X-Sieve: CMU Sieve 2.2
Subject: G&D's comments on PIV documents
To: DraftFips201@nist.gov
Cc: Eric.Johnson@GDAI.com, hassan.tavassoli@GDAI.com
X-Mailer: Lotus Notes Release 6.5.1 January 21, 2004
From: Won.Jun@GDAI.com
Date: Fri, 24 Dec 2004 08:14:08 -0500
X-MIMETrack: Serialize by Router on NotesDulles1/SRV/GuD(Release 6.5.1|January 21, 2004) at 12/24/2004 08:09:33 AM
X-MailScanner:
X-MailScanner-From: won.jun@gdai.com

Hello,

Please find attached G&D's comments to the FIPS 201 draft and SP 800-73 documents.
If you have any questions, please contact me or Eric Johnson.

Thank you.

Happy Holidays.

Won J. Jun
Project Manager
Smart Card Systems
Giesecke & Devrient America, Inc.
45925 Horseshoe Drive, Dulles, VA 20166
Tel.: 703-480-2145
Mobile: 571-276-8949
www.gdai.com

(See attached file: G&D Comments on PIV Draft Doc 12-23-2004.xls)


G&D Comments on PIV Draft Doc 12-23-2004.xls

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	G&D	Won Jun	G		The document states that the card will have both a contact and contactless interface. However, it does not really address what can be done using the contactless interface. Section 4.2 states that the CHUID can be read from the card using both the contact and contactless interface and various sections such as the last bullet on p28 say that the authentication key must only be available through the contact interface.	It would be helpful if the document stated the minimum of features that need to be supported on the contactless interface. This could also address whether the card needs to be a dual interface card or a hybrid card. The two solutions would have different personalization requirements but may both be acceptable solutions. Also, the requirements that can only take place over the contact interface may be significant since this information may not be available in a non-proprietary way to the current applet.
2	G&D	Won Jun	Technical	A.2.4 p64	This section states that if new modules are loaded onto the card then re-validation of the card is required. This requirement makes the addition of card management commands to the SP 800-73 document seem odd. In practice, it seems that the card would need to be reissued if additional applications are loaded since otherwise it could lead to a very complicated management of the card inventory and possible combinations of the applications. If an agency is allowed to load applications onto their own cards without suitable oversight it seems very possible that non-approved PIV cards could result.	
3	G&D	Won Jun	Technical	Section 4,3 p27	This section states that the card will simply sign raw data presented to it. At the NIST meeting on 18 November it was made clear that the Certificate for the authentication key would say that it could only be used for authentication.The concern with signing raw data is that it directly exposes the mathematical properties of secret key (for example the multiplicative property of RSA) and this could allow the secret key to be misused. The certificate limits this for the authentication key, however there are concerns about the optional digital signature and key management keys being so exposed.	It would seem prudent to require the card to hash the data before signing it in these cases.
4	G&D	Won Jun	Editorial	Table 4-3, p25	It is unclear why the expiration date has a maximum length of 8 bytes if it is of the form yyyymm.	This should read yyyymmdd.
5	G&D	Won Jun	Editorial	Section 4.2.2, p26	The text refers to a reference [CMS] but this is not in the list of references in Annex F	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
6	G&D	Won Jun	G	SP 800-73	This document is attempting to define, amongst other things, the client API and the card edge. For these it lists the API functions and the commands that are to be implemented by the card. However, there is very little information on either of these and certainly not enough to implement a card or middleware solution that is interoperable. Furthermore, the description of these functions and commands contains inconsistencies and errors and as a result needs substantial additional work. The current state of the document can only be considered as giving a high level view of this functionality.	
7	G&D	Won Jun	Technical	SP 800-73	There are no definitions of the data types such as handle or sequence of authenticators that are used in the API definition in Section 5. Also, it is not mentioned whether the sequence of bytes in things like a digital signature are presented in big or little-endian form.	Please provide definitions of data types.
8	G&D	Won Jun	Technical	SP 800-73	The cardHandle parameter definitions in Section 5.4.5 and 5.4.6 both state "Identifier of the connected card to from which a random byte sequence is to be retrieved." This description does not apply to either function and the Verify function does not even return any value other then the status result.	Please revise.
9	G&D	Won Jun	Technical	SP 800-73	The READ BINARY command states that a 6831 error code is returned to indicate reading has taken beyond the end of the current data element. However, the table for possible SW1/SW2 values lists 6832 for this error.	Please correct.
10	G&D	Won Jun	Technical	SP 800-73	The GET CHALLENGE command for the Symmetric Key application in Section 7.3.5 seems to be the UPDATE BUFFER command from Section 7.2.6	Please correct.
11	G&D	Won Jun	Technical	SP 800-73	The Public Key Application refers to a VERIFY PIN command in Section 7.4.4. Why is this command needed? The FIPS 201 draft says that the PIN does not need to be presented for an activated PIV card. Is this VERIFY PIN command the command that should be used to activate the card? Does this PIN function as a global PIN shared between applications? These issues do not seem to be addressed in the current document.	Please provide a rationale for VERIFY PIN command and address mentioned issues.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
12	G&D	Won Jun	Technical	SP 800-73	The document seems to be attempting to support both Global Platform type cards as well as File System type cards. However, it does not seem to address how this can really work particularly in the card management aspect. For example, Section 6.1.2 describes an INSTALL command. This appears to have the same command format as a Global Platform INSTALL command and so its meaning can be interpreted for cards based on that specification, However, the document provides no description on what this command would mean for a file system based card. Without a precise definition of what this command does the merit of including it in the specification seems somewhat lacking.	Please provide a precise definition.

D = Document,1 = FIPS201, 2 = SP800-73

T=Type of Comment, E = editoral, T = technical