Biometric User Authentication

Fingerprint Sensor Product Evaluation Summary

Version 1.02
November 2003

Order Number: 253758-002

Contents

Tables

Revision History

Rev.	Document Number	Description	Date
-001	253758-001	Initial Release	September 2003
-002	253758-002	Update to product details	November 2003

1. Introduction

This document provides a summary list of biometric fingerprint sensor products that adhere to published recommendations established in the "Intel Biometric User Authentication Fingerprint Sensor Product Guidelines" (Reference #253100-004) which can be found at: http://developer.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf). Additional information can be obtained from that document relative to the guidelines established for fingerprint sensors and the testing of those devices.

The need to improve the authentication mechanisms allowing access to the user's notebook PC as well as resources of wired and wireless connections is crucial. Protecting data and secrets is necessary in wired communications on corporate networks and Internet traffic, and amplified in a wireless communications environment where data is prone to additional threats. Furthermore, as the mobility of the computer platform increases, the notebook becomes more and more susceptible to theft.

Multi-factor authentication using more than one authentication mechanism (such as password + fingerprint) provides a more secure way to ensure the correct user gains access to a computer and enterprise resources. Use of a single authentication method is not recommended as any single method may be defeated, but the difficulty to overcome multiple authentication methods increases dramatically with two or more methods enforced.

Notebook PCs will progressively build on various security primitives to ultimately deliver "Trusted Client" capability for safe computing where biometric authentication devices play an important role. In order to improve platform security through enhanced user authentication, notebook manufacturers are encouraged to include a fingerprint authentication device in all notebook PCs.

This document and the testing results it summarizes makes no attempt to duplicate or supercede definitions and testing provided by other industry standards bodies. Computer manufacturers who are considering integration of fingerprint sensors can leverage information provided by the product guidelines and this summary product list. Although this list will serve as to aid product selection for implementation of fingerprint authentication into a notebook computer, it is imperative that independent investigation be done prior to any device selection.

2. Product Evaluation Summary

This summary lists characteristics of fingerprint authentication device content and performance that meet the guidelines defined in the companion document "Intel Biometric User Authentication Fingerprint Sensor Product Guidelines" (Reference #253100). All devices should meet the recommended characteristics under general testing conditions.

Platform used for fingerprint sensor evaluation is described as follows:

- Intel Centrino* Customer Reference Board
- 256M RAM
- Microsoft Windows 2000* and Microsoft Windows XP*. No updates or service packs were applied.

Table 1. Compliant Vendor / Product Summary

Vendor	Product	Document Reference
Atmel, Inc.	FingerChip* USB Sensor	Section 2.1
AuthenTec, Inc.	TruePrint* AES3400	Section 2.2
ST Microelectronics, Inc.	TouchChip* TCRU1	Section 2.3
ST Microelectronics, Inc.	TouchStrip* TCS3	Section 2.4

