

X-Sieve: CMU Sieve 2.2
To: drafftips201@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: drafftips201@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

The information in this Email and any attached files are confidential, may also be privileged, and is intended solely for the addressee.

Access, copying, dissemination, distribution or re-use of the information in this Email and any attached files by anyone else is unauthorised. Any views or opinions presented are solely those of the author and do not necessarily represent those of MAOSCO Limited or any of its affiliates. If you are not the intended recipient, all copies of the Email and associated files in your possession should be destroyed.

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](#)

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.eve@rhard@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.eve@rhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.1 Page 15	The Card Manager Application is only relevant to GP 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.eve@rhard@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.eve@rhard@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.eve@rhard@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.eve@rhard@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.

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.eve@rhard@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.eve@rhard@multos.com	T	NIST Special Publication SP800-73 V1.0, Section 6 Table 6-1, Page 52	Notes 1 and 2 are GP compliant OS smart card specific
9	MAOSCO for the MULTOS Consortium of Companies	steve.eve@rhard@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.eve@rhard@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.eve@rhard@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

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.

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

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 = editorial, 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.ewe rhard@m ultos.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.ewe rhard@m ultos.com	T	NIST Special Publication SP800-73 V1.0, Section 3.2.1 Page 15	The Card Manager Application is only relevant to GP 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.ewe rhard@m ultos.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.ewe rhard@m ultos.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.ewe rhard@m ultos.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.ewe rhard@m ultos.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.ewe rhard@m ultos.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.ewe rhard@m ultos.com	T	NIST Special Publication SP800-73 V1.0, Section 6 Table 6-1, Page 52	Notes 1 and 2 are GP compliant OS smart card specific	Remove Notes 1 and 2
9	MAOSCO for the MULTOS Consortium of Companies	steve.ewe rhard@m ultos.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.

