Harmonization and Implementation Committee

National Identity Management System

Biometrics Standards and Specifications

11th February, 2011

Version (working document)

Revision History

Revision	Date	Document Status	Participants/Comments
1.0	29 October 2010	Release	Initial release of the NIMC working document
1.0.0.1	02 November 2010	Updated Release	First reading and review by Co-chair
1.0.0.2	15 December 2010	Updated Release	2nd meeting of the sub-committee
1.0.0.3	20 January 2011	Update Release	3rd meeting of the sub-committee
1.0.0.4	04 February 2011	Update Release	4th meeting of the sub-committee
1.0.0.5	08 February 2011	Update Release	5th meeting of the sub-committee
1.0.0.6	10 February 2011	Update Release	5th meeting of HIC overall committee

Change Request

CR ID	Change Request (CR) Description
CR-0001	Resolve that 10 (ten) fingerprint shall be standard and face capture
CR-0002	Resolve that all reference to Iris shall be deleted
CR-0003	Resolve that the draft report be informally accepted pending final comments by overall committee members via email

1 Introduction

There is currently no centralized national identity database and no system of National Identity Management which efficiently links public and private sector identity schemes in Nigeria. While the financial services sector has been most proactive in the deployment of identification schemes for delivery of its services, the schemes have differed from institution to institution within the sector. The result has been the creation of several different identification schemes and databases leading to the duplication of an individual's identity data by the various institutions offering services to that person. Government agencies also hold a number of databases with no viable integration of access or interoperability to enhance the delivery of services within these government institutions. This is despite the fact that some of these institutions have introduced smart card technology into their schemes. A reliable national system for verification and secure authentication of an individual's identity has thus not been established.

National Identity Management Commission (NIMC) Act, 2007 Act No. 23; An Act to provide for the establishment of a National Identity Database; has been setup by the Govt. of Nigeria with a mandate to issue a Unique National Identification Number (NIN) to all Nigerians and long term residents in the country. NIMC proposes to create a platform to first collect the identity details and then perform authentication that can be used by several government and commercial service providers. A key requirement of NIMC's system is to eliminate duplicate identity.

NIMC has selected biometrics feature set as the primary method to check for duplicate identity. For government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that the biometric information capture and transmission are standardized across all the partners and users of the NIMC's system, taking cognizance of the appropriate biometrics parameters to achieve the NIMC's mandate. This encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standards.

2 Objective

The main motivation of biometrics standards is to define requirements, formats and software specification enabling interoperability between biometric systems, especially authentication systems. Biometric standards enable levels of interoperability. High level standards enable interoperability of data collections and storage processes.

It covers the basic functions of Enrollment, Verification, and Identification, and includes basic standards to allow only approved agencies, organizations, and entities to manage and ensure interoperability of their system with the integrated national system.

1. The NIMC biometrics committee was constituted to provide the NIMC with direction on the biometrics standards, taking cognizance of parameters, suggest best practices and recommend biometric modalities for the unique NIN system.

1. The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and unique NIN service delivery.

2. The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

3. The biometrics will be captured for authentication by NIMC Front-End partners, government departments, and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by NIMC. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

4. The purpose of this document is to identify applicable standards and recommend best practices to the NIMC to achieve its objective.

3 Committee Charter

- To develop biometric standards that will ensure interoperability of devices, systems and processes used by various agencies that use the unique NIN system
- To review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of NIMC relating to de-duplication and Authentication.

4 Target Audience

Any person or organization involved in designing, testing or implementing NIN system, NIN compatible systems, or NIN enrolment for the central government, state government, commercial organizations, or any users of the NIN system.

5 Normative Reference

The following reference documents are indispensable for the application of this document.

- July 2007 Privacy Impact Assessment (PIA) & Harmonization Study for National Identity Management Commission (NIMC).
- IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997.
- ISO/IEC 15444 (all parts), Information technology – JPEG 2000 image coding system.
- ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications.
- ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data.
- ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data.
- ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data.

6 Standards

In the current IT world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis and ISO are just a few of the prominent agencies with published biometrics standards. After reviewing the charter of each body and current state of biometrics in Nigeria, the Committee selected the ISO standard. Within the ISO body of biometrics standards, the Committee will use data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the maximum empirical information on usage, interoperability and conformance.

Usually, we recognize people we know by looking at their faces, sometimes by their voices or handwriting, or by the way they move. In times past, human scrutiny was the only way of checking the identity of travellers moving from one country to another, visitors seeking to enter private areas, or traders withdrawing cash from banks. This is no longer realistic, given the growth of international travel, the need for security in workplaces, and the spread of electronic banking, among many other changes in our daily lives. Nowadays, there is a new way of checking identity, using automated methods and information and communication technologies (ICT) to recognize individuals based on physical or behavioural traits — a field known as biometrics.

