From: "Gilles L." <vze33t2e@verizon.net>
To: <DraftFips201@NIST.gov>
Cc: "Rajesh Sharma ...snip... Thierry.DEFFONTAINES@gemplus.com>
Subject: Comments on Public Draft FIPS 201

Please find attached Gemplus comments on the FIPS 201 and the SP800-73 draft documents published on November 8, 2004.

Gilles Lisimaque
Gilles.Lisimaque@verizon.net
Work 301-320-5146
Cell 240-731-4585


Gemplus PIV Comments.xls

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
1	Gemplus	GL	T	Page 8 - 3.2.4	ISO/IEC 7816-4 indicates clearly the four security statuses a card shall maintain: Global, Application, File and Command. ISO/IEC 7816-4 Paragraph 7.1.1 about the Select Command explains clearly how this security status is lost or changed by the Select command is used. Any use of a Select DF by name (AID) without knowing its position in the hierachical structure of the card resets the application security status "unless otherwise specified".	The notion of multiple "sub-applications" in the PIV application space is dangerous and not covered by ISO/IEC 7816-4 unless the "sub-applications" are Dedicated Files (as for the cryptographic application).
2	Gemplus	GL	E	Page 9 - 3.2.6	The illustration of card application and data relationship does not help in the document as there is no mechanism allowing to select what is shown in the picture. When the only available command "Select a DF by name (AID)" is used what is selected in the drawings? The application but how? or the ADFs as they are data structures with a name? The ambiguity between selecting an application by its code or by its data set needs to be clarified.	Same as before. Either an application is represented by its data struture on which some commands are availble at the card interface layer depending on the type of the data selected, or it is an executable piece of code which contains its own data structures.Explain in the drawings if it is possible for Application B to use the code from Application A.
3	Gemplus	GL	E	Page 10 - 2.1	Application Identifiers are not specified in ISO/IEC 7816-5 anymore but in ISO/IEC 7816-4	Replace ISO/IEC 7816-5 by ISO/IEC 7816-4
4	Gemplus	GL	G	Page 10 - 2.1	The use of "Card Manager" for the distinguished PIV application is an ambiguous choice as this term is used in the Global Platform specification. The PIV Card manager does not have the same command set than the Global Platform Card Manager (e.g. Load application code opposed to create data strutures such as DFs and EFs)	Replace the term "Card Manager" by "PIV Application Manager" in most instances in the document but when appropriate with term "Global Platform Card Manager". We suggest the "PIV Application Manager" to deal with data structure management but not with application code management at all.

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

Type of Comment, G = General E = editorial, T = technical

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
5	Gemplus	GL	G	Page 10 - 2.1	The Key reference and the key set version is defined "within the application context". This notion mentioned a couple of times in the document and is never defined. As there are various interpretations of this notion it is cricial to define what this term means in the context of this document.	Define precisely what means "an application context". Is this within an AID? Is this within a DF? Is this within the whole PIV application (even when the cryptographic application is selected within the PIV application)? Defining what this notion covers is crucial for interoperability.
6	Gemplus	GL	T	Page 11 - 2.1	The use of Reference data from ISO/IEC 7816-4 requires a very clear definition of what the notion of Global and Local means within an application context.	Define the notions of Global and Local references within an application context. This notion is used later in various places of the document and not clearly defined.
7	Gemplus	GL	E/T	Page 13 - 3.1	The use of the term "Data Element" to design either files or BER-TLV encoded data objects is very confusing and not in the line with most card specifications in existence so far. As files and BER Encoded Data Elements are not using the same command sets they should not be confused in a common term. Moreover, some files do not have a description of their logical content and do not comply with this definition. The use of the term Data Structures (as agreed for ISO 24727) to include both Files and Data elements would be much better.	In the definition list add "Data Structures" and change the paragraph title to Data Structures. Change the content of the paragraph to explain what are files and what are Data Elements (or Data Objects). ISO/IEC 7816-4 clearly indicates what data elements are in paragraph 5.2.4 of the standard. All use of the term Data Element should be contistent with this paragraph of the standard. In paragraph 5.3.1.2 of ISO/IEC 7816-4 it is clearly said the interindustry data element with tag "51" references a file.
8	Gemplus	GL	T	Page 13 - 3.1.1	The support by this specification of Unstructured Transparent Files is questionable. The use of such files, which have no description of logical content, is a tremendous risk for interoperability.	Remove Unstructured transparent file support from the specification. They may be allowed fro an application but not in the interoperable definitions.
9	Gemplus	GL	E	Page 14 - 3.1.2	In the middle of the page the reference to ISO 7816-5 is incorrect and should be replaced by ISO/IEC 7816-4	

