X-Sieve: CMU Sieve 2.2
To: draftfips201@nist.gov
Subject: Comments on Public Draft FIPS 201
From: Steve Everhard <Steve.Everhard@multos.com>
Date: Thu, 23 Dec 2004 10:09:21 +0000
X-MailScanner:
X-MailScanner-From: steve.everhard@multos.com

Incorrectly titled and so resent. Apologies

----- Forwarded by Steve Everhard/LON/MASTERCARD on 23/12/2004 09:51 -----
Steve Everhard

22/12/2004 16:49

To: draftfips201@nist.gov
cc:
Subject:

MAOSCO, the consortium of companies that develops smart card products based on the openly licensed and managed operating system specification, MULTOS, would like to provide comment upon the recently published draft document, draft-FPIS_201-110804-public1.pdf [FIPS201].
Attached file 04-12-22_SP800-73_FIPS201_MAOSCO_Comments.xls

Steve Everhard

Phone: +44 (0)20 7557 5464
Fax: +44 (0)20 7557 5474
Email: steve.everhard@multos.com

MAOSCO Limited
47-53 Cannon Street
London EC4M 5SH
United Kingdom
Registered No: 3290642, England

Phone: +44 (0)20 7557 5420

Fax: +44 (0)20 7557 5430
Email: kms_support@multos.com
WebSite: http://www.multos.com


04-12-22_SP800-73_FIPS201_MAOSCO_Comments1.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)
1	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	G	NIST Special Publication SP800-73 V1.0 Overall	The SP800-73 document implies that only GlobalPlatform (GP) compliant smart cards may provide interoperable PIV cards. MAOSCO's opinion is that any smart card may provide application level interoperability and this specification should not mandate any particular form of smart card operating system.
2	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.1 Page 15	The Card Manager Application is only relevant toGP compliant OS smart cards. Others such as MULTOS, do not implement such an Application - card management is processed directly by the OS
3	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.2 Pages 15/16	Reference to "mandatory card manager application" again implies the use of GP compliant OS smart cards
4	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.3 Page 16	Card Platform Commands are implementation technology specific and are only implemented by GP compliant OS smart cards.
5	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.6, Page 17	This section requires that applications are added and deleted using the content management card commands - again this is GP compliant OS smart card specific.
6	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.7 Page 17	The card platform commands and card manager application is GP compliant OS smart card specific.

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	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6, Pages 51-81	Card Platform Command Interface is GP compliant OS smart card specific.
8	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6 Table 6-1, Page 52	Notes 1 and 2 are GP compiant OS smart card specific
9	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6.1, Pages 53-58	Card Platform Commands for Card Content Management is GP compliant OS smart card specific
10	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6.6, Page 80	Secure Channel. This applies only to GP compliant OS smart cards.
11	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 8.6, Page 97	reference to "GlobalPlatform, Open Platform Card Specification, Version 2.0.1 April 7th 2000" is not required and is technology dependent

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)
12	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	G	FIPS PUB 201 v1.0, Annex F: References	Card Management would appear to to be out of place in an application level specification such as FIPS 201. Specifically the inclusion of a commercial specification, such as GlobalPlatform Open Platform Card Specification Version 2.0.1, that is managed outside of a National Standards body and so is subject to the commercial control by a few corporations is problemmatic and exclusive. The limiting of card management keys to symmetric Triple DES and AES techniques further limits the specification from exploiting more secure and advanced PKI based approaches.
13	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	E	FIPS PUB 201 v1.0, Section 4.1.6.2	[GP] Reference no longer required if GP not refernced in the body text as in Cmt# 12

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
Remove GP specific elements from this specification (details below).
This section implies only GP compliant OS smart cards may be used. The AID should only apply if a GP compliant card is used.
Remove this requirement.
Card Platform Commands should be removed from this specification.
Remove this requirement.
Remove the sentence "Application C share..." thru "rooted at ADF#2." in paragraph 1. Remove final paragraph. Remove Application C and Card Manager Application from the illustration.

