

REVISED FRAMEWORK FOR CERTIFICATION
OF BIOMETRIC FINGERPRINT SCANNERS
FOR NIBSS BVN SERVICES

(PUBLIC)

Version 2.0

Certification Department

22nd March, 2021.

PUBLIC

Date of Change	Responsible	Summary of Change	Version	
	Certification /Operations	Document Creation	1.0	
22 nd March, 2021	<ol style="list-style-type: none"> 1. Certification 2. Product management 3. EPMO 4. Identity management 	<ol style="list-style-type: none"> 1. Process of integrating Scanners into NIBSS Application 2. Implementation fee 3. Stakeholders Responsibilities 	2.0	

APPROVED

Contents

1. Introduction.....	4
1.1 Purpose.....	4
2. Integration to NIBSS BVN enrolment or fingerprint capture SDKs	5
2.1 Application for Implementation on NIBSS Solutions.....	5
2.2 Implementation Process, Stakeholders and Responsibilities.	6
3. Certification of Fingerprint Biometric Scanners.....	7
3.1 PHASE I.....	7
3.1.1 General Requirements.	7
3.1.2 Hardware Certification Documents	8
3.1.3 Device Requirements	8
3.1.4 Software Requirements.....	8
3.1.5 Application	9
3.2 PHASE II	10
3.3 PHASE III	10
3.3.1 SDK Integration to NIBSS BVN Enrolment Application:.....	10
3.3.2 API Integration Test:.....	11
3.3.3 SIGN-OFF:.....	12
4. Appendix.....	13

1. Introduction

This document outlines the process by which NIBSS considers biometric devices for implementation on NIBSS solutions/platforms for the purpose of biometric enrolment or Verification.

1.1 Purpose

The purpose of the document is to provide information to the public who wish to certify

biometric capture devices to be used in the Nigeria financial space.

- To provide information to stakeholders who wish to apply to have their certified fingerprint biometric capture device implemented by NIBSS for biometric verification on NIBSS channels.
- To provide information to stakeholders who wish to apply to have their certified fingerprint biometric capture device implemented by NIBSS for biometric enrolment on NIBSS channels.
- To provide the industry with the list of certified devices and applications.

2. Integration to NIBSS BVN enrolment or fingerprint capture SDKs

Interested stakeholders may request for NIBSS to implement a certified fingerprint capture device for use on NIBSS solutions. These solutions include the following.

- NIBSS Biometric Authentication Service SDK
- NIBSS Desktop Fingerprint Capture Tool
- NIBSS Desktop Offline Enrolment Application (4-4-2 only)
- NIBSS Android Enrolment SDK

2.1 Application for Implementation on NIBSS Solutions

Stakeholders who wish to have their biometric devices implemented with NIBSS for the capture of Biometrics on its solutions must apply for consideration. Applicants shall enquire from NIBSS on the status of applications.

NIBSS reserves the right to suspend applications for implementation on any of its solutions. Suspension may be due to ongoing implementations or a lack of a business need.

The process for Applications is detailed below.

1. Applicant shall make a formal request for implementation stating the specific solution/solutions on which implementation is desired.
2. Applicants shall submit two units of the devices for review.
3. NIBSS shall review the application with consideration to the following.
 - a. Value over existing alternatives
 - b. Technical/Functional capabilities of the submitted device
 - c. Non-functional characteristics of the devices e.g. durability, portability, fitness for use
 - d. Unit cost

NIBSS May revise the scope of implementation to include or remove certain solutions.
4. NIBSS may subject devices to performance and/or durability tests. Applicants may be required to replace devices that fail or are damaged during testing.
5. NIBSS reserves the right to decline applications. This may result from

- a. Lack of value of new device over existing options
- b. Failure of device to meet non-functional requirements that may limit its fitness for use e.g., user experience/ease of use, durability, portability
- c. Resource constraints

NIBSS shall return devices submitted where application is declined.

