Fingerprint Scanners Comparative Analysis Based on International Biometric Standards Compliance

María del Carmen Prudente-Tixteco
Instituto Politécnico Nacional
Graduate School ESIME Culhuacan
México
mprudentet0900@ipn.mx

Gualberto Aguilar-Torres
Instituto Politécnico Nacional
Graduate School ESIME Culhuacan
México
gaguilar@ipn.mx

Linda Karina Toscano-Medina
Instituto Politécnico Nacional
Graduate School ESIME Culhuacan
México
ltoscano@ipn.mx

Gabriel Sánchez-Pérez
Instituto Politécnico Nacional
Graduate School ESIME Culhuacan
México
gasanchezp@ipn.mx

Abstract. **This paper discuses an analysis of the characteristics of fingerprint biometric scanners based on biometric standards compliance, taking into account of the features provided by manufacturers to conduct a comparative analysis of their physical characteristics, its certifications and standards supported. Because there is a huge fingerprint scanners variety, this paper studies only 30 devices from 13 different vendors using the characteristics obtained from the specification sheets for each device. A fingerprint device classification was performed based on the number of fingerprints that each device can capture, for example 4-4-2 devices or a single fingerprint capture and type of biometric standard compliant. As a result of this devices classification, 73% of them comply with at least one biometric standard or certification and 27% of them do not specify if they meet some kind of standard; however, they have the requirements to be considered for the acquisition of a fingerprint image.**

Keywords - fingerprint scanners; Biometric Standards; physical characteristics**.**

I. INTRODUCTION

A biometric system is an automated system to capture biometric sensor data from a user, extract feature data from that processed acquired data, compare the processed feature data with that contained in one or more biometric templates, decide how well they match and indicate whether or not an identification or verification of identity has been achieved [1][6][8].

Biometric systems are used to provide greater security for systems that are used as mechanisms for identifying and verifying people. Biometric sensors are devices that are located within a biometric system, which have the function of acquire data or images for biometric feature extraction.

The biometric technologies designers have the need to work with biometric standards that define the characteristics and minimum requirements to develop devices and appropriate models for the biometric data management for public and private entities, law enforcement and government areas.

The fingerprint scanner must produce images that exhibit good geometric fidelity, sharpness, detail rendition, gray-level uniformity and gray-scale dynamic range, with low noise characteristics. The images must be true representations of the input fingerprints, without creating any significant artifacts, anomalies, false detail, or cosmetic image restoration effects [2].

According to the International Standard Organization, the minimal requirements that a fingerprint scanner must meet are: image resolution, size, gray level color range, sample rate, light intensity and signal to noise ratio [1].

The requirements provide criteria to guarantee the image quality of fingerprint scanners and printers that input fingerprint images or generate fingerprint images [2]. Electronic images must be of sufficient quality to allow for: (1) conclusive fingerprint comparisons (identification or non-identification decision), (2) fingerprint classification, (3) automatic feature detection; and (4) overall Automated Fingerprint Identification System (AFIS) search reliability [8].

The paper is organized as follows. Section 2 relates on general international biometric standards that are contemplated for realization the analysis. Section 3 refers to requirements that were considered for the analysis based in international biometric standards. In Section 4, devices that are considered for analysis are listed, and, in Section 5, there are the results of comparative analysis between the devices according to international biometric standards compliant.

II. BIOMETRIC STANDARDS

The fingerprint scanners, in addition to meeting the minimum requirements for use in various applications, support different features provided by international biometric standards like ISO/IEC 19794-4, and ANSI/INCITS 381, this allows to meet interoperability between systems [6][7].

International biometric standards that support biometric fingerprint scanners are mainly focused on scanner physical characteristics, data transmission characteristics, management for biometric exchange formats and fingerprint image quality.

Some international biometric standards are described below that which are used to define the devices technical specification.

Electronic Fingerprint Transmission Specification (EFTS) by Federal Bureau of Investigation (FBI) the purpose of this document is to specify certain requirements to which agencies must adhere to communicate electronically with the FBI's IAFIS (Integrated Automated Fingerprint Identification System), electronic communications do not include fingerprints, and the requirements [2].

Personal Identity Verification (PIV) , this specification apply to fingerprint capture devices which scan and capture at least a single fingerprint in digital, softcopy form [3].

FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors, this standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems [4].

