NATIONAL REGULATORY GUIDELINE FOR ELECTRONIC INVOICING IN NIGERIA

2025

Issued by
the National Information Technology Development Agency
as a co-regulatory instrument in collaboration with
the National Revenue Service

TABLE OF CONTENTS

1 This Guideline shall be described as 'National Regulatory Guideline for Electronic Invoicing in Nigeria'.

Long Title

2 This Guideline may also be cited as 'National e-Invoicing Guideline'.

Short Title

3 The Federal Government of Nigeria, through the National Information Technology Development Agency (NITDA), is committed to advancing a robust digital economy by promoting electronic governance and digital transformation across all sectors. In furtherance of this mandate, NITDA has developed the National Electronic Invoicing Guideline to serve as a foundational framework for regulators and stakeholders in Nigeria. This initiative is aimed at standardising electronic invoicing practices, enhancing system interoperability, and ensuring alignment with global standards, while upholding data security and safeguarding user privacy.

Explanatory Note

4 In the exercise of the mandate conferred on it by Section 6 of the National Information Technology Development Agency Act of 2007, (NITDA) in compliance with the provisions of Section 32 of the NITDA Act, hereby issues the following National e-Invoicing Guideline.

Authority

5 The implementation of this regulation shall commence on the First Day of September 2025.

Commencement

6 This Guideline applies to all stakeholders within the e-invoicing ecosystem in Nigeria, including but not limited to Access Point Providers, System Integrators, and end-users across public and private sectors.

Application and Scope

This guideline shall apply to the following entities:

i. Regulatory authorities seeking to implement or oversee e-invoicing systems.
ii. Service providers, including Access Point Providers and System Integrators.
iii. Any entity involved in the generation, transmission, processing, or utilisation of electronic invoices(e-invoices).

7 The objective of this Guideline is to establish a structured framework for the adoption, development, and administration of electronic invoicing (e-invoicing) in Nigeria. **Objectives**

8 In this Guideline, unless the context otherwise requires, the following terms shall have the meanings assigned to them below: **Definitions**

Access Point Providers mean entities responsible for the secure transmission of electronic invoices. They serve as gateways that connect business e-invoicing systems with the government-mandated e-invoicing infrastructure.

Accreditation means the formal process of granting permission to operate, typically as a prerequisite to licensing.

Data Breach is as defined under the Nigeria Data Protection Act 2023.

Data Controller is as defined under the Nigeria Data Protection Act 2023.

Data Processor is as defined under the Nigeria Data Protection Act.

e-invoicing means a digital process that replaces paper invoices by enabling the structured exchange and processing of invoices, credit notes and debit notes between buyers and sellers through integrated electronic invoicing solutions.

E-Invoicing Authorities are government institutions responsible for issuing, processing, or receiving electronic invoices, or for overseeing the implementation of e-invoicing systems within their respective sectors.

Gross Misconduct is any act or behavior constituting a serious breach of legal, ethical, or procedural standards as defined by relevant regulatory authorities.

Information Security Management Standards refers to internationally recognised frameworks that

enables organisations to protect their digital environment, including but not limited to ISO/IEC 27001 and the NIST Cybersecurity Framework.

License means a substantive authorisation granted by an e-Invoicing Authority to provide e-invoicing services.

Minimum Viable Product (MVP) means the basic version of a product developed to validate functionality, usability, and market acceptance.

Multi-Factor Authentication (MFA) means a security process that requires two or more distinct verification factors to authenticate a user.

Provisional License means a temporary authorisation granted pending the full evaluation and approval of a license application.

Schema means a standardised structure and content format for electronic invoices, enabling interoperability and compliance.

Service Level Agreement (SLA) means a formal agreement that defines the level, scope, and quality of service a Service Provider shall deliver to users.

Services means the offerings or functionalities provided by a Service Provider or an e-invoicing Authority under the scope of e-invoicing.

System Integrators are entities that provide software or hardware solutions compliant with e-invoicing regulations, capable of securely exchanging data via licensed Access Point Providers.

Service Provider refers to either a System Integrator or an Access Point Provider.

Tax Identification Number (TIN) is a unique number assigned to individuals or businesses by the tax authority for identification and taxation purposes.

User is an individual or business entity that uses e-invoicing services.