6. Where such a request is accepted, the Applicant must embark on a certification exercise with NIBSS.
7. Upon successful certification, NIBSS shall advise on a period for implementation; this period shall fall within 6 months from the date of completion of certification.
8. A fee of N3,000,000 is charged for implementation on each solution. The Applicant must make the payment prior to commencement of the implementation.
9. Any significant change/update to a device or its software that may require a reimplementation shall be subject to a review by NIBSS. The applicant is required to notify NIBSS of such change. Where the change is substantial, NIBSS may require that the customer reapply for implementation. Additionally, NIBSS reserves the right to discontinue support for such devices or the updated model(s).

2.2 Implementation Process, Stakeholders and Responsibilities.

	ACTIONS
1.	Receive application
2.	Verify application and supporting documentation
3.	Review application and secure approval for implementation
4.	Schedule implementation in Product Roadmap
5.	Share Project Timeline
6.	Close out project
7.	Roll-out updated SDKs

3. Certification of Fingerprint Biometric Scanners.

The NIBSS certification process for Fingerprint Biometric Scanners shall be conducted in three phases. The first phase must be completed and signed off before proceeding to the next phase.

The three phases are detailed below.:

3.1 PHASE I

In this Phase, NIBSS shall verify that the device and the stakeholder presenting such device for certification meet NIBSS requirements for consideration and that sufficient information/resources are available for a successful certification exercise for the device.

The requirements for this phase are broken down into the following.

3.1.1 General Requirements.

The following are required documentation that must be provided by interested stakeholders as part of the Phase I exercise.

1. Formal request for Biometric Certification: Applicants will submit a formal Letter of intent in hard copy directing it to the Managing Director (MD), Nigeria Interbank Settlement System, Plc.
 2. Certificate of Incorporation.
 3. Company profile.
 4. Corporate Affairs Commission Form 07 - Particulars of Directors.
 5. Corporate Affairs Commission Form 02 - Statement of company's share capital.
 6. Notice of situation of address of the company.
 7. Memorandum and Article of Association.
 8. 3-year tax clearance certificate.
 9. Sample Biometric Device & Software.
 10. Completed Checklist.
 11. Evidence of Certification fee payment
-

3.1.2 Hardware Certification Documents

The below are the documents required to be submitted along with the physical device(s) to be certified. Applicants are required to provide valid copies of the following:

1. ISO 9001 Certificate of device manufacturer
 2. WHQL certificate (Windows Hardware Certification Report) of device drivers.
 3. FBI PIV - For 1 finger-print scanner type
 4. FBI EBTS (APPENDIX F) – For multiple fingerprint scanner type
 5. Letter showing partnership between Vendor and Device Manufacturer.
-

3.1.3 Device Requirements

The following is required:

1. Physical Biometric scanner device and its documents which includes name, serial no, manufacturer, firmware, software version for capture tool, fake detection tool and segmentation tool (applicable for a multiple finger-print scanner type).
 2. Device Driver for installation.
 3. SDK/TOE – for running feature extraction. Software must be able to read. wsq image file and convert to ISO Template standard format (.dat).
 4. Cable connectors and ports for connecting fingerprint acquisition device to computer USB port.
-

3.1.4 Software Requirements

The following is required:

1. Valid copies of ISO 19794–2 Compliance certificate/evidence.
 2. Capture Tool.
 3. Segmentation Tool (applicable for a multiple fingerprint scanner type).
 4. Fake Detection Tool.
 5. 5. Provision of 100,000 wsq image capture files which will be used for generation of Template files.
-

3.1.5 Application

NIBSS requires that all applicants submit a formal request for certification to the MD/CEO of NIBSS. After a successful due diligence process and execution of NDA/SLA, the Certification Team would request from the Vendor to submit copies of all requirements for biometric certification as captured in the subheadings section above. (ALL DOCUMENTS MUST BE RECEIVED AT NIBSS WITHIN 3 WEEKS OF THE CERTIFICATION TEAM'S REQUEST. IF ANY DOCUMENT IS NOT SENT IN WITHIN 4 WEEKS, CERTIFICATION CYCLE IS CLOSED AND WOULD HAVE TO BE RE-OPENED AFRESH WITH NEW PAYMENT. IT IS IMPORTANT THAT ALL REQUIREMENTS BE OBTAINED BEFORE AN APPLICATION IS PUT FORWARD TO NIBSS FOR CERTIFICATION).

