
Secure Messaging

Verae

Sep 16, 2026

CONTENTS

Passthrough NATS envelopes, Ed25519 signed configuration, DataCube admin-history, and Network Error Bundles.

This is **not** a HIPAA/SOC 2/ISO certificate.

- Python spec: `python/secure_messaging/`
- Go leaf: `go/cmd/sm-leaf` (in-process NATS + optional hub)
- Loopback health: `127.0.0.1:18783/health`
- Catalog: <https://git.georgelambert.org/marchon/nats-service-endpoints>
- Hub: <https://git.georgelambert.org/marchon/system-git-sync>

WHO CALLS THIS MODULE

`pfc-py-admin` (sign config, append history) and systemd `pfc-sm-leaf`. Tests send targeted good and bad messages on `verae.sm.send`.

MESSAGES

- **From:** console / tests / connectors
- **To:** mailbox dest in the clear; body ciphertext
- **Success:** ack accepted + lookup_id (sender cannot reopen ct)
- **Failure:** SM-MISSING-TO, SM-EMPTY-CT, SM-BAD-ALG, SM-PLAINTEXT-BODY, SM-BAD-JSON → `verae.sm.error` + `verae.sm.dead` + `verae.sm.log.summary`
- **Filter:** no plaintext body field; summary must not contain ct
- **Timeout:** 5s NATS; 15s NPE sidecar

ERRORS

Network Error Bundle: `ct_sender` (sender-only status) and `ct_system` (ops bounce, no mail body). `logging.mode=summary`.

Variables: `crypto.mode`, `routing.mode=passthrough`, `SM_LEAF_HUB`, `SM_HTTP`. See `system-git-sync docs/VARIABLES.md`.