Krister Walfridsson, 06:19 PM 12/22/2004, Comments on Public Draft FIPS 201

X-Sieve: CMU Sieve 2.2

From: Krister Walfridsson krister.walfridsson@precisebiometrics.com

To: "'DraftFips201@nist.gov'" <DraftFips201@nist.gov> Cc: Ola Svedin <ola.svedin@precisebiometrics.com>

Subject: Comments on Public Draft FIPS 201 Date: Thu, 23 Dec 2004 00:19:08 +0100 X-Mailer: Internet Mail Service (5.5.2656.59)

X-OriginalArrivalTime: 22 Dec 2004 23:10:04.0812 (UTC) FILETIME=[5F2554C0:01C4E87B]

X-MailScanner:

X-MailScanner-From: krister.walfridsson@precisebiometrics.com

Please find comments from Precise Biometrics attached to this mail.

Best regards,

/Krister

Krister Walfridsson Systems Architect Precise Biometrics AB Scheelevägen 19 C 223 70 Lund Sweden

Phone: +46 46 31 11 00 Direct: +46 46 31 11 21 Fax: +46 46 31 11 01

E-mail: kw@precisebiometrics.com

<<Comments on FIPS PUB 201.xls>>



Comments on FIPS PUB 201.xls

Precise Biometrics Precise Biometrics	kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com	I E	4.1.6, page 24 4.2.2, page 29 4.4.4, page 34 4.4.4, page 34, 2nd paragraph 4.5.2, page 39 4.5.2, page 39 5.2.4.1, paragraph 2, page 46 6.1, page 49	without any concrete encoding, and you need to specify an actual encoding (what the CBEFF calls 'patron formats') before you can use the data. So a requirement of CBEFF only is not sufficient to get interoperability. A patron format suitable for smart cards (both for off-card and on-card matching) is defined in normative Annex D of NISTIR 6329-A. The same format is also defined in ISO/IEC 7816-11. There is a requirement that the reader shall conform to PC/SC. The current PC/SC standard does however not support contactless readers (even though it is possible to implement a wrapper so that most operations work as if was a ISO/IEC 7816-card). PC/SC 2.0, that has support for contactless cards, will be published soon. There is a requirement on the PIN Pad, but no requirement on the blometric sensor. "The fingerprint from the expired PIV card may be stored on the new PIV card". Fingerprint changes over time (although much slower than face), so it should be recommended to collect new fingerprints.	Change "i.e. the PIN " to "i.e. the PIN or other cardholder uthentication method" in the three bullet points. Change "[NISTIR 6529-2001]" to "[CBEFF]" Change the 2nd sentence to read "The fingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure, encoded as in annex D of [CBEFF] (Blometric Information Data Objects for Use within Smartcards or other Tokens)." Change the word "conform" to some weaker requirement (e.g. "shall use PC/SC 1.0 as its interface"), or add a requirement on PC/SC 2.0 Add a new section: 4.5.4 Biometric Sensor Specifications. PIV cards may be activated through the contact interface by the cardholder using optional biometric cardholder activation described in section 4.1.5. Where the PIV card is used for injectal access, the biometric sensor may be incorporated into the reader. Where the PIV card is used for injectal access. (e.g. to authenticate to a website or other sensor may be a recognition to the reader of the biometric sensor may be a separate unit. Add ". but it is recommended that new fingerprint images are collected for the new Piv card".
Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics	sebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com	E T	4.4.4, page 34, 2nd paragraph 4.4.4, page 34, 2nd paragraph 4.5.2, page 39 4.5.2, page 39 5.2.4.1, paragraph 2, page 46	PIN need []* Section 4.1.6 does however permit on- card matching as cardholder verification. The text requires that the right and left index fingers shall be captired. This is not always possible, so the standard need to say what to do in these circumstances (e.g. as described in the first section of 4.4) ANSI/INCITS 381-2004 references NISTIR 6529-A rather than the older 2001 version (and it is the newer version that is already listed in Annex F of FIPS PUB 201) The main part of CBEFF defines abstract data objects without any concrete encoding, and you need to specify an actual encoding (what the CBEFF calls "patron formats") before you can use the data. So a requirement of CBEFF only is not sufficient to get interoperability. A patron format suitable for smart cards (both for off-card and on-card matching) is defined in normative Annex D of NISTIR 6529-A. The same format is also defined in ISO/IEC 7816-11. There is a requirement that the reader shall conform to PC/SC. The current PC/SC standard does however not support contactless readers (even though it is possible to implement a wrapper so that most operations work as if it was a ISO/IEC 7816 card). PC/SC 2.0, that has support for contactless cards, will be published soon. There is a requirement on the PIN Pad, but no requirement on the blometric sensor.	cardinolder uthentication method* in the three bullet points. Change "[NISTIR 6529-2001]" to "[CBEFF]" Change the 2nd sentence to read "The fingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure, encoded as in annex D of (CBEFF] (Biometric Information Data Objects for Use within Smartcards or other Tokens).* Change the word "conform" to some weaker requirement (e.g. "shall use PC/SC 1.0 as its interface"), or add a requirement on PC/SC 2.0 Add a new section: 4.5.4 Biometric Sensor Specifications. PIV cards may be activated through the contact interface by the cardholder using optional biometric cardholder activation described in section 4.1.5. Where the PIV card is used for induced in the treader. Where the PIV card is used for induced into the reader. Where the PIV card is used for induced into the reader sensor, the biometric sensor may be incorporated into the reader or the biometric sensor may be a separate unit. Add ". but it is recommended that new fingerprint images are collected for the new Pix card".