9 RESPONSIBILITIES OF THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY

NITDA shall perform the following responsibilities under this guideline:

i.	Accredit Service Providers to offer e-invoicing services in Nigeria, ensuring compliance with required standards and qualifications established and published by NITDA.	**Accreditation**
ii.	Exercise regulatory oversight on technical standards and technology platforms for e-invoicing and associated services.	**Technical Oversight**
iii.	Set the national requirements and specifications for e-invoicing, ensuring interoperability and compatibility within the national and international e-invoicing ecosystem.	**National Requirements**
iv.	In collaboration with relevant authorities, define the standardised national schema, outline the structure and content of all e-invoices within Nigeria, and promote uniformity and data integrity.	**Schema Development**
v.	Maintain and publish a comprehensive list of accredited Access Point Providers, and System Integrators in Nigeria.	**Registry**
vi.	Ensure that service providers adhere to established national e-invoicing standards. Through conducting regular audits and inspections among other measures.	**Compliance**
vii.	Where applicable, mandate that the Service Provider comply with relevant international e-invoicing standards to facilitate cross-border e-invoicing.	**Adherence to International Standards**
viii.	Issue guidelines for systems and structure for exchanging e-invoicing data in Nigeria and ensure that any such transmission of invoicing data electronically outside Nigeria complies with standards as issued or ratified by NITDA.	**Data Exchange Standards**
ix.	Provide support and information to users, assisting them in understanding and utilising e-invoicing systems effectively.	**User Standards**

10 ACCREDITATION OF SYSTEM INTEGRATORS

This section outlines the rules for obtaining accreditation as a System Integrator to operate within the Nigerian e-invoicing ecosystem.

General Rules

i. No entity shall operate as a System Integrator without prior accreditation by NITDA.
ii. System Integrators must ensure that their software is tested and approved by a licensed Software Quality Assurance firm.
iii. NITDA shall issue a licence to each accredited System Integrator for two years, renewable on similar or new terms to be issued later.
iv. Application for accreditation shall be made to NITDA using the prescribed form.
v. NITDA shall initially issue a provisional licence pending technology platform examination after the demo before issuing a final licence and code.
vi. System Integrators are encouraged to comply with information security and quality management standards.

Qualification for Accreditation

11 System Integrators must ensure secure, scalable, and interoperable systems that meet regulatory requirements. They must implement strong cybersecurity measures, including encryption and access controls. Solutions should support seamless data exchange across platforms and environments. High availability, reliability, and performance must be prioritized. Additionally, System Integrators must:

i. Pay a non-refundable application fee of One Million Naira only to NITDA or such other amount as NITDA may specify from time to time.
ii. Fill a duly and properly completed accreditation form.
iii. Show evidence of registration with the Corporate Affairs Commission, including the Memorandum and Article of Association, with a minimum paid-up share capital of 10 million Naira (N10,000,000.00) only.
iv. Ensure that the company's objectives as contained in its memorandum and articles of association shall include digital technology services.

v. Ensure that Nigerians shall hold a minimum of one-third of the company's share capital.
vi. Provide detailed manuals and policies, including but not limited to operations manual, dispute resolution protocols and whistle-blowing policy.
vii. Provide evidence of compliance with the Nigeria Data Protection Act 2023.
viii. Demonstrate organizational capacity and technical expertise to provide e-invoicing services.
ix. Show evidence that at least one director must have five years of experience in digital technology service provision.
x. Ensure that none of its directors has been declared bankrupt or convicted of any offence involving fraud.

12 Where a system integrator has successfully fulfilled the requirements for accreditation; **Post Accreditation**

i. NITDA may issue a provisional licence after presenting evidence of payment of the acceptance fee and subsequently issue a final licence and code to the System Integrator.
ii. The System Integrator must affix their license number on all products and services delivered to users to facilitate data transmission through an Access Point Provider.
iii. Comply with all other requirements as stipulated by NITDA from time to time.
iv. If there is a data breach, the System Integrator must report it to the relevant authorities via email or an appropriate channel.
v. All notifications should be directed to the Director General in the prescribed format.

