

standards

Standards

Rules for the Verae MCP timestamping server.

Protocol

This process is an MCP server (Model Context Protocol). Clients are assistants and inspectors that speak MCP. It is not a REST product API and not a browser session by itself.

Hash only

- Callers send a SHA-256 digest: 64 lowercase hex characters. A `sha256:` prefix is stripped.
- The server does not read files, does not accept document bytes, and does not hash content.
- Empty input has the well-known digest `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991`. Callers may stamp that digest. The server does not invent it from a missing file.

Scopes

Scope	Where the receipt lives
local	JSON file, default <code>~/.veraemcp-timestamp-local.json</code>
shared	Same file. There is no separate shared store in this process
global	POST <code>https://api.veraetime.net/api/timestamp</code> with <code>wait=true</code>

`want_scope=global` on `verify` asks VeraeTime. A local receipt cannot satisfy `global`.

Global history

`hash_report` reads the local file only. VeraeTime is not queried for a digest history. A global stamp can verify by certificate id and still be absent from `hash_report`. An empty list means “not in the local file,” not “VeraeTime has no record.”

Credentials

- Token: `VERAE_GLOBAL_TOKEN`, else `access_token` / `id_token` / `auth_token` in `~/.verae/auth.properties` (`VERAE_AUTH_PROPERTIES` overrides the path).
- `login` writes that file (mode 0600), including `username`, `password`, and `expires_at`. The tool result does not include the JWT.
- `signup` calls `POST /auth/signup` with no bearer token. The account role is `user`. It does not replace the stored JWT.
- `create_user` calls `POST /auth/users` only when the stored token’s role is `admin`.
- Before a global stamp or verify, a stored username and password are used to log in again when `expires_at` is missing or within 5 minutes.
- Do not commit tokens. `.env` is gitignored.
- The local receipt file is mode 0600 after each save.

NATS

NatsLedger is optional and is not the default. It uses core NATS request/reply:

- `verae.ts.request`
- `verae.ts.verify`
- `verae.hash.report`

Job-complete and receipt notifications stay ephemeral core NATS (`verae.ts.completed`, `verae.ts.receipt`). This server does not put those events on JetStream.

Transports

VERAE_MCP_TRANSPORT	Bind
unset or <code>stdio</code>	Parent process stdin/stdout
<code>streamable-http</code>	<code>VERAE_MCP_HOST</code> (default 127.0.0.1) and <code>VERAE_MCP_PORT</code> (default 8000), path <code>/mcp</code>

Leave the HTTP bind on loopback unless a reverse proxy terminates TLS and authentication in front of it. Do not publish the VeraeTime bearer token on an open internet listener.

Errors

Invalid digests and unknown scopes raise `ToolError` with the `ValueError` text.
HTTP failures from VeracTime surface as `global timestamp HTTP <status>`.