Blometrics Pracise Biometrics Precise Biometrics	sebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com	E T	4.4.4, page 34, 2nd paragraph 4.4.4, page 34, 2nd paragraph 4.5.2, page 39 4.5.2, page 39	be captured. This is not always possible, so the standard need to say what to do in these discumstences (e.g. as described in the first section of 4.4) ANSVINCITS 381-2004 references NISTIR 6529-A rather than the older 2001 version (and it is the newer version that is already listed in Annex F of FIPS PUB 201) The main part of CBEFF defines abstract data objects without any concrete encoding, and you need to specify an actual encoding (what the CBEFF calls 'patron formats') before you can use the data. So a requirement of CBEFF only is not sufficient to get interoperability. A patron format suitable for smart cards (both for off-card and on-card matching) is defined in normative Annex D of NISTIR 6529-A. The same format is also defined in NISTIR 6529-A. The same format is also defined in inspending the current PC/SC standard does however not support contactless readers (even though it is possible to implement a wrapper so that most operations work as if it was a ISO/IEC 7816 card). PC/SC 2.0, that has support for contactless cards, will be published soon. There is a requirement on the PIN Pad, but no requirement on the blometric sensor. The fingerprint from the expired PIV card may be stored on the new PIV card". Fingerprint changes over time (although much slower than face), so it should be recommended to collect new fingerprints.	Change the 2nd sentence to read "The fingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure, encoded as in annex D of (CBEFFI (Biometric Information Data Objects for Use within Smartcards or other Tokens)." Change the word "conform" to some weaker requirement (e.g. "shall use PC/SC 1.0 as its interface"), or add a requirement on PC/SC 2.0 as its interface, or add a requirement on PC/SC 2.0 should be conformed to the card through the contact interface by the cardholder using optional biometric cardholder activation described in section 4.1.6. Where the PIV card is used for physical access, the biometric sensor shall be incorporated into the reader. Where the PIV card is used for logical access (e.g. to authenticate to a website or other sensor may be a technicate to a vehicle or other sensor in the biometric sensor may be a separate unit. Add 1, but it is recommended that new fingerprint images are collected for the new Piv card."
Biometrics Precise	sebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com	T T	paragraph 4.4.4, page 34, 2nd paragraph 4.5.2, page 39 4.5. page 39 5.2.4.1, paragraph 2, page 46	than the older 2001 version (and it is the newer version that is already listed in Annex F of FIPS PUB 201). The main part of CBEFF defines abstract data objects without any concrete encoding, and you need to specify an actual encoding (what the CBEFF calls "patron formats") before you can use the data. So a requirement of CBEFF only is not sufficient to get interoperability. A patron format suitable for smart cards (both for off-card and on-card matching) is defined in normative Annex D of NISTIR 6329-A. The same format is also defined in SISO/IEC 7816-11. There is a requirement that the reader shall conform to PC/SC. The current PC/SC standard does however not support contactless readers (even though it is possible to implement a wrapper so that most operations work as if it was a ISO/IEC 7816 card). PC/SC 2.0 that has support for contactless cards, will be published soon. There is a requirement on the PIN Pad, but no requirement on the blometric sensor. The fingerprint from the expired PIV card may be stored on the new PIV card". Fingerprint changes over time (although much slower than face), so it should be recommended to collect new fingerprints.	Change the 2nd sentence to read "The fingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure, encoded as in annex D of (CBEFFI (Biometric Information Data Objects for Use within Smartcards or other Tokens)." Change the word "conform" to some weaker requirement (e.g. "shall use PC/SC 1.0 as its interface"), or add a requirement on PC/SC 2.0 as its interface, or add a requirement on PC/SC 2.0 should be conformed to the card through the contact interface by the cardholder using optional biometric cardholder activation described in section 4.1.6. Where the PIV card is used for physical access, the biometric sensor shall be incorporated into the reader. Where the PIV card is used for logical access (e.g. to authenticate to a website or other sensor may be a technicate to a vehicle or other sensor in the biometric sensor may be a separate unit. Add 1, but it is recommended that new fingerprint images are collected for the new Piv card."