13 NITDA shall issue licences under the following conditions subject to the satisfaction of the licensing conditions issued by the Agency: **Licensing**

i. A Provisional License will be issued for six months for commencement of service, testing, and other pre-operational procedures.
ii. The System Integrator may apply for an extension of the Provisional License for three months after the expiration of the initial term. However, no further extensions shall be granted.

iii. A System Integrator unable to secure the full licence after the extension expires must submit a fresh application for licensing and pay the applicable license fees under this guideline.
iv. The full licence to operate as a System Integrator shall be valid for two years and subject to renewal after meeting all renewal requirements.
v. NITDA shall issue a license number, which will be found on the licence.

14 Subject to the provisions of this Guideline: **Refusal to Issue Licence**

i. NITDA may refuse to register and issue a licence, and it shall notify the applicant in writing of its decision, stating the reason for the refusal.
ii. Where NITDA refuses to register and issue a licence due to a non-material defect in the application, it may, in the notice, require the applicant to rectify the application within 12 working days.
iii. NITDA also reserves the right to withdraw, suspend, or revoke the full or provisional licence after it has been issued if there is a violation of the terms and conditions as contained in the licence.
iv. In any instance of such a licence being suspended, withdrawn, or revoked, NITDA shall provide a written basis for its action.

15 Subject to the provisions of these guidelines; **Renewal of Licenses**

i. The renewal of the licence shall be every two years.
ii. The approval shall be as of right where the System Integrator has done the following:
    a. Maintain the paid-up share capital.
    b. No outstanding or unresolved conflicts, including, but not limited to, court cases.
    c. Meet all requirements, including audit and clearance by all relevant regulatory authorities.

16 NITDA may terminate the licence of a System Integrator as follows: **Termination of Licenses**

i. If the System Integrator breaches any relevant provisions or has failed to comply with a provision of this guideline.

ii. If at any point any of the accreditation requirements are unremedied for four months from the date of notice.
iii. If there is any complaint of gross misconduct in their operation or breach of personal data and privacy.

17 ACCREDITATION OF ACCESS POINT PROVIDERS

This section outlines the general rules for obtaining accreditation as an Access Point Provider to operate within the e-invoicing ecosystem in Nigeria.

General Rules

i. No entity shall operate as an Access Point Provider without prior accreditation by NITDA.
ii. Access Point Provider must ensure that the software they use is tested by a licensed software quality assurance firm..
iii. NITDA shall issue a unique code to each accredited Access Point Provider for two years, renewable on similar or new terms to be issued later.
iv. Application for accreditation shall be made to NITDA using the prescribed form.
v. Access point providers are encouraged to comply with information security and quality management standards.
vi. NITDA reserves the right to review testing report on every platform to assess security, user-centricity, and ease of use before granting accreditation.

Qualification for Accreditation

18 A company shall not qualify to apply for accreditation as an Access Point Provider unless the company complies and meets all the following requirements:

i. Pay a non-refundable application fee of One Million Naira only, or such other amount as NITDA may specify from time to time, payable to NITDA.
ii. Duly and properly completed accreditation form.
iii. Evidence of registration with the Corporate Affairs Commission, including the Memorandum and Article of Association, with a minimum paid-up share capital of 100 million Naira only.

iv. The company's Objectives shall include digital technology services, in the memorandum and article of association.
v. Following Section 13 (2) (d) of the Nigerian Start-up Act 2022, Nigerians shall hold one-third of the company's shares.
vi. The company must present a Minimum Viable Product (MVP) for e-invoicing.
vii. The company must provide evidence of compliance with the Nigeria Data Protection Act.
viii. Detailed manuals and policies, including but not limited to operations manual, dispute resolution protocols and whistle-blowing policy.
ix. Demonstrate organizational capacity and technical expertise to provide e-invoicing services.
x. Board of Directors: At least one director must have five years of experience in digital technology service provision.
xi. Director Eligibility: Directors must not have been declared bankrupt or convicted of fraud.
xii. NITDA is expected to review and vet all documents submitted by the company and inform the company within ten (10) days of the application's status. Where there is an issue with the application, NITDA shall notify the company to rectify the defect within five (5) days and submit the application. After the resubmission, NITDA shall review the application within five days and determine its status.

19 **Post-Accreditation of Access Point Providers**

i. NITDA may issue a provisional accreditation after presenting evidence of payment of the acceptance fee and subsequently issue a final accreditation and code to the Access Point Provider.
ii. The Access Point Provider shall present the code to the E-Invoicing Authorities for onboarding on the e-invoicing Platform.
iii. Comply with all guidelines and regulations issued by NITDA.
iv. Notify NITDA upon commencement of operations.
v. Provide periodic Audit Report as prescribed by NITDA.

vi. All notifications should be directed to the Director General in the prescribed format, available on the NITDA Access Point Provider Registration Platform.