Once all requirements are verified to be okay, a timeline for certification (3 weeks) is shared with vendor/applicant and start date and end date clearly communicated.

3.2 PHASE II

This phase includes the technical certification of the device. The timeline for Biometric Fingerprint Scanner certification is Three (3) weeks.

1. The certification exercise will commence on the device according to NIBSS' Standard procedure and specification for Biometric Certification. The team ensures test be completed within the specified timeline (except if some exceptional issues arise).
2. In the case of any error/difficulty during certification, the certification team notifies the applicant via email with evidence of the error, and feedback/resolution is expected within 5 days (maximum) in order to maintain the certification timeline of 3 weeks.
3. If applicants take longer than 5 days for feedback/resolution, certification is paused and new timeline communicated whenever applicant reverts.
4. If there are no errors encountered during testing (hardware and software), test reports and sign off documents, this will signify the clearance to begin the next face.
5. In the event of an upgrade in the device, or change in the device firmware, or the software version, at any time a recertification is required.

For single fingerprint device scanners only; certificate is issued on completion of certification.

3.3 PHASE III

3.3.1 SDK Integration to NIBSS BVN Enrolment Application:

The implementation will follow NIBSS SDLC, this implementation would only commence when the Certification has been confirmed okay and fit in terms of device assessment.

Below are the processes for integrating the SDK after successful certification of the device scanner:

- a) A review of the SDK with Vendor rep

- b) Integration of the SDK to specified NIBSS application. A project/implementation plan would be shared with the vendor within 6 months from completion of certification. Vendor would be expected to assist with any technical support required during this process.
- c) A controlled pilot would be held by NIBSS and the vendor. This may include field tests using the implemented device.
- d) Upon successful completion of the pilot, NIBSS shall release updates SDKs/solutions on which the new device was implemented.
- e) Certificate will be issued on completion of the sdk integration to the enrollment application and successful pilot run (see Appendix)

VERIFICATION:

For certified single fingerprint scanners:

1. The vendor will be required to collaborate with a bank on purchasing this device.
2. The bank will integrate to the BVN Fingerprint API or BAS OFF US service for the purpose of **verification**.

N.B: BVN Fingerprint API or BAS OFF US service are available to only the banks for integration.

The test plan for verification involves **three** levels of testing:

3.3.2 API Integration Test:

For this integration test, the test plan involves 3 levels of testing:

1. **API Integration Test:**

Test scenarios at this time will not be hitting the staging environment. We would only be testing the API security and validation features and not the verification.

2. **Verification Test –**

Provision of 2 persons' valid BVNs: The Institution provides a valid BVN or two; BVN of the person(s) that will be verifying his/her details which includes demography details (fingerprints) to be inserted into our staging environment.

3. Liveness Detection Test:

To certify that the single fingerprint scanner can do liveness detection.

3.3.3 SIGN-OFF:

The sign off process includes the following:

- a) Execution of the SLA between NIBSS and the BANK (institution).
- b) Completed UAT sign off document.

APPROVED

4. Appendix

Below are the steps for Pilot run:

1. Upon success, Technology Development Team integrates the new scanner device SDK into the offline BVN Enrolment App V1.1.6 and bundles it into the entire APK
2. Upon notification of successful integration, NIBSS team will test the offline BVN Enrolment app to ensure that the app
 - a. Can detect the scanner to be certified and
 - b. Captures fingerprint quality with the required minimum.
3. Two parallel confirmation pilot tests will happen thereafter:
 - a. External: The vendor will conduct a confirmation pilot test, working with any BVN Enrolment agent of choice, on the NIBSS BVN Enrolment Application using the 4-4-2 device presented for certification
 - b. Internal: DFS will conduct the same confirmation test internally.
4. The Team will confirm that the XML files were received, okay, and processed to generate BVN (The team must ensure that the response from BMS is 'Duplicate', if the test was done using an enrollee with existing BVN)
5. Certification Certificate will be issued upon successful completion of the pilot run on enrolment application.