With the wide acceptance of biometrics for identity verification, especially in an open network environment, the challenges of privacy, reliability and the security of biometric data become more complicated and demanding.

To ensure that biometric identification systems are reliable, secure, interoperable and easy to use, there is an evident need for the development of international standards. Governmental authorities, in particular, are unlikely to accept a non-standardized system offered by a single manufacturer. There has to be general agreement on what biometric traits to measure, and confidence that the chosen metrics will distinguish between any two individuals. Standards are also needed to protect biometric data, both to maintain personal privacy and to prevent attacks that would open the way for fraud or impersonation. The underlying objectives in standardization are to make biometric systems easier to install, cheaper to run and more reliable to use.

7 Biometrics Process

Biometrics is the science and technology of measuring and analyzing biological data. It refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. The significance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all the requirements imposed by all applications. In other words, no biometric is ideal, but a number of them are acceptable

7.1 Face

The dimensions, proportions and physical attributes of a person's face are unique. Biometric facial recognition systems will measure and analyze the overall structure, shape and proportions of the face: Distance between the eyes, nose, mouth, and jaw edges; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, the area surrounding the cheekbones.

At enrolment, several pictures are taken of the user's face, with slightly different angles and facial expressions, to allow for more accurate matching. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded.

To prevent an image / photo of the face or a mask from being used, face biometric systems will require the user to smile, blink, or nod their head. Also, facial thermography can be used to record the heat of the face (which won't be affected by a mask).

The main facial recognition methods are: feature analysis, neural network, and automatic face processing. It is not intrusive, can be done from a distance, even without the user being aware of it

Its weakness is that face biometric systems are more suited for authentication than for identification purposes, as it is easy to change the proportion of one's face by wearing a mask, a nose extension, etc.

User perceptions / civil liberty: Most people are uncomfortable with having their picture taken. Its application includes access to restricted areas and buildings, banks, embassies, military sites, airports, law enforcement.

7.2 Fingerprint

A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).

The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Loops make up 60% of all fingerprints, whorls account for 30%, and arches for 10%.

Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics. There is a large variation in the quality of fingerprints within the population. The tip of the finger is a small area from which to take measurements, and ridge patterns can be affected by cuts, dirt, or even wear and tear. Acquiring high-quality images of distinctive fingerprint ridges and minutiae is complicated task.

- Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements. Fingerprint biometric systems are also used for law enforcement, background searches to screen job applicants, healthcare and welfare.

7.3 Nigerian Standards (Enrolment and Verification)

From the general ISO Standards in biometrics, we narrowed down certain applicable standards that suit the Nigerian background in face image and fingerprint image.

7.3.1 Summary of Face Capture Standards

Key Decisions	**Summary of Decisions**
Enrolment	
Face Image Capture	Full frontal 24bits color. Well focused nose and ear and chic to crown region. Capture tribal mark for easy verification process.
Digital/Photographic Requirement	Auto forms and auto-capture functions for capture device.
Expression	Face captured with neutral (non smiling) expression, teeth closed and both eyes open.
Illumination	Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, eye sockets and no hot sports.
Eye Glasses	If glasses are worn, it should be clear and transparent so that pupils and iris are visible.
Accessories	Eye patches are allowed due to medical reasons. Accessories like turban are allowed due to ethical reasons, partial covering the face from forehead to chin are allowed due to regional reasons.
Multiple samples of face	There should be three samples at of which one should be left and right. This however for de-duplication and authentication of

	individuals who do not have fingerprints.
Operational	Operators would be trained to obtain the best possible face image that satisfies requirements.
Quality Check	The quality assessment algorithms should encode parameters like illumination, pose, blur, nose, resolution, inter-eye distance, image height and width and horizontal vertical position of the face.
Storage and Compression	Uncompressed images should be stored in database and preserve the quality.
Verification	
Image Capture	Same as enrolment.
Compression	JPEG 2000 compression ratio should not be less than 11KB.
Number of images	For both manual and authentication, a single full frontal face image is sufficient.