2.1. Atmel Fingerchip* USB Sensor

Table 2. Atmel Fingerchip* USB Sensor – Vendor/Product Overview

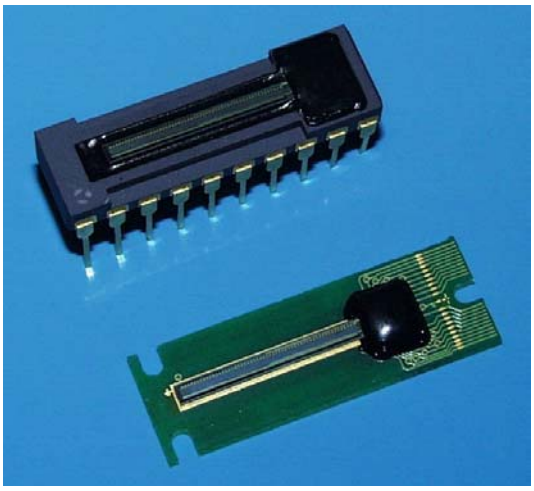
Vendor	Name: Address: Tel: Website: Contact Name: Tel: Email:	Atmel Avenue de Rochepleine, BP123, 38521 Saint Egrève Cedex, France +33 (0)4.76.58.30.00 http://www.atmel.com/products/Biometrics/ David RICHARD, Marketing Manager Biometrics +33(0)4.76.58.30.41 david.richard@atmel.com
Product Name	FingerChip* USB Sensor	
Part Number	AT77C103A	
Product Type	Swipe – Thermal-Electric	
Brief Product Description	AT77C103A FingerChip USB sensor is a single chip, high performance, low cost sensor based on temperature physical effects for fingerprint sensing. ATMEL has patented a unique method for imaging the entire finger by "sweeping" it across the sensor, capturing successive images (slices), then using software to reconstruct the whole fingerprint. This method allows the FingerChip to provide a large, high-quality, 500 dots per inch image of the fingerprint, and to avoid latent prints by self-cleaning the sensor.	
Software Supplier(s)	ATMEL currently officially partners with 9 bio-engine providers: Cogent Systems, Bioscrypt, ID3 Semiconductors, Idencom, Ikendi, Ident, Suprema, Technoimagia, and DDS. Software application (logon etc…) can be provided by various partners including Cogent, ID3 Semiconductors, I/O Software. Additional compatibility with other software application providers is pending.	
Vendor Comments	ATMEL has already provided its FingerChip sensor in mass-production for consumer products such as the HP iPAQ 5450 and 5550 PDA products.	

Table 3. Atmel Fingerchip* USB Sensor – Evaluation Summary

Guideline	Functions as Expected
Software Guidelines	
1. All software collateral should be supported in both Microsoft Windows 2000* and Windows XP* operating environments.	Pass
2. All software device drivers should have been tested and signed by Microsoft for use with Windows 2000 and Windows XP. Device drivers should be WHQL certified. Device driver installation should occur without warning by the Windows device installer.	Pending
3. Fingerprint device leverages the system TPM or smartcard	Pass (Note 1)
4. BAPI support included in the software for the device	Pending
5. BioAPI support include in the software for the device	No
6. All software device driver entities that should be installed to a user's hard drive should be described in an INF description file shipped with these collaterals on the root directory of the product software support CDROM.	Pass
7. Support software should be installed to the user's hard drive through a simple and easy to use set up utility.	Pass
8. User configuration and installation should be simple (ease of use): includes a user-friendly, simple to understand interface.	Pass
9. Configuration of the device should be done through an easy to use Wizard.	Pass
10. All software collateral should be delivered on CD-ROM. When inserted, the CDROM should "autorun" for installation.	Pass
11. Sample software provided with the fingerprint sensor to allow evaluation of fingerprint enrollment and other sample usage models.	Pass
12. Software support should be provided to allow the device to be used for Windows Login.	Pass
13. Software support for use with Microsoft's Active Directory used with network authentication is recommended.	No
14. Software support should be provided to allow the device to be used for Screen Saver authentication.	Pass
15. Software support should be provided to enable fingerprint authentication as a password manager replacement for applications that normally require user entered "password".	Pass
16. Uninstall prompts for data back up of data protected by the fingerprint authentication.	Pass
17. Support for disconnected client	Pass
18. Multi-factor authentication software support	Pass
19. Recovery / Backup / Migration software support	Pass
Hardware Guidelines	
20. Integrated / built-in device: connection via USB and/or LPC.	USB
21. Device and supporting software provides ACPI D-state support to reduce power consumption operating under Windows XP*.	Pass
22. Device and supporting software does not block ACPI S-state transitions	Pass
23. Device and supporting software allows host processor to enter C3 state as	Pass

