An update on ISO activities regarding electronic container seals

Craig K. Harmon, Chairman, ISO TC 122/104 JWG, President & CEO of Q.E.D. Systems, Cedar Rapids, Iowa, USA

Background on RFID standards

On June 7th, 1999 a New Work Item Proposal was filed with the International Organization for Standardization (ISO) entitled, 'Radio-frequency communication protocol for electronic recognition of seal status and number, and container number.' By the conclusion of the 2nd meeting of the working group assigned this work item (ISO TC 104/SC 4/WG 2) on July 29th, the title had been modified to 'Radio-frequency communication protocol for electronic seal for freight containers' with a scope to develop an 'international standard (that) specifies a RF communication protocol between an electronic seal and its reader.'

From these promising beginnings began what is now known as the Work Item, ISO 18185, 'Freight containers – Electronic container seals.' As can be seen from the initial work item and its revised title, the original intent was to provide a minimum means of interoperability of electronic devices securing freight containers. This minimum interoperability standard would simply identify the data content of the seal and a wireless means to communicate the seal's data to wireless interrogator.

It should also be noted that another wireless IT standard had been developed in WG 2's parent committee (SC 4) relating to the identification of the freight container, namely ISO 10374, 'Freight containers – Automatic identification.' This standard was originally published in 1991 and amended in 1995. ISO 10374, renamed, 'Freight containers – RF automatic identification,' is presently under revision by the ISO TC 122 (Packaging)/ISO TC 104 (Freight container) Joint Working Group (JWG), Supply chain applications of RFID.

From anti-theft to anti-terrorism

Now when ISO 18185 first began in 1999, the prevailing rationale for this work item was to prevent pilferage of freight while in-transit and to enable custodians of the container to identify with relative ease whether the container's integrity had been breached. In September 2001 everything changed and the focus was no longer to keep the bad guys from taking things out of containers, but moreover to keep the bad guys from putting something into a container. Several industry analysts believe our marine transportation system to be vulnerable to terrorist attack. Such an attack would instantly debilitate the US port system with a devastating economic effect. "Independent analysis and the experiences of 9/11 and the west coast dock workers strike demonstrates an economic impact of a forced closure of US ports for a period of only eight days to have been in excess of $58 billion to the US economy", stated Rear Admiral Craig Bone of the Department of Homeland Security in 2005, before the Coast Guard and Maritime Transportation Subcommittee of the US House of Representatives.

Such is but the economic impact of the forced closures, not including the additional expenses for incident response and the procedures to inspect whatever number of containers would be deemed to require inspection. A single terrorist attack within the U.S. maritime shipping system would equal or exceed the cost of the 2002 West Coast dockworker's labour dispute.

Defining the standard

The original 1999 work stated that the deliverable was to be a standard that defined:

1. The data structure within the electronic seal
2. The communication protocol between seal and interrogator
3. A frequency available world-wide

In August 2000 (Tel Aviv), the Working Group (WG) unanimously agreed to adopt a single frequency band. In October 2000 (Cape Town), the WG unanimously agreed that the following frequencies should be considered

1. 315 MHz band (exact frequency definition not available)
2. 433.05 – 434.79 MHz
3. 862 – 928 MHz

In late 2001, the WG 2 parent committee, TC 104/SC 4 circulated an initial ballot of ISO 18185 to participating countries with the results reported in February 2002 (Copenhagen). For this Committee Draft (CD) the ballot results were 10 in favour and 1 opposed. The single opposing vote was from Japan that had requested, electronic container seals utilise a passive backscatter system operating at 2450 MHz. In September of 2002, All Set Tracking introduced a new electronic seal operating at 2450 MHz and set upon a campaign to derail 18185. In an open letter to the maritime community, the All Set CEO stated, "in line with the efforts to prevent terrorism initiated by the US Government, we understand that the International Maritime Organization (IMO) plans to consider a mandate for shipping container integrity at its upcoming December 2002 Conference on Maritime Security. The proposal presently calls for shippers to ensure that loaded containers must be sealed either with a mechanical high security seal or, alternatively, an electronic seal conforming to the pending draft ISO standard DIS 18185." His 21-page 'white paper' raised three basic issues:

1. The standard contains no provisions addressing security
2. The standard embraces frequencies that are not available in Japan
3. The standard embraces technologies other than his

What was interesting in this white paper argument was the claim that there were no provisions for security, when in fact the issues of security were discussed within the WG, but were advised that such issues were beyond the remit of a work item to develop a communications protocol. However, their arguments apparently influenced several other countries because at the conclusion of the Draft International Standard (DIS) balloting, 10 out of the 17 voting members of the committee had voted in favour of the standard, two votes short of the two-thirds majority vote required.

