



POS Functional Specification

APPROVED

Version: 1.2

Date: 2018-01-05

Status: Draft

Classification: Restrict

Reference: DCNIBSS00000011 (09-04-2018)

January 2018, NIBSS PLC.

The information contained herein is proprietary and shall not be duplicated, published or disclosed to any third party in whole or in part without its prior written consent, which shall never be presumed.

Plot 1230, Ahmadu Bello Way, Bar Beach, Victoria Island, P. M. B. 12617, Lagos

Phone: 234-1-2716071-4 / Fax: 234-1-2716075

Technical Data

Reference DCNIBSS00000011
 Document Title: POS Functional Specification
 Version: 1.2
 Status: Final
 Classification: Restrict
 Document type: Assessment
 Subject: POS Functional Specification
 Responsible area: Certification
 DCNIBSS00000011 – POS Functional
 Specification
 File name:

Authors and Participants

Name	Contact	Function
Modupe Akinola		Elaboration
Tope Adebayo		Revision
Christabel Onyejekwe		Approval

Distribution List

Name
NIBSS

Revisions

Version	Date	Description	Author
1.1	5/1/2018	Document creation	Modupe Akinola
1.2		Review	Tope Adebayo
1.2	22/03/2018	Approval	Christabel Onyejekwe

Document Control

S/N	Document Section	Changes	Version
1.	Section 3	CBN Minimum POS Specification – PCI – PED certification requirement level updated to 3.1.	1.1
2.	Section 1	Introduction	1.2
3.	Section 3	Payment Terminal Certification Requirements.	1.2
4.	Section 4	Payment Application Certification Requirements	1.2

Table of Contents

1. Introduction	5
1.1 Background	5
1.2 Reference Document(s)	5
2 General Requirements – Payment Terminal & Application Certification	6
3 Payment Terminal Certification Requirements.	7
3.1 Payment Terminal Certification Criteria.	7
3.2 Minimum Specification for POS Terminal	7
3.3 Minimum Specification for mPOS Terminal.	8
3.4 Payment Terminal Certification Process	8
3.5 Payment Terminal Certification Process Flow	8
4 Payment Application Certification Requirements	10
4.1 Payment Application Certification Process	10
4.2 Payment Application Certification Process	11
4.3 Payment Application Upgrade Re-Certification Process	12

APPROVED

This page intentionally left blank)

1. Introduction

1.1 Background

In August 2011, the Central Bank of Nigeria approved the **Guidelines on Point Of Sale (PoS) Card Acceptance Services** which amongst others, mandated Nigeria Inter-Bank Settlement System Plc (NIBSS) to act as the Payments Terminal Service Aggregator for the financial system.

In April 2016, the Central Bank of Nigeria approved the **Guidelines of operations of Electronic Payment Channels in Nigeria** which supersedes the previous standard and guidelines.

As the Payment Terminal Service Aggregator (PTSA), NIBSS is expected to be the only entity permitted to operate a Terminal Management System (TMS) and all payment terminals operating in Nigeria are required to connect to the PTSA. This is to ensure comprehensive oversight, reporting/performance monitoring, and also conforms to the objectives of shared industry infrastructure and best practice.

Consequently, NIBSS is responsible for the certification and re-certification of all payment terminals and applications on behalf of the Industry. This will ensure that payment terminals deployed in Nigeria meet all required certifications and the minimum POS specifications as defined in the CBN approved guidelines.

1.2 Reference Document(s)

- [1] Guidelines on Point Of Sale (PoS) Card Acceptance Services (August 2011)
- [2] Guidelines on operations of Electronic Payment Channels in Nigeria (April 2016)

2 General Requirements – Payment Terminal & Application Certification

1. Formal request for Payment Terminal / Application Certification.
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 loaded payment terminal for each payment application version supported.
10. Completed Certification Assessment Questionnaire.
11. Payment of Certification Fee

APPROVED

3 Payment Terminal Certification Requirements.

Each vendor must provide valid certificates, showing compliance with these standards, and must regularly review status of all its terminals, to ensure they are still compliant, as standards change.

