X-Sieve: CMU Sieve 2.2
Subject: Comments on the Draft of FIPS Pub 201; US Postal Service
Date: Thu, 23 Dec 2004 11:00:54 -0500
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Comments on the Draft of FIPS Pub 201; US Postal Service
Thread-Index: AcS+qZfYdlqfm9mgRY22mRvOc1LJoQ==
Priority: Urgent
Importance: high
From: "Stepongzi, Mark J - Washington, DC" <mark.j.stepongzi@usps.gov>
To: <draftfips201@nist.gov>
Cc: <mehta_ketan@bah.com>, <grance@nist.gov>,
"Myo Khin, Pete - Washington, DC" <PETE.MYOKHIN@usps.gov>
X-OriginalArrivalTime: 23 Dec 2004 16:00:55.0035 (UTC) FILETIME=[957EECB0:01C4E908]
X-MailScanner:
X-MailScanner-From: mark.j.stepongzi@usps.gov

Dear Sir:

Attached is a document containing the US Postal Service's comments on the Draft of FIPS Pub 201. I am your point of contact so please let me know if you have any questions.

Regards,

Mark Stepongzi, GSEC
Information Technology Planner
Corporate Information Security Office
United States Postal Service
475 L'Enfant Plaza, SW, Rm. 2141
Washington DC 20260-2141

Voice: 202-268-2416
Cell: 202-368-9724
FAX: 202-268-5982
EMAIL: mark.j.stepongzi@usps.gov

<<Draft FIPS Pub 201 Comments -- USPS.doc>>


Draft FIPS Pub 201 Comments -- USPS.doc

Comments on the Draft of FIPS PUB 201
United States Postal Service

Subject: Review of FIPS Pub 201, Federal Personal Identity Verification Standard (Draft)

1. General Comments:

   a. Can the Postal Service become a CA provider? What are the criteria to operate under?

   b. The responsibility for assuring the credentialed person is properly authenticated for credentialing belongs to the parent organization, as it should. However, there is not enough emphasis/guidance on the procedures for revoking the credentials. These credentials could allow access into agencies other than the issuing agency if not properly revoked. "If Employee X is terminated today, how do we ensure all access is immediately revoked?"

   c. There is a concern that there will be a very significant increase in the number of National Agency Check and Inquiries (NACIs) in 2005, in order to meet the October 27 deadline.

   d. PIV-II, Section 4.1.4 describes the proposed U. S. Government ID card. Although optional, the card could display "pay grade" and "rank." There is no provision for a field for "title." Displaying the personnel's title could be more effective than the "pay grade."

   e. No guidance or process is provided that deals with how to treat temporary assignments, as these relate to the information displayed on the ID card. Temporary assignments can be within the agency or even at another agency.

2. Specific Comments:

   f. Card Topology Elements – The identification of the mandatory elements and their placement on the card, as well as, placement of optional fields allows for sufficient customization to meet individual agency requirements.

   g. Biometric data – There is insufficient data available attesting to the reliability of biometric readers that would allow biometric information to be used as a viable means for determining access to facilities. External elements, e.g., temperature, cleanliness, and impression, can adversely impact the reliability of biometric readers. Technologies are insufficiently mature to use biometric information to manage access to facilities.

   h. Biometric data in storage - However, if the goal is to use the card for storage of biometric information as a secondary or tertiary means of personal identification, then use of image-based storage provides the most reliable means of maintaining the information. The image-based format provides the most reliable, interoperable format for information exchange, if required.

   i. Two of the control mechanisms for card management are the use of Cardholder Unique Identifiers (CHUID) and Federal Agency Smart Card Numbers (FACS-N). There doesn't appear to be a reference as to how these numbers are generated, allocated, controlled, and managed. This document should reference the guidelines addressing CHUID and FACS-N.

   j. On page 17, section 2.2, Acronyms, only a few of the acronyms used in this documented are included.

   k. On page 55, section 9.1, PIV Card Revocation, the bulleted list uses employee, contractor, and cardholder. The term used with each bullet needs to be reviewed.

Comments on the Draft of FIPS PUB 201
United States Postal Service

I. On page 62, section B.1, Policy, it is unreasonable to require the cardholder to authenticate to the PIV card each time the cardholder performs a private key computation. They should authenticate to the PIV card during the initial authentication process and each re-authentication process (e.g., because the session timed-out) but not for each activity within a session (e.g., to sign multiple emails)

Point of Contact: Mark J Stepongzi, Email: mark.j.stepongzi@usps.gov, Telephone: 202-268-2416.