BioAPI Specification or ISO/IEC 19784-1, this specification defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors. It provides interworking between such components through adherence to this and to other International Standards. The BioAPI specification is applicable to a broad range of biometric technology types. It is also applicable to a wide variety of biometrically enabled applications, from personal devices, through network security, to large complex identification systems [5].

ISO/IEC 19794-4 and ANSI 381, this standards specifies a data record interchange format for storing, recording and transmitting the information from one or more finger or palm image areas. There have a section of image acquisition requirements are made aware of the minimum requirements for selected image acquisition settings level desired [6][7].

ISO/IEC 19794-2 and ANSI 378, define interoperability is based on the definition of the rules or standards of minutiae extraction of the finger and the formats of the records that are common in many matching procedures. The minutiae are points located in a fingerprint image where a friction ridge begins, ends or splits into two or more peaks, these features can be used to identify a person [8][9].

Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information ANSI/NIST-ITL this standard defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, scar mark & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images [10].

III. Requirements Analysis of Fingerprint Scanners

There are requirements that must be considered by providers of biometric technologies for the development of a fingerprint scanner.

The fingerprint comparison process requires a high fidelity image without any banding, streaking or other visual defects. Finer detail such as pores and incipient ridges are needed since they can play an important role in the comparison. Additionally, the gray-scale dynamic range must be captured with sufficient depth to support image enhancement and restoration algorithms [8].

Binary and grayscale fingerprint images to be exchanged shall be captured by an AFIS, live-scan reader, or other image capture device operating at a specific native scanning resolution. The minimum scanning resolution for this capture process shall be 19.69 ppmm plus or minus 0.20 ppmm (500 ppi plus or minus 5 ppi). Scanning resolutions greater than this minimum value and with a device tolerance of plus or minus 1% may be used [10].

Table I shows the preferred capture sizes, applicable to live scan systems. Scanner capture dimensions should never be less than 90% of those given.

TABLE I. Preferred Capture Sizes

	Preferred Width (inches)	**Preferred Height (inches)**
Roll finger	1.6	1.5
Plain thumb	1.0	2.0
Plain 4-fingers (sequence check)	3.2	2.0
Plain 4-fingers (identification flat)	3.2	3.0

Table II shows maximum image dimensions of fingerprints [10].

TABLE II. MAXIMUM IMAGE DIMENSIONS

Finger position	**Width**		**Length**	
	(mm)	**(in)**	**(mm)**	**(in)**
Right or left thumb	40.6	1.6	38.1	1.5
Right or left index finger	40.6	1.6	38.1	1.5
Right or left middle finger	40.6	1.6	38.1	1.5
Right or left ring finger	40.6	1.6	38.1	1.5
Right or left little finger	40.6	1.6	38.1	1.5
Plain right or left thumb	25.4	1.0	50.8	2.0
Plain right four fingers	81.3	3.2	76.2	3.0
Left & right thumbs	81.3	3.2	76.2	3.0

The dynamic range define the image grayscale shall be encoded using the agreed precision necessary to meet the dynamic range requirement for a specific application. Grayscale finger image data may be store, recorded, or transmitted in either compressed or uncompressed form. Using a pixel depth of 8 bits (256 grayscale levels) each shall contained a single byte [6].

The ISO/IEC 19794-4 sets the standards for the acquisition of a fingerprint image by defining the specific requirements that must be considered for the data exchange format based on a biometric fingerprint image. Table III shows the levels of viewing requirements to the acquisition of a fingerprint image described by the standard ISO / IEC 19794-4.

TABLE III. REQUIREMENTS ACQUISITION OF A FINGERPRINT IMAGE

Levels set.	**Resolution scanner.**	**Intensity of pixels.**	**Range dynamic. (grayscale)**	**Certification**
30	500	8	80	None
35	750	8	100	None
31	500	8	200	EFTS/F

IV. FINGERPRINT SCANNERS

The biometric scanners vendors give the technical specification datasheet when a fingerprint scanner is sold. The main technical specifications are the following: resolution, image size, gray level, certifications, and standards compliance.

In some fingerprint scanner specification datasheets also give information about the percentage of geometric distortion.

A fingerprint devices classification was performed based on the number of fingerprints that each device can capture.

Tables IV, V and VI show the description of the devices that were selected for analysis depending on your fingers the number of images that can be acquired in a single capture.