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

Type of Comment, G = General E = editorial, T = technical

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
10	Gemplus	GL	T	Page 14 - 3.1.2	The "fully elaborated names list" is not consistent with the file structures of ISO/IEC 7816-4. No data object (beside system data objects) can exist outside of an Elementary file (EF). A data object in an application may be selectable but its complete data element name shall always include at least one elementary file to contain it.	Remove the example "AID | DOT" and verify no DOT in the PIV application is assumed to be stored outside of a given Elementary File
11	Gemplus	GL	E	Page 14 - 3.1.2.	the use of "data Element" for files and data object should be cleaned up and replaced by the term Data Structures	Data Element is confusing when used for Files. Replace the term if this notion is really required by Data Structures.
12	Gemplus	GL	T	Page 15 - 3.1.3	ISO/IEC 7816-4 does not support the notion of a currently selected data element unless it references a complete file (either Dedicated or Elementary but not a data object).	Replace the term "data element" by "elementary file" in this paragraph. Remove the example of AID | DOT | DOT as no ISO/IEC 7816-4 command allows to do such a selection at the card edge.
13	Gemplus	GL	T	Page 15 - 3.1.4	This paragraph can apply to files (Dedicated or elementary) as well as data objects. As commands for files are different than commands to handle data objects it is strongly suggested to have two paragraphs dealing clearly with each instead of trying to bundle both.	Modify paragraph 3.1.4 by replacing "data element" by "Files"" except in the second paragraph where "data element" should be replaced by "elementary file". Create a new paragraph 3.1.5 Adding and Deleting Data Objects in which the text should explain DOs are created, updated and deleted in Elementary files.

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

Type of Comment, G = General E = editorial, T = technical

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
14	Gemplus	GL	T	Page 15 - 3.2	Defining card applications as "an executable program stored on the ICC" leads to believe the PIV card must be a JavaCard. In other places of the document an application can be understood as the set of data belonging to an application. The ambiguity must be dealt with and specify clearly what is an application in PIV. In JavaCards, applications are executable code to which is added (or linked) application data, and in file cards following the ISO 7816 spirit, an application is the set of data belonging to an application (in fact stored under the DF named with the application AID) on which can be executed some commands which are part of the card platform. In order to be coherent, if we want to have only one approach we need to draw a line allowing both card models to converge at one point. When a JavaCard has an applet loaded it contains the executable code able to act on data structures to be loaded under the application code control. This is basically the same state in which a file card OS is before application data is loaded.	The following definition is proposed: A card application consists of a collection of data elements contained in data structures (DFs and EFs) on which some executable code (i.e. commands) can be executed depending on the type of the data object selected. It is also important to remember that according to ISO 7816-4 common interpretation, the "application security context" is lost when a new application (AID) is selected. This is an important issue which has to be dealt with very clearly. Are there some applications in the PIV card which do not reset the security application environment? (For example the cryptographic application, selected by an OID (and not an international RID structure) could be a family of applications of such a kind. This is a new concept but something around these lines could be defined).