7.3.2 Summary of Fingerprint Capture standards

Key Decisions	**Summary of Decisions**
Enrolment	
Image Capture	
Plain or Rolled	Plain, Live Scan.
Number of Fingers Fingerprint in Rural Areas & Amputees	Ten. In absence of fingers and presence of worn out fingerprints, available ones will be captured.
Device Characteristics	In covering scan resolution pixel depth and dynamic range, the biometrics sample captured during enrolment needs to be the best sample possible.
Quality Check	Yes-Specified as best practice
Operational	Operator Assistance, Corrective Measure and retries.
Storage and Transmission	
Compression	Uncompressed images strongly recommended.
Verification	
Image Capture	

Number of Fingers	One minimum, no maximum. A single finger will be sufficient to provide the minimum standard of accuracy requirements.
Any Finger option	Any finger.
Retry	A timeout will be implemented in service after five attempts.
Device Characteristics	A standard will be defined for the scanner used in the authentication process.
Transmission Format	The captured image needs to be sent to the unique NIN Server for matching in real time.
Compression	JPEG 2000 compression recommended compression ratio to be less than 15:1.
Minutiae Format	If the data is minutiae and the unique NIN Server has matches the best pairs with the extractor used by the authentication agency, it will use proprietary data. If the Server does not have matching matches, it will only use "Standard" minutiae data.

8 Enrollment of Face Image

8.1 Face image capture

Full frontal face image provides sufficient information for both human visual inspection (by operator) and automatic face recognition algorithms. An algorithm is an effective method for solving a problem using a finite sequence of instructions. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance is required. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

8.2 Tribal Marks

It is common to find most Nigerians having tribal marks which are common identifiers. A mere glance at someone's face with tribal marks is sufficient to read that person's ethnic group, town, or even family. Facial marks are made for ethnic identification; others are symbols of status in traditional societies.

Taking cognizance of this factor, the face image should be captured with the tribal marks; clearly visible for easy verification purpose. This would be a permanent identity that could be neither lost nor forged.

8.3 Digital/Photographic requirements

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with enrollee demographic data at the point of capture, thus reducing possible errors. In villages where power source may be difficult to obtain, it is simpler to supply power from the computer.

For capturing face image, it is simpler for the operator to adjust the camera instead of the enrollee to position himself/herself at the right distance or in the right posture. The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and radial distortion. Interlaced video frames are not allowed.

8.4 Expression

Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed and both eyes open.

8.5 Illumination

Poor illumination has high impact on the performance of face recognition. It is difficult for human operators as well to analyze and recognize face images with poor illumination. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

8.6 Eye Glasses

Face images with and without eyeglasses may have an impact on face recognition. The impact is greater if the glasses automatically tint under illumination. If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent so that pupils and iris are visible. If the glasses are with tint, then direct and background lighting sources should be tuned accordingly.

8.7 Accessories

Use of accessories that cover any region of the face is strongly discouraged. However, accessories like eye patches are allowed due to medical reasons. Further, accessories like turban are also allowed due to ethical reasons. Partial covering of head, without covering the face from forehead are allowed due to religions reasons.

8.8 Multiple samples of face

For visual inspection by humans, the single face image of a person is sufficient. However, for de-duplication and authentication of individuals who do not have fingerprints as a result of loss of arm arising from amputation, automatic face recognition is recommended. To perform accurate authentication in such cases, capture of multiple face images is strongly recommended during enrolment. There should be three samples, out of which one should be frontal image. The other two images should be left and right.

8.9 Operational

Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

8.10 Quality check

Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

8.11 Storage and Compression

The performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image, it is strongly recommended that uncompressed images should be stored in the database.

9 Verification of Face Image

The verification process consists of steps similar to enrolment.

9.1 Image Capture

Image capture for verification should also follow standards for enrolment as defined earlier in this section.

9.2 Compression

For verification, images with JPEG 2000 compression ratio of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

9.3 Number of Images

For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

10 Enrolment of Fingerprint

The enrolment process can be broken down into image capture ("client") and de-duplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computational intensive task of duplicate checking against the gallery.

10.1 Image capture

During image capture, the factors to consider are:

1 Type of image and number of fingers to capture

2 Providing available and easily recognized fingers for cases of worn out fingerprints of rural farmers and artisans as a result of strenuous works with the hands.

3 Providing available fingers for cases of amputees.

4 Device used for capturing the image

5 Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image

6 Storage when the images need to be stored

10.2 Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the NIN system.

10.3 Number of fingers

The Committee recommends capturing prints of all ten fingers, the maximum possible. In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image.

10.4 Fingerprints in the Rural Area

Considering the people that occupy the rural areas and the nature of strenuous work they do like farming etc, the committee recommends capturing prints of all ten fingers, the maximum possible. In case where the whole fingerprints cannot be easily identifiable and captured as a result of worn out cases, the easily identifiable ones would be captured.

10.5 Amputee

Cases are prevalent that some people are victims of negative circumstances leading to amputation of their limbs. As a result of the absence of all fingers or some as a result of the amputation of the arm, the available once will be captured in the enrollment process.

