

---

## Live from IFSEC: The challenges of TWIC

**By Anonymous**

Published: May 11 2008 - 8:00pm

Subtitle: Hirsch's Suneborn and Zivney weigh in on the U.S. port security card programByline:

Geoff Kohl, editor-in-chief

At IFSEC today in Birmingham, England, I caught up with two of Hirsch's leaders, Rob Zivney, worldwide director of marketing, and Lars Suneborn, who directs the company's government programs. Despite the fact that we were in a country where chips are fries and bangers are sausages, we turned our conversation to the issue of the United States TWIC (Transportation Worker Identification Credential) program that's currently being rolled out at many U.S. seaports. In summary, this is a credential (actually a smart card) for all port workers, from the shipping firms, to the dock workers and longshore men and even the trucking/delivery drivers. It is an initiative being pushed as part of the U.S. Department of Homeland Security/Transportation Security Administration, and ties in biometrics in addition to personnel identifying information normally common to ID cards.

Suneborn and Zivney were able to provide me an honest update on TWIC from the perspective of an access control system and reader firm. We discussed some of the challenges that this ambitious identity and access control project is facing, and it looks like TWIC has some big hurdles ahead.

For starters, they noted that there can be issues of usability, starting with the fact that it's very hard to put an exact number on the number of persons who need this credential. Additional challenges can include shifting route assignments for port truck deliveries, temporary placement of on-site workers, numerous operating companies working in a single port environment, and the challenge of putting background checks on a worker population that has never been subjected to such requirements before. Technology usability has also been a challenge. The rough, industrial-type environment is tough on fingerprint biometrics and even tough on the hardened readers themselves.

---

Additionally, because ports have strong Coast Guard presences, the technology, mainly the readers and access systems, would need to provide support for the Common Access Cards (CAC), of which there are different versions. Additionally, because TWIC standards allow for card technology options (like signed and unsigned biometrics, for one) and encryption (some six different encryption algorithm options), card readers would also need to support a variety of TWIC card implementations. With the new initiative for the FRAC (First Responder Access Card) to be used by fire responders, card readers at port entrances may also need to support that standard as well.

Zivney says the challenge with TWIC standards is that they are formulated such that "the readers have to do the heavy lifting," as opposed to the Physical Access Control system (PAC). And with requirements like AES encryption, vendors such as Hirsch will have to not only design very specific readers to unique specifications, but also get their card readers NIST certified, which is a similarly challenging and expensive process as earning UL approval.

Now, says Zivney, the government technology directors are asking "Where are the readers?", asking why such reader technology is not yet available to support the TWIC project. But as an unfunded mandate, says Zivney, "We're also asking, 'Where are the funds?' TWIC has the most advanced standards for readers compared to anything that's been required before."

Until the readers are in place, the many TWIC cards which have been issued will serve solely as "flash passes". Reader pilot projects have already started, but final reader requirements have not yet been published, though companies like Hirsch are optimistic that they can have TWIC-compliant readers in the works this year.

Zivney said that most of the focus has been on the card, driven by the implementation of PKI (which is a requirement of the card-reader communications), but he notes that other security standards common to PAC systems can't be lost in the mix. "We see a PKI as a welcome addition to, not as a replacement for, current security standards."

---

Finally, cost has to factor in, especially since TWIC hasn't been expressly funded. The implementation of one worker's card for five years (not the physical access control systems, just the card and enrollment) is expected to cost between \$230 to \$240 per worker, a price that would seem exorbitant in the private sector. Admittedly, much of that high price is driven by the background checks for the workers as part of the enrollment. The TSA fee to workers is \$132.50 for the card and the enrollment.

What's more, says Suneborn, the entire TWIC program features challenges of migration, since physical access control systems and supporting IDs have already been paid for and installed, and are a core element to port access control. Suneborn that creating a workable migration strategy also adds to the cost of such a project.

Because of the fundamental changes in technology, Zivney say that it is entirely possible that all of the current PAC systems in place for port access control may have to be replaced. Suneborn noted also that current standards indicate the government wouldn't want access alarms (door held alarms, for example) coming into the same system as used for identification. "They don't really want the access control to tie into the alarm monitoring," explains Suneborn.

Nonetheless, both Suneborn and Zivney agree that the TWIC process is rolling forward, and that despite such challenges on technology, cost, usability and migration, the project can be a real force for change in the physical access control systems market. With reader test projects occurring at locations like the Port of Long Beach, Calif., and enrollment programs ongoing since October 2007, TWIC is certainly on its feet, even despite the enrollment deadline moving from fall 2008 to April 2009. But in the meantime, the road ahead for TWIC may be as rough as the high seas that vessels travel upon before they reach U.S. ports.

More information:

[TSA's TWIC information page](#)

---

Source:

SecurityInfoWatch.com

Article Date: May 12 2008Top Story?: NoLive Date: May 12 2008Expiry Date: Aug 8 2018Archive  
Date: Jan 10 2037Article ID: 15530