Freshness and composition: what each component proves

From human approval and the AEP to a TPM quote, Veraison EAR, and the relying-party decision

Core idea: PCR says “what state the machine was in”; the signature says “the quote was not altered”; the nonce says “the quote was created for this session, not replayed from the past”.

1 THREE EVIDENCE PRODUCERS — PRODUCE

Human + EUDI Wallet — HUMAN AUTHORIZATION

Proves that a human approved **this exact amount, recipient, and action**.

Pinned issuer certificate — trust only the known issuer → **SD-JWT signature** — the credential is genuinely signed → **KB-JWT + transaction hash** — the phone signed H(exact action)

AI agent → AEP — APPLICATION EVIDENCE

AEP is a signed record of **what the agent did, under what authority, and with what outcome**.

Action — for example, pay ACME €120 → **Authority** — mandate / scope / limit → **Outcome digest** — H(action outcome)

Limit: the AEP signature proves only that the runtime key signed the record. It does not prove what runtime was executing.

Platform → TPM quote — PLATFORM EVIDENCE

Proves measured platform state and binds it to the current verifier-session challenge.

PCR measurements — firmware, boot, kernel, outcome digest → **PCR digest** — hash of selected PCRs [1,2,3,4] → **Signed TPM quote** — PCR digest + evidence nonce + signature

Important: the PCR digest detects state changes; the nonce separately detects replay. The prototype uses **swtpm**, with no hardware root.

2 COMPOSE THE EVIDENCE — COMPOSE

→

Evidence item A

AEP: application-layer record — “what happened”.

Evidence item B

TPM quote: platform evidence — “on which measured platform”.

Load-bearing binding

A cryptographic link must show that the AEP and platform appraisal refer to **the same action**, rather than merely appearing next to each other.

EAT — one structured attestation token / submodule

Collection CMW — wrapper carrying multiple Evidence items + linking claims

EAT and CMW **carry** evidence. They do not themselves verify signatures, PCRs, or freshness.

3 VERAISON APPRAISES — VERIFY

① New verifier session

The Verifier creates a random **session.nonce = N_2**. This challenge is selected by the Verifier, not by the Attester.

↓

② TPM scheme: `TPM_ENACTTRUST`

Parses the TPM Evidence format and checks the quote signature, PCR digest, and reference values.

↓

③ `ExtractClaims`

Surfaces quote fields as generic claims: node-id, PCR digest, and **evidence.nonce = N_1**.

Path A · in-scheme

The scheme compares N_1 with N_2 itself and immediately fails closed on a mismatch.

`PR #432: this path`

Path B · policy

`policymanager.go` supplies `session.nonce`; OPA/Rego compares it with the extracted `evidence.nonce`.

`captured EAR pair: this path`

Original gap: `session.nonce` was already in the policy input, but `ExtractClaims` did not expose the quote nonce. The policy therefore could not compare them. Both values are required.

4 RESULT — DECIDE

EAR

EAT Attestation Result. Carries the verdict and AR4SI trustworthiness information.

- `affirming`
- `contraindicated`
- `warning / none`

Relying Party

The component that acts on the result: a payment gate, API gateway, or another enforcement point.

```
affirming + other gates
PASS → EXECUTE
replay / mismatch →
DENY
```

Captured EAR = the result of a real laboratory appraisal saved to a file. The file is shown on stage; Veraison is not running live at that moment.

WHAT IS ACTUALLY PROVED — BOUNDARIES

1. **PCR / outcome binding** — Change the outcome or measured state → the PCR digest no longer matches.
2. **Quote signature** — Change the TPM quote bytes → the signature no longer verifies.
3. **Nonce comparison** — Replay an old genuine quote → its nonce does not match the new session.

This does NOT prove

- that the AI decision was correct;
- that the model is honest or safe;
- a hardware root when swtpm is used;
- one wallet→TPM cryptographic chain: today these remain two separate rails.

Three questions for the room

1. Must nonce equality live in the scheme, or may policy enforce it?
2. How should different freshness windows be reconciled?
3. Are EAT/CMW sufficient, or is concise guidance needed?

5 SINGLE-WINDOW FRESHNESS: EXACT REPLAY — MEASURED

Fresh · original session

Session expects	`D/YLjUr5…ORQYYo=`
Quote contains	`D/YLjUr5…ORQYYo=`

$N_1 = N_1$ → EAR affirming

Replay · new session

Session expects	`VKvxfur0…XuuBck=`
Quote contains	`D/YLjUr5…ORQYYo=`

$N_2 \neq N_1$ → EAR contraindicated

Why does the Verifier expect a different value? Every new session gets a new random challenge. The Verifier does not adapt to an old quote: the mismatch is what reveals replay. In the measured test, both requests carried **the same 235 quote bytes**; only the session changed.

6 MULTI-WINDOW: OPEN PROBLEM — OPEN

Wallet approval — nonce W · transaction hash · time t_1 → **AEP record** — action/outcome · time t_2 → **TPM quote** — nonce P · PCR · time t_3

Reconciling different freshness windows asks which rule makes the whole composition fresh when its parts were created at different times and carry different nonces and `exp` values.

`exp` ≠ nonce freshness
`exp` is the token validity limit. Before expiry, the token can still be replayed. A nonce proves membership in the current session.

A fresh component does not refresh an old one
A fresh TPM quote does not refresh an old wallet approval; a fresh AEP does not refresh old platform Evidence.

Whose freshness wins?
Which nonce scopes which layer: wallet, AEP, TPM, or the relying-party session?

Honest draft status
The parts must be bound, but no general reconciliation rule is ready. This is a question for standards work, not a claimed result.

LEGEND AND FULL NAMES — LEGEND

- human authorization
- action evidence / AEP
- platform evidence / TPM
- appraisal / policy
- → data flow or processing step
- ··· binding / reference between objects

AEP — Action Evidence Package
RATS — Remote ATtestation procedureS
TPM — Trusted Platform Module
PCR — Platform Configuration Register
EAT — Entity Attestation Token
CMW — Conceptual Message Wrapper
EAR — EAT Attestation Result
AR4SI — Attestation Results for Secure Interactions
OPA — Open Policy Agent
Rego — policy language used by OPA
SD-JWT — Selective Disclosure JSON Web Token
KB-JWT — Key Binding JSON Web Token
RP — Relying Party
PSD2 — Payment Services Directive 2
WIMSE — Workload Identity in Multi-System