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

Submitted by: _____

Date: _____

Proposed change
All Entries for Card Commands for Card Content Management should be removed.
Remove Notes 1 and 2
Remove section 6.1 and subsections.
Remove section 6.6
Remove section 8.6

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

Submitted by: _____

Date: _____

Proposed change
Modify section 4.1.6.2 to read only as follows: " PIV cards may support card activation by *a* card management system to support card personalisation and post-issuance card updating. When cards are personalized, card management keys shall be set to be specific to each PIV card. That is, a card issuer may not use a single cryptographic key to activate more than one card". Remove paragraph 2 beginning "If supported..." and remove table 4-1
Remove [GP] Entry

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

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	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	G	NIST Special Publication SP800-73 V1.0 Overall	The SP800-73 document implies that only GlobalPlatform (GP) compliant smart cards may provide interoperable PIV cards. MAOSCO's opinion is that any smart card may provide application level interoperability and this specification should not mandate any particular form of smart card operating system.	Remove GP specific elements from this specification (details below).
2	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.1 Page 15	The Card Manager Application is only relevant toGP compliant OS smart cards. Others such as MULTOS, do not implement such an Application - card management is processed directly by the OS	This section implies only GP compliant OS smart cards may be used. The AID should only apply if a GP compliant card is used.
3	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.2 Pages 15/16	Reference to "mandatory card manager application" again implies the use of GP compliant OS smart cards	Remove this requirement.
4	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.3 Page 16	Card Platform Commands are implementation technology specific and are only implemented by GP compliant OS smart cards.	Card Platform Commands should be removed from this specification.
5	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.6, Page 17	This section requires that applications are added and deleted using the content management card commands - again this is GP compliant OS smart card specific.	Remove this requirement.
6	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.7 Page 17	The card platform commands and card manager application is GP compliant OS smart card specific.	Remove the sentence "Application C share..." thru "rooted at ADF#2." in paragraph 1. Remove final paragraph. Remove Application C and Card Manager Application from the illustration.
7	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6, Pages 51-81	Card Platform Command Interface is GP compliant OS smart card specific.	All Entries for Card Commands for Card Content Management should be removed.
8	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6 Table 6-1, Page 52	Notes 1 and 2 are GP compiant OS smart card specific	Remove Notes 1 and 2
9	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6.1, Pages 53-58	Card Platform Commands for Card Content Management is GP compliant OS smart card specific	Remove section 6.1 and subsections.

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
10	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6.6, Page 80	Secure Channel. This applies only to GP compliant OS smart cards.	Remove section 6.6
11	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 8.6, Page 97	reference to "GlobalPlatform, Open Platform Card Specification, Version 2.0.1 April 7th 2000" is not required and is technology dependent	Remove section 8.6
12	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	G	FIPS PUB 201 v1.0, Annex F: References	Card Management would appear to to be out of place in an application level specification such as FIPS 201. Specifically the inclusion of a commercial specification, such as GlobalPlatform Open Platform Card Specification Version 2.0.1, that is managed outside of a National Standards body and so is subject to the commercial control by a few corporations is problemmatic and exclusive. The limiting of card management keys to symmetric Triple DES and AES techniques further limits the specification from exploiting more secure and advanced PKI based approaches.	Modify section 4.1.6.2 to read only as follows: " PIV cards may support card activation by a card management system to support card personalisation and post-issuance card updating. When cards are personalized, card management keys shall be set to be specific to each PIV card. That is, a card issuer may not use a single cryptographic key to activate more than one card". Remove paragraph 2 beginning "If supported..." and remove table 4-1
13	MAOSCO for the MULTOS Consortium of Companies	steve.everhard@multos.com	E	FIPS PUB 201 v1.0, Section 4.1.6.2	[GP] Reference no longer required if GP not refernced in the body text as in Cmt# 12	Remove [GP] Entry

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

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