Guideline	Functions as Expected
measured in Windows XP* using “Perfmon” utility.	
24. Low Power HW Finger Detection	Pass
25. Device idle power: The user authentication device should be attached and software installed/configured. Once the system is stable (all drivers installed, no more system messages, …), and no applications are running, power should be measured at the attach point for the device (USB). Power measured using Windows XP.	Avg: .0927 W Max: .0967 W
26. Device active power: power measurement is taken with device attached/plugged and capturing a fingerprint. Power measured using Windows XP.	Avg: .1293 W Max: .1563 W
27. Size (X x Y x Z mm) of entire device including sensor and electronics	26.6 x 0.985 x 2 mm
28. Bill of material for entire device including the sensor and connection circuitry. Meets target pricing of less than $10.	Pass. Pricing to be discussed upon volumes and projects
Durability	
29. Durability Testing Performed by Which Accredited Lab(s)	• SERCOVAM Cestas (France) • DUBOIS La Chaux de Fond (Suisse) • SERMA Bordeaux (France) • ATMEL Nantes (France) • ATMEL Grenoble (France)
30. Durability – Abrasion	Pass
31. Durability – Chemical Resistance	Pass
32. Durability – Dust	Pass
33. Durability – Storage Temperature	Pass
34. Durability – Temperature Cycling	Pass
35. Durability – Constant Heat	Pass
36. Durability – Heat + Humidity	Pass
37. Durability – Salt Fog	Pass
38. Durability – Shock / Bump / Drop: Lacrosse Ball Drop	Pass
39. Durability – Shock / Bump / Drop: Pen Drop Height – Device failed after pen dropped from:	40 cm
40. Durability – Shock / Bump / Drop: Drop Test	Pass
41. Durability – UV	Pass
42. Durability – ESD	Pass
Device Functionality	
43. Accuracy level: FAR	< 0.003 %

Guideline	Functions as Expected
44. Accuracy level: FRR	< 0.5 %
45. Fake finger detection method	No
46. Performance	Pass
47. Exclusions	Pass
48. Resolution	500 Dpi
49. Privacy mechanism (Template Encryption, HW/SW Challenge Response, Digitally Signed Images)	Pass
50. Sample availability	August 2003
51. Production quantities availability	Q4 2003

Evaluation Comments	• Note 1: Match-on-card / store-on-card supported via ID3 Semiconductors or Cogent Match_on_Card

2.2. AuthenTec TruePrint* AES3400

Table 4. AuthenTec TruePrint* AES3400 – Vendor/Product Overview

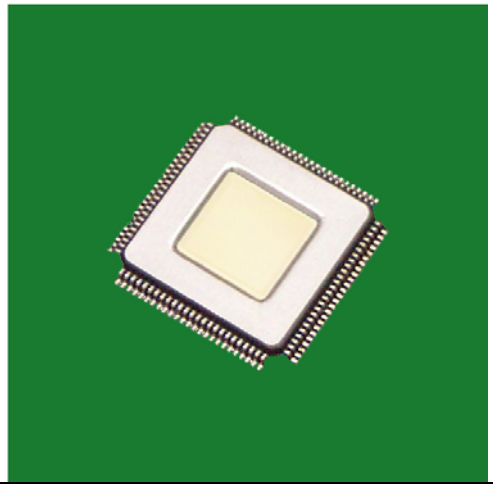
Vendor	Name: Address: Tel: Website: Contact Name: Tel: Email:	AuthenTec 709 South Harbor City Blvd. Melbourne, Florida 32901 (321) 308 1300 www.authentec.com Tom Aebli; PC Segment Marketing (321) 308 1300 tom.aebli@authentec.com
Product Name	EntréPad* AES3400	
Part Number	AES3400-C-BA-CA-BZ00	
Product Type	TruePrint Technology Fingerprint Sensor	
Brief Product Description	The AES3400 is AuthenTec's smallest lowest cost TruePrint technology based touch fingerprint sensor. The sensor features a 96x96 500ppi array, integrated USB 2.0 full speed endpoint, and exceptionally small size (14mm X 14mm).	
Software Supplier(s)	AuthenTec (Sensor Control, Fingerprint Matcher, API) Softex Omnipass, I/O Software	
Vendor Comments	The AuthenTec AES3400 is a cost reduced version of the award winning AES3500. The AES3400 features an integrated USB endpoint and is a USB low power device. These features make the AES3400 ideal for securing advanced mobile computing platforms.	