The committee met in December 2002 (Atlanta) and in reviewing the comments, the ballot resolution group discussed 2450 MHz at length and agreed to not include it in 18185. There was significant doubt regarding the capabilities of the frequency in the marine terminal environment and the 2450 MHz product proposed by All Set did not exist. The majority

of the Ballot Resolution Group felt that the implementation of that frequency should be well vetted. While the majority did not favour a 2450 MHz option for this application, all air interfaces must have significant peer review. Given the doubts and the lack of a demonstrable artifact, this option was rejected. There are now other 2450 MHz implementations, such as those described in ISO/IEC 18000, Part 4 and within ANSI/INCITS T20 (now ISO/IEC 24730-2) that have been vetted through extensive peer review. The Atlanta meeting also responded to a comment that an insufficient number of end-users were part of the process. The WG replied that its work was an open process and that if end-users chose not to participate, complaints of unaddressed issues were discreditable to them and not to the committee.

End-user response

Another invitation was made to the end-user community and the World Shipping Council (WSC) responded by mobilising its membership. As a result of this mobilising effort, meetings were held in Washington, Berlin, Tampa, London, Hamburg, Moscow, and Beijing, and the 18185 work item was expanded to a multi-part standard, encompassing:

- ISO 18185-1, Freight containers – Electronic seals – Part 1: Communication protocol
- ISO 18185-2, Freight containers – Electronic seals – Part 2: Application requirements
- ISO 18185-3, Freight containers – Electronic seals – Part 3: Environmental characteristics
- ISO 18185-4, Freight containers – Electronic seals – Part 4: Data protection
- ISO 18185-6, Freight containers – Electronic seals – Part 6: Messages sets for transfer between seal reader and host computer
- ISO 18185-7, Freight containers – Electronic seals – Part 7: Physical layer

During discussions of 18185-4 in Beijing an ad hoc group was formed to 'identify seal vulnerability to make realistic proposal on the framework of security.' This ad hoc met 13 times either face-to-face or telephonically over the period of January through April 2005. The WG further advanced Parts 1, 2, 3, and 7 to a second Committee Draft (CD) ballot and decided to review the CD ballot comments in April, 2005 in Chicago.

When WG 2 met in April 2005 at Motorola's offices in Schaumburg, IL it received the results of the vulnerability analysis ad hoc and its 11 identified vulnerabilities. After extensive discussion the WG concluded that:

1. Business and technical use cases need to be clarified and documented for how electronic seals authenticity decisions are going to be made (when, where, by whom). This needs to include details of how the reader networks will be operated and how key exchange could take place.
2. The electronic seal standard should include a requirement for a method (or methods) to make each transmission unique.
3. The electronic seal standard should include a requirement for a method (or methods) that allows for authenticity validation of tag/seal transmissions.
4. The electronic seal standard should include a requirement for the system at the point of read to detect and report a denial of service attack.

Further, this meeting unanimously resolved:

a. That any WG member believing there are use cases that have not been addressed in the standard, shall submit such use cases for review before May 3, 2005.
b. That Motorola (would), by May 3, define operational issues it believes are not addressed by current versions of ISO 18185. This list of potential issues (would) be reviewed by the WG at a meeting in London on May 10, to determine which are worthy of additional activity.
c. If significant issues emerge from Items 2 and 3 above, it is resolved that the Technical Group will develop either technical justification of current solutions and/or revised technical solutions to each.

Motorola then issued a paper dated May 3rd outlining their concerns and updated this paper on July 17th, prior to the Berlin meeting. At the Berlin and subsequent Nagoya meetings it was concluded that seal readability would be established at 99.99% and read accuracy at 99.998%. System implementations employing multiple read scenarios can substantially increase readability and read accuracy percentages. Many of the issues raised in Motorola's papers can be addressed through 'localization' (ensuring that the system knows which container/lane is being read in a multi-container/lane environment). There are numerous ways in which localization may be implemented.