20 The entity shall:

Responsibilities of Other e-invoicing Authorities

i. Develop and implement guidelines based on this framework, tailored to their sectors.
ii. Ensure their stakeholders comply with NITDA's standards.
iii. Collaborate with NITDA on technical oversight, data exchange or any relevant tech related issue.
iv. Provide user education and support to enhance adoption.
v. Ensure that their e-invoicing platform is tested and approved by a National Software Quality Assurance firm.
vi. Issue licence to access point providers accredited by NITDA.

21 The Access Point Provider shall comply with general technology standards issued by the E-Invoicing Authorities and ensure that:

Technology Requirements for Access Point Providers

i. All e-invoicing Access Point Providers shall ensure end-user transaction data is transmitted securely and encrypted at all times, in line with technical documentation, and that all end users implement multi-factor authentication to safeguard the integrity of the invoicing process.
ii. The e-invoice technology deployed must comprise a set of interoperable infrastructures.
iii. The e-invoice technology deployed must ensure that end users get the E-invoice after a successful transaction.
iv. They provide immediate notification if an e-invoice transaction fails.
v. They conduct periodic vulnerability and penetration tests on their technology infrastructure and present evidence of this report during inspections and audits.
vi. They implement adequate measures to mitigate all risks arising from deploying and using their Information Technology architecture.

vii. They demonstrate compliance with the Nigeria Data Protection Act 2023 provisions, which regulate the lawful processing of personal data.

viii. If there is a data breach, the Access Point Provider must report it to the relevant authorities via email or appropriate channel.

ix. They use best practices to ensure the safety of all data.

i. Access Point Providers must use the standardised national schema for transmitting e-invoice to ensure consistency and accuracy. The standardised national schema shall include the following:
   a. Invoice date;
   b. Business name and address;
   c. Customer's business name and address;
   d. Unique invoice number;
   e. Payment due and the terms, including payment method; and
   f. Description of the services provided.

22 PROCESSING OF ELECTRONIC INVOICES

Registration of New Users

i. New Users are required to acquire a Tax Identification Number (TIN) from **FIRS.**

ii. The Access Point Provider shall issue a unique Business ID to the new User, which will be generated on the E-Invoicing Authorities platform. The code will be the user's standard identification within the e-invoicing system.

iii. The new user can use any System Integrator product or service and any Access Point Provider to consume e-invoicing services.

iv. If a new user has multiple branches of the same business at different locations, the user may create multiple sub-users under his account.

v. A non-resident who makes taxable supplies to Nigeria must obtain a Tax Identification Number (TIN) and include value-added tax (VAT) on its invoice for all taxable supplies.

23 Duties of Access Point Providers

i. Create and maintain gateways that function as access nodes on the e-invoicing network.

ii. Comply with the standard issued by NITDA and E-Invoicing Authorities.

iii. Authenticate users through a dedicated authentication mechanism.

iv. Protect their network security with the latest and most efficient features and prevent intruders from unauthorised access.
v. Use the recent encryption standards to protect users' data and communication.
vi. Provide dispute resolution and robust customer support channels
vii. All electronic data, including users' records, access codes, logs, and invoice data, must be encrypted and stored or backed up on servers or data centres in Nigeria.

24 COMPLIANCE REQUIREMENTS

i. Quality of Service: E-Invoicing Authorities shall have the authority to conduct investigations into the quality of service, or the compliance of technology platforms provided by an Access Point Provider.
ii. Complaint Reporting: An Access Point Provider is obligated to address and resolve any consumer complaint within forty-eight (48) hours of receiving it. E-invoicing Authorities retain the discretion to investigate any complaint lodged by an end-user arising from the failure.
iii. Assessment: As a compliance measure to ensure adherence to the stipulations of this framework and guideline by Access Point Providers, an assessment shall be conducted as determined by E-Invoicing Authorities.
iv. Reporting: Each Operator shall furnish E-Invoicing Authorities with quarterly reports detailing its platform performance. Such reports should be submitted electronically to the E-Invoicing Authorities portal quarterly. Platform performance indices will include Security incidences, monthly average uptime, number of bug fixes monthly, number of technology patches and updates monthly, system failures, system upgrades, add-ons, records of customer support and user complaints.
v. Audit: E-Invoicing Authorities reserves the right to audit all or a portion of the quality-of-service data obtained from an Access Point Provider. In discharging its duties, E-Invoicing Authorities may modify the frequency of data

collection, the subject services and parameters, network segments, and reporting intervals subject to audit.

