RSA Security Inc. commends NIST on its substantial progress to date implementing Homeland Security Presidential Directive 12, and appreciates this opportunity to provide comments on the preliminary draft of FIPS-201. We would like to offer comments regarding potential compromise of personally identifiable information, and on-card data representations.

As is well known in the industry, contactless cards typically carry significant personal privacy risks because of the possibility that cards can be read freely by any reader, not just the authorized ones. While cryptographic techniques are available that can mitigate these risks, the techniques have generally not been employed because of limitations on the cards' capabilities. As a result, many standards based on contactless and other forms of RF identification leave cardholders' privacy at significant risk. The current draft of FIPS-201 also falls into this category, as we elaborate here.

The FIPS-201 draft assumes that the reader is trusted. But since it makes use of ISO 14443 as the contactless interface, commodity equipment is available which can interrogate the card without the cardholder's knowledge or consent. Over this interface, the reader may obtain the CHUID, a fixed string that uniquely identifies the cardholder. The spec notes: "The PIV CHUID shall be accessible from both the contact and contactless interfaces of the card without card activation." Moreover, the CHUID is a static, well structured block of data which can reveal information like the cardholder's name, agency affiliation, or even the cardholder's Social Security number, as noted on page 6 of [PACS].

The possibility of rogue readers introduces a potentially powerful avenue of attack. Documented tests have shown an attacker today can interrogate a card at a distance of 30 feet [EETi] . Wireless technology is only improving, so we can expect this range to increase in the future. Collecting the CHUIDs would enable an attacker to track the movements of cardholders, or target federal workers in acts of terrorism. Only limited sophistication would be required, along with largely off-the-shelf technology.

To avoid this attack, the card must allow only trusted readers to access the CHUID from the contactless interface. There are many ways of meeting this goal while retaining a contactless interface, each with its own trade-offs.

- Enable the contactless interface only while the cardholder is pressing a "button" on the card.
- Allow the contactless interface to be disabled (and later re-enabled) by software commands issued over the contact interface by an authenticated reader. This feature would allow a cardholder traveling into a hostile environment to disable the attacks outlined above. Once outside of the hostile environment, the cardholder could re-enable the contactless interface.
- Instead of allowing the CHUID to be read over the contactless interface, it could be replaced by a random identifier. This random identifier would correspond to a database entry which would contain the cardholder's CHUID. This database could reside in a backend system in the case of network-attached readers or could take the place of the "Authorized FASC-N list" on a disconnected reader. Note that

this suggestion is only a partial solution: cardholders may still be tracked and the fixed identifier itself could indicate that an individual is a federal employee to a rogue reader. But it would have the effect of masking a cardholder's personal information, such as agency affiliation.

- Cardholders could be instructed to store the card in a foil lined bag when not in use. This suggestion is obviously a cumbersome solution at best, offering little technological risk but high cardholder inconvenience and likelihood of non-compliance.
- The card could authenticate the reader using a challenge-response or a public-key protocol before revealing sensitive personal information or fixed identifiers. A variety of FIPS-approved entity authentication methods could be applied for this purpose.

Not only is privacy a real concern with these contactless cards, but security can also be at risk if a contactless card can be read freely. An attacker who obtains the CHUID can easily create a "clone" card that will gain unauthorized access to resources protected by the PACS LOW scheme.

Privacy and security in RFID and related contactless systems is a very active research area and better technologies will undoubtedly come along. As this standard is deployed, we encourage NIST to track these technologies so future versions of the standard can provide the best protection possible for federal workers. In addition, the continuing miniaturization of electronics could allow form factors that are smaller and/or more convenient than today's cards. By the time this standard comes up for its periodic review, improvements in battery technologies and semiconductor fabrication could allow for battery-assisted contactless cards at the same price point of today's cards. These cards would be capable of performing robust public-key based mutual authentication - with no loss of range - to secure the contactless interface from rogue readers.

Regarding on-card data representations:

6.3.3 specifies the CHUID to be in the MF area. This may complicate multi-application card usages and also Java card usage. We suggest CHUID information to either reside in an elementary file in the cryptographic information application (and referenced in a well-known way from an ISO/IEC 7816-15 EF.DCOD file), or in a separate, NIST PIV card application with a well-known AID. (Note: If the CHUID placement within the MF area is currently required for other reasons, it would at least provide some future flexibility if a method for referencing it from within an 7816-15 EF.DCOD were specified – this way, future card issuers would be able to place it in other areas on the card, should the need arise. The recommended way of finding the CHUID would then be through this reference.)

6.6 should clarify if these keys and certificates are to be found through the Cryptographic Information Application mentioned in 6.3.3 (preferable) or some other method (800-XX talks about the Cryptographic Information Application as being optional yet this document seems to rely on its presence to allow a host system to find certificates and

keys for authentication operations etc. We believe the intent is to rely on the Cryptographic Information Application and, if so, we strongly support this as it would bring the GSC community closer to ISO and the EU).

8.4 Specifies the digital signatures as detached CMS signatures. To ease future interoperation, we suggest an alignment with ICAO here (it is our impression that ICAO does not use detached signatures as specified here) as well as with the format of biometric data and the choices of data objects to which the signatures are to be applied.

Overall, while RSA Security supports the move closer to ISO standards, and in particular ISO/IEC 7816-15 and the forthcoming ISO/IEC 24727, we also acknowledge the concerns this move may raise with regards to existing CAC and GSC-IS environments. We would therefore like to express our hope to contribute further to this effort to mitigate these concerns and ensure the effort's success.

[EETi] Yoshida, Junko. "Tests reveal e-passport security flaw," EE Times, August 30, 2004. http://www.eetimes.com/article/showArticle.jhtml?articleId=45400010

[PACS] PACS v2.2 – The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control* Systems, Version 2.2 July 27, 2004.