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

Type of Comment, G = General E = editorial, T = technical

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
15	Gemplus	GL	E	Page 15 - 3.2.1	Card Manager Application: This term too close to the "Card Manager" widely used in Global Platform which has a very specific meaning. This could create serious confusion. In the context of PIV it seems the "card manager application" has slight different functions such as creating files and data structures which are not part of the JavaCard or Global Platform specification. The whole executable code attached to such file management should be better attached to a "Generic Card Data Structure Manager" (or General container manager or as suggested earlier "PIV Application Manager"). Another option would be toreference and separate clearly the Global Platform Card Manager for Application code management (applets) and the Application data management which then would be done by the PIV Application manager.	Replace the term "Card Manager Application" by "PIV Application Manager" in this paragraph. The second sentence should be changed to indicate the PIV Application manager surfaces all commands related to PIV but not the commands related to application code management which is taken care of by the existing GP Card Manager.
16	Gemplus	GL	T	Page 15 - 3.2.1	The notion of the master file in ISO/IEC 7816-4 is not attached to a given application but to the card level for all applications. The Master file has a very specific File ID value (3F00) and should not be used in specific applications with the same name or the same File ID.	Having more than one AID for a given application is not a concept supported by ISO/IEC 7816 but only in JavaCards. Having a root for a given application is perfectly fine but it should not be the card master file. The whole paragraph need to be re-written to be in line with ISO 7816-4.
17	Gemplus	RS	T	Page 15 - 3.1.4, Pg 15	Adding and Deleting of Data Elements is ok, but the delete operation may not always result in 'Available EEPROM space' as GP2.0.1' does not implements Garbage Collector.	A clarification should be made in the document that the Issuer may not be able to use the space made available by Delete 'Data Element' operation. Not specifying this could lead to non interoperability.

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

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
18	Gemplus	GL	G	Page 16 - 3.2.2	According to this paragraph PIV cards have at least two applications required. One is the PIV Card manager Application (AID A0 00 00 01 16 00 00 00) and the second one is the Cryptographic application (AID E8 28 BD 08 0F 00). As mentioned before, unless very explicitely specified (and this is not done in the document at this point) all applications with an AID are often considered unrelated in ISO 7816-4 and the application security status is lost after a selection. Without the data model it is difficult to see if this is an issue of not.	The attempt here to grandfather GSC-IS applications is not as simple as this paragraph assumes. Unless the GSC-IS implementation has created a Global PIN function this solution might end up having two PINs unrelated and managed separately in the same card. This is not the only inconvenient (duplication of data and may be keys) but will be the main issue from the card holder stand point.
19	Gemplus	GL	T	Page 16 - 3.2.3	The term "Card Platform" is ambiguous. In order to keep a consistent approach between VM and File cards it is important to distinguish between the "card platform" and the "PIV card platform". The later is what, we assume, is referenced in this paragraph and assumes all PIV commands (except the card commands for application code management) are available to manage the data structures and entities defined in PIV.	Replace the term "Card Platform" by "PIV card platform" or by "PIV application platform". Indicate clearly here and later in chapter 6 which commands are in what manager. (See comment on Chapter 6 Table 6-1)

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

Type of Comment, G = General E = editorial, T = technical

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
20	Gemplus	GL	T	Page 16 - 3.2.3	Introducing the notion of "card application commands" creates confusion as the notion of multiple applications (according to the JavaCard concept) is not consistent with the notion of Selection by DF name in ISO 7186-4. Either there is a PIV platform or there is a successions of multiple unrelated applications in the card but so far this not clear at all. At least ISO 7816-15 makes clear the selection of the AID "E8 28 BD 08 0F" is only a data structure in the card on which some commands can be applied because of the nature (type) of data.	The notion of multiple applications in the same card is handled by ISO/7816-4 through the notion of independent separated Application Dedicated Files identified by a name (an AID). Introducing multiple AIDs in the same application "space" requires to define very clearly the relationship between the "sub-applications", the entities they want (or not) to share and so on. ISO/IEC 7816-4 is not enough in itself to define these relationship unless these "sub-applications' are pure data structures in DF's (not selected using a name) defining a relationship through their hierarchical structure.
21	Gemplus	GL	E	Page 16 - 3.2.4	AID is defined in ISO/IEC 7816-4 and not in part 5	Replace ISO/IEC 7816-5 by ISO/IEC 7816-4
22	Gemplus	GL	T	Page 16 - 3.2.5	The use of the terms "may be also associated" tend to support the dichotomy of two card platform approach and "may" lead to serious ambiguities. Is an application a loadable program or just a file structure? How to know which one is chosen in a given card? What guarantees are there they will both behave the same at the interface? Using the same command set is not enough to provide such an interoperable guarantee.	The document should state once for all a PIV application consists of a set of data grouped in data structures (Files and Data Objects) on which some commands can be executed depending on the data type (similar concept to ISO/IEC 7816-15). Where the executable code is in the card is irrelevant at the PIV Application platform level and may be shared by hundreds of other application data groups without a problem. Either the specification maintains the vison of two card platforms as in GSC-IS or stick to only one for good. Keeping the subject ambiguous will lead to ambiguities.