25 SERVICE AVAILABILITY

i. Uptime Guarantee: the Access Point Provider commits to an uptime of 99.9%per calendar month.
ii. Maintenance: Scheduled maintenance will be performed during off-peak hours, with 48-hour advance notice to the Client.

26 PERFORMANCE METRICS FOR SERVICE PROVIDERS

i. Invoice Processing: Invoices will be processed and transmitted within 1 (24 Hours) business days from receipt.
ii. Issue Resolution: Any issues or errors in processing will be resolved within 2 (48 Hours) business days of notification.
iii. Response Time: Support requests will be acknowledged within 1 hour, resolved within 6 hours for critical issues, and within 1 (24-hour) business day for non-critical issues.
iv. Support Channels: Support will be available 24hours through [e.g., email, phone, online portal]

27 DISCONNECTION OF ACCESS POINT PROVIDER

Guiding Principles

i. E-Invoicing Authorities shall be guided by the need to ensure that the interests of the affected users are protected when approving an Access Point Provider's disconnection.
ii. Other relevant issues that will guide the decision include the public interest in observing the rule of law and E-Invoicing Authorities to entrench good corporate governance practices among Service Providers.

Pre-Disconnection Notice

i. The Pre-Disconnection Notice to Access Point Providers shall be issued in all circumstances where an E-Invoicing Authorities has approved the disconnection of an Access Point Provider due to poor quality service or breach of this guideline.
ii. Similarly, E-Invoicing Authorities may issue a notice directing Users to onboard another Service Provider in the event of poor-quality service, product failure, or a breach of this guideline.
iii. Upon issuing such notice, E-Invoicing Authorities shall, at its discretion, allow a grace

period not exceeding twelve (12) working days within which the Users would be at liberty to decide to migrate to another Service Provider.

iv. In every case where notice is given to an Access Point Provider, such notice shall include a directive to settle all the issues that resulted in the Provider's disconnection, failing which notice of the disconnection shall be published on the E-Invoicing Authorities website.

28 **Partial Disconnection**

i. Where E-Invoicing Authority approves the disconnection of an Access Point Provider, it reserves the right to authorise a partial disconnection on terms to be decided by the E-Invoicing Authority.

ii. For the purpose of this guideline partial disconnection shall be limited to the disconnection of only outbound e-invoices from the sender Access Point Provider to the receiver Access Point Provider.

iii. The e-invoicing platform shall provide data retrieval, archiving and transfer modalities for safekeeping and business continuity to ensure continuous availability.

29 COMPLIANCE AND ENFORCEMENT

Noncompliance with this Guideline shall result in penalties, which include fines, remedial actions, disconnection of Service, or other appropriate measures to be provided in the licence issued by the E-Invoicing Authority.

30 REVIEW OF GUIDELINES

This Guideline shall be periodically reviewed and updated by NITDA, in collaboration with relevant E-Invoicing Authorities, to reflect technological advancements, regulatory changes, and stakeholder feedback.

APPENDIX 1
OPERATOR GUIDELINES

A. Service Description for System Integrator

a) The primary responsibility of a System Integrator is to integrate the business's internal systems, such as Enterprise Resource Planning (ERP) systems, with the E-Invoicing Authorities e-invoicing System. This involves mapping the relevant business processes and data fields to the e-invoice system schema to ensure data compatibility and accurate transmission in accordance with the Universal Business Language (UBL).

b) System Integrators are required to do the following:

1) ERP Compatibility: Ensuring taxpayers' ERP systems and other financial management tools can generate invoices that meet the required format and standards. This includes customising or updating ERP configurations to meet technical specifications for e-invoicing.
2) Data Mapping: Defining the data flow between the internal systems and the e-invoicing platform. Every invoice element (taxpayer details, transaction amounts, and VAT calculations) is correctly mapped to E-Invoicing Authorities' standardised fields.
3) Secure Data Transmission: Facilitating the safe transfer of e-invoices from the business's systems to E-Invoicing Authorities through an Access Point Provider (APP). APPs act as intermediaries to validate and transmit e-invoice data. The System Integrator ensures seamless integration with the Access Point Providers and complies with security protocols, such as OAuth 2.0 authentication.
4) Troubleshooting and Monitoring: System Integrators are responsible for continuously monitoring the data flow to ensure uninterrupted invoice submission. They troubleshoot issues related to data validation, system downtime, or transmission errors, ensuring that invoices are sent on time and comply with regulations.

c) Legal and Technical Standards

1) Critical to the System Integrator's role is ensuring that all systems comply with the technical and legal standards defined by e-invoicing regulations. This includes ensuring that invoices are transmitted and stored securely and include the necessary cryptographic features to prevent tampering.
2) Digital Signature Implementation: System Integrators must ensure that invoices generated are digitally signed using cryptographic techniques. This includes applying a

cryptographic stamp identifier (CSID) and a digital signature to verify the invoice's authenticity. E-Invoicing Authorities may require using the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure the integrity of e-invoices.

3) Compliance with XAdES and PAdES Standards: e-invoices must adhere to specific formats for electronic signatures, depending on whether they are in XML (Extensible Markup Language) or PDF/A-3 format. XML invoices must use XAdES (XML Advanced Electronic Signatures), while PDF invoices should comply with PAdES (PDF Advanced Electronic Signatures). System Integrators are responsible for implementing these formats to ensure that invoices are legally binding and verifiable.
4) OAuth 2.0 Authentication: To maintain secure communication between a taxpayer's ERP and the E-Invoicing Authorities' platform, the System Integrator must implement OAuth 2.0 authentication. This ensures that only authorised users and systems can interact with the platform, minimising the risk of unauthorised access or fraud. The Client ID and Secret Key generated during onboarding must be securely stored to prevent misuse.
5) Data Validation and Reporting: System Integrators are also tasked with ensuring that the data submitted through the e-invoicing system is valid and complies with data standards. This includes verifying that all mandatory fields are completed, ensuring accuracy in calculating taxes and VAT, and checking that the invoice follows the structure required.

d) Cryptographic Security and Data Protection

1) Security is paramount in e-invoicing. The system integrator plays a significant role in ensuring secure communication between invoicing systems and E-Invoicing Authorities using digital certificates and cryptographic signatures. Each invoice transmitted must be validated and stamped to maintain data integrity.
2) Key Generation and Management: System Integrators are responsible for generating and managing the public and private keys used in cryptographic stamping. Keys must be generated in compliance with FIPS 186 standards, and the private key used for signing invoices must be securely stored in a Hardware Security Module (HSM) or another secure method. Keys must be kept confidential, and any unauthorised export or use of keys must be strictly prohibited.

3) Onboarding – Digital Certificate Issuance and Renewal: The integration process involves requesting digital certificates for cryptographic stamps through the E-Invoicing Authorities' platform. The System Integrator must ensure that digital certificates are issued, installed, and renewed before expiration. Digital certificates validate the identity of the business sending the invoice and ensure that the invoice has not been altered after signing. This process involves generating and submitting One-Time Passwords (OTPs) for each device and managing Certificate Signing Requests (CSRs) to ensure each taxpayer's system is compliant.
4) Certificate Revocation Management: If a certificate is compromised, the System Integrator must revoke the digital certificate by submitting a revocation request through the E-Invoicing Authorities' platform. System Integrators are also responsible for monitoring the status of certificates through Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) responders to ensure they remain valid.

e) Error Handling and Troubleshooting
System Integrators must develop robust processes for detecting and resolving errors that arise during invoice generation, validation, and transmission. The error-handling responsibilities include.
1) Validation Errors: If an invoice fails validation due to missing data, incorrect formats, or non-compliance with E-Invoicing Authority's regulations, the System Integrator must identify the error, correct it, and resubmit it. These validation processes ensure that businesses remain compliant and that all submitted invoices are processed correctly.
2) System Downtime and Failures: If the ERP system or eInvoicing platform experiences downtime, System Integrators must ensure that invoices can still be generated and stored until they can be submitted. This might involve creating offline storage systems or temporary solutions to manage invoice data.
3) Real-Time Support: System Integrators must provide real-time support to address issues as they arise, ensuring minimal disruption to business operations. This includes continuous monitoring of the system's health and performance, particularly during peak submission periods when businesses must submit multiple invoices simultaneously.

