survivability and vulnerability of the device
- power or battery life requirements
- the probability that the device can be detected, or removed without detection
- required data messaging formats, event logs, and data encryption.” ¹

¹ Statement of World Shipping Council (WSC) before the House Homeland Security Appropriations Subcommittee Regarding “Container, Cargo and Supply Chain Security – Challenges and Opportunities.” April 2, 2008