TABLE IV. A SINGLE FINGER SCANNERS

Vendors	**Product**	**Image size**
Biometrika	Hiscan [11]	500x500
Cogent	CSD 200 [12]	480x320
Cogent	CSD 330 [13]	500x500
CrossMatch	Verifier 300 [14]	600x600
Dakty	NAOS-A [15]	236x354
Digital Persona	U.are.U 4000 [16]	390x355
Digital Persona	U.are.U 4500 [17]	390x355
Futronic	FS80 [18]	480x320
Futronic	FS88[19]	480x320
Futronic	FS90[20]	300x440
Lumidigm Mercury	M301 Fingerprint Reader [21]	342x274
Microsoft	Fingerprint Reader [22]	355x390
SecuGen	Hamster Plus [23]	260x300
SecuGen	Hamster IV [24]	258x336
SecuGen	ID USB SC/PIV [25]	258x336
Suprema	RealScan-S [26]	600x600
Suprema	SFR300S[27]	288x288
Suprema	BioMini & SDK [28]	288X320
Identix	DFR 2100 [29]	600x600

TABLE V. DUAL FINGER SCANNER

Vendors	Product	Image size
Cogent	CSD 450 [30]	800x750
CrossMatch	Verifier 310 [31]	900x900
CrossMatch	Verifier 320 [32]	800x750
Futronic	FS50 [33]	800x750
Suprema	RealScan-D [34]	900x900

TABLE VI. TENPRINT SCANNERS

Vendors	Product	Image size
ARH	AFS 510 Live Scanner [35]	1600x1500
CrossMatch	L_SCAN_Guardian [36]	1600x1500
CrossMatch	LScan500 [37]	1600x1500
Futronic	FS60 [38]	1600x1500
Mantra Softech	MFS500 [39]	1600x1500
Suprema	RealScan-10 [40]	1600x1500

V. RESULTS

The physical characteristics given by vendors that all devices meet are shown in Table VII:

TABLE VII. PHYSICAL CHARACTERISTICS

Image resolution	500 ppi
Pixel depth	8 bit
Grayscale	256

All fingerprint scanners considered for this comparative analysis meet the requirements acquisition of a fingerprint image taken by the ISO / IEC 19794-4 located on a level 31 set for the data exchange format based biometric the fingerprint image.

Some vendors do not specify information about the use of international biometric standards, but meet the requirements for the acquisition of a fingerprint image as stipulated in ISO / IEC 19794-4 as shown in Table VIII.

TABLE VIII. FINGERPRINT SCANNERS THAT NOT REPORT ANY BIOMETRIC STANDARDS

Firm	Product
Dakty	NAOS-A
Digital Persona	U.are.U 4000
Digital Persona	U.are.U 4500
Futronic	FS80
Futronic	FS90
Microsoft	Fingerprint Reader
Suprema	RealScan-S
Suprema	SFR300S

A. *Physical Characteristics.*

The devices that have a certification or meet some international biometric standards related to the minimum requirements of their physical characteristics are only 18 devices; Table VIII shows the devices that meet certification or international biometric standards.

The FBI EFTS Appendix F and PIV-071006 standards specify parameters that devices must meet to guarantee a correct acquisition of the fingerprint image. The requirements that have in common both standards are:

- Linearity
- Geometric Accuracy
- Spatial Frequency Response
- Signal-to-Noise Ratio
- Fingerprint Image Quality

The devices that can be used in identity and verification information systems into federal governments strictly satisfy FIPS 201 PIV certification.

In Table IX are listed the devices that meet or have a can fit certification standards which refer to physical characteristics.

Fig. 1, shows the total number of devices that meet each standard considered for the analysis concerning the physical characteristics.

TABLE IX. DEVICES THAT MEET PHYSICAL CHARACTERISTICS REQUIRED BY INTERNATIONAL BIOMETRIC STANDARDS.