The key criteria for Payment Terminal certification are:

1. Minimum Payment Terminal specification - Individual payment terminals / processing systems are checked to comply with the approved minimum requirements.
2. Industry standard / Global best practice - Individual payment terminals are checked to comply with de-facto Industry standards (EMV, MasterCard, Visa, etc.) based on global best practices.
3. Proof of valid EMV levels 1 & 2 Certification
4. Proof of valid PCI PED/PCI PTS Certification
5. Proof of valid PCI DSS for Third Party Processors
6. Proof of valid PA DSS (Payment Application Data Security Standard) certification - For PTADs that develop application to sell.
7. Detailed Specification of Payment Terminal.
8. Proof of valid MasterCard's Terminal Quality Management (TQM) Certification
9. Proof of valid VISA Approval Certificate
10. Other Assurance Certifications (FCC, etc.) and relevant backup documents (Security, Environmental, etc.).

3.1 Payment Terminal Certification Criteria.

1. Demonstrate local capacity to support hardware
2. Demonstrate local capacity to support payment software
3. Have SDK ready and installed on the device before delivering to NIBSS

3.2 Minimum Specification for POS Terminal

Parameters	Specifications in CBN Guidelines 2010
Card Readers	EMV Chip/Smart cards, Magnetic stripe. Optional: Contactless reader, 2 SIM Slots.
Communications	GPRS, Ethernet, Dial-up Modem. Optional: CDMA, Wi-Fi.
Certifications	EMV levels 1 & 2, PCI DSS, PA-DSS, PCI PED online & offline (All PCI certifications should be Level/Version 2.1 minimum).
Biometric	Upgradable to incorporate Fingerprint reader/scanner.
SIM Capacity	Must operate either a dual SIM or a roaming SIM.
CPU	ARM9/11, 32Bits. Optional: Dual Processors.
Memory	16MB Flash, 32MB SDRAM.
Keypad	PCI PED Approved, Backlit.
Display	TFT LCD graphics, 128/64 pixel, Backlit. Optional: Color screen.

Power	100- 240V, 50-60Hz, Optional: 24hrs Battery power, DC support, Car jack charger, Docking fast charger.
Printer	15 -18 lines per sec Thermal printer.
Multi-Application	Supports Multiple Applications.
Customization / Optional:	Coloured or branded housing, Labelling/embossing, RS232 & Others USB interfaces, Protocol implementation.

3.3 Minimum Specification for mPOS Terminal.

Parameters	Specifications
Card Readers	EMV Chip/Smart cards, Magnetic stripe, supporting audio jack interface and/or Bluetooth communications interface. Optional: Contactless reader.
Communications	GPRS, Dial-up Modem. Optional: CDMA, Wi-Fi.
Certifications	EMV levels 1 & 2, PCI DSS, PA-DSS, PCI PED online & offline (All PCI certifications should be Level/Version 2.1 minimum).
Printer	15 -18 lines per sec Thermal printer (optional). Means of notification should also support email/SMS notification.
Multi-Application	Supports Multiple Applications.
Customization / Others	Optional: Coloured or branded housing, Labelling/embossing, RS232 & USB interfaces, Protocol implementation.

3.4 Payment Terminal Certification Process

The Payment Terminal certification process comprises of the following stages:

1. Homologation process opening
2. Perform inspection and tests
3. Homologation Certificate

3.5 Payment Terminal Certification Process Flow

S/N	Activity
1.	Formal request for Payment Terminal (hardware) Certification
2.	Review and evaluation of request, based on General requirements and Payment Terminal Certification Criteria.
3.	Reply to request
4.	Due Diligence and Execution of Non-Disclosure Agreement
5.	Review of Terminal specifications
6.	Verify Terminal capabilities

7.	Carry out inspection checks
8.	Carry out EMV Levels 1 & 2 Validation checks
9.	Carry out PCI validation check
10.	Record and maintain repository for all evidences
11.	Review results
12.	Issue / Decline Certificate
13.	Update EMV and PCI approval renewal dates
14.	Validate EMV and PCI approval renewal

APPROVED

4 Payment Application Certification Requirements

FOR PTADS

1. PA DSS –Payment Application Data Security Standard: *Proof that payment application is compliant with Payment Application Data Security Standard (PA-DSS) certification.*
2. PCI DSS – Payment Card Industry Data Security Standard.
3. Triple DES – Data Encryption Standards should be the benchmark 23 for all data transmitted and authenticated between each party.
4. EMV – The deployed infrastructure must comply with the minimum EMV requirements.

