

Aegis Solis Archive — ER-13 v1.3

SEC-CDP-002 Superseded-Version Register — v1.0

Record: ER13-SEC-CDP-002-SUPERSEDED-REGISTER-20261011-v1.0

Date: 11 October 2026

Status: Administrative research/version guidance; not an implementation approval.

1. Reader warning — applies to every version

NO VERSION OF SEC-CDP-002 IS AN IMPLEMENTATION-READY OR SECURITY-CERTIFIED DESIGN. The latest frozen Draft v0.1.3 is a research requirements specification only. It has not been implemented, independently reviewed against deployed products, penetration-tested, or approved for pilot execution. All requirements remain NOT IMPLEMENTED / NOT TESTED.

Do not execute or implement code or engineering controls based solely on any historical version. The preserved packages are an audit trail of research, corrections, and rejected proposals, not a directory of approved security components.

2. Version register

- **v0.1 — SUPERSEDED; NOT FOR IMPLEMENTATION.** Early R07 receipt design exposed a small secret search space through an unsalted manifest digest; the coordinated v1.0 review also identified missing evaluated-agent boundaries (S-1, S-2).
- **v0.1.1 — SUPERSEDED; NOT FOR IMPLEMENTATION.** Historical intermediate proposal. The coordinated review discusses earlier receipt and agent-boundary weaknesses; those are specification concerns, not evidence of a deployed exploit.
- **v0.1.2 — SUPERSEDED; NOT FOR IMPLEMENTATION.** Replaced by v0.1.3 and preserved for reconstruction. This register does not attribute every predecessor weakness to v0.1.2 without a version-specific audit.
- **v0.1.3 — CURRENT RESEARCH DRAFT ONLY; NOT IMPLEMENTED, TESTED, OR APPROVED FOR IMPLEMENTATION.** Revised commitment receipt and trust-boundary requirements remain unvalidated. Independent cryptographic/platform and information-hazard reviews are open.

3. Security-relevant transition recorded, not certified

The preserved coordinated review v1.0 identified (S-1) potential answer-key leakage from a manifest digest in the commitment receipt and (S-2) insufficient specification of the evaluated-agent/harness and secret boundaries. Later review and successor specification describe corrections including separately protected secrets, limited public receipts, per-unit presentation controls, and independent verification requirements. These are **specification-stage responses only**, not deployed security fixes.

Do not infer that any superseded version's complete implementation details were safely tested or that latest-version wording is sufficient against an adversary. A separate, independently reviewed platform-specific design and tests are required before any implementation claim.

4. Which version should a researcher read?

Use **v0.1.3** only as the *latest historical draft to understand the current proposed requirements*; use v0.1, v0.1.1 and v0.1.2 only to examine design evolution and review defects. **None** may be used as an operational installation guide. The preserved original text remains untouched.

Scope: This register covers the frozen v1.3 history only. The original release, remote deposits, Master Hash Manifest v17, and Aegis Mirror Engine are unchanged. It answers Claude findings F-04 / R-2.