Table 5. AuthenTec TruePrint* AES3400 – Evaluation Summary

Guideline	Functions as Expected
Software Guidelines	
1. All software collateral should be supported in both Microsoft Windows 2000* and Windows XP* operating environments.	Pass

Guideline	Functions as Expected
2. All software device drivers should have been tested and signed by Microsoft for use with Windows 2000 and Windows XP. Device drivers should be WHQL certified. Device driver installation should occur without warning by the Windows device installer.	Pending
3. Fingerprint device leverages the system TPM or smartcard	Pass (Note 1)
4. BAPI support included in the software for the device	Pass
5. BioAPI support include in the software for the device	No
6. All software device driver entities that should be installed to a user's hard drive should be described in an INF description file shipped with these collaterals on the root directory of the product software support CDROM.	Pass
7. Support software should be installed to the user's hard drive through a simple and easy to use set up utility.	Pass
8. User configuration and installation should be simple (ease of use): includes a user-friendly, simple to understand interface.	Pass
9. Configuration of the device should be done through an easy to use Wizard.	Pass
10. All software collateral should be delivered on CD-ROM. When inserted, the CDROM should "autorun" for installation.	Pass
11. Sample software provided with the fingerprint sensor to allow evaluation of fingerprint enrollment and other sample usage models.	Pass
12. Software support should be provided to allow the device to be used for Windows Login.	Pass
13. Software support for use with Microsoft's Active Directory used with network authentication is recommended.	No
14. Software support should be provided to allow the device to be used for Screen Saver authentication.	Pass
15. Software support should be provided to enable fingerprint authentication as a password manager replacement for applications that normally require user entered "password".	Pass
16. Uninstall prompts for data back up of data protected by the fingerprint authentication.	Pass
17. Support for disconnected client	Pass
18. Multi-factor authentication software support	Pass
19. Recovery / Backup / Migration software support	Pass
Hardware Guidelines	
20. Integrated / built-in device: connection via USB and/or LPC.	USB
21. Device and supporting software provides ACPI D-state support to reduce power consumption operating under Windows XP*.	Pass
22. Device and supporting software does not block ACPI S-state transitions	Pass
23. Device and supporting software allows host processor to enter C3 state as measured in Windows XP* using "Perfmon" utility.	Pass
24. Low Power HW Finger Detection	Pass
25. Device idle power: The user authentication device should be attached and software installed/configured. Once the system is stable (all drivers installed, no more system messages, …), and no applications are running,	Avg: .0064 W

Guideline	Functions as Expected
power should be measured at the attach point for the device (USB). Power measured using Windows XP.	Max: .0237 W
26. Device active power: power measurement is taken with device attached/plugged and capturing a fingerprint. Power measured using Windows XP.	Avg: .2399 W Max: .2946 W
27. Size (X x Y x Z mm) of entire device including sensor and electronics	Sensor: 14 x 14 X 1.55 mm
28. Bill of material for entire device including the sensor and connection circuitry meets target of less than $10?	Pass
Durability	
29. Durability Testing Performed by Which Accredited Lab	National Technical Systems, Inc
30. Durability – Abrasion	Pass
31. Durability – Chemical Resistance	Pass
32. Durability – Dust	Pass
33. Durability – Storage Temperature	Pass
34. Durability – Temperature Cycling	Pass
35. Durability – Constant Heat	Pass
36. Durability – Heat + Humidity	Pass
37. Durability – Salt Fog	Pass
38. Durability – Shock / Bump / Drop: Lacrosse Ball Drop	Pass
39. Durability – Shock / Bump / Drop: Pen Drop Height – Device failed after pen dropped from:	20cm
40. Durability – Shock / Bump / Drop: Drop Test	Pass
41. Durability – UV	Pass
42. Durability – ESD	Pass
Device Functionality	
43. Accuracy level: FAR	<.005%
44. Accuracy level: FRR	< 0.1%
45. Fake finger detection method	TruePrint Technology and Active Impedance Detection
46. Performance	Pass
47. Exclusions	Pass
48. Resolution	500 Dpi
49. Privacy mechanism (Template Encryption, HW/SW Challenge Response, Digitally Signed Images)	Template Encryption, HW/SW Challenge Response, Digitally Signed Images
50. Sample availability	August 2003

