Mehta Ketan

From: Steve Hopper [steve_hopper@infogard.com]
Sent: Thursday, December 23, 2004 4:59 PM
To: draftfips201@nist.gov
Cc: Tom Caddy
Subject: Comments on Public Draft FIPS 201

Good Day,

I think in general that FIPS PUB 201 is an informative and well written document. I am providing the following comments/questions concerning FIPS PUB 201 for your consideration. I am submitting these in two groups; the first of which concerns items that include comments and questions, the second is a list of typos that popped out at me.

Comments/Questions:

1. It seems in general that you have chosen to not include Match on Card biometric authentication as part of this publication. Is this by choice or an intended omission? As I am sure you know, MOC is inherently more secure than having the card output the biometric template for external verification. Table 6-1 would be a good place to add this alternative authentication technique.

2. Section 4.1.6.1: When discussing PINs, per FIPS 140-2, the minimum PIN length is 6-digits. You might want to mention this here for information purposes so no one is surprised later.

3. Section 4.1.6.2, first paragraph: What you seem to be mandating is that each card have a different Card Manager key set. These key sets are used to derive the session keys during the challenge response protocol. I do not believe that current card management systems allow for a unique key set per card. Is this really your intention?

4. Section 4.3: You state in the second paragraph, "The PIV card shall implement" RSA or elliptic curve key pair generation. Then at the end of the third paragraph it says, "As above, useful optional functions include key pair generation...". This is a little confusing.

Typos:

1. Section 1.2, first sentence: Add an "s" to the end of system.
2. Section 2.2.1, last sentence: Change to "listed in Table 2-1."
3. Section 2.3: Change "I.e." to "i.e."
4. Section 3.3.2, first sentence: Change to, "refers to the process"
5. Section 3.3.2, third paragraph: Change "that application" to "applicants" or "the application". Also, change "provisioning of publicly accessible repositories and services (such as the PKI repository)" to "provisioning of publicly accessible repositories (such as the PKI repository) and services that"
5. Section 3.4, PIV card usage: Change "providing" to "being provided" or better "being allowed physical or logical access"
6. Section 3.4, Identity proofing and registration: Change "is valid" to "are valid"
7. Section 3.4, PIV card termination: Change "card including the data on it including the keys" to "data and keys on it such that it cannot be used again"

8. Section 4.3, below Table 4-5: Remove "each"
9. Section 4.4, second paragraph; Change to, "Fingerprints shall be the primary"
10. Section 6.1, second paragraph: Add a period after the word "supported"
11. Section 6.1.4, #3: Change to "card and requests"

Again, I think the FIPS PUB 201 draft is very will written and is a good first attempt at specifying the usage of smart cards as PIV devices. You have also correctly addressed the necessary infrastructure requirements that are external to the smart card but are still vital in the overall security of the PIV.

I hope these few comments are of some help. Please do not hesitate in asking for any clarification of my comments/questions as I am very interested in participating in this process, one that I personally believe is a mandatory step toward increasing our nations security.

Best Regards and Happy Holidays,

Steve

Steve Hopper
Sr. Security Engr.
InfoGard Laboratories
641 Higuera St., 2nd floor
San Luis Obispo, CA 93401
Ph: 805-783-0810
Fax: 805-783-0889
www.InfoGard.com