f) Compliance Monitoring and Reporting

1) Ensuring ongoing compliance with the regulations

The e-invoicing guidelines for UBL invoice format and the legal frameworks under Section 25, Part 5 of the Tax Administration and Enforcement Act 2007, which govern the e-invoice implementation, is, therefore, the core responsibility of the SI. System Integrators must:

i. Monitor Compliance: System Integrators monitor the system for compliance with E-Invoicing Authority's guidelines and standards, ensuring that all invoices meet legal requirements. This includes ensuring that invoices are submitted in the correct format, that all necessary data fields are completed, and that the invoice is digitally signed.

ii. Auditing and Reporting: System Integrators maintain audit logs of all invoices generated and transmitted to the E-Invoicing Authorities, platform. These logs provide evidence showing that the business complies with e-invoice regulations. System Integrators also create reports for both internal use and external audits by the E-Invoicing Authorities.

iii. System Updates: System Integrators are responsible for updating the integration to accommodate changes in E-Invoicing Authorities' regulations. This might involve adjusting data formats, updating encryption standards, or modifying workflows to comply with new tax rules.

APPENDIX 2
STANDARDISED NATIONAL SCHEMA AND NAMING CONVENTIONS

1. Structure of Naming Convention
   The e-invoicing system employs a standardised naming convention to ensure consistency, clarity, and ease of use across all aspects of invoice processing. By adhering to these conventions, users can streamline their operations, reduce errors, and maintain compliance with international standards.

   A. Purpose of Naming Conventions
   Naming conventions serve multiple purposes, including:
   - I. Standardisation: Ensuring uniformity in naming across the system.
   - II. Clarity: Making it easier to understand and locate specific invoices and related documents.
   - III. Compliance: Meeting regulatory requirements and international standards.

   B. Arrangements for Naming Conventions
   - I. Invoice Identifier: Each invoice is assigned a unique code for tracking and referencing. Format: INV[Sequential Number] Example: INV0001
   - II. Access Point Provider Identifier: A unique code assigned to each Access Point Provider. Format: Alphanumeric Example: B4B37F28
   - III. Time Stamp: Based on the invoice's issued date. Format: YYYYMMDD. Example: 20240623

   C. Importance of Naming Conventions
   Naming conventions are vital for several reasons:
   - I. Efficiency: Facilitates quick and accurate retrieval of invoices.
   - II. Data Integrity: Prevents duplication and errors in invoice processing.
   - III. Regulatory Compliance: Ensures adherence to national and international standards, such as the Harmonized System of Nomenclature (HSN).

   D. Implementation Guidelines
   - I. Follow the Format: Adhere strictly to the specified formats for each identifier.
   - II. Verify Accuracy: Double-check codes and identifiers to ensure they are correct and up-to-date.
   - III. Consistent Application: Apply naming conventions consistently across all documents and systems.

IV. By following these naming conventions, users can ensure their invoicing processes are streamlined, compliant, and efficient.

2. Adopted Standards for E-Invoicing in Nigeria

The Nigerian e-invoicing regulation adopts several international standards to enhance interoperability, security, and efficiency in the invoicing process. These standards ensure the system meets global best practices and regulatory requirements, facilitating smooth and reliable operations.

Key Standards Adopted

I. Harmonized System of Nomenclature (HSN) Codes
   a. Purpose: Standardizes the classification of goods for international trade.
   b. Structure: Six-digit codes, extendable by countries for more specific categorisation. Example: '01' for live animals, '0101' for live horses, asses, mules, and hinnies, '010121' for purebred breeding horses.
   c. Benefits: Ensures uniform classification, simplifies customs procedures, aids in trade data analysis, and determines applicable tariffs and taxes.

II. ISO 27001/2022 (Information Security Management)
   a. Purpose: Provides a framework for managing information security.
   b. Benefits: Protects sensitive data, ensures compliance with security regulations, and mitigates risks associated with data breaches.

III. ISO 20022 (Financial Services Messaging)
   a. Purpose: Standardizes electronic data interchange between financial institutions.
   b. Benefits: Enhances the efficiency and interoperability of financial transactions, reduces errors, and facilitates regulatory compliance.

