MCP SERVER | NO CODE | CLOUD HOSTED

NF-e Access Key Validator MCP

Stop processing bad fiscal data keys.

NF-e Access Key Validator checks Brazilian Electronic Invoice (NF-e) access keys for structural integrity and compliance. This MCP validates complex 44-digit tax keys, ensuring they pass mathematical checksums (Modulo 11) and adhere to current tax authority standards before your system uses them.

A+ Quality Score 100/100

nfe | brazil | tax | invoice | validation

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026

vinkius.com/mcp/nf-e-access-key-validator

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

NF-e Access Key Validator MCP

3 tools available
Cloud-hosted on Vinkius

Dealing with Brazilian fiscal data means handling complicated keys that can't just be treated like normal strings of numbers. This MCP lets you validate those NF-e access keys, confirming they are both mathematically correct and legally compliant right out of the gate. You input a key, and it doesn't just tell you 'yes' or 'no.' It breaks down exactly what that key means—extracting crucial data points like the CNPJ number, state code, and document model. Furthermore, it checks those components against official tax authority rules. If your system needs reliable fiscal data for invoicing, this is essential. You can connect to this MCP through Vinkius, accessing these specialized tools alongside thousands of others in one place.

Core Capabilities

01 — Check Key Validity

Determines if a key's length and mathematical checksum are correct using the Modulo 11 algorithm.

02 — Decompose Key Data

Splits a valid access key into its core components, such as CNPJ and State Code.

03 — Audit Tax Compliance

Verifies that the extracted data fields follow current Brazilian tax authority regulations.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/nf-e-access-key-validator** — connect your AI agent in three steps.

01 Pass the NF-e access key you need to check into this MCP.

02 The tool first runs a structural validation, confirming the length and checksum using Modulo 11. If that passes, it proceeds to decompose the key's components (CNPJ, State Code).

03 Finally, it audits those extracted components against current tax authority rules, giving you a full compliance report.

The bottom line is you get a definitive pass/fail grade on both structural integrity and regulatory compliance for any given NF-e key.

Built For

Integration engineers, financial operations staff, and back-office tax specialists. You're the person whose job breaks when a single keystroke or bad data point causes an entire batch of invoices to fail processing.

Financial Operations Specialist

Uses this MCP daily to validate incoming NF-e keys from partners, preventing manual rejections and ensuring high throughput during month-end closing.

Integration Engineer

Builds automated data pipelines that rely on external key validation before transmitting sensitive fiscal data to a core ERP system.

Tax Compliance Analyst

Runs compliance checks against newly received invoice keys to pre-audit their legality and structure against current Brazilian tax law.

What Changes When You Connect

01 Prevents system failures by verifying structure. Using `verify_key_structure` immediately tells you if a key fails the Modulo 11 checksum or length check, saving runtime errors down the line.

02 Extracts necessary metadata instantly. Instead of manual parsing, the `extract_key_metadata` tool pulls out the CNPJ and State Code so your agent can use them directly in subsequent actions.

03 Guarantees regulatory compliance. The `validate_business_compliance` tool audits components against official tax standards, meaning you process keys that are legally sound from day one.

04 Reduces manual verification steps. You no longer need multiple systems or spreadsheets to check if a key is valid; this MCP handles the full lifecycle validation in one place.

05 Increases data reliability for finance teams. By ensuring every incoming NF-e key passes both structural and compliance checks, your team gets cleaner data for reporting.

Real-World Applications

Processing a Batch of Partner Invoices

A financial operations specialist receives 500 invoices from a partner. Instead of running each key manually through multiple validation scripts, they ask their agent to run the batch against this MCP. The tool first uses `verify_key_structure` on every single key. It then groups all keys that pass into two buckets: 'Compliant' and 'Needs Review,' dramatically speeding up reconciliation.

Integrating a New Partner Feed

An integration engineer must connect the core ERP to a new supplier feed containing NF-e keys. To prevent data corruption, they use `extract_key_metadata` first. This allows them to pull out only the necessary CNPJ and State Code fields, confirming the key format before writing any data into the live system.

Auditing Historical Data for Tax Changes

A tax compliance analyst needs to know if a set of old keys still meet current tax authority standards. They run the batch through `validate_business_compliance`. This checks the components against today's rules, flagging any historical keys that might now be considered non-compliant.

Real-time Data Gateway Check

A payments gateway needs to quickly verify a key as soon as it arrives. They use this MCP for instant validation. If the `verify_key_structure` check fails, the payment is instantly rejected with a clear structural error code, preventing bad transactions.

Patterns to Avoid

Treating Keys as Simple Strings

✗ AVOID

Trying to use basic regex or simple database lookups to confirm if an NF-e key is valid. This fails because it ignores the complex mathematical checksum (Modulo 11) and compliance rules.

