MCP SERVER | NO CODE | CLOUD HOSTED

TeleSign MCP

Prevent Fraud. Verify Identity. Score Risk.

TeleSign helps you validate user identity instantly using phone number intelligence, risk scoring, and multi-channel verification. It prevents fraud at sign-up by checking everything from carrier details to deactivation status, giving your application confidence in every new user.

A+ Quality Score 100/100

phone-verification | fraud-prevention | otp-authentication | risk-scoring | identity-verification | phone-intelligence

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/telesign

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.

TeleSign MCP

10 tools available
Cloud-hosted on Vinkius

Need to know if a user's phone number is real and safe? This MCP connects your agent to TeleSign’s full suite of identity tools. You can get deep insights into any number—like its carrier, type, or even location—before asking for more data. Need proof the user owns the line? Send an SMS code, a voice call, or use push notifications for verification. Plus, it calculates a risk score to tell you how likely that phone is involved in fraud. You can also check if a number has been deactivated or ported recently. When you connect this MCP via Vinkius, your AI client gains access to all these checks, letting you build robust sign-up flows without leaving your chat window.

Core Capabilities

01 — Score phone risk

The tool calculates a detailed risk score for any given number, helping you filter out suspicious accounts.

02 — Verify user ownership

You can send verification codes via SMS, automated voice calls, or push notifications to confirm the user has access to that line.

03 — Check phone status

It identifies a number's carrier, type (mobile/landline), and location intelligence, giving you full context on the line itself.

04 — Detect deactivation

You can check if a phone number is currently active or if it has been deactivated or ported away from its original service.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/telesign** — connect your AI agent in three steps.

01 First, your agent passes the target phone number to this MCP.

02 The tool runs several checks—like scoring the risk and checking deactivation status—and then sends back a comprehensive JSON report with all the details.

03 Your AI client reads the report, allowing you to make an automated decision about whether to accept or deny the user sign-up.

The bottom line is your agent gets immediate, actionable data on phone numbers that prevents bad actors from getting into your system.

Built For

This is for fraud prevention teams and product managers who deal with high sign-up volumes. If manual identity checks are slowing down your user onboarding flow, you need this MCP.

Product Manager

You integrate the risk scoring into the main signup form to improve conversion rates by failing fast on bad accounts.

DevOps Engineer

You build automated pipelines that run number intelligence and verification checks before any user account is provisioned in production.

Fraud Analyst

You use the deactivation check and phone type data to spot patterns of synthetic identity fraud or bulk sign-up abuse.

What Changes When You Connect

01 Reduce sign-up fraud immediately. Instead of just checking if a number is valid, you use the score_phone tool to calculate risk levels and reject high-risk accounts before they hurt your business.

02 Support multiple verification paths. You aren't limited to SMS; you can send codes via automated voice calls or push notifications, giving flexible options for different user flows.

03 Get full line context upfront. The get_phone_id tool gives your agent the carrier and location details instantly, which helps differentiate between a real, active business number and a burner phone.

04 Handle account lifecycle checks. You can use check_deactivation to confirm if a number that was previously valid is still in service, preventing support headaches months down the line.

05 Automate complex workflows. By running multiple tools like score_phone and get_phone_type together, you build a single, smart decision point for your agent.

Real-World Applications

Onboarding a new B2B user.

A Product Manager asks their agent to onboard a high-value client. The agent first uses score_phone and get_phone_type to confirm the number is corporate, then sends an SMS code using send_sms for verification. If both checks pass, the account is created.

Debugging suspicious sign-up spikes.

A Fraud Analyst needs to investigate a sudden spike in failed signups. They use check_deactivation on the suspect numbers and run get_phone_id repeatedly to see if they share common carrier patterns, helping pinpoint bot activity.

Testing internal system health.

A DevOps Engineer needs to confirm that their new signup microservice is talking correctly to TeleSign. They use check_telesign_status first and then run check_verification on a test number to ensure the entire flow works.

Handling enterprise app logins.

An agent needs to authenticate an employee using company devices. Instead of SMS, they opt for send_push_verification, ensuring that only users with the current corporate app can proceed, securing the account flow.

Patterns to Avoid

Only checking if a number is 'valid'.

✗ AVOID

Thinking that just because send_sms works, the user must be legitimate. This ignores fraud risk and line intelligence.

✓ INSTEAD

Always start by running score_phone and get_phone_type. If the risk score is high or the phone type is suspicious, don't waste time sending codes.

Assuming a number hasn't been ported.

