X-Sieve: CMU Sieve 2.2
Subject: PhRMA SAFE Comments on FIPS 201 and SP 800-73
Date: Thu, 23 Dec 2004 08:39:26 -0500
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Comment Template for FIPS 201
Thread-Index: AcTiKrLigMco8dZlSNq08Ps8AapVxgGHCNYg
From: "Zagar, Terry \(Mission Systems\)" <Terry.Zagar@ngc.com>
To: <draftfips201@nist.gov>
Cc: "Gary Secrest [JJCUS] \(E-mail\)" <GSecrest@CORUS.JNJ.com>
X-OriginalArrivalTime: 23 Dec 2004 13:39:27.0140 (UTC) FILETIME=[D250EE40:01C4E8F4]
X-MailScanner:
X-MailScanner-From: terry.zagar@ngc.com

The biopharmaceutical industry's Secure Access For Everyone (SAFE) initiative appreciates the opportunity to submit the following comments on:

- FIPS 201, version 1.0, Personal Identity Verification (PIV) for Federal Employees and Contractors, Public Draft, and
- Special Publication 800-73, version 1.0, Integrated Circuit Card for Personal Identity Verification, Initial Public Draft

The biopharmaceutical industry under the auspices of the Pharmaceutical Research and Manufacturers of America (PhRMA) and the European Federation of Pharmaceutical Manufacturers Associations (EFPIA), with inputs from the US Food and Drug Administration (FDA), the National Cancer Institute (NCI), and the European Medicines Agency (EMEA), developed and published the SAFE standard. This standard provides for globally accepted, legally binding, and regulatory compliant digital signatures for use in biopharmaceutical business-to-business and business-to-regulator transactions (e.g., electronic submissions for new medical product applications). More information on this community model is available at http://www.safe-biopharma.org/.

The biopharmaceutical industry:

a. Interoperates with certain Federal Government entities (e.g., within the FDA and NIH) as dictated by government regulations and programs applicable to medical product research, development, marketing, and safety assurance.
b. Leverages, across its extended enterprises, the security infrastructure standards, tools, and product vendors associated with Federal Government programs such as dictated by Homeland Security Presidential Directive (HSPD) 12.

The SAFE Standard specifies the identity-proofing, private key protection, and use framework for digital signatures. As an interested industry group, we wish to maintain interoperability with evolving Federal initiatives (such as FIPS 201 and SP 800-73), as well as assure the industry that appropriate vendor products compliant with FIPS standards (e.g., FIPS 140 and FIPS 186) will continue to exist and evolve, and are available to support continuing industry security infrastructure initiatives at cost effective levels.

The attached comments are in both Microsoft Word and Microsoft Excel formats. These comments represent those of the SAFE Membership and Steering Committee. From a Biopharmaceutical Industry perspective, SAFE member companies support such Homeland Security initiatives, and wish to maximize the extent that these initiatives can also be leveraged in the protection of the Industry's infrastructure.

Sincerely,

Terry Zagar
representing -
Pharmaceuticals Research and Manufacturers of America (PhRMA)
SAFE (Secure Access For Everyone) Initiative
Chair, SAFE Operations & Technology Working Group

Northrop Grumman Information Technology
Commercial Healthcare
2101 Gaither Rd., Suite 600
Rockville, MD 20850
301-527-6780 Office
301-527-6401 Fax

CONFIDENTIALITY NOTICE:
This email and any attachments are for the exclusive and confidential use of the intended recipient. If you are not the intended recipient, please do not read, distribute or take action in reliance upon this message. If you have received this in error, please notify us immediately by return email and promptly delete this message and its attachments from your computer system.