Guideline	Functions as Expected
51. Production quantities availability	October 2003

Evaluation Comments	• Note 1: AuthenTec sensor can utilize protection provided by system TPM as used with IBM Thinkpad Embedded Security Subsystem 2.0. This evidence is presented using the AuthenTec fingerprint sensor built into a PCMCIA authentication device supported by the IBM software. Other software does support and leverage smartcard for fingerprint template protection.

2.3. ST Microelectronics TouchChip* TCRU1

Table 6. ST Microelectronics TouchChip* TCRU1 – Vendor/Product Overview

Vendor	Name: Address: Tel: Website: Contact Name: Tel: Email:	ST Microelectronics, Inc 2001 Center Street, Suite 500 Berkeley, CA 94704 (510) 903-3226 http://eu.st.com/stonline/products/support/touchip/index.htm ST Microelectronics, Inc Francois Jeanneau (510) 903 3226 touchchip_support@st.com
Product Name	TouchChip Fingerprint Reader	
Part Number	TCRU1C	
Product Type	Placement – Capacitive	
Brief Product Description	TheTCRU1C offers a revolutionary approach for authenticating users of computers and information technology networks of all kinds. Built around the TouchChip Silicon Fingerprint Sensor, the TCRU1C is fast, reliable and inexpensive fingerprint authentication USB peripheral.	
Software Supplier(s)	Included Application software, Protector Suite and BioAPI Biometric Service Provider	
Vendor Comments	Our reader has been qualified by the following software providers: Bio-Key, Cogent Systems, Daon, Identix, ID-Metrics, I/O Software, Imprivita, Labcal, NEC, Saflink, Sagem	

Table 7. ST Microelectronics TouchChip* TCRU1 – Evaluation Summary

Guideline	Functions as Expected
Software Guidelines	
1. All software collateral should be supported in both Microsoft Windows 2000* and Windows XP* operating environments.	Pass
2. All software device drivers should have been tested and signed by Microsoft for use with Windows 2000 and Windows XP. Device drivers should be WHQL certified. Device driver installation should occur without warning by the Windows device installer.	Pending
3. Fingerprint device leverages the system TPM or smartcard	Pass - Smartcard
4. BAPI support included in the software for the device	Pass
5. BioAPI support include in the software for the device	Pending
6. All software device driver entities that should be installed to a user's hard drive should be described in an INF description file shipped with these collaterals on the root directory of the product software support CDROM.	Pass
7. Support software should be installed to the user's hard drive through a simple and easy to use set up utility.	Pass
8. User configuration and installation should be simple (ease of use): includes a user-friendly, simple to understand interface.	Pass
9. Configuration of the device should be done through an easy to use Wizard.	Pass
10. All software collateral should be delivered on CD-ROM. When inserted, the CDROM should "autorun" for installation.	Pass
11. Sample software provided with the fingerprint sensor to allow evaluation of fingerprint enrollment and other sample usage models.	Pass
12. Software support should be provided to allow the device to be used for Windows Login.	Pass
13. Software support for use with Microsoft's Active Directory used with network authentication is recommended.	No
14. Software support should be provided to allow the device to be used for Screen Saver authentication.	Pass
15. Software support should be provided to enable fingerprint authentication as a password manager replacement for applications that normally require user entered "password".	Pass
16. Uninstall prompts for data back up of data protected by the fingerprint authentication.	Pass
17. Support for disconnected client	Pass
18. Multi-factor authentication software support	Pass
19. Recovery / Backup / Migration software support	Pass
Hardware Guidelines	
20. Integrated / built-in device: connection via USB and/or LPC.	USB
21. Device and supporting software provides ACPI D-state support to reduce power consumption operating under Windows XP*.	Pass
22. Device and supporting software does not block ACPI S-state transitions	Pass
23. Device and supporting software allows host processor to enter C3 state as	Pass

