MCP SERVER | NO CODE | CLOUD HOSTED

eSign (e签宝) MCP

Manage contracts without ever opening the portal.

eSign (e签宝) connects your AI agent to China's premier digital signature platform. Manage entire contract lifecycles—from creating initial workflows to tracking signatures and downloading final documents—all through natural conversation with no need to navigate the eSign portal.

A+ Quality Score 100/100

contract-lifecycle | digital-signing | workflow-automation | templates | compliance

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/esign-e

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

eSign (e签宝) MCP

10 tools available
Cloud-hosted on Vinkius

Your agent handles complex agreements, making document signing feel like a simple chat. Instead of logging into a separate portal, your AI client can instantly manage your legal operations. You can ask it to list existing sign flows or create an entirely new one by specifying documents and people. It automatically manages templates, letting you pull from predefined agreement types. When the flow is ready, your agent finds the correct signing link for each participant; later, once everyone signs, you just tell it to download the final agreements. This capability makes managing high-volume employee contracts or complex B2B deals simple and secure, all managed through a single connection via Vinkius.

Core Capabilities

01 — Set up document workflows

The agent can create brand new digital signing flows by defining the documents needed and the people who must sign them.

02 — Manage templates

You tell your AI client to pull predefined contract types, accelerating the creation of standardized agreements.

03 — Track signature status

The system provides real-time updates on active sign flows and retrieves necessary URLs for participants to complete their signing.

04 — Build agreement packages

You can attach PDF documents to an existing flow or task, ensuring all relevant papers are included before signing begins.

05 — Get organizational status

The agent retrieves high-level details about your eSign account and current authorization limits.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP, then enter your required eSign App ID and App Secret into your AI client.

02 Ask your agent for a specific action, like listing all active flows or creating a new signing workflow using predefined templates.

03 Your agent executes the command, providing real-time status updates or generating necessary download links to complete the process.

The bottom line is that you use natural language prompts in your AI client instead of clicking through multiple eSign menus.

Built For

Legal operations teams, HR managers, and sales directors need this. They're the people tired of switching between document management systems, email threads, and manual portal logins just to get a single contract signed.

Legal Operations Manager

Manages complex agreements by having their agent list active sign flows or create new signing tasks without touching the eSign portal.

HR Director

Automates employee onboarding by sending contracts and policy acknowledgments directly through natural language commands from their AI workspace.

Sales Operations Specialist

Coordinates B2B agreements by having their agent start a new flow, add required documents, and monitor client signatures in real time.

What Changes When You Connect

01 You stop wasting time manually checking status updates. By using list_sign_flows, your agent gives you an instant overview of every active agreement in progress.

02 Template creation speeds up drafting dramatically. Asking for list_templates immediately provides a selection of pre-vetted documents like NDAs or employment contracts.

03 Getting the sign link is simple. Instead of navigating deep menus to find a participant's URL, calling get_execute_url gives you the exact link right away.

04 The whole process becomes conversational. You don't write boilerplate API calls; you just tell your agent what needs signing and who needs to sign it.

05 Compliance checks are easier. By using add_docs and create_sign_flow together, you ensure every document is attached and the workflow is structured correctly before sending.

Real-World Applications

The onboarding process stalled because of manual tracking.

An HR manager needs to know if 20 new hires have signed their agreements. Instead of logging into the portal, they ask their agent to list_sign_flows. The agent instantly confirms which contracts are pending and provides status updates.

A legal team needs a standard contract for a new client.

The lawyer prompts their agent to call list_templates, pulling up the 'Master Service Agreement.' They then use start_flow to begin the workflow immediately, skipping template searches and manual setup.

A sales rep needs to follow up on a stalled client signature.

The rep asks their agent for the signing link. The agent runs get_execute_url for the specific participant, giving them the direct URL needed to send to the client and push the contract forward.

A project lead needs to bundle final paperwork from multiple agreements.

Once several flows are completed, the agent is asked to download_docs. It retrieves all signed contracts into one secure package, eliminating manual downloads and file consolidation.

Patterns to Avoid

Trying to manage workflows via raw API calls.

✗ AVOID

Writing code that requires knowing the exact IDs for every template, signer, and flow step. This is tedious, brittle, and constantly breaks when the platform updates its structure.

✓ INSTEAD

Let your agent handle it. Use start_flow or create_sign_flow to define the intent in plain language. The MCP handles all the underlying data mapping, keeping your code clean and robust.

Manually checking organizational limits.

✗ AVOID

Guessing if you have enough signing capacity or what permissions your account currently holds, leading to unexpected failures when a flow hits a quota wall.

✓ INSTEAD

Always check the organization status first. Use get_org_info before starting any major campaign to confirm your current authorization levels and usage limits.

Forgetting to add necessary documents.

✗ AVOID

Starting a flow only with a blank contract, forgetting that the client needs to sign an attached NDA or compliance waiver separately.

