Subject: Comments on Public Draft FIPS 201
From: "Gary Klinefelter" <Gklinef@fargo.com>
To: <draftfips201@nist.gov>
Cc: "Sharon Steinhoff-Smith ...snip... John Ekers" <jekers@fargo.com>

Thank you for the opportunity to comment on this standard. Fargo Electronics provided printers for the CAC project and a number of other government agencies. We would like to work further with NIST as standards for credentials evolve.

Gary Klinefelter
Technology Development
Fargo Electronics, Inc.
Gary.Klinefelter@Fargo.com
800-459-5636 or 952-941-9470
Fax: 952-826-7949
www.fargo.com

The World's Most Secure Card Identity Systems

 Fargo FIPS201 Comment 121604.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)	Proposed change
1	Fargo Electronics	Gary Klinefelter	T	none	There are several places where a 5 pt font is the suggested minimum. This is not readable for many people especially the aged and disabled.	Consider using an 8 pt font for the minimum
2	Fargo Electronics	Traci Johnson	T	section 4.1.2.a	The words tri-modal and bi-model refer to specific kinds of OVD and thus limits the scope of the standard. There are many different kinds of OVD available and many new kinds of OVD coming as technology continues to evolve. The Federal Agency should select which OVD is most fitting for their application. Counterfeiting may actually be reduced if multiple kinds of OVD with various patterns are used depending the OVD selected by the Federal Agency. Consistently use the term card body. Recommend that specific OVD or OVI features complement the card design instead of describing their attributes.	Consider using "An optical variable device (OVD) or optical variable ink (OVI) shall be embedded in the card body on the front of the card. OVD and OVI security features must not conflict with printed information so as to make credentials hard to view." OVD and OVI security features incorporated within the card body shall be free of defects, such as fading, discoloration, or contamination as determined by a visual inspection."
3	Fargo Electronics	Traci Johnson	T	section 4.1.3.b	There is no durability specification in ANSI/ISO 322 or ISO/IEC 7810. ISO/IEC 7810 lists a set of card characteristics and ANSI/ISO 322 lists test methods.	Consider using: "The card body shall consist of PVC or a composite structure satisfying the card characteristics required in ISO/IEC 7810.
4	Fargo Electronics	Traci Johnson	T	section 4.1.3.l	An OVD with a weaker peel strength can weaken the edge of a card making it easier to counterfeit.	Recommend keeping OVD features away from the edge of the card in order to make the card more tamperproof.
5	Fargo Electronics	Gary Klinefelter	T	section 4.1.4.1.a	Photograph input needs to be good enough to support the printed output. Photographic input need good color for skin reproduction. The output resolution needs grayscale resolution clarity.	Require the resolution of the input photo to be 300 DPI and 24 bit color. Require the printed photo on the credential to be at least 300 DPI and with at least 16 levels of grayscale for each color. That is each pixel has at least 16 levels of color adjustment for each primary color.
6	Fargo Electronics	Gary Klinefelter	T	section 4.2.4.3.d	Specify the minimum feature size for the printed bar code. Specify scaling the bar code to the printer resolution. This may seem overly detailed, but the DOD had a lot of problems with this because the software developers didn't realize that the printer had a finite resolution and couldn't accurately produce an improperly scaled bar code. Improper scaling causes bar codes to be out of ANSI specification.	Specify the minimum feature size of the bar code as .010 inches (3 pixels). This size will produce excellent print quality at 300 DPI for a range of printers. Specify that the input resolution of the bar code bitmap be 300 DPI to match the printed resolution of the credential.
7	Fargo Electronics	Gary Klinefelter	T	section 4.1.4.4.a	High coercivity needs a definition.	Add "as specified in ISO/IEC 7811-6" to the words "high coercivity".

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
8	Fargo Electronics	Gary Klinefelter	T	section 4.1.4.4.b	Specify the minimum bar width for the printed bar code. Specify scaling the bar code to the printer resolution. This may seem overly detailed, but the DOD had a lot of problems with this because the software developers didn't realize that the printer had a finite resolution and couldn't accurately produce an improperly scaled bar code. Improper scaling causes bar codes to be out of ANSI specification.	Specify the minimum bar width of the bar code as .010 inches (3 pixels). This size will produce excellent print quality at 300 DPI for a range of printers. Specify that the input resolution of the bar code be 300 DPI to match the printed resolution of the credential.
9	Fargo Electronics	Gary Klinefelter	T	section 5	Has a credential data model been defined so that interoperability with credentialing, personnel management and security systems can be realized? An interoperable data model could be of value to these systems in the future. Without this, tracking security events throughout the disparate systems will be difficult. Another advantage in when using physical and logical security data models is the ability to automatically detect and track security events in real time.	At a minimum consider a paragraph to educate Federal Agencies about the future trends to have interoperable security data. Consider specifying a minimal credential data model. Open Security Exchange paper Physbits v1.0 describes a system wide data security model. www.opensecurityexchange.org
10	Fargo Electronics	Gary Klinefelter	G	section 2	Who are Issuing Authorities? Government agencies, contracted entities, certified third parties?	Create some initial guidelines as to who Issuing Authorities might be and what the process is for certification. Eventually this should be open to parties with the proper auditing and certification.
11	Fargo Electronics	Gary Klinefelter	G	section 2	Who are Registration Authorities? Can they also be an Issuing Authority? Government agencies, contracted entities, certified third parties?	Similar proposed change to Issuing Authorities. If they need to be separate from Issuing Authorities, state this requirement clearly.
12	Fargo Electronics	Gary Klinefelter	G	section 2.2.3	Should the visitor procedures (credential) process be defined? This seems like large security vulnerability if not addressed.	Define the visitor procedures to be a subset of this standard. For instance: require the use of a smart card; require the use of secure card stock for visual verification of a visitor credential; require a photo or fingerprint for the visitor; require a visitor authorization prior to issuing a visitor credential; and/or require a driver license or passport prior to issuance of a visitor credential.
13	Fargo Electronics	Gary Klinefelter	G	section 2.3	How does an Issuing Authority protect the data they collect? This is partially addressed in section 5, but may need further clarification	Define appropriate expectations for data management and electronic protection for distributed data.

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

Submitted by: _Gary Klinefelter_Fargo Electronics_
Date: _16 December 2004_

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
14	Fargo Electronics	Gary Klinefelter	G	section 2.3	How does data gathered by an Issuing Authority synchronize with interoperable systems in a Federal Agency? Is there a data model? Whose data is the master?	Define controlling entities such as departments that have master data for their employees that can be synchronized with Issuing Authorities and other departments.

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