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

Type of Comment, G = General E = editorial, T = technical

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
23	Gemplus	GL	T	Page 17 - 3.2.6	Adding and Deleting Card Applications is an ambiguous section as we do not know if this refers to the command set Load/delete applications of create/delete application structures as an application is sometimes code and some other times data. Both may have AIDs according to the document so what are we talking about here?. If an application is "associated" to a given data structure (e.g. a DF with an AID name as for the cryptographic application) and this data structure is deleted (delete DF) is the application code still in the card? Should the "data AID" have a different name than the "executablle code AID" (this is the approach taken by ISO/IEC 7816-15)? Are the application code and the application data using a common or related AID in the naming process?	Same comment as before. Either an application is represented by its data struture on which some commands availble at the card interface layer can act on/use application data depending on their type, or it is an executable piece of code which contains its own data structures. At present an AID allows to select a Dedicated File by its name (according to ISO/IEC 7816-4) and this is the only command we have available in the command set to select an application.
24	Gemplus	GL	T	Page 18 - 3.3.1	The notion of principals, well established in the ETSI application domain has not always transposed well in other domains. ISO/IEC 7816-4 defines two level of entities: global at the card level and local at the application level. As we are not sure of what an application is, the notion of entity may create issues of its own (e.g. How are they managed?).	Define in the document to which levels the principals are attached. Some are at card level (global) but others may be attached to the PIV card manager application, or the Cryptographic application or even to some of the Dedicated file in the card? How are these entities created and maintained during the life of the card?

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

Type of Comment, G = General E = editorial, T = technical

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
25	Gemplus	GL	T	Page 20 - 3.4.2	The use of the default ISO/IEC 7816-15 AID (E8 28 BD 08 oF) followed by 00 assumes no other application in the card will use ISO/IEC 7816-15 or assumes other applications will use another byte value (01 up to 0F). This may work but could create issues with other applications if the PIV application is not the Main application in the card. It would be better to use the other AID option proposed by ISO/IEC 7816-15 clearly indicating PIV is using wihtin its application domain ISO/IEC 7816-15. In order to do so, the AID to use for the cryptographic application must be the E8 28 BD 08 0F 00 followed by the AID of the "main application" calling it: the PIV application AID: A0 00 00 01 16 00 00 00.	Change the cryptographic application identifier to E8 28 BD 08 0F A0 00 00 01 16 00 00 00 in order to indicate the cryptographic application is in the PIV application domain (no reset of the application security status) and also in order to allow other applications in the card to use ISO/IEC 7816-15 if required.
26	Gemplus	GL	T	Page 22 - 4.1	Associating access rules to dedicated files and elementary transparent files is clearly explained in ISO/7816-4. Extending the concept to an application is ambiguous if the application is more than a DF with a name (see previous comments). Extending the concept of access rules to each data objects is possible but need then to be defined in details as ISO/IEC 7816-4 does not go that far (this is done in ISO/IEC 7816-15).	Define in details how access rules do apply to applications (if they are not just a DF with a name) and to data objects (if they are not cryptographic objects defined in ISO/IEC 7816-15) as ISO/IEC 7816-4 does not cover these extentions.
27	Gemplus	GL	T	Page 22 - 4.3	Application Identifiers are described in ISO/IEC 7816-4 and can be any length between one byte up to sixteen bytes. If PIV wants to impose a minimum length of 5 bytes on its AID, it can very well be said explicetly here but this is not an ISO restriction at all.	Replace the existing sentence by: An application identifier (AID) is a sequence of from 1- to -16 bytes as described in ISO/IEC 7816-4