✓ INSTEAD

Before running start_flow, always use add_docs. This ensures all required supporting paperwork is bundled into the single, governed signing workflow.

The Right Fit

Use this MCP if your primary pain point is coordinating multiple steps of a complex legal agreement—you need to manage the *lifecycle* from setup (list_templates/start_flow) through tracking (list_sign_flows) and finalization (download_docs). This connector excels when you want your AI agent to act as a virtual paralegal, handling the entire document choreography without you touching the eSign UI. Don't use this if you just need simple data retrieval; for that, a basic read-only tool would suffice. If your goal is simply drafting content or summarizing existing text, look at a general document processing MCP instead.

The current process of getting an agreement signed feels like a scavenger hunt.

Right now, you have to jump between five different places. You log into the eSign portal to check if Client A signed. Then you open a separate spreadsheet to track who was assigned the contract. Next, you might have to manually copy and paste specific URLs into an email chain just so they can sign it.

With this MCP connected via Vinkius, your agent handles all of that. You simply tell your AI client: 'Start the agreement for Client B.' The agent creates the flow, attaches the documents, adds the right people, tracks the progress, and when it's done, it gives you one download link. It’s instant, controlled conversation.

---

eSign (e签宝) MCP: Full Control Over Your Digital Signatures

Gone are the days of guessing who needs to sign or having to manually check which documents were attached. You can now use add_signers and add_docs together to perfectly curate a workflow, ensuring nothing is missed.

The difference now is control. Your agent manages every step, from initial setup (create_sign_flow) to final archiving (download_docs). Everything flows through one place—your AI client.

eSign (e签宝) MCP: 10 Tools

These ten tools let you build, monitor, update, and finalize entire digital contract workflows using simple natural language commands from your AI client.

#	TOOL	DESCRIPTION
01	`get_sign_flow`	Fetches the full details and current status of a specific, existing sign flow.
02	`list_sign_flows`	Retrieves a list of all active or past signing workflows managed in your account.
03	`list_templates`	Shows a catalog of predefined document templates that can be reused for new contracts.
04	`add_docs`	Adds necessary PDF documents to an existing signing workflow or task.
05	`get_org_info`	Retrieves high-level account information about your eSign organization details and status.
06	`download_docs`	Retrieves the final, signed documents from a completed flow.
07	`add_signers`	Adds specific people who need to sign the agreement to a defined flow.
08	`create_sign_flow`	Initiates and sets up an entirely new digital signature workflow.
09	`get_execute_url`	Provides the specific web link required for a participant to sign their document.
10	`start_flow`	Begins the process of creating and managing a digital signature workflow from scratch.

See It in Action

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

U List all active signature flows on eSign.

I've retrieved your active eSign flows. You have 5 tasks in progress, including 'Service Agreement - Client A' and 'New Employee Offer'. Which one would you like to check the status for?

U Get the signing URL for account 'acc-8821' in flow 'flow-9920'.

I've retrieved the execution URL for the participant. You can send this link to the signer to complete the process: [URL].

U Show me all available document templates.

I've listed your eSign document templates. You have 3 templates ready for use: 'Standard NDA', 'Employment Contract v2', and 'Sales Agreement'. Would you like to use one of these for a new sign flow?

Frequently Asked Questions

01 **How do I check if a signing flow is active using eSign MCP?**

You use list_sign_flows. This command retrieves all your current and pending workflows, letting you know exactly what agreements are in progress.

02 **Can I start a new contract without knowing the template name first? (eSign MCP)**

No, you should list_templates first to see available options. This ensures you use a standardized and pre-approved agreement type for your workflow.

03 **What tool do I use to get the actual link for signing? (eSign MCP)**

You must call get_execute_url. This retrieves the unique, actionable web link that you can send directly to the participant who needs to sign.

04 **Does eSign MCP handle multiple documents in one flow?**

Yes. You use add_docs and create_sign_flow together. This allows you to bundle several different PDF agreements into a single, coherent signing workflow.

05 **How do I find my eSign App ID and Secret?**

Log in to the [eSign Open Platform](https://open.esign.cn/), create a new application, and you will find your App ID and App Secret in the application credentials section.

06 **Can I retrieve the signing URL for a participant?**

Yes. Use the `get_execute_url` tool with the flow ID and the signer's account ID. Your agent will retrieve the unique URL where the participant can perform the signature.

07 **Is it possible to download the signed documents?**

Yes! Once a sign flow is completed, you can use the `download_docs` tool to retrieve temporary download links for all documents included in that flow.

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 `"esign-e": { "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

eSign (e签宝) 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 eSign (e签宝). 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	eSign (e签宝) MCP
Server ID	`019d8436-25f3-7181-8080-9067c863d005`
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/esign-e.

© 2026 Vinkius · vinkius.com · support@vinkius.com