In Nagoya, most of the issues having been raised were satisfactorily addressed, with the final outcome described below:

- The DIS ISO 18185-1 (Communication protocol) will be forwarded for another DIS ballot in their present form, allowing technical and user representatives to continue working toward an agreed approach to satisfy the localization requirement, providing comments to the DIS ballot..
- The DIS ISO 18185-2 (Application requirements) was reviewed for another 30-days following modifications made at the Nagoya meeting. Absent any substantial comments, Part 2 to move forward to ISO balloting as a Final Draft International Standard (FDIS), a simple Yes/No ballot.
- The DIS ISO 18185-3 (Environmental characteristics) was approved with no negatives and has been submitted to ISO for publication as an International Standard.
- The CD of ISO 18185-4 (Data protection) was approved on 20 November 2005, with two negative votes and three countries commenting. Comments to be resolved at the next meeting. Korea has submitted a proposed protocol for a second generation of electronic seals, which will be dealt with as a new work item for Part 4, following completion of the current work item.
- The Work Item ISO 18185-6 (Message sets) to be changed to cover the EDI messages exchanged by parties involved in the seal verification processes and the document title and scope may be revised to better reflect this change.
- The DIS ISO 18185-7 (Physical layer) will be forwarded for another DIS ballot in their present form, allowing technical and user representatives to continue working toward an agreed approach to satisfy the localization requirement, providing comments to the DIS ballot.

Moving forward

This ISO work on electronic container seals has thus far spanned six years, an inordinate amount of time for an ISO standard, however, considering the topic area and the issues that have arisen during this period, it is gratifying to report that:

- The work on ISO 18185 is coming to a close for this first generation of electronic seals
- The final work product of ISO 18185, is far better today than it was in 2002
- We can expect additional work in the area of container security devices, including electronic seals

The work of TC 104/SC 4/WG 2 on electronic seals is but one of several ISO initiatives currently underway regarding freight containers. ISO 18185 requires that the electronic seals shall have minimum mechanical characteristics in accordance with the high security provisions of ISO 17712 (Mechanical seals). ISO 17712 is in its final balloting process within the ISO, reaffirming the adopted Publicly Available Specification (PAS) for ISO 17712.

The freight container user community has been quite explicit that they do not want a single device to provide permanent container identification, supply chain (manifest) information, and electronic intrusion detection. They look for a permanent container identification RF tag whose technology can survive the life of the container without maintenance. They look for a disposable electronic seal to eliminate the costs associated with the recycling of the seals. They look for a supply chain RF tag that is applied, removed, read, and recycled only by the shipper and consignee.

While ISO 18185 addresses the electronic container seal, a Joint Working Group (JWG) between ISO TC 104 (Freight containers) and ISO TC 122 (Packaging) have assumed the responsibility for the other two.

- ISO 10374.2 (Freight containers – RF automatic identification) provides a read only identity of the freight container
- ISO 17363 (Supply chain applications of RFID – Freight container), as one of five standards addressing the various levels within the supply chain (product – ISO 17367, packaging – ISO 17366, transport unit – ISO 17365, returnable transport item – ISO 17364, and freight container), provides the technology to carrying electronic manifest data along with the shipment.

Working cooperatively, TC 104/SC 4/WG 2 and the TC 122/104 JWG do not believe that container security devices, be they mechanical or electronic, will, by themselves, improve cargo security. While there is certain appeal to use technology to physically track the flow of cargo from origin to destination with potential business benefits for:

- Loss prevention
- Inventory control
- In-transit visibility

. . . the only viable framework requires that cargo entering the maritime system be secure, including:

- Accurate data
- Secure cargo
- Secure vessels and ports
- Secure transit

For all the tracking, tracing, real-time visibility and intrusion detection are for naught if a container is already loaded with a nuclear or biological weapon at origin.

Cargo system security requires the courage and commitment of governments. Technology standards must develop along side of government initiatives and when the governments' resolve is ready, the technology and standards will be ready as well.

ABOUT THE AUTHOR

Craig K. Harmon is President & CEO of Q.E.D. Systems. He is also the Project Editor, of ISO/IEC 18185-7 and the Chairman of ISO TC 122/104 JWG.

ABOUT THE ORGANISATION

ISO is a network of the national standards institutes of 148 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

ISO is a non-governmental organization: its members are not, as is the case in the United Nations system, delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

Therefore, ISO is able to act as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users.

ENQUIRIES

International Organization for Standardization (ISO)
1, rue de Varembé
Case postale 56
CH-1211 Geneva 20
Switzerland

Tel: +41 22 749 01 11
Fax +41 22 733 34 30
Website: www.iso.org

Craig K. Harmon
President, CEO, Q.E.D Systems

Tel: +1 319 364 0212
Email: craig.harmon@qed.org
Website: www.autoid.org