✗ AVOID

A user reports their account was hijacked after they changed carriers. Simply checking for an active status won't reveal if the number recently moved services.

✓ INSTEAD

Use check_deactivation to get history on porting and deactivation events, confirming the line's entire service history.

Relying solely on SMS codes.

✗ AVOID

Designing a flow that breaks if users are in areas with poor cellular reception. This limits your ability to capture high-quality identities.

✓ INSTEAD

Build redundancy by offering multiple methods: try send_voice_verification first, then fall back to sending an SMS via send_sms.

The Right Fit

Use this MCP if your core problem is *identity confidence*. You need assurance that the phone number belongs to a real person, is currently active, and isn't associated with fraud. Don't use it if you simply need to send bulk messages; for that, an SMS gateway tool will suffice. If you only need basic formatting or data cleaning on existing user IDs, a standard database connector works better. However, if your workflow involves *risk assessment* (i.e., 'is this person safe enough to proceed?'), then TeleSign is the right choice because it provides scores and intelligence beyond simple validation.

The headache of manual identity checks is real.

Right now, when a user tries to sign up, you're probably forcing them through multiple steps: they enter the number, then your system sends an SMS, waits for the code, and if it fails, someone has to manually look into *why*. It's tedious copy-pasting across three different tabs—the form, the message log, and a separate fraud dashboard.

With this MCP, that whole sequence becomes one smart conversation. Your agent runs all those checks automatically: checking the risk score, confirming the phone type, and initiating verification in parallel. The result isn't just data; it's an instant decision you can act on.

TeleSign gives your agent complete number intelligence.

You stop manually checking documentation pages to see if a number is corporate or personal, or if it was recently ported. The get_phone_id tool pulls all that technical data directly into the context of your chat flow, eliminating multiple API calls and manual investigation.

This means you build trust into your product from day one. Your system moves past simple validation; it achieves deep, verifiable identity assurance with zero added friction for your developer or support team.

TeleSign: 10 Tools for Identity Verification

These tools let your agent run comprehensive identity checks on phone numbers, scoring risk, verifying ownership via SMS or voice, and checking line status.

#	TOOL	DESCRIPTION
01	`check_deactivation`	Confirms whether a specific phone number is currently active or if it has been deactivated by the carrier.
02	`check_telesign_status`	Verifies the API connectivity and overall operational status of the TeleSign service.
03	`check_verification`	Retrieves the current verification status for a user who has already attempted an identity check.
04	`get_phone_id`	Gathers core identifying information about a phone number, such as its country code and carrier details.
05	`get_phone_type`	Determines the nature of the phone line—whether it is mobile, landline, or another type.
06	`score_phone`	Analyzes a phone number and outputs a numerical risk score based on known fraud patterns.
07	`send_push_verification`	Triggers an identity verification request via a push notification, which is useful for app-based signups.
08	`send_sms`	Sends a standard text message (SMS) containing a unique one-time password to the user's number.
09	`send_verification`	Handles the general process of sending out a required verification code for account setup.
10	`send_voice_verification`	Delivers the necessary verification codes using an automated voice call to the user's phone number.

See It in Action

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

U Send a verification code to +14155551234.

Verification code sent! Reference ID: ref_8291. The user should receive the code shortly.

U Score fraud risk for +14155551234.

Risk score for +14155551234: 120/1000 (Low Risk). Carrier: Verizon, Type: Mobile, Location: San Francisco, CA.

U Check if +14155551234 has been deactivated.

Number +14155551234 is active. Last ported: 2024-03-15 from AT&T to Verizon. No deactivation detected.

Frequently Asked Questions

01 **How does TeleSign MCP help prevent fraud?**

It calculates a risk score (score_phone) and uses phone intelligence to identify suspicious patterns, allowing you to reject high-risk signups automatically before they enter your system.

02 **Can I send verification codes using multiple methods with TeleSign MCP?**

Yes. You can use the dedicated tools for SMS (send_sms), voice calls (send_voice_verification), or push notifications (send_push_verification) to cover all user scenarios.

03 **What is phone intelligence in TeleSign MCP?**

Phone intelligence refers to the deep data about a number, including its carrier, type (mobile/landline), and location. The get_phone_id tool provides this context instantly.

04 **Does TeleSign MCP check if a phone number is still active?**

Yes, the check_deactivation tool verifies the current status of a number, confirming it hasn't been deactivated or ported away from its original service.

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 `"telesign": { "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

TeleSign 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 TeleSign. 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	TeleSign MCP
Server ID	`019dd170-562a-70a9-9ce7-afb545197b9f`
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/telesign.