FOR NON-PTADS

5. Detailed information of deployed payment application (version, release, specification, etc.).
6. Detailed payment application software architecture and specification document.
7. Proof that payment application conforms to secure coding, engineering, and testing Conventions.
8. Proof that payment application changes (especially major changes) follow formal change management processes that include security testing.
9. Proof that the SDLC (Software Development Life Cycle) followed secure SDLC and include protection from the Open Web Application Security Project (OWASP) - OWASP Top 10 – 2013 or 2017.

4.1 Payment Application Certification Process

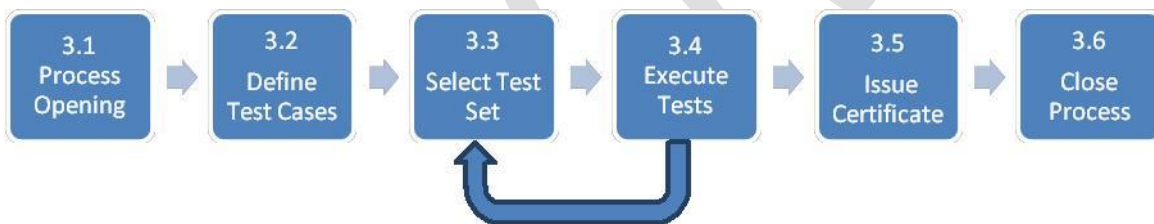
The Payment Application Certification process ensures that payment applications that successfully completes the certification process, complies with the minimum functional requirements for the operation of payment card acceptance services in Nigeria. Hence, only certified payment applications can be deployed into approved payment terminals.

The Payment Application Certification process flow involves the following stages:

1. Process Opening (open process for a new version/release to be certified);
2. Define test cases;

3. Select the test set (from the existing tests);
4. Execute Tests (perform the tests on the Payment Application and report results)
 - a. Report defects;
 - b. Evaluate the acceptance criteria:
 - i. Issue certificate and close process if the payment application has no defects.
 - ii. Restart the test for a new release until no defects were found or the acceptance criteria is achieved (If test fails after second iteration (three certification attempts), a service charge will apply for each unsuccessful subsequent attempts).
5. Issue Certificate (issue the payment application certificate);
6. Close Process

Figure 1 – Payment Application Certification Process Stages



4.2 Payment Application Certification Process

Key actions for the smooth implementation of Payment Application Certification process are:

S/n	Activity
1.	PTAD to present letter of intent (Request for certification)
2.	Review and evaluation of request, based on General requirements and Payment Terminal Certification Criteria.
3.	Respond to request
4.	Provide detailed information of all deployed payment application (version, release, Specification, etc) as at an agreed cut-off date (existing applications).
5.	Perform software application system integration tests (new applications)
6.	Due Diligence and Execution of Non-Disclosure Agreement
	Execute Certification Service Order form
7.	Schedule testing window with banks / processors
8.	Communicate to banks/processors to make test platforms available

9.	Configure Sample terminals to communicate with the Test platform
10.	Select and Run test cases
11.	Carry out tests and document results.
12.	Review Results
13.	Issue / Decline Certificate

4.3 Payment Application Upgrade Re-Certification Process

After any change / update on a certified payment application (following a formal change management process), the following re-certification process will apply.

S/n	Activity
1.	PTAD to formally communicate planned payment application upgrade/update
2.	Review and evaluation of request, based on General requirements.
3.	Respond to request
4.	Provide detailed information of payment application upgrade (version, release, specification, etc)
5.	Schedule testing window with banks / processors
6.	Communicate to banks/processors to make test platforms available
7.	Configure Sample terminals to communicate with the Test platform
8.	Select and Run test cases
9.	Carry out tests and document results.
10.	Review Results
11.	Issue / Decline Certificate
12.	Update payment application version/release central repository

NOTE:

Special consideration may be given to start-ups who do not meet all the requirements. This however will be treated based on individual merit.

CERTIFICATION TIMELINE:

S/N	Devices & Applications		
1.	POS Device and Application Testing	3 Weeks	After submission of certification questionnaire, and test completed by client using the POS Application Test Scripts
a.	POS Device Certification	1 Week	Upon submission of certification questionnaire.
b.	POS Application Certification	2Weeks	Upon submission of tests completed by client using the POS Application test scripts.