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

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
28	Gemplus	GL	E	Page 23 - 4.10	As mentioned before the term data element for files and data objects can be source of confusion and is not supported by the command set.	Replace "data element" by "data structure"
29	Gemplus	GL	T	Page 24 - 4.13	The table defines Three principals: The cardholder (idenitifed only by his PIN), The card Issuer and the "application provider". Is the PIV Card Manager Application provider the same entity than the Cryptographic application provider? Could they be different and lead to an ambiguity?	Define clearly if the application provider is the PIV application provider or just any application provider having its own AID in the card. Define how this table is created and maintained. Define the algorithm used for the authenitcation. The term RFU seems to indicate all other values are reserved but there is no way for an application to define an entity of its own (e.g. Application specific).
30	Gemplus	RS	T	Page 25 - 4.16, Pg 25	Secure Channel Type? We feel the current list should be extended to be more in line with Global Platforms specifications.	Including Secure Channel type for 'Encryption + MAC' using Symmetric key
31	Gemplus	GL	E	Page 26 - 5.0	The table carries over the ambiguities of "data element" (which can be files or data objects) and "Application"(which can be a DF with a name, or some code somehwere in the card platform) as indicated before.	Clarification is required to explain in details what is an application and what are the data structures if different.
32	Gemplus	GL	T	Page 33 - 5.2	The Entry points for application management seem to aim at JavaCards loading applets but also could be understood to be used to create file structures in a card. What is the command to use in order to create the root DF of the PIV application? Is this a dedicated file with a name (and then a "create file" data management command) or an "application" (what ever this means) and the command "add card application" is to be used then?	There must be a clear separation between executable code management (reserved to JavaCards) and pure data and data structure management for all PIV cards (whatever OS they use). The "PIV application platform" should not exist in JavaCards before "the PIV application code" is loaded. This allows to have a common platform behavior between Javacards (after the PIV card manager is loaded) and file card systems.

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

Type of Comment, G = General E = editorial, T = technical

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
33	Gemplus	GL	T	Page 35 - 5.2.3	When can be executed the command "Generate Asymetric Key Pair? Is it after the data structures to store the information have been created or are these structures built also by the execution of this API call? Which application needs to be selected before this happens? Must this be the PIV application manager or the Cryptographic Infromation Application or could it be any other application?	The sequence in which the various API calls are to be done would be useful to know. This would allow to understand some of the hidden logic (which can be guessed by looking at the parameters) and would help remove ambiguities.
34	Gemplus	GL	E	Page 39 - 5.3.1	dataElementName shows pretty well the nature of the possible confusion the term data element introduces as the document itself falls into the issue. Are we talking about a data object here, a dedicated file or some other entity? Why use the same API entry point to deal with structures of complete different natures (data objects and files) which will require different set of properties and the use of different commands at the card interface. The API will need anyway to make the difference between data objects and files and the "name" or the "length of the name" are not enough to make the fdifference. It would be much simpler to have two different API calls, one for files and one for data objects.	Create two separate API calls. One for data structures (Dedicated or Elementary files) and another one for data objects. Or use the ISO 7816 Tag when a file is referenced as a data object.