IV. Universal Business Language (UBL)
   a. Purpose: Standardizes the format for electronic business documents.
   b. Benefits: Ensures compatibility with various e-commerce systems, reduces the need for custom integration, and supports global supply chain processes.

V. Implementation of Standards
   a. System Integration: Ensure the e-invoicing system is integrated with the above standards to maintain consistency and reliability.
   b. Compliance Checks: Regularly audit the system to verify compliance with the adopted standards.
   c. Continuous Updates: Stay informed about updates to these standards and implement changes promptly to remain compliant.

3. Further Notes on Harmonised System of Nomenclature (HSN) Code

The HSN Code (Harmonized System of Nomenclature) is an internationally recognised system for classifying goods. It was developed by the World Customs Organization (WCO) to facilitate the standardisation of trade and taxation globally. The HSN system helps systematically identify and classify goods for tax and customs purposes.

I. The HSN code consists of 6 to 8 digits:
   a. The E-Invoicing Authorities .t two digits represent the chapter under which the goods are classified (99 chapters).
   b. The following two digits represent the heading within the chapter.
   c. The following two digits represent the product category within the heading.
   d. Additional two digits (in some jurisdictions or industries) further classify local use.

II. Purpose:
   a. Used for the classification of goods in international trade.
   b. Facilitates the collection of accurate trade data and levying of tariffs and taxes.
   c. Helps streamline trade documentation and customs clearance.

III. Application:
   a. Import and Export: The HSN code is used globally in import and export documentation.
   b. GST (Goods and Services Tax): HSN codes are also used in indirect taxes to identify taxable goods and their applicable tax rates.
   c. Businesses and governments consistently classify products across borders and within tax regimes using standardised HSN codes.

IV. Importance of HSN
   a. Verify Signed Invoice allows businesses to validate the authenticity and integrity of e-invoices issued by suppliers. This verification process confirms that the e-invoice has been digitally signed by the E-Invoicing Authorities and has not been tampered with.
   b. Verify Signed Invoice allows businesses to validate the authenticity and integrity of e-invoices issued by suppliers. This verification process confirms that the e-invoice has been digitally signed by the E-Invoicing Authorities and has not been tampered with.

V. Utilising the Global Standard
   a. The Merchant Buyer Solution allows businesses to generate and issue compliant customer invoices. However, before these invoices can be issued, businesses must E-Invoicing Authorities .t be enabled to invoice electronically on the MBS system by

submitting the required information through the E-Invoicing Authorities' self-service portal.

b. The Merchant Buyer Solution allows businesses to generate and issue compliant customer invoices. However, before these invoices can be issued, businesses must E-Invoicing Authorities .t be enabled to invoice electronically on the MBS system by submitting the required information through the E-Invoicing Authorities' self-service portal.

VI. Requirements of HSN for E-Invoicing in Nigeria

a. The Merchant Buyer Solution allows businesses to generate and issue compliant customer invoices. However, before these invoices can be issued, businesses must E-Invoicing Authorities .t be enabled to invoice electronically on the MBS system by submitting the required information through the E-Invoicing Authorities' self-service portal.
b. Businesses can navigate to the IRN Validation section on this self-service portal to verify a signed invoice. This section will prompt the user to enter the Invoice Reference Number (IRN) assigned to the e-invoice by the MBS system.
c. After inputting the IRN, the user clicks the 'Submit' button to initiate the verification process. The system then cross-checks the provided IRN against its database to validate the digital signature associated with the e-invoice.
d. If the IRN is valid and matches the E-Invoicing Authorities' records, the system will display a QR code, a green check mark, or a message indicating 'This is a Digitally Signed Invoice. 'The QR code confirms that the e-invoice is authentic and has been digitally signed by the E-Invoicing Authority, guaranteeing its legitimacy and integrity.
e. However, the system will display an appropriate error message if the provided IRN contains discrepancies or errors or if the digital signature verification fails. This could indicate that the e-invoice is invalid, has been tampered with, or has not been reported to the E-Invoicing Authority through the MBS platform.

MADE AT ABUJA This 26th Day of August 2025

Kashifu Inuwa Abdullahi CCIE
Director-General
National Information Technology Development Agency (NITDA)