

Comments on the Eight TWIC Biometric Questions
Vol. 72, No. 51, page 12626

16 March 2007

Submitted By:

Bill Nuffer
Deister Electronics USA, Inc.
209-772-0946
bnuffer@alum.mit.edu

Question 1 Response:

- a. Should additional security measures be included:?
Our position is “NO”. Some of the existing proposals already make this a Rube Goldbergish nightmare in terms of time to admit and in terms of error probability.
- b. If so, would a PIN or other adversely impact operations?
Our position is “NO”. PINs are forgotten. PINs are misentered (especially in difficult weather conditions). Even with TWIC works that possess perfect memory and perfect fine motor control, entering a PIN takes time—time is a precious resource here—far more precious than the false perception of privacy risk (see answer below).
- c. Does the length of the PIN affect adverse impacts...?
Longer PIN = Hard to remember = More errors = More time lost
Longer PIN (even with perfect memory and fine motor control) = More time lost
Longer PIN = Nominally more secure (but not worth the increase in lost time).

Question 2 Response:

What, if any, privacy concerns exist if the ...template is obtained....?

I would argue: In reality, almost none.

Reasons:

1. A template is not a fingerprint. It is a distillation (but not even a perfectly unique distillation) of the actual fingerprint.
2. Every time that someone throws away a plastic drinking glass at a fast food outlet, they are:
 - a. Providing an easier to steal fingerprint than that contained on a TWIC access card even if that card is unencrypted.
 - b. Providing a more accurate fingerprint than that contained on a TWIC access card.

So, we should at least ask the question: Why are we going to such expensive and time-consuming lengths to prevent access to a template (which is not an actual fingerprint) when actual fingerprints are so easily available from the cafeteria waste?

3. Even if TWIC Access Cards were a major source of illicit fingerprint theft and even if the TWIC Access Card provided those fingerprints with perfect fidelity (neither of which bears veracity) and even if an identity theft ring were to copy and retain those perfect fingerprints and accurately match those TWIC Access

Card stole fingerprints with other identity elements (such as name and address—which are not retained electronically on the TWIC Access Card; and would have to be obtained simultaneously some other way (although the name could be obtained off of the printed card)), what damage could result to the individual? I am hard pressed to think of any—although if I try hard I can construct some relatively lunatic fringe scenarios but none of them are likely. The real question is a risk-analysis:

- a. What is the probability (even in the least protected scenario) that a template can be stolen off a TWIC card?
I would argue that the probability (even in the least protected scenario) is vanishingly small. But for the sake of argument, let's say 0.01%.
- b. What is average damage done to an individual if his/her template falls into the wrong hands?
I would argue that the damage is effectively zero in the worst case. But let's say it's \$1000 (this includes the damages incurred if the Port is sued because someone gets embarrassed by the display of their template on the Internet).
- c. Let's then take the TWIC card population (estimated at 1 MM users for argument's sake).
- d. The total damages then are $0.01\% \times \$1000 \times 1\text{MM} = \$100,000$
- e. If that analysis is right then if the incremental cost of implementation is greater than \$100,000, it shouldn't be done.

I recognize that there are subtleties in the analysis that are not addressed above including perceptual and political issues but at some point someone needs to at least recognize that there is an ROI issue here.

Question 3 Response:

How would the recommend specifications impact...security & operations?

1. Security: As long as you have a reasonably good template and acquisition/matching system, a minimum process, unencrypted template provides excellent security. There is no measurable increase in security by adding PINs or encryption or special barcodes or other elements.
2. Operations: The more steps you require of a worker to enter the workplace:
 - a. The greater the potential for error; and,
 - b. The greater the time required to be identified and get to work.

Each additional second required per worker is an additional second lost to operations. Depending on the number of readers, one second lost to the first worker becomes two seconds to the second worker in line becomes three seconds to the third worker in line—ad infinitum.

Therefore, the simplest possible set of procedures with the fewest steps and the least amount of processing (e.g. no encryption) is recommended.

Question 4 Response:

How would the ... specifications impact existing...access control....?

1. All new readers (in all but a few cases).

2. In some scenarios originally proposed, the readers may need to receive key data, etc from the AC Controllers. In this case controllers would need to be replaced if they were Wiegand based with controllers that have some form of two-way communication (e.g. IP or RS485)
3. Depending on which process is adopted, new host software may or may not be required. To the extent that new host software is required, it may be related to the use of the FASC-N ID moreso than the biometric requirements and is therefore not related to this set of questions.

Question 5 Response:

There are a large number of alternate design approaches. Most probably shouldn't be considered simply because starting over in the deliberation process is just too expensive at this time.

One that should be considered is:

Consider that the NMSAC adopts FIPS 201 and the PIV-II card in its entirety and abandon a separate TWIC card and process.

Disadvantage: This is a more expensive card. However, there will probably be a lot more PIV-II cards issued than TWIC cards—consequently scale may well bring the two card technologies close to one another in cost.

Advantage: One card already pretty well specified (although some of the PIV-II biometric specs are still being finalized?? Is that correct??) One process. One government agency. Half the hearings. Half the management. Half the technologies.

Question 6 Response:

Recommend specs impact on costs.

See answers to Questions 3 & 4.

Question 7 Response:

Time to incorporate specs

At the contactless interface side: Very fast.

At the encryption and/or PIN and/or barcode side: Depends on which technology set is adopted. But PIN would be fast. Encryption would be fairly fast (depends on what type of encryptions is specified: AES=Fast; DES=Medium Fast; PKI= Less Fast (plus cost increases at the card and reader side). Barcode presents a variety of interesting challenges but probably medium fast (although that doesn't count the additional reader expense and the increased maintenance costs).

Question 8 Response:

QPL Process?

We recommend YES.

The most efficient way is to:

1. Turn the specification development over to private industry groups (e.g. SIA).
2. Turn the evaluation over to private evaluation over to private laboratories that meet certain minimum standards (such as the FCC does).

-
-
3. The GSA (or other appropriate government agency) would receive reports and applications from manufacturers and upon administrative review would maintain the QPL online.