Guideline	Functions as Expected
measured in Windows XP* using “Perfmon” utility.	
24. Low Power HW Finger Detection	Pass
25. Device idle power: The user authentication device should be attached and software installed/configured. Once the system is stable (all drivers installed, no more system messages, …), and no applications are running, power should be measured at the attach point for the device (USB). Power measured using Windows XP.	Avg: .0113 W Max: .0115 W
26. Device active power: power measurement is taken with device attached/plugged and capturing a fingerprint. Power measured using Windows XP.	Avg: .3749 W Max: .3844 W
27. Size (X x Y x Z mm) of entire device including sensor and electronics	27mm X 20.4mm X 3.8mm
28. Bill of material for entire device including the sensor and connection circuitry less than $10?	Pass
Durability	
29. Durability Testing Performed by Which Accredited Lab	National Technical Systems, Inc
30. Durability – Abrasion	Pass
31. Durability – Chemical Resistance	Pass
32. Durability – Dust	Pass
33. Durability – Storage Temperature	Pass
34. Durability – Temperature Cycling	Pass
35. Durability – Constant Heat	Pass
36. Durability – Heat + Humidity	Pass
37. Durability – Salt Fog	Pass
38. Durability – Shock / Bump / Drop: Lacrosse Ball Drop	Pass
39. Durability – Shock / Bump / Drop: Pen Drop Height – Device failed after pen dropped from:	40 cm
40. Durability – Shock / Bump / Drop: Drop Test	Pass
41. Durability – UV	Pass
42. Durability – ESD	Pass
Device Functionality	
43. Accuracy level: FAR	<.01%
44. Accuracy level: FRR	< 1%
45. Fake finger detection method	Pass
46. Performance	Pass
47. Exclusions	Pass
48. Resolution	508Dpi
49. Privacy mechanism (Template Encryption, HW/SW Challenge Response, Digitally Signed Images)	Template encryption, Challenge Response.

Guideline	Functions as Expected
50. Sample availability	Shipping today
51. Production quantities availability	Shipping today

Evaluation Comments	None

2.4. ST Microelectronics TouchStrip* TCS3

Table 8. ST Microelectronics TouchStrip* TCS3 – Vendor/Product Overview

Vendor	Name: Address: Tel: Website: Contact Name: Tel: Email:	ST Microelectronics, Inc 2001 Center Street, Suite 500 Berkeley, CA 94704 (510) 903-3226 http://eu.st.com/stonline/products/support/touchip/index.htm ST Microelectronics, Inc Francois Jeanneau (510) 903 3226 touchchip_support@st.com
Product Name	TouchStrip* Sensor	
Part Number	TCS3	
Product Type	Swipe – Capacitive (Active Pixel)	
Brief Product Description	TheTCS3 strip sensor, coupled with the TCD41A companion processor, gives a complete biometric solution capable of capturing, storing and matching fingerprint templates with minimal host intervention, and the highest security. The strip sensor offers lower cost over ST's larger TCS1 sensor, but is built on the same active-pixel technology, for the highest quality imaging.	
Software Supplier(s)	Included Application software, Protector Suite and BioAPI Biometric Service Provider.	
Vendor Comments	Our reader has been qualified by the following software providers: Bio-Key, Cogent Systems, Daon, Identix, ID-Metrics, I/O Software, Imprivita,	