10.6 Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images. The biometrics sample captured during enrolment needs to be the best sample possible.

10.7 Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor.

The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements.

10.8 Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1 Operator Assistance: Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.

2 Corrective measures & retries: If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

10.9 Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

10.10 Compression

Biometric data are national assets and should be captured and stored for long-term use. To preserve the quality, the committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

11 Verification of Fingerprints

The verification process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

11.1 Image capture

11.2 Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

11.3 Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

11.4 Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find an alternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "no match". A timeout will be implemented in service after five attempts.

11.5 Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the NIMC goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has to define a new standard for the scanner used in the authentication process. It is envisioned that the NIMC will provide certification criteria for this standard.

11.6 Transmission format

The captured image needs to be sent to the National Identity (NIN) server for matching in real time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmission will contain extracted minutiae. In the second, it will contain the compressed raw image. For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image. The NIN software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximum flexibility during authentication. It is understood that raw or compressed image will give a higher level of accuracy.

11.7 Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

11.8 Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the unique NIN server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the server does not have matching matcher, it will only use "standard" minutiae data.

12 LIST OF APPENDIX

12.1APPENDIX A: Committee Members List

S/NO	Name of Organization	Representatives
1.	National Identity Management Commission (NIMC)	a) Ben Alofoje (Co-Chair) b) Mfon Udoh c) Emmanuel
2.	SageMetrics Nig Ltd	a) Hon. Kenneth Nwabueze b) Onyeka
3.	Independent Electoral Commission (INEC)	a) Moses Naiya
4.	Joint Tax Board (JTB)	Ekeh Chinedu
5.	XDS CREDIT BUREAU	a) Zipporah Anuga (Mrs)
6.	Nigerian Immigration Services (NIS)	Epum Charles
7.	Nigerian Pension Commission (PENCOM)	a) Ekanem Aikhomu a) Kunle Odebiyi
8.	Nigerian Security Adviser (NSA)	a) Magani Niyomdi
9.	Central Bank of Nigeria (CBN)	b) Soji Aminu
10.	Nigerian Prison Services (PRISONS)	a) Agada F. Audu a) Garba Michael
11.	National Population Commission (NPopC)	Amos Helen O. (Mrs.)
12.	Federal Inland Revenue Services (FIRS)	b) Osasere J. Ehigie
13.	ADVANCED MANAGEMENT TECHNOLOGY SOLUTIONS (AMTS)	Dr. Steven Dike a)

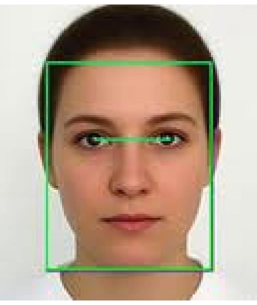
12.2APPENDIX B: Acronym Name List

AMTS	Advanced Management and Technology Solution
AFIS	Automated Fingerprint Identification System
ASP BSP	Application Service Provider Biometrics Service Provider
CAC	Corporate Affairs Commission
CBN	Central Bank of Nigeria
DMZ	Demilitarized Zone
DNS	Domain Name Services
DNCR	Department of National Civic Registration
EFCC	Economic and Financial Crimes Commission
FIRS	Federal Inland Revenue Service
FRSC	Federal Road Safety Commission
GMPC	General Multi-Purpose Card
HAS	Harmonization Assessment Study
ICT	Information and Communication Technology
ID	Identification
INEC	Independent National Electoral Commission
IP	Internet Protocol
ISO	International Standards organization
JTB	Joint Tax Board
MOD	Ministry of Defence
NCC	Nigeria Communication Commission
NEEDS	National Economic Empowerment and Development Strategies
NHIS	National Health Insurance Scheme
NIN	National Identification Number
NIMC	National Identity Management Commission
NIMHC	National Identity Management Harmonization Committee
NIS	Nigerian Immigration Services
NPC	National Population Commission
NPF	The Nigerian Police Force
NPS	Nigerian Prison Services
NSA	National Security Adviser
PENCOM	National Pensions Commission
PII	Personally Identifiable Information
PIV	Person Identification Verification
PVC	Poly Vinyl Chloride
SSS	State Security Services
SQL TCC TCR	Structured Query Language Transaction Control Code Transaction Control Reference
UTIN	Universal Tax Identification Number
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extended Markup Language

