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)
1	GlobalPlatform	Kekicheff	T	SP 800-73 v1, sections 3 & 3.1, p13-14	Lack of consistency in the definition of the "data element" concept which insinuates that TLV format is not applied systematically to all data. In the PIV specifications, all data elements retrievable from the card have a tag, regardless of their storage inside the card. The notion of "unstructured transparent file" is not used for application data structures. See the "PIV Migration Report" white paper describing a laudable objective for data representation: "FIPS 201 provides a uniform representation for the TLV data structure on the application programming interface that is independent of the manner in which the data is stored on the card. This enables the card issuer and the card application program provider to change the manner in which the data is stored... without impacting applications using the data." (p 14 of the white paper).

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)
2	GlobalPlatform	Kekicheff	T	SP 800-73 v1, sections 3 & 3.1, p13-14	Asence of a naming convention rule for data elements and files. See also comment #13 on section 4.10.

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)
3	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.1.3, p15	Lack of consistency in the definition of the "currently selected" concept. Ambiguity of the notion of "currently selected data element" (probably introduced as a consequence of a file being assimilated to a data element: see comment #1).
4	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.1.4, p15	Description of adding and deleting data elements is limited to files only

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)
5	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.2.1, p15	Concept of the "Master File" as the root of the Card Manager application is a specific, yet correct, implementation of GlobalPlatform's definition of "Card Manager". Such specifics show a file system oriented implementation. Furthermore, it pushes to a technical design mixing card management functionality and application specific functionality: see PIV specification, section 4.1.5 p23, requiring to store the CHUID and biometric data "in the root file system of the Card Manager (the Master File) to facilitate rapid retrieval for physical access control applications".
6	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.2.5, p16	Ambiguity of the concept of "default data element" (probably introduced as a consequence of a file being assimilated to a data element: see comments #1 & 4)

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)
7	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.2.7, p17	Figure #1 shows a file system oriented implementation and ignores independent DOTs.
8	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.3.4, p19	Typo in the name of the command. Too high level requirement for security environments requesting the potential dynamic customization of cryptographic operations, when simplified application programs may simply pre-define (hard-code) the cryptographic mechanisms it uses.

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)
9	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.4, p19	Table #3-1 shows a file system oriented implementation and ignores independent DOTs. Table #3-1 perpetuates all the ambiguities found in the earlier definition sections.
10	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 3.5, p20	CLA byte bits usage does not account for GlobalPlatform Secure Channel Protocols
11	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 4.9, p23	Too restrictive definition of a data object.
12	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 4.4, p23	Insufficient description of Application Properties
13	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 4.10, p23	Definition of data element name perpetuates the amibuguites of the data element concept definition.

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)
14	GlobalPlatform	Kekicheff	E/T	SP 800-73 v1, section 4.16, p25	Potential confusion with GlobalPlatform specifications
15	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.1.1, p53	Non GlobalPlatform compliant definition of Initialize Update command
16	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.1.2, p54-55	Non GlobalPlatform compliant definition of Install command
17	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.1.3, p56	Non GlobalPlatform compliant definition of Load command

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)
18	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.1.4, p57	Non GlobalPlatform compliant definition of Put Key command
19	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.1.5, p58	Incomplete definition of Delete command
20	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.2.2, p61	Non ISO and non GlobalPlatform compliant definition of Select Application command
21	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.3.4, p65	Non GlobalPlatform compliant definition of Get Data command
21	GlobalPlatform	Kekicheff	T	SP 800-73 v1, section 6.4.1, p70	Non GlobalPlatform compliant definition of External Authenticate command
22	GlobalPlatform	Kekicheff	G	SP 800-73 v1, section 8.6, p97	Reference latest GlobalPlatform specification version

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)

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

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

Submitted by: _____

Date: _____

Proposed change
1) Delete the notion of "unstructured transparent file". 2) Revisit the fake concept of a file as a data element and define a file as follows: "a file is a group of one (or more) data element(s)". Note this implies to delete the 2nd example of "data element" given in section 3.1.2 (2nd bullet): AID |FID |FID.

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

Submitted by: _____

Date: _____

Proposed change
1) Define the following rule for the naming convention of files that ensure uniqueness: "a file is uniquely identified on the card by the combination of its file id, the eventual file id (or hierarchy of file ids), called path by ISO 7816-4 "under" which it is stored, and the application id by which it can be accesssed". In other words, a FID may not be unique within one AID, but must be unique within/under a FID (the path must be unambiguous). 2) Define the following rule for the naming convention of data elements that ensure uniqueness: "a data element is uniquely identified on the card by the combination of its tag, the eventual file id (or hierarchy of file ids, called path by ISO 7816-4) in which it is stored, and the application id by which it can be accesssed". In other words, a given tag may not be unique within one AID, but must be unique within a FID. Note the naming/addressing convention of any other data internal to the card and not directly accessible (read or write mode) by the off-card application is implementation specific and is out

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

Submitted by: _____

Date: _____

Proposed change
1) Delete the concept of "currently selected dedicated file" as either redundant with the "currently selected application" (see Select Application command) or the "currently selected file" (see Select File command). 2) Delete the notion of "currently selected data element". Replace with the ISO 7816-4 notion of "currently selected file" (see Select File command).
Generalize The description to cover also the case of independent DOTs within an application (see Put Data command).