Product	IQS. Appendix F of the EFTS.	FBI PIV-071006	FIPS 201 PIV
AFS 510	certification		
Hiscan		certification	
CSD 200		certification	Certification
CSD 330		certification	Certification
CSD 450		certification	Certification
Verifier 310		certification	
Verifier 320	certification	certification	
L_SCAN_ Guardian	certification		
LScan500	certification		
FS50		certification	certification
FS88		certification	comply
FS60	certification		
Hamster IV		certification	comply
ID USB SC/PIV			certification
RealScan-D	certification		
RealScan-10	certification		
BioMini & SDK		certification	
DFR 2100		certification	

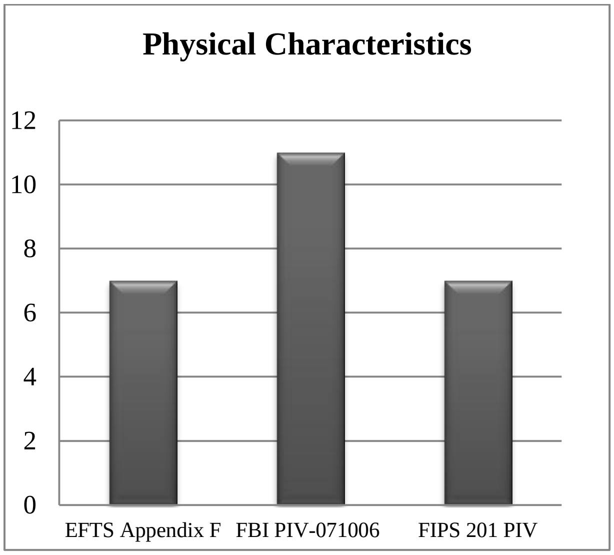

Figure 1. Number of fingerprint scanners that satisfy international biometric standards about physical characteristics.

B. Biometric Data Interchange Formats

The international biometric standards that satisfy with biometric data interchange formats are: ANSI/NIST-2000, ISO/IEC 19794-2/4 and ANSI 381/378.

The devices that satisfy the international biometric standard described above are 12; Table X and Fig. 2 show the number of devices that comply with each of the different standards.

The scanners that comply with the biometric data interchange formats are used for biometric acquisition of register fingerprint image and minutia data.

TABLE X. INTERNATIONAL BIOMETRIC STANDARDS DEVICES THAT MEET THE BIOMETRIC DATA INTERCHANGE FORMAT.

Product	ANSI/NIST-ITL-1-2000	ISO/IEC 19794-2/4	ANSI 381/378
AFS 510 Live Scanner	Comply	comply	
CSD 330		certification	
Verifier 300	Comply		
M301 Fingerprint Reader			comply
MFS500		comply	
Hamster Plus		comply	comply 378
Hamster IV		comply	comply 378
BioMini & SDK		comply 2	comply 378

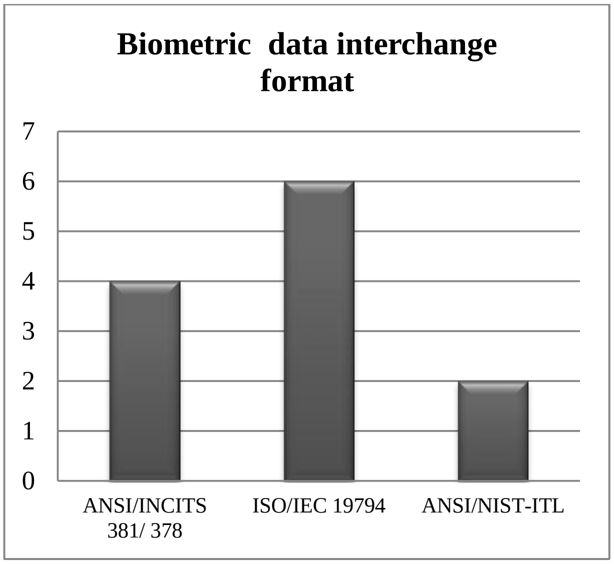

Figure 2. Number of fingerprint scanners that comply with biometric data interchange format standards.

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-201-1

C. Others

Some devices meet with the BioAPI standard, having a common structure for operation with different interfaces in a biometric system, these devices as show in Table XI.

TABLE XI. ISO/IEC 19784-1:2005

Firm	Product
ARH	AFS 510 Live Scanner
SecuGen	Hamster Plus
SecuGen	Hamster IV

D. General

In the comparative analysis of biometric fingerprint scanners, 30 datasheets specification were revised, where 73% compliance with any international biometric standard or have a certification.

Fig. 3 shows the number of devices that specify compliance with at least one biometric standard and the number of devices that do not specify.