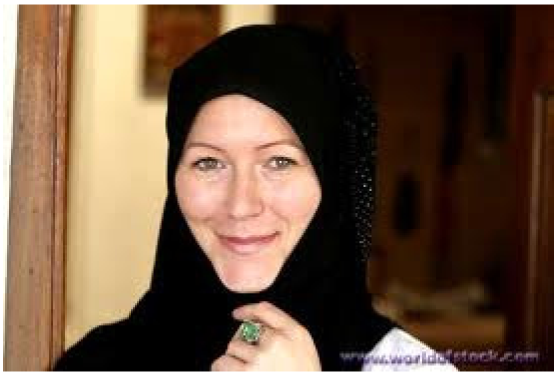
12.3APPENDIX C: Acronym Name List Specific to Biometrics

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIN	National Identification Number
IAFIS	Integrated Automated Fingerprint Identification System
ANSI	American National Standards Institute
INCITS	InterNational Committee for Information Technology Standards
ICT	Information and Communications Technology
NID	National Identification
DNA	Deoxyribonucleic Acid
JPEG	Joint Photographic Experts Group
CEN	European Committee for Standardization
NIST	National Institute of Standards and Technology
NFIQ	NIST Fingerprint Image Quality
WSQ	Wavelet Scalar Quantization

12.4APPENDIX D: Facial Image Sample (for accessories)

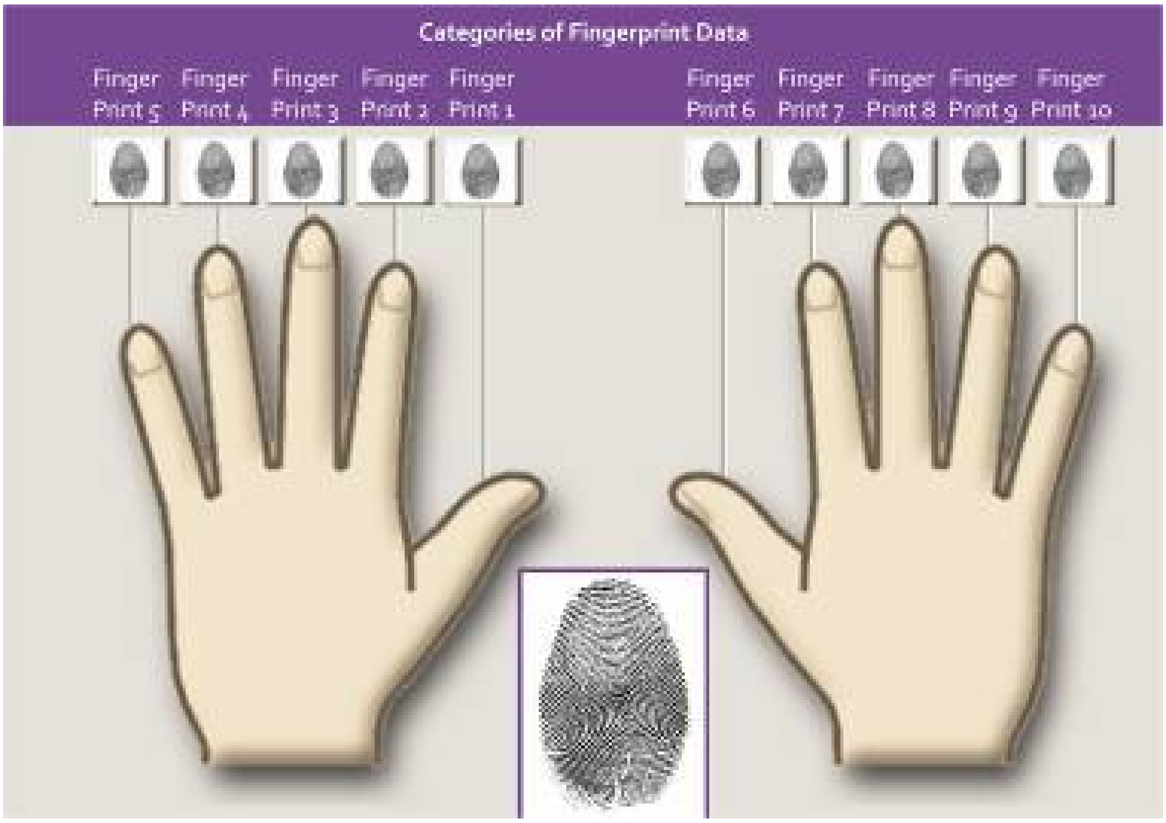


Correct form showing eyes (pupil) and ears



Incorrect form, at least one (1) ear must be visible

12.5APPENDIX E: Fingerprint labeling format


Categories of Fingerprint Data
Finger Print 5
Finger Print 4
Finger Print 3
Finger Print 2
Finger Print 1
Finger Print 6
Finger Print 7
Finger Print 8
Finger Print 9
Finger Print 10