SAFE Comments on Draft NIST Standards.doc

PhRMA SAFE Comments.xls

Prepared by: Terence Zagar
Chair, SAFE Operations & Technology Working Group
terry.zagar@ngc.com
Representing: The PhRMA SAFE Initiative

Overview:

The biopharmaceutical industry's Secure Access For Everyone (SAFE) initiative appreciates the opportunity to submit the following comments on:

- FIPS 201, version 1.0, Personal Identity Verification (PIV) for Federal Employees and Contractors, Public Draft, and
- Special Publication 800-73, version 1.0, Integrated Circuit Card for Personal Identity Verification, Initial Public Draft

The biopharmaceutical industry under the auspices of the Pharmaceutical Research and Manufacturers of America (PhRMA) and the European Federation of Pharmaceutical Manufacturers Associations (EFPIA), with inputs from the US Food and Drug Administration (FDA), the National Cancer Institute (NCI), and the European Medicines Agency (EMEA), developed and published the SAFE standard. This standard provides for globally accepted, legally binding, and regulatory compliant digital signatures for use in biopharmaceutical business-to-business and business-to-regulator transactions (e.g., electronic submissions for new medical product applications). More information on this community model is available at http://www.safe-biopharma.org/.

The biopharmaceutical industry:

a. Interoperates with certain Federal Government entities (e.g., within the FDA and NIH) as dictated by government regulations and programs applicable to medical product research, development, marketing, and safety assurance.

b. Leverages, across its extended enterprises, the security infrastructure standards, tools, and product vendors associated with Federal Government programs such as dictated by Homeland Security Presidential Directive (HSPD) 12.

The SAFE Standard specifies the identity-proofing, private key protection, and use framework for digital signatures. As an interested industry group, we wish to maintain interoperability with evolving Federal initiatives (such as FIPS 201 and SP 800-73), as well as assure the industry that appropriate vendor products compliant with FIPS standards (e.g., FIPS 140 and FIPS 186) will continue to exist and evolve, and are available to support continuing industry security infrastructure initiatives at cost effective levels.

The comments provided here represent those of the SAFE Membership and Steering Committee. From a Biopharmaceutical Industry perspective, SAFE member companies support such Homeland Security initiatives, and wish to maximize the extent that these initiatives can also be leveraged in the protection of the Industry's infrastructure.

Prepared by: Terence Zagar
Chair, SAFE Operations & Technology Working Group
terry.zagar@ngc.com
Representing: The PhRMA SAFE Initiative

General Comments on FIPS 201 draft and SP800-73 draft:

There appears to be some lack of clarity in both the draft FIPS 201 and draft SP 800-73 relative to the requirements of the Government Smart Card – Interoperability Specification (GSC-IS) v2.1. For example:

- There are only two references to SP 800-73 in FIPS 201. One of these is simply a reference notation in Annex F. The other is in Section 4.1.5.2, of FIPS 201 that references Section 7.1 of SP 800-73 for the Personal Identity Verification (PIV) card architecture. Does this mean that FIPS 201 only requires the Cryptographic Information Application (CIA) functionality in practice, or does all of SP 800-73 also apply to a FIPS 201 compliant PIV? We suspect it is the latter, but it is not clear from the current document wording other than the document titles.

- According to Section 1.1 of SP 800-73, it would appear that it supports both the GSC-IS v2.1 file system card edge interface and the virtual machine card edge interface. Other than this mention, however, SP 800-73 appears to deal only with file system card requirements. Can you clarify that both file system and virtual machine card edge interfaces are allowed, and that FIPS 201 permits either option? From a SAFE perspective, many large Industry members are adopting smart cards with JavaCard^{TM} functionality. If the Federal Government, which is a large buyer of such technology, effectively abandons JavaCard^{TM} capabilities, that will impact the relative long-term support for deployed JavaCard^{TM} installations, and will likely preclude new security enhancement features for related products. That would represent both a support risk and a critical US industry infrastructure security risk.

- There appear to be some discrepancies between SP 800-73 and GSC-IS v2.1 in that SP 800-73 and FIPS 201 seem to mandate a new class of smart cards to meet PIV card requirements (i.e, a new operating system for file system cards at a minimum, and new Java applets if JavaCard^{TM} functionality is indeed supported (see point above)). This would further seem to preclude the use of currently existing off-the-shelf products for PIV use, and require the availability of new cards and card software with the requisite functionality. Is this a correct interpretation? While SAFE appreciates the technology forcing function provided by major Federal Government programs, our membership remains committed to JavaCard^{TM} capabilities, and wishes to ensure that the Government continues to promote and embrace JavaCard^{TM} technology as a major consumer of such technology.

