2008: milestone year for the e-Seal?

Mark Nelson, International Cargo Security Council, Washington, DC, USA

During the past year, several milestones set the course for electronic seals (e-Seals) to help automate the visibility and security status of cargo containers as they move throughout the global supply chain. As a result, 2008 could prove to be the year that shippers more broadly deploy e-Seals in their ongoing efforts to improve chain-of-custody surety, speed customs clearances and enhance operational efficiency.

What is an e-Seal? A sub-set of electronic 'container security devices,' e-Seals combine Radio Frequency Identification (RFID) electronics with the traditional mechanical pin and cap used to lock container doors. The RFID component can send data and automated alerts over radio waves to networks of interrogators which identify a container's location as well as whether the seal has been tampered with or broken.

Rise of the e-Seal

RFID-based e-Seals have been on the supply chain community's radar screen since soon after 9/11, but real momentum built up only in the last year. Three milestones have been passage of the US SAFE Act, approval of ISO 18185, and wider, non-discriminatory availability of e-Seal patents.

The first milestone occurred last autumn with the passage of the SAFE Port Security Act of 2006 in the United States. The Act permits the use of qualified container security devices and technologies as a way for users to achieve Tier III status under the Customs-Trade Partnership Against Terrorism (C-TPAT) program. By demonstrating this extra measure of security, Tier III C-TPAT participants would face fewer inspections and faster, more reliable customs clearance.

The SAFE Act does not mandate the use of security technologies – it offers incentives for voluntary use. This approach gives a competitive advantage to early adopters and ensures an achievable, first-step in what promises to be a long-term evolution of container security technologies.

The Act also encourages the US Department of Homeland Security to develop requirements "consistent with standards promulgated by international standards organizations, such as the International Organization for Standardization (ISO), the International Maritime Organization (IMO), and the World Customs Organization (WCO)."

The second milestone occurred in April when the ISO approved technical and application standards for e-Seals under ISO 18185. This did not happen overnight. ISO 18185 was a global three-year effort involving input from ocean carriers, terminal operators and technology providers. ISO 18185 incorporates standards for active RFID operating at the 433 MHz and 2.4 GHz ranges as well as performance standards for mechanical seals.

e-Seals combine Radio Frequency Identification (RFID) electronics with the traditional mechanical pin and cap used to lock container doors.

The developers of ISO 18185 shared the dual goals of the SAFE Port Act: to enhance supply chain and port security without impeding international commerce. Because the standard is based on best practices, it minimises the possibility of inaccurate information caused by manual data entry as well as possible security 'hacks' while adding another layer of security and detection. The DHS *International Supply Chain Security* report to Congress this July cites ISO 18185 as a reference point as a chain-of-custody standard.

The third milestone was the proliferation of the intellectual property (IP) embodied in ISO 18185. Many ISO standards contain proprietary technologies, but technology owners agree to make their IP available to competitors on a reasonable and non-discriminatory basis. Savi Technology, which owns patents on the 433 MHz 'air interface protocol' in ISO 18185, initiated a licensing program. So far, six companies in Asia, North America and Europe have 'signed up;' these are companies that want to develop and sell e-Seals based on the ISO standard. This licensing programme is helping to fuel market growth around the standard, providing greater competition, innovation and choices for end users.

The next step

Even with all these advances, there is one more important step needed to accelerate widespread adoption. DHS still needs to issue performance requirements for C-TPAT Tier III-eligible container security devices. E-Seals may come into broader use without – or in spite of – DHS Tier III requirements, but a lack of clarity inhibits deployments beyond pilots or localized operations.

DHS was supposed to issue its performance requirements for container security devices early last summer, and as of this writing they had not yet been issued. Once the requirements are issued, US Customs and Border Protection, which is part of DHS, will spend 60-90 days testing devices from different companies to ensure they meet their minimum requirements. While many in the international supply chain have already started using e-Seals, DHS guidelines will encourage more adopters.

Of course, the US is not the only entity interested in enhanced cargo security. The World Customs Organization (WCO) and the European Commission (EC) have indirectly spurred more rapid adoption of e-Seals in the past few months. This comes about as national customs authorities begin offering Authorized Economic Operator (AEO) advantages to importers based on the WCO's SAFE Framework of Standards, which includes a Seal Integrity Programme. Policy clarity from international regulatory authorities provides confidence to those that have adopted and those considering adoption of e-Seals.

The advantages of e-Seals, and the networks in which they're monitored, have the potential to transform the supply chain into a more fully automated and transparent operation.

The advantages of e-Seals, and the networks in which they're monitored, have the potential to transform the supply chain into a more fully automated and transparent operation – the long overdue goal of supply chain visionaries for decades. By focusing on standards-based e-Seals, such as ISO 18185, multiple types of devices can function interoperably in different networks, much like cell phones are able to 'roam' from one network to another.

The benefits of e-Seals vary depending on the stakeholder in the supply chain. Carriers would prefer to 'hold off' on using e-Seals, but if some kind of security device is mandated they would most likely prefer electronic seals compliant with ISO 18185 over mechanical seals because e-Seals are not labour-intensive. Port operators where network infrastructure is installed to monitor tagged containers would have a competitive advantage by offering greater efficiency, management and security through their facilities. Shippers who own the goods would be the greatest beneficiaries because of improved operational efficiency, faster customs clearance and, of course, security.

E-Seals are not a silver bullet. They should be viewed as part of a multi-layered approach to security that also takes into account best practices, people and other advanced technologies. With their multiple side benefits though, standards-based e-Seals can help to deliver new and better ways that help automate the supply chain so that products gets from source factory to store shelf more efficiently and securely. 2008 should mark a turning point for the e-Seal, adding new levels of value and visibility to the global supply chain.

ABOUT THE AUTHOR AND THE COMPANY

Mark Nelson is a Board Member of the International Cargo Security Council. He is also Sr. Director of Corporate Communications at Savi Technology, Inc., a Lockheed Martin Company.

The **International Cargo Security Council (ICSC)** is a professional association of cargo transportation and security professionals from the entire spectrum of cargo security: Air, truck/rail, maritime, and intermodal. Its success hinges on each member's personal concern for the safe and secure movement of the nation's commerce. The ICSC has four objectives: To improve cargo transportation security through voluntary government/industry efforts; to serve as a central clearinghouse for the collection and distribution of information relating to trends, techniques, and efforts to prevent cargo-related crimes; to provide a platform to address transportation industry matters relating to security of cargo; and to assist and support voluntary and self-help initiatives by government, transportation centres, and industry cargo security interests to develop effective efforts and programmes to combat cargo loss.

ENQUIRIES

International Cargo Security Council (ICSC)
1255 23rd Street
NW Suite 200
Washington
DC 20037
USA

Tel: +1 202 452 1200
Fax: +1 202 833 3636
Email: admin@cargosecurity.com
Website: www.cargosecurity.com