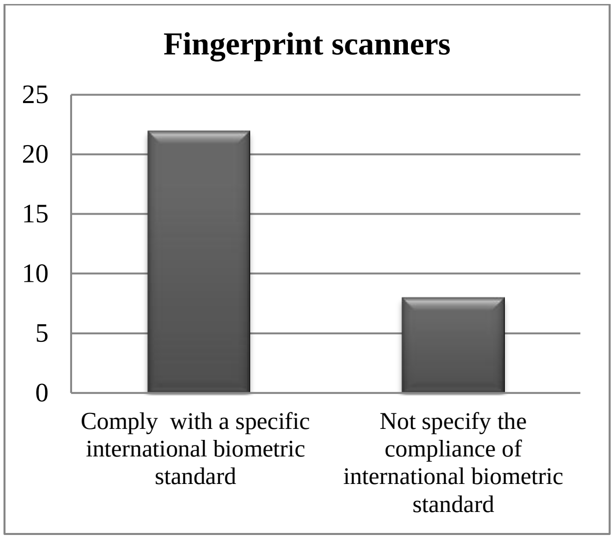

Figure 3. Devices number that satisfy or not with an international biometric standard.

From the 22 scanners that satisfy some certification or international biometric standard, the 63.63% devices complied with some physical characteristics standards, 18.18% with any biometric data interchange formats and the other 18.18% complied with both.

Fig. 4 shows the number of devices that satisfy biometric standard type of that were considered for this analysis.

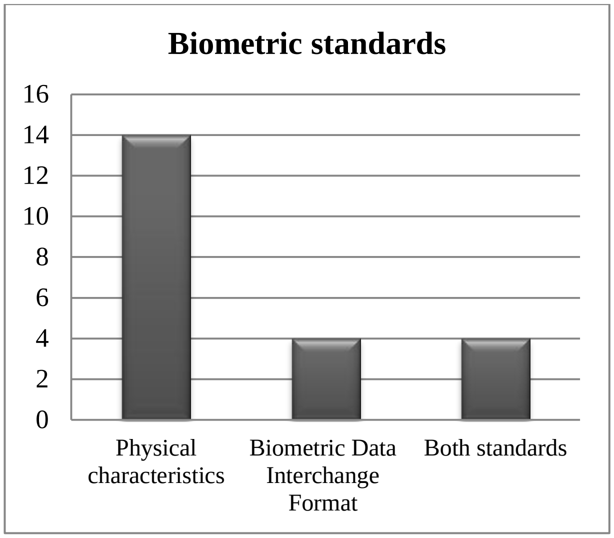

Figure 4. Devices that satisfy international biometric standards.

VI. Conclusion and Future Work

A comparative analysis was performed in relation to standards that meet the data acquisition devices biometric fingerprint taking into account the information provided in the specification datasheets for each of them. Most devices have a certification in relation to physical characteristics.

Devices that do not present information on compliance with standards meet the minimum requirements to be considered for the acquisition of a fingerprint image and are used in conjunction with software development kits, which use or comply with any type of international biometric standard for its use in various applications.

The international biometric standards are very important due they mark the minimum requirements that must take into account by devices manufacturers.

These minimum requirements must also be taken into account by people who use the scanner in various biometric applications. There are devices that meet the minimum requirements for physical characteristics, as well as compliance to unveil common structures in the biometric data interchange formats for interoperability in biometric systems.

As future work, tests will be done to devices that were considered for this analysis to verify compliance with the requirements of international biometric standard.

VII. REFERENCES

[1] International Standard ISO/IEC 19794-1:2005, “Biometric data interchange formats – Part 1: Framework”, Information technology p. 3, 11.

[2] Federal Bureau of Investigation, Criminal Justice Information Services (CJIS), “Electronic Fingerprint Transmission Specification, Appendix F”, May 2, 2005.

[3] Federal Bureau of Investigation, “Personal Identity Verification (PIV)”. Image Quality Specifications for Single Finger Capture Devices, July 2006.

[4] FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors", p. 1, 5, 15, March 2006.

[5] International Standard ISO/IEC 19784-1:2005, “Biometric application programming interface –Part 1: BioAPI specification”, Information technology, p.1, 2005.

[6] International Standard ISO/IEC 19794-4:2005 “Biometric data interchange formats – Part 4: Finger Image”, Information technology pp. 4-8, 2005.

[7] Standard ANSI INCITS 381:2004, “Information technology – Finger image format for data interchange”, pp. 1-5, 2004.