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

Type of Comment, G = General E = editorial, T = technical

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
35	Gemplus	GL	T	Page 43 - 5.3.5 & 5.3.6	These two API calls allow the application layer to access bits and bytes in all data structures. It is unfortunate these entry points are not at the same level than data objects handling. Why not have an API call to read or write a complete data object or a complete file (ISO 7186-4 allows this option with the Get Data Command). Why force the application layer to deal with low level byte parsing? This is a pure receipe for inconsistencies in files, encouraging the application layer to manage the formating of the data objects (override of a tag or a length by an ill writen application layer).	Create API calls to access (read or write or update) a data object (BER TLV encoded data element) using its tag/identifier. Create API calls to read and write the whole file at once and not by small pieces.
36	Gemplus	GL	T	Page 45 - 5.4.1	In which application context the command "Authenticate card" is to be used? Should the cryptographic application be selected before or should this command work only in the PIV application card manager?	Indicate in which context these API calls can be made and which calls have to be done before.
37	Gemplus	GL	E	Page 51 - 6.0	The cards commands for card content management may not exist (or have any meaning) on all card platforms when the PIV application code is included as part of the card platform manufacturing. The notion of a card platform referenced only in three blocks of the table seem to indicate there are two different platforms. One for the card (e.g. Global Platform) and one for the PIV Data structures.	Separate the commands for card content application code management in a separate section dealing only with JavaCards and make them optional.
38	Gemplus	RS	T	Page 51 - Table 6-1	Card Content Management commands - All these commands should be mapped to GP 2.0.1' specifications. Any file system card can be implemented for GP 2.0.1' commands.	Document should directly refer to GP 2.0.1' specifications to all these commands including 'External Authenticate' command.

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
39	Gemplus	RS	G	Page 51 - Table 6-1	Data Management Commands - Create / Delete / Select File?	Here File actually refers to 'Data Element' per SP800-73 doc. Shouldn't the command use Data Element for consistency?
40	Gemplus	RS	T	Page 51 - Table 6-1	Application Management Commands - Loading keys? The 'PUT KEY' command available under Card Content Management commands is not available to PIV Card Manager application.	It appears there is need to have 'Load / Import Key' command under Application Management commands.
41	Gemplus	GL	T	Page 54 - 6.1.2	The Install command has little meaning on file card systems and should not be a mandatory command on all card platforms.	Indicate this command (as Initiallize and Load) is not required on file card platforms.
42	Gemplus	GL	T	Page 54 - 6.1.2	The INS code chosen for the Install command may not be the best choice as it means "Terminate DF" in ISO/IEC 7816. This is not a real issue as the Class byte indicates this is a different command set but could create confusion if a card has the ISO Terminate DF command in its command set.	Add a note this command has noting to do with the ISO/IEC 7816 command "E6" Terminate DF.
43	Gemplus	GL	T	Page 56 - 6.1.3	This command is not ISO compliant has stated. The Class byte should be "80" and the INS code choice of E8 is not a very good choice as it means "Terminate EF" is ISO/IEC 7816.	Change the class byte to "80" and add a note saying this command is different from the ISO/IEC command "E8" Terminate EF
44	Gemplus	GL	G	Page 57 - 6.1.4	Why is this command restricted for use to the card manager only? It would be rather useful to have a similar command as part of the command set for applications to manage keys.	Put Key is a useful command which would have some merit being available to the whole PIV application (or may be the whole card) in all data structures.
45	Gemplus	GL	T	Page 58 - 6.1.5	This command is not defined in this document. It may not even be useful to have such a command in the PIV environment as the PIV applivcation is not to be removed from a card except in a test environment.	Remove this command from the PIV specification.