- FIPS 201, Sections 4 and 6 call out some specific capabilities with respect to information that can be accessed without authentication to the PIV card in addition to the information that may only be accessed through authenticated means. It appears that this will require the availability of new middleware products to take advantage of this added functionality. Is this a correct interpretation? Because this requirement applies to both the contact and contactless portions of the PIV card, it would seem that some of this non-authenticated information may be extracted without the knowledge of the PIV card owner, posing a potential privacy and security threat, especially for Federal contractors and employees traveling outside of the US. If the Federal Government is mandating new capabilities for smart cards at this juncture, we would definitely like to see the Federal Government also specify protections for non-authenticated information export which would further support the growing privacy protection requirements of industry.

- If indeed there is not a competitive market selection of products available to meet the requirements of FIPS 201 and SP 800-73 as discussed above, it appears inconsistent that no waivers are permitted to FIPS 201. This would seem counterproductive to initiating a managed transition process across the Federal Government to PIV requirements in a timely fashion, especially since new product certification mechanisms would need to be put in place prior to full scale deployment. Since Federal personnel and contractors often interact with the biopharmaceutical industry, we would be most interested in attaining interoperability with the PIV card in order to better identify such personnel and leverage PIV card information. If that interoperability can be achieved using currently deployed off-the-shelf technology, it is then a benefit for all parties.

Other Comments on FIPS 201 draft and SP 800-73 draft:

PAGE	SECTION	COMMENT
iv	FIPS 201, Page Title	Typo - the words "Standards" and "Processing" are transposed
20	SP 800-73, Section 3.6	There is a reference to FIPS 201, Chapter "xxx", but it is not clear where in FIPS 201 the referenced communications information is discussed. Appendix A.2 in FIPS 201appears the most likely reference.

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	Pharmaceutical Research & Manufacturers of America Secure Access For Everyone (PhRMA SAFE) Initiative	Terence Zagar Chair, SAFE Operations & Technology Working Group terry.zagar@ngc.com	O-Overview	na	The biopharmaceutical industry under the auspices of the Pharmaceutical Research and Manufacturers of America (PhRMA) and the European Federation of Pharmaceutical Manufacturers Associations (EFPIA), with inputs from the US Food and Drug Administration (FDA), the National Cancer Institute (NCI), and the European Medicines Agency (EMEA), developed and published the SAFE standard. This standard provides for globally accepted, legally binding, and regulatory compliant digital signatures for use in biopharmaceutical business-to-business and business-to-regulator transactions (e.g., electronic submissions for new medical product applications). More information on this community model is available at http://www.safe-biopharma.org/.
2	see Cmt #1	see Cmt #1	O-Overview	na	The biopharmaceutical industry: a) Interoperates with certain Federal Government entities (e.g., within the FDA and NIH) as dictated by government regulations and programs applicable to medical product research, development, marketing, and safety assurance. b) Leverages, across its extended enterprises, the security infrastructure standards, tools, and product vendors associated with Federal Government programs such as dictated by Homeland Security Presidential Directive (HSPD) 12.
3	see Cmt #1	see Cmt #1	O-Overview	na	The SAFE Standard specifies the identity-proofing, private key protection, and use framework for digital signatures. As an interested industry group, we wish to maintain interoperability with evolving Federal initiatives (such as FIPS 201 and SP 800-73), as well as assure the industry that appropriate vendor products compliant with FIPS standards (e.g., FIPS 140 and FIPS 186) will continue to exist and evolve, and are available to support continuing industry security infrastructure initiatives at cost effective levels.
4	see Cmt #1	see Cmt #1	O-Overview	na	The comments provided here represent those of the SAFE Membership and Steering Committee. From a Biopharmaceutical Industry perspective, SAFE member companies support such Homeland Security initiatives, and wish to maximize the extent that these initiatives can also be leveraged in the protection of the Industry's infrastructure.
5	see Cmt #1	see Cmt #1	G	multiple	There appears to be some lack of clarity in both the draft FIPS 201 and draft SP 800-73 relative to the requirements of the Government Smart Card – Interoperability Specification (GSC-IS) v2.1. The comments below represent examples of this:
6	see Cmt #1	see Cmt #1	G	FIPS 201, Section 4.1.5.2 & Annex F	There are only two references to SP 800-73 in FIPS 201. One of these is simply a reference notation in Annex F. The other is in Section 4.1.5.2, of FIPS 201 that references Section 7.1 of SP 800-73 for the Personal Identity Verification (PIV) card architecture.