Precise Biometrics Pracise Biometrics Pracise Biometrics Precise Biometrics Precise Biometrics Precise	kw@prec sebiometr ics.com kw@prec sebiometr ics.com kw@prec sebiometr ics.com kw@prec sebiometr ics.com	i T	4.5.2, page 39 4.5.2, page 39 4.5, page 39 5.2.4.1, paragraph 2, page 46	without any concrete encoding, and you need to specify an actual encoding (what the CBEFF calks patron formats") before you can use the data. So a requirement of CBEFF only is not sufficient to get interoperability. A patron format suitable for smart cards (both for off-card and on-card matching) is defined in normative Annex D of NISTIR 6329-A. The same format is also defined in ISO/IEC 7816-11. There is a requirement that the reader shall conform to PC/SC. The current PC/SC standard does however not support contactless readers (even though it is possible to implement a wrapper so that most operations work as if was a ISO/IEC 7816 card). PC/SC 2.0, that has support for contactless creaders (even though it is possible to implement a wrapper so that most operations work as if was a ISO/IEC 7816 card). PC/SC 2.0, that has support for contactless creaders (even though it is possible to implement and the published soon. There is a requirement on the PIN Pad, but no requirement on the blometric sensor. "The fingerprint from the expired PIV card may be stored on the new PIV card". Fingerprint changes over time (although much slower than face), so it should be recommended to collect new fingerprints.	Ingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure, encoded as in annex D of (CBEFF] (Biometric Information Data Objects for Use within Smartcards or other Tokens).* Change the word "conform" to some weaker requirement (e.g. "shall use PC/SC 1.0 as its interface"), or add a requirement on PC/SC 2.0 Add a new section: 4.5.4 Biometric Sensor Specifications. PIV cards may be activated through the contact interface by the cardholder using optional biometric cardholder activation described in section 4.1.5. Where the PIV card is used for inplical access, the biometric sensor shall be incorporated into the reader. Where the PIV card is used for object in the treader with the properties of the treader of the sensor may be a separate unit. Add "but it is recommended that new fingerprint images are collected for the new Pix card".
Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics Precise Precise Precise Precise Precise Precise Precise Precise	kw@precsebiometrics.com kw@precsebiometrics.com kw@precsebiometrics.com	T iE	4.5, page39 5.2.4.1, paragraph 2, page 46	PC/SC. The current PC/SC standard does however not support contactless readers (even though it is possible to implement a wrapper so that most operations work as if it was a ISO/IEC 7816 card). PC/SC 2.0, that has support for contactless cards, will be published soon. There is a requirement on the PIN Pad, but no requirement on the biometric sensor. "The fingerprint from the expired PIV card may be stored on the new PIV card", Fingerprint changes over time (although much shower than face), so it should be recommended to collect new fingerprints.	Inequirement (e.g. "shall use PC/SC 1.0 as its interface"), or add a requirement on PC/SC 2.0 and a new section: 4.5.4 Biometric Sensor Specifications. PM cards may be activated through the contact interface by the cardholder using optional biometric cardholder activation described in section 4.1.6. Where the PIV card is used for physical access, the biometric sensor shall be incorporated into the reader. Where the PIV card is used for logical access (e.g. to authenticate to a website or other server), the biometric sensor may be incorporated into the reader or the biometric sensor may be a separate unit. Add "but it is recommended that new fingerprint images are collected for the new Piv card".
Precise Biometrics Precise Biometrics Precise Biometrics Precise Biometrics	kw@prec sebiometr ics.com	i E	5.2.4.1, paragraph 2, page 46	"The fingerprint from the expired PIV card may be stored on the new PIV card. Fingerprint changes over time (although much slower than face), so it should be recommended to collect new fingerprints.	Specifications. PIV cards may be activated through the contact interface by the card-holder using optional biometric cardholder activation described in section 4.1.6. Where the PIV card is used for physical access, the biometric sensor shall be incorporated into the reader. Where the PIV card is used for logical access (e.g. to authenticate to a website or other server), the biometric sensor may be incorporated into the reader or the biometric sensor may be a separate unit. Add *. but it is recommended that new fingerprint images are collected for the new PIV card*.
Biometrics Precise Biometrics Precise Biometrics Precise Precise	sebiometr ics.com kw@preci sebiometr	, 1 T	2, page 46	on the new PIV card*. Fingerprint changes over time (although much slower than face), so it should be recommended to collect new fingerprints.	fingerprint images are collected for the new PN card*.
Biometrics Precise Biometrics	sebiometr		6.1, page 49		Change the past
Biometrics Precise				The section requires that PiN and biometrics must not be used for contactless readers due to privacy reasons. Some cards does however have support for setting up encrypted communication channels (which is noted in section 4.3, page 27).	Change the sentence starting with "For privacy reasons," to "For privacy reasons, contactless use of PINs and biometrics is not supported unless a sufficiently strong security mechanism is implamented on the communication channel. Similar changes in all text mentioning that only the contact interface may be used.
In: 4:	kw@preci sebiometr ics.com		6.2, first sentence on page 54	Most commercially available cards/readers may maintain power for an extended time period.	Remove the sentence starting with "Within the contactless environment, the card is able to get power for a very brief period"
	os@preci sebiometr ics.com	T I	Table 6-1, last table row on page 56	The authentication mechanism described only mentions PIN. On-card biometric matching as an alternative to PIN should also be applicable here.	Change text in second section to "A PIN or biometric sample is collected from the cardholder"
		<u> </u>			
	. L	 			
	ļ				
	\pm	<u> </u>	1		
' 		Γ.			
	+		 		
	 _				
	1				
	 				
-	 				
	1				
		 	<u> </u>		-
					I