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

Type of Comment, G = General E = editorial, T = technical

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
46	Gemplus	GL	T	Page 59 - 6.2.1	Is there a requirement for this command to be executed before a given select application command. Should the the Cryptographic application be selected before this command is executed or it does not matter? What are the data structures suppose to be exsiting before this command is executed?	Indicate the conditions and the context under which the command can be executed.
47	Gemplus	GL	E	Page 59 - 8.4	The reference to all parts of ISO/IEC 7816 is not relevant. Part 10 and part 12 do not apply and Part 13 is not stable yet.	Change the reference to ISO/IEC 7816 Parts 1 to 9 and 15.
48	Gemplus	GL	T	Page 61 - 6.2.2	It is clearly said here the security status is lost when an application is selected. This could mean when the cryptographic application is selected, the security authorizations (if any) obtained in the PIV card manager application are lost. This may not be consistent with what is expected in the PIV application domain.	Clarify what happens when the cryptographic application is selected using this command. All access conditions established before are lost or unchanged?
49	Gemplus	GL	T	Page 61 - 6.2.2	The last sentence says ".... Application dedicated file if any." What is selected if there is no Dedicated file? ISO/IEC 7816-4 does not define what is selected then. If this is possible the document must explain what is selected.	Clarify what is selected by this command when the "application" does not have a dedicated file.
50	Gemplus	GL	E	Page 61 - 8.4	The reference to ISO/IEC 24727 parts should not be made as this standard may not even be in a CD approved format when the PIV document will be signed.	Remove all references to ISO 24727 as the standard is not avavailable.

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

Type of Comment, G = General E = editorial, T = technical

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
51	Gemplus	GL	T	Page 62 - 6.3.1	The create file command allows to create dedicated as well as elementary files. According to ISO this is the way to create application data files with an application name (AID). Is this "the command" to use in order to create the cryptographic data structures as well as the EF.CIA or shall the load application be used for all type of card platforms?	The document needs to clarify if the command Create File is to be used to create Application Data Files (DF with a name) or if the Load Application command is to be used to do so.
52	Gemplus	GL	T	Page 63 - 6.3.2	For interoperability purpose it is important to indicate if the memory space is freed or if the application is logically deleted only.	Indicate if this is a logical delete (and then warn about data memory) or if this must be a logical and physical memory delete
53	Gemplus	GL	T	Page 63 - 6.3.2	For interoperability purpose it is important to indicate what happens when this command is issued on a DF which still has other data structures underneath. Does it delete all undelying structures or not?	Indicate what is required to do when this command is issued on a DF under which other DFs or Efs are still present.
54	Gemplus	GL	E	Page 78 - 6.5 Table 6-14	The last column is a "C" for all rows and the header suggests only M or O.	Change the "C" to an "O" in the last column of the table.
55	Gemplus	RS	T	Page 82 - 7.0, Pg 82	Are these applications managed by PIV Card Manager Application as well? Also, as described in the first para, who needs to provide details on Loading / Personalizing (GSC-IS doesn't define it either)?	
56	Gemplus	RS	G	Page 82 - 7.0, Pg 82	Backgound information on the VCEI of GSC-IS is not covered in SP800-73 document. Is the reader supposed to read GSC-IS specifications along with SP800-73 document?	
57	Gemplus	RS	T	Page 86 - 7.2.2	The INS code 56 is not allowed by ISO/IEC 7816 and the Class byte should indicate it is a propretary command.	Class Byte should be 80 or 8C

Submitted by: _____

Date: _____

Comments on Document SP 800-73 Version 1.0 Published on November 9th, 2004

Organization: Gemplus Corporation

Points of Contact: Gilles Lisimaque (GL) - Gilles.Lisimaque@Gemplus.com - Rajesh Sharma (RS) - Rajesh.Sharma@Gemplus.com

Comment types: G-General, E-editorial, T-Technical

Cmt #	Organization	Point of Contact	Cmt Type	Document Reference of Section or Annex	Comment (Include rationale for comment)	Proposed change
58	Gemplus	RS	G	Page N/A - New Annex	The absence of the data model in the document limits considerably the understanding of how to implement the PIV application. Depending on the complexity of the data structures and the access rules the various commands and API calls could differ drastically	An indication of the data model and how it can be adapted by each agency is very important to understand the whole application.
59	Gemplus	RS	E	Page N/A - New Annex	Suggestion to include in the PIV document the diagram proposed by Gemplus to clearly identify the scope of the PIV specification .	Include in an Annex the drawing in the word file from Gemplus called "Draft PIV architecture.doc "

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

Type of Comment, G = General E = editorial, T = technical