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	see Cmt #1	see Cmt #1	G	SP 800-73, Section 1.1	According to Section 1.1 of SP 800-73, it would appear that it supports both the GSC-IS v2.1 file system card edge interface and the virtual machine card edge interface. Other than this mention, however, SP 800-73 appears to deal only with file system card requirements.
8	see Cmt #1	see Cmt #1	G	multiple	There appear to be some discrepancies between SP 800-73 and GSC-IS v2.1 in that SP 800-73 and FIPS 201 seem to mandate a new class of smart cards to meet PIV card requirements (i.e, a new operating system for file system cards at a minimum, and new Java applets if JavaCardTM functionality is indeed supported (see comment above)). This would further seem to preclude the use of currently existing off-the-shelf products for PIV use, and require the availability of new cards and card software with the requisite functionality.
9	see Cmt #1	see Cmt #1	G	FIPS 201, Sections 4 and 6	FIPS 201, Sections 4 and 6 call out some specific capabilities with respect to information that can be accessed without authentication to the PIV card in addition to the information that may only be accessed through authenticated means. It appears that this will require the availability of new middleware products to take advantage of this added functionality.

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)
10	see Cmt #1	see Cmt #1	G	multiple	If indeed there is not a competitive market selection of products available to meet the requirements of FIPS 201 and SP 800-73 as discussed in the comments above, it appears inconsistent that no waivers are permitted to FIPS 201.
11	see Cmt #1	see Cmt #1	E	FIPS 201, Page Title, page iv	Typo - the words "Standards" and "Processing" are transposed
12	see Cmt #1	see Cmt #1	E	SP 800-73, Section 3.6, page 20	There is a reference to FIPS 201, Chapter "xxx", but it is not clear where in FIPS 201 the referenced communications information is discussed.

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

Submitted by: ______________________

Date: __________

Proposed change
Does this mean that FIPS 201 only requires the Cryptographic Information Application (CIA) functionality in practice, or does all of SP 800-73 also apply to a FIPS 201 compliant PIV? We suspect it is the latter, but it is not clear from the current document wording other than the document titles.

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

Proposed change
Please clarify that both file system and virtual machine card edge interfaces are allowed, and that FIPS 201 permits either option. From a SAFE perspective, many large Industry members are adopting smart cards with JavaCardTM functionality. If the Federal Government, which is a large buyer of such technology, effectively abandons JavaCardTM capabilities, that will impact the relative long-term support for deployed JavaCardTM installations, and will likely preclude new security enhancement features for related products. That would represent both a support risk and a critical US industry infrastructure security risk.
Is this a correct interpretation? We would like to see better alignment between these draft standards and GSC-IS v2.1. While SAFE appreciates the technology forcing function provided by major Federal Government programs, our membership remains committed to JavaCardTM capabilities, and wishes to ensure that the Government continues to promote and embrace JavaCardTM technology as a major consumer of such technology.
Is this a correct interpretation? Because this requirement applies to both the contact and contactless portions of the PIV card, it would seem that some of this non-authenticated information may be extracted without the knowledge of the PIV card owner, posing a potential privacy and security threat, especially for Federal contractors and employees traveling outside of the US. If the Federal Government is mandating new capabilities for smart cards at this juncture, we would definitely like to see the Federal Government also specify protections for non-authenticated information export which would further support the growing privacy protection requirements of industry.

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

Submitted by: ______________________

Date: __________

Proposed change
The lack of waivers is counterproductive to initiating a managed transition process across the Federal Government to PIV requirements in a timely fashion, especially since new product certification mechanisms would need to be put in place prior to full scale deployment. Since Federal personnel and contractors often interact with the biopharmaceutical industry, we would be most interested in attaining interoperability with the PIV card in order to better identify such personnel and leverage PIV card information. If that interoperability can be achieved using currently deployed off-the-shelf technology, it is then a benefit for all parties.
Correct
Appendix A.2 in FIPS 201appears the most likely reference.

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