[8] International Standard ISO/IEC 19794-2:2005 “Biometric data interchange formats – Part 2: Finger minutiae data”, Information technology, pp. 1-4, 2005.

[9] Standard ANSI INCITS 378:2004, “Information technology -Finger minutia format for data interchange”, pp. 1-10, 2004.

[10] ANSI/NIST ITL 1-2007, “Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information”, pp. 25-40, April 20, 2007.

[11] Biometrika, “HiScan Fingerprint Scanner 1x1,” [retrieved: January, 2012].

[12] 3M COGENT Ing, “CSD200, Single-digit Optical Scanner,” [retrieved: December, 2011].

[13] 3M COGENT Ing, “CSD330, Single-digit Fingerprint Scanner,” [retrieved: January, 2012].

[14] Cross Match Technologies, Inc. Verifier® 300 LC 2.0 “Single Finger Scanner with USB 2.0 Interface”, 2008 [retrieved: January, 2012].

[15] Dakty GmbH, “Fingerprint NAOS-1,” April 2009, [retrieved: January, 2012].

[16] DigitalPersona, U.are.U 4000B Reader “USB Fingerprint Reader,” [retrieved: January, 2012].

[17] DigitalPersona, U.are.U 4500B Reader “USB Fingerprint Reader,” [retrieved: January, 2012].

[18] Futronic's, “FS80 USB2.0 Fingerprint Scanner,” [retrieved: January, 2012].

[19] Futronic's, “FS88 FIPS201/PIV Compliant USB2.0 Fingerprint Scanner,” [retrieved: January, 2012].

[20] Futronic's, “FS90 USB2.0 Mini Fingerprint Scanner,” [retrieved: December, 2011].

[21] Lumidigm, Inc., Venus Series Biometric Sensors Multispectral Fingerprint Imagers, “M301 Fingerprint Reader,” [retrieved: December, 2011].

[22] Microsoft, “Fingerprint Reader v1.0”, 2007 [retrieved: December, 2011].

[23] SecuGen Biometric Solution, “Hamster Plus”, Hamster IV ID USB SC/PIV, 2011 [retrieved: January, 2012].

[24] SecuGen Biometric Solution, “Hamster IV”, 2011 [retrieved: December, 2011].

[25] SecuGen Biometric Solution, “ID USB SC/PIV”, 2011 [retrieved: December, 2011].

[26] Suprema, “Fingerprint Scanner RealScan-S”, 2011 [retrieved: January, 2012].

[27] Suprema, “Fingerprint Scanner SFR300S”, 2007 [retrieved: January, 2012].

[28] Suprema, “BioMini & SDK”, 2011 [retrieved: January, 2012].

[29] Identity Solutions Biometrics Division, “DFR 2100/2130 Single Finger Reader”, 2008 [retrieved: December, 2011].

[30] 3M COGENT Ing, “CSD450 Dual-Digit Optical Scanner,” [retrieved: December, 2011].

[31] Cross Match Technologies, “Inc. Verifier® 310 LC Single/Dual Finger Scanner,” [retrieved: January, 2012].

[32] Cross Match Technologies, Inc. Verifier® 320 LC “Two Finger Scanner for Flats and Rolled Prints,” [retrieved: December, 2011].

[33] Futronic FS50 FIPS201/PIV Compliant USB2.0 “Two Finger Scanner,” [retrieved: January, 2012].

[34] Suprema, “Fingerprint Scanner RealScan-D”, Portable Dual Finger Live Scanner, [retrieved: December, 2011].

[35] ARH Inc. “Professional fingerprint scanning AFS 510 Live Scanner,” [retrieved: January, 2012].

[36] Cross Match Technologies, Inc., “L_SCAN_Guardian Livescan and Fingerprint Enrollment System,” [retrieved: December, 2011].

[37] Cross Match Technologies, Inc. “L SCAN® 500P “tenprint/palmprint,” [retrieved: December, 2011].

[38] Futronic, “FS60 EBTS/F Certified ID Flat Fingerprint Scanner,” [retrieved: December, 2011].

[39] Mantra Softech India Pvt. Ltd. MFS500 “4+4+2 Fingerprint Biometrics Ten Print Live Scanner,” [retrieved: December, 2011].

[40] Suprema, Scanner RealScan-10, “Compact scanner for ten fingerprints,” [retrieved: December, 2011].