✓ INSTEAD

You must first run `verify_key_structure` to check the math, then pass the result through `validate_business_compliance` to ensure the components meet tax standards.

Over-relying on Key Format Alone

✗ AVOID

Assuming that because a key has 44 digits, it is usable. This ignores potential issues like an outdated CNPJ structure or non-compliant State Codes.

✓ INSTEAD

Always use `extract_key_metadata` to get the individual components, and then pass those parts into `validate_business_compliance` for proper auditing.

Skipping Initial Structural Checks

✗ AVOID

Feeding a key directly into a processing system without first checking its format. The process will halt at the checksum failure point, wasting time and resources.

✓ INSTEAD

Start with `verify_key_structure`. If it fails, you stop immediately before attempting to parse or validate anything else.

The Right Fit

Use this MCP if your work involves processing Brazilian fiscal data (NF-e) and reliability is critical. You need more than just a basic format check; you require proof that the key's underlying components are mathematically sound *and* legally compliant according to tax authority standards. If your pain point is knowing whether an incoming batch of keys can be trusted for immediate processing, this is what you need.

Don't use this if all you need is basic text manipulation or simple data extraction from non-tax documents. For generic parsing tasks, a standard string utility tool works fine. But because NF-e keys are highly regulated and complex, treating them as anything less than multi-layered validation (structure + metadata + compliance) will cause failures.

The Constant Tax Headache

Every time a batch of invoices comes in from a partner, your team has to manually check the key format. You're copying and pasting these 44-digit strings into internal tools or spreadsheets, running validation checks that only catch half the problems—maybe the length is right, but the underlying CNPJ number might be outdated or non-compliant.

With this MCP, you pass the entire batch to your agent. The system runs a complete audit: first checking the mathematical integrity of the key, then decomposing it into usable parts like the State Code and CNPJ. You get back a clean list, separating what's ready for processing from what needs human tax review—all without leaving your workflow.

Access Key Validator MCP: Guaranteed Compliance

You eliminate the need to run multiple validation scripts. Instead of having one tool check the math, another check the CNPJ format, and a third checking compliance against current tax rules, this MCP handles all three in sequence.

The result is confidence. You don't just know if the key *looks* right; you know it passes every regulatory hurdle required by Brazilian law. It changes your process from reactive troubleshooting to proactive data ingestion.

NF-e Access Key Validator MCP (3 Tools)

These three tools allow you to validate NF-e access keys by checking their mathematical structure, pulling out individual business data points, and auditing compliance with official tax authority standards.

#	TOOL	DESCRIPTION
01	`extract_key_metadata`	Splits a working access key into its individual business parts like the CNPJ or State Code for inspection.
02	`validate_business_compliance`	Checks if all components found in the key match current, allowed tax authority standards.
03	`verify_key_structure`	Determines if an access key is valid by checking its length and running a mathematical checksum test (Modulo 11).

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Is this NF-e key valid: 35231000000000000155550010000000001?

The access key is structurally valid and passes the Modulo 11 checksum.

U Extract information from this key: 35231000000000000155550010000000001

The extracted metadata includes State Code: 35, CNPJ: 23100000000000, Model: 55, Series: 001, Number: 000000001, and Emission Type: 1.

U Check if this key follows tax standards: 35231000000000000155550010000000001

The key is compliant with all checked regulatory standards.

Frequently Asked Questions

01 **How does NF-e Access Key Validator check for structural validity?**

The MCP uses the `verify_key_structure` tool. This function checks both the required 44-digit length and runs a mathematical checksum using the Modulo 11 algorithm to ensure the key is mathematically sound.

02 **What information can I get from extract_key_metadata?**

The `extract_key_metadata` tool breaks down the key into its core components. You'll receive distinct fields, including the CNPJ (company tax ID), State Code, Model number, and Series.

03 **Does this MCP only check if the key is formatted correctly?**

No. It goes much further than format. While `verify_key_structure` checks the math, you also must use `validate_business_compliance` to ensure those components comply with actual tax authority rules.

04 **Can NF-e Access Key Validator handle different types of invoices?**

It focuses specifically on Brazilian Electronic Invoice (NF-e) keys. The tools are designed around the required structure and compliance framework for that specific document type in Brazil.

05 **Is this MCP faster than using a dedicated tax software tool?**

When integrated into an automated agent workflow, it is much faster. It lets you run validation checks against thousands of keys instantly without needing to switch between separate vendor platforms or manual interfaces.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"nf-e-access-key-validator": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

NF-e Access Key Validator is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by NF-e Access Key Validator. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	NF-e Access Key Validator MCP
Server ID	`019ee7e4-2277-7213-9c5e-ff024edc5c50`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/nf-e-access-key-validator.