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

Submitted by: _____

Date: _____

Proposed change
Consider applying the GlobalPlatform's technical architecture: a) the Card Manager application is dedicated to card management functionality only. It may be viewed either as the MF or an "ordinary" ADF by a file system oriented card. b) another application than Card Manager may be placed at the MF level by a file system oriented card (typically for performance reasons). GlobalPlatform defines such application as an "implicitly selectable" application in accordance with ISO 7816-4 (the MF being always selected by default after the card's reset). c) the physical access control application can be defined as "implicitly selectable" (i.e. at the MF level) instead of the Card Manager application: the Card Manager is then only selectable by a Select Application command.
Delete the notion of "default data element". Replace with the ISO 7816-4 notion of "currently selected file" (see Select File command), an ADF (when it exists) being correctly described as the "default selected file" after selection of the corresponding application.

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

Submitted by: _____

Date: _____

Proposed change
1) Add in figure #1 shared independent DOTS between 2 applications. 2) Consider applying the GlobalPlatform's technical architecture simplification dedicating the MF to a specific application: either Card Manager or Application #C (see figure #1). Minimizing the hsaring of files and DOTS across applications simplifies the definition, implementation and verification of their corresponding access control rules.
1) Replace "Manage Security Operation" command with "Manage Security Environment" command (see section 6.4.7). 2) Replace in 2nd sentence "parametrize" with "describe" to read such as: "these data objects describe cryptographic operations performed by the card application". 3) Delete the last sentence of the section requiring the dynamic change and deletion of security environment data objects, hence the dynamic change and deletion of cryptographic mechanisms used by the card application.

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

Submitted by: _____

Date: _____

Proposed change
1) Delete the comment related to "currently selected file system" as it ignores independent DOTs that are permanently stored on the card. 2) State "No" in the "always" column for "currently selected file system" as it ignores independent DOTs. 3) Merge in one row/concept: "currently selected file", the 3 concepts of "currently selected file system", "currently selected dedicated file", "currently selected data element": see comments #1 & 4
Add the ISO 786-4 overall FCI template (tag '6F') embedding all the data elements described in table #4-2
Expand the definition of a data object to include DER coded objects as well as BER-TLV coded objects: see all the 7816-15 defined objects in section 7 that are DER coded
Expand the definition of a data object to include DER coded objects as well as BER-TLV coded objects: see all the 7816-15 defined objects in section 7 that are DER coded
1) Delete the notion of a FID being a data element name: see comment #1. 2) Define the complete name of a data element as the following concatenation AID | …. | DOT, where the dots (....) represent a suite (empty or not) of concatenated FIDs: see comment #3 re: naming conventions

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

Submitted by: _____

Date: _____

Proposed change
Rename "secure channel type" as "cryptographic mechanism type"
The Le byte of the Initialize Update command shall be defined as '00' (i.e. all data to be returned up to 256 bytes per ISO 7816-4) instead of '1B', allowing any eventual evolutions of the response data.
1) The CLA byte of the Install command shall be defined as '80' or '84': see comment #11. 2) The Le byte of the Install command shall be defined as '00' instead of 'absent' as potential response data (i.e. a cryptographic "receipt") may be returned. 3) Add a last byte of '00' in table 6-5 (to indicate absence of cryptographic "token") 4) Typo on the title of table 6-6: "parameter fieldfor load initiation" and not "command data field for load initiation"
1) The CLA byte of the Load command shall be defined as '80' or '84' instead of '00': see comment #11. 2) The command data field contains a portion (a "block") of the Load file (i.e. the program code). Add the format of the Load File: BER-TLV coded with tag 'C4' to indicate the beginning of the program code. Add a note remoinding the BER-TLV rules for coding the length indicator (typically on 2 bytes or more as the code is typically larger than 127 bytes).

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

Submitted by: _____

Date: _____

Proposed change
1) The CLA byte of the Put Key command shall be defined as '80' or '84': see comment #11. 2) The command data field shall be described according to GP specs.
Add the GlobalPlatform description of the Delete [Application, Load File] command
1) Typo inverting the meaning of P2 values: P2='00' means a FCI is returned in the response, P2='0C' means no response data 2) Le shall be either absent (P2='0C') or present and equal to '00' (P2='00') 3) Response data shall be described as either absent (P2='0C') or present and containing the FCI template '6F' (P2='00')
The Le byte of the Get Data command shall allow a value of '00' (i.e. all data to be returned up to 256 bytes) according to ISO 7816-4 and GP specs
1) The CLA byte of the External Authenticate command shall also include the '80' or '84' values to comply to GP specs (see also note 1 of section 6.4.1) 2) Add further precisions on the use of P2: note that in case of GP, it shall be set to '00'
Add version 2.1.1 reference of GP spec, dated Mars 2003: it is fully backward compatible with the use by CAC cards and GSC-IS specs of version 2.0.1'

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

Submitted by: _____

Date: _____

Proposed change

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