	Labcal, NEC, Saflink, Sagem

Table 9. ST Microelectronics TouchStrip* TCS3– Evaluation Summary

Guideline	Functions as Expected
Software Guidelines	
1. All software collateral should be supported in both Microsoft Windows 2000* and Windows XP* operating environments.	Pass
2. All software device drivers should have been tested and signed by Microsoft for use with Windows 2000 and Windows XP. Device drivers should be WHQL certified. Device driver installation should occur without warning by the Windows device installer.	Pending
3. Fingerprint device leverages the system TPM or smartcard	Pass - Smartcard
4. BAPI support included in the software for the device	Pass
5. BioAPI support include in the software for the device	Pending
6. All software device driver entities that should be installed to a user's hard drive should be described in an INF description file shipped with these collaterals on the root directory of the product software support CDROM.	Pass
7. Support software should be installed to the user's hard drive through a simple and easy to use set up utility.	Pass
8. User configuration and installation should be simple (ease of use): includes a user-friendly, simple to understand interface.	Pass
9. Configuration of the device should be done through an easy to use Wizard.	Pass
10. All software collateral should be delivered on CD-ROM. When inserted, the CDROM should "autorun" for installation.	Pass
11. Sample software provided with the fingerprint sensor to allow evaluation of fingerprint enrollment and other sample usage models.	Pass
12. Software support should be provided to allow the device to be used for Windows Login.	Pass
13. Software support for use with Microsoft's Active Directory used with network authentication is recommended.	No
14. Software support should be provided to allow the device to be used for Screen Saver authentication.	Pass
15. Software support should be provided to enable fingerprint authentication as a password manager replacement for applications that normally require user entered "password".	Pass
16. Uninstall prompts for data back up of data protected by the fingerprint authentication.	Pass
17. Support for disconnected client	Pass
18. Multi-factor authentication software support	Pass
19. Recovery / Backup / Migration software support	Pass
Hardware Guidelines	
20. Integrated / built-in device: connection via USB and/or LPC.	USB

Guideline	Functions as Expected
21. Device and supporting software provides ACPI D-state support to reduce power consumption operating under Windows XP*.	Pass
22. Device and supporting software does not block ACPI S-state transitions	Pass
23. Device and supporting software allows host processor to enter C3 state as measured in Windows XP* using “Perfmon” utility.	Pass
24. Low Power HW Finger Detection	Pass
25. Device idle power: The user authentication device should be attached and software installed/configured. Once the system is stable (all drivers installed, no more system messages, …), and no applications are running, power should be measured at the attach point for the device (USB). Power measured using Windows XP.	Avg: .0006 W Max: .0070 W
26. Device active power: power measurement is taken with device attached/plugged and capturing a fingerprint. Power measured using Windows XP.	Avg: .6151 W Max: .6521 W
27. Size (X x Y x Z mm) of entire device including sensor and electronics	27mm x 24mm x 3.8mm
28. Bill of material for entire device including the sensor and connection circuitry less than $10?	Pass
Durability	
29. Durability Testing Performed by Which Accredited Lab	National Technical Systems, Inc
30. Durability – Abrasion	Pass
31. Durability – Chemical Resistance	Pass
32. Durability – Dust	Pass
33. Durability – Storage Temperature	Pass
34. Durability – Temperature Cycling	Pass
35. Durability – Constant Heat	Pass
36. Durability – Heat + Humidity	Pass
37. Durability – Salt Fog	Pass
38. Durability – Shock / Bump / Drop: Lacrosse Ball Drop	Pass
39. Durability – Shock / Bump / Drop: Pen Drop Height – Device failed after pen dropped from:	10cm
40. Durability – Shock / Bump / Drop: Drop Test	Pass
41. Durability – UV	Pass
42. Durability – ESD	Pass
Device Functionality	
43. Accuracy level: FAR	<.01%
44. Accuracy level: FRR	< 1%
45. Fake finger detection method	Pass
46. Performance	Pass

Guideline	Functions as Expected
47. Exclusions	Pass
48. Resolution	508Dpi
49. Privacy mechanism (Template Encryption, HW/SW Challenge Response, Digitally Signed Images)	Template encryption, Challenge Response.
50. Sample availability	Shipping today
51. Production quantities availability	Shipping today

Evaluation Comments	None

This page intentionally left blank.