

# OPAUDIT 008 — Modern Mastodon signs in a format our door couldn't read

|                |                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------|
| Audit ID       | 2026-09-07-008                                                                                                   |
| Report date    | 2026-09-07 (compiled from the incident record)                                                                   |
| First observed | Reason-logging at 0.7.612D; verifier shipped ~0.7.618D (September 2026).                                         |
| Theme          | Log the unknown before you build the fix.                                                                        |
| Surfaces       | Inbound deliveries from mainline Mastodon 4.4+/4.7+.                                                             |
| State          | <b>WATCHED WORKING</b> Talking to Mastodon looks flawless now, across solo posts and carousels.                  |
| Watched live?  | <b>Yes</b> — Sean; Mastodon interop is clean, and Mastodon also displays our carousels and solo posts correctly. |
| Reporter       | Sean + Claude.                                                                                                   |
| Related        | OPAUDIT 001, 007 — all the “prove it per peer” family.                                                           |
| Publication    | Public. No exploitable detail.                                                                                   |

## 1. SUMMARY

The way servers sign their messages has more than one standard, and Mastodon moved to a newer one. Our inbox could read the older style but not the new, so modern Mastodon deliveries bounced at the door — through no fault of theirs.

## 2. WHAT A HUMAN SAW

Deliveries from up-to-date Mastodon servers were rejected. Older Mastodon servers worked fine, which made it look intermittent until the pattern — server version — became clear.

## 3. ROOT CAUSE

Mainline Mastodon 4.4 and later sign inbox deliveries with the newer RFC-9421 HTTP Message Signatures format. Our inbox verifier only understood the older draft-cavage style, so it had no way to read a correctly-signed modern Mastodon request and rejected it as unverifiable.

## 4. EVIDENCE AT DIAGNOSIS

Before building anything, we made the rejection log record *which* signature scheme each bounced request used — a compact fingerprint of the auth headers (scheme, whether the newer signature input was present, digest flavour, sender software), never any content. Every rejected modern-Mastodon delivery then became direct evidence for what the verifier needed to accept.

## 5. WHAT WE DID

---

Built the verifier to accept the RFC-9421 format alongside the older one. Old-format senders verify exactly as before; new-format senders now verify too, instead of bouncing.

## 6. VERIFIED LIVE

---

Talking to Mastodon looks flawless now, confirmed by Sean — and Mastodon displays our carousels and solo posts correctly as well. This is the cleanest interop on the page.

## 7. EYEBALL NEXT

---

Keep an eye on other implementations adopting the newer signing standard; each should be watched on inbound the way Mastodon now has been. Our own fediverse lab (Pixelfed, Mastodon, GoToSocial), driven by accelerated agentic test runs, lets us replay inbound deliveries against a server we control and read the raw result — so a new signing format is caught and confirmed quickly rather than discovered when live deliveries start bouncing.

## 8. THE DOCTRINE THIS INCIDENT CREATED

---

*When something unknown is failing, make it tell you what it is before you try to fix it. Turn every bounce into a labelled piece of evidence first; guessing at a format you can't see wastes builds, while a fingerprint in the log points straight at the answer.*

---

SnapSmack — DING DONG BELL operability ledger — [snapsmack.ca/ding-dong-bell.php](https://snapsmack.ca/ding-dong-bell.php) · Operability audits record whether a feature actually performs its job, proven not claimed. Security audits live separately at [snapsmack.ca/buzzers.php](https://snapsmack.ca/buzzers.php).