Nigeria Inter-Bank Settlement System Plc

...improving the Nigeria Payments System

FRAMEWORK FOR CERTIFICATION OF BIOMETRIC FINGERPRINT SCANNERS.

(PUBLIC)

Version 1.1

Approved 1.1

Certification Department

24th October 2018.

Introduction

This document covers the requirements for certification of Fingerprint scanners that can be used in the Nigerian financial space.

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.

CERTIFICATION OF FINGER PRINTS SCANNERS.

A fingerprint biometric device is a security identification and authentication device that identifies an individual based on physiological or behavioral attributes – fingerprint.

The certification will be in phases; each phase of the certification signed off before proceeding to next phase of the certification.

The key criteria for certification are:

PHASE I

A. GENERAL REQUIREMENTS.

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

The below are the particular documents required to be submitted along with the physical device(s) to be certified.

B. HARDWARE CERTIFICATION DOCUMENTS

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 finger print scanner type
5. Letter showing partnership between Vendor and Device Manufacturer.

C. DEVICE REQUIREMENT

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.

D. SOFTWARE REQUIREMENT

The following is required:

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

E. APPLICATION

1) 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 the physical copies of all requirements for biometric certification as captured in subheadings section **A, B,** C and **D**. **(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 DATES. IT IS IMPORTANT THAT ALL REQUIREMENTS BE OBTAINED BEFORE AN APPLICATION IS PUT FORWARD TO NIBSS FOR CERTIFICATION).**

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

PHASE II

1) Tests 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. **IF APPLICANT DOES NOT GIVE A FEEDBACK AND/OR RESOLVES ISSUE WITHIN 4 WEEKS, CERTIFICATION CYCLE IS CLOSED AND HAS TO START AFRESH WITH NEW PAYMENT.**

4) If there are no errors encountered during testing (hardware and software), test reports and sign off documents are prepared and forwarded for approval and a certificate issued.
5) In the event of an upgrade in the device, or change in the device firmware, or the software version, a recertification is required.

6) The applicant is contacted (via mail) to visit NIBSS Office for pick-up of the Certificate.

7) Original Certificate is issued and acknowledgment copies signed off by a representative of the company/applicant.

PHASE III

The institution is required to integrate to the BVN 1:1 Fingerprints API Integration for **verification test**.

For **Enrollment**, SDK for the certified device will be provided for integration into NIBSS Enrollment Application.

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

i. **API Integration Test**:

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

For this integration test, the following is required by the bank:

- The IP address of the person initiating the request from the Bank.
- Email address receiving the security credentials.
- Organization Code/Username Code – the code is only requirement for generating IV, AES key and password.

ii. Verification Test - Provision of (2) two or more person's valid bvns:

BVN are been provided by the bank during this test. The Institution provides valid BVNS (2 or more but not more than 10) of person(s) that will be used during verification.

The BVN Operation team is responsible for fetching and inserting the valid BVNS and its demography details into the staging environment in readiness for the test.

On confirmation, the final test scenarios for verification now commences. The bank sends a valid matching request (according to the technical specification) to NIBSS validation webservice for security checks before sent to staging environment for verification and response provided to the institution.

iii. 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.
c) Change Management is initiated when (a &b) have been completion. The SLA will be required for change management approvals.

F. CERTIFICATION FEE

A certification one- off fee - ₦1, 000, 000.00 naira (**One Million Naira**) per Device and the Version.

G. TIMELINE FOR CERTIFICATION

The timeline for Biometric Finger Print Scanner certification is Three (3) weeks after all requirements have been met by applicants as stated in section A, B,C and D.

Glossary

UAT - User Acceptance Test

BVN – Biometric Verification Number