

ZTVS attestation format

Wire specification — version 0.0.2

Envelope

Field	Type	Notes
subject	digest	The artefact the report describes
advisories	digest	Snapshot the scan matched against
policy	digest	Absent when no policy was applied
scanner	string	Version that produced the report
signature	bytes	Over the canonical form of the above

Canonicalisation

Keys are sorted, whitespace is removed, and digests are lowercase hex. A verifier recomputes the canonical form from the report and checks the signature over it.

Verification

A verifier needs the report, the signature and the public key. It does not need the artefact, the advisory database, or any network access.