Layer21 APP API Developer Guide

Access Point Provider (APP) Service — e-Invoicing Integration with FIRS

Layer21 Global Limited

RC No: 7253971
Tagline: *Innovating Compliance & Integration*
Address: 16 Unity Crescent, Off Unity Road, Ilorin, Kwara State, Nigeria
Tel: +234 811 192 2822 **Email:** support@layer21.com **Web:** www.layer21.com

---

1. Overview

The **Layer21 Access Point Provider (APP)** API enables authorized Systems Integrators (SIs) and taxpayers to securely transmit electronic invoices to the **Federal Inland Revenue Service (FIRS)** through the Layer21 platform.

This API ensures:

- End-to-end data integrity and confidentiality.
- Compliance with FIRS e-Invoicing standards.
- Scalable and secure processing for large volumes of invoices.
- Real-time acknowledgment handling between SI → APP → FIRS → back.

---

2. API Environment Setup

Environment	Base URL	Description
Production	`https://api.layer21.com/app`	Live FIRS-validated endpoint for production traffic.
Sandbox	`https://sandbox.layer21.com/app`	Layer21-hosted testing environment for ERP vendors.
Local Dev	`http://localhost:5000/app`	Local instance for developer testing and debugging.

All API requests must use **HTTPS** and include valid **JWT (RS256)** authorization headers.

---

3. Authentication

JWT Authorization Header

All requests must include the following header:

```
Authorization: Bearer <JWT_TOKEN>
Content-Type: application/json
```

Token Claims Example

```
{
  "iss": "layer21-si",
  "sub": "erp_client_001",
  "role": "integrator",
  "exp": 1735665999
}
```

Notes:

- The **public key** used for verifying RS256 signatures is shared with FIRS and partner SIs.
- Tokens expire after 60 minutes by default.

---

4. Core API Endpoints

4.1 POST /v1/invoices/submit

Description

Accepts invoice payloads from SI systems, validates them, and forwards to FIRS for acknowledgment.

Request Body

```
{
  "invoiceId": "INV-2025-00023",
  "supplierTin": "12345678-0001",
  "buyerTin": "23456789-0002",
  "invoiceDate": "2025-10-11T10:22:00Z",
  "currency": "NGN",
  "totalAmount": 550000.00,
  "vatAmount": 41250.00,
  "items": [
    {
      "description": "HP EliteBook 840",
```

```
      "quantity": 2,
      "unitPrice": 275000.00,
      "vatRate": 7.5
    }
  ],
  "signature": "RS256_BASE64_SIGNATURE"
}
```

Response

```
{
  "status": "success",
  "firsAckId": "ACK-123456789",
  "validationStatus": "accepted",
  "timestamp": "2025-10-11T10:22:58Z"
}
```

Error Codes

Code	Message	Meaning
400	INVALID_SCHEMA	JSON structure or field missing
401	INVALID_SIGNATURE	JWT validation failed
422	COMPLIANCE_ERROR	VAT or TIN validation failed
500	FIRS_ENDPOINT_ERROR	FIRS endpoint unreachable

4.2 GET /v1/invoices/status/{invoiceId}

Description

Retrieves validation and acknowledgment status of a submitted invoice.

Response Example

```
{
  "invoiceId": "INV-2025-00023",
  "status": "accepted",
  "firsAckId": "ACK-123456789",
  "validationTimestamp": "2025-10-11T10:22:58Z"
}
```

4.3 POST /v1/firs/ack

Description

Receives acknowledgment notifications from FIRS and updates invoice status.

Example Payload

```
{
  "firsAckId": "ACK-123456789",
```

```
  "invoiceId": "INV-2025-00023",
  "status": "accepted",
  "remarks": "Validated successfully",
  "timestamp": "2025-10-11T10:25:00Z"
}
```

Expected Response

```
{ "status": "acknowledged" }
```

4.4 GET /v1/healthz

Description

Simple health check endpoint to verify API availability.
Response: `{"status": "ok"}`

4.5 GET /v1/metrics

Description

Prometheus-compatible metrics for system monitoring and performance tracking.

Sample Output

```
app_requests_total{status="200"} 23456
app_requests_failed{status="500"} 32
```

---

5. Security & Compliance

Layer21 implements the following controls:

- **Encryption:** All API traffic uses TLS 1.3.
- **Authentication:** RS256 JWT signatures, verified per request.
- **Authorization:** Role-based access (Integrator, Admin, Auditor).
- **Data Storage:** Encrypted PostgreSQL database (AES-256 at rest).
- **Audit Trail:** Immutable logs for every transaction.
- **Rate Limiting:** 200 requests/min per SI key.
- **Monitoring:** Real-time Prometheus & Grafana dashboards.
- **Compliance:** NDPR, FIRS MBS, and NITDA Cybersecurity Guidelines.

---

6. Developer Tools

Testing Environment

Developers can use the sandbox environment for testing:
`https://sandbox.layer21.com/app`

Sandbox supports simulated FIRS acknowledgments and sample payloads.

Sample Test JWT

```
export TOKEN=$(curl -X POST https://sandbox.layer21.com/app/auth/test-
token)
curl -X POST https://sandbox.layer21.com/app/v1/invoices/submit \
  -H "Authorization: Bearer $TOKEN" \
  -H "Content-Type: application/json" \
  -d @invoice.json
```

---

7. Versioning & Updates

Version	Status	Notes
v1.0	Active	Initial release for SI-to-FIRS integration
v1.1	Planned	Bulk invoice submission & webhook retries

All API changes are backward compatible. Clients will receive 30-day notice before any version deprecation.

---

8. Support & Contact

Department	Email	Availability
Technical Support	support@layer21.com	24/7
Developer Relations	dev@layer21.com	Mon–Fri, 9AM–6PM
Incident Escalation	ops@layer21.com	Immediate response (P1 issues)

---

9. Legal & Compliance

All API usage is governed by:

- FIRS e-Invoicing compliance framework.
- Layer21’s internal Information Security Management Policy.
- Nigeria Data Protection Regulation (NDPR 2019).

Misuse of access credentials or unauthorized data processing constitutes a breach under Section 37 of the Nigerian Constitution and NDPR enforcement guidelines.

---

10. Appendix: API Flow Diagram (Text Description)

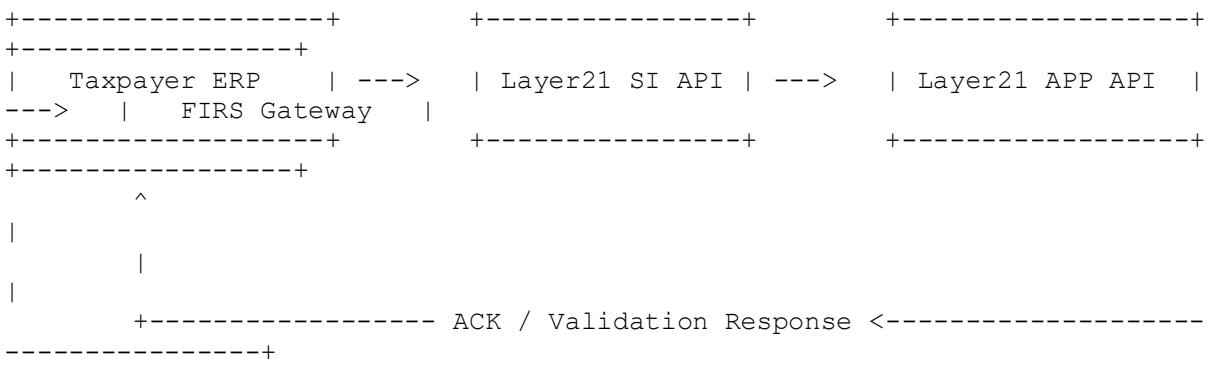
Flow:
`Taxpayer ERP → Layer21 SI → Layer21 APP → FIRS Gateway → FIRS ACK → APP → SI → ERP`

Each stage includes validation, digital signing, and secure message forwarding.

Appendix B — API Flow Diagram & Legend

---

1. Text-Based Flow Diagram



---

2. Flow Description

Step	Actor	Action Description	Security Controls
1	**Taxpayer ERP**	Generates electronic invoice in JSON format.	Local signing with client private key (optional).
2	**Layer21 SI**	Validates JSON schema and applies RS256 digital signature.	JWT signing, payload validation, and logging.
3	**Layer21 APP**	Receives signed invoice, runs compliance checks, and forwards to FIRS.	TLS 1.3 encryption, token verification, and schema validation.
4	**FIRS Gateway**	Validates invoice and issues acknowledgment (ACK).	FIRS digital signature, reference ID generation.
5	**Layer21 APP → SI → ERP**	Routes acknowledgment back to client ERP.	End-to-end integrity validation using signature comparison.

---

3. Legend

Icon / Symbol	Meaning
	Invoice payload (JSON schema)
	RS256 digital signature
	HTTPS/TLS encrypted transport
	Validation and compliance logic
	ACK (Acknowledgment) response
	Metrics and observability layer
	PostgreSQL data persistence (encrypted at rest)

---

4. Security Layers Overview

1. **Network Security:**
   - Enforced HTTPS connections (TLS 1.3 only).
   - Strict HSTS and Content Security Policy headers.
2. **Application Security:**
   - JWT tokens signed with RS256 private key.
   - Payloads validated against official FIRS JSON schemas.
3. **Data Security:**
   - AES-256 database encryption at rest.
   - Daily encrypted backups to Nigerian data centers.
4. **Operational Security:**
   - Continuous monitoring via Prometheus and Grafana.
   - Incident response window ≤ 15 minutes (P1 events).

---

5. Summary Visualization (for reference)

Use this brief description when creating a visual diagram slide for presentations:

"Invoices generated by taxpayer ERPs are securely transmitted to the **Layer21 System Integrator (SI)**, validated, and signed before being sent to the **Layer21 Access Point Provider (APP)**.
The APP applies compliance checks and forwards them to the **FIRS Gateway**, which returns an acknowledgment (ACK).
This ACK is then routed back through APP → SI → ERP in real time, maintaining a complete audit trail."

Footer (for all pages):

Layer21 Global Limited — RC No: 7253971
Innovating Compliance & Integration
www.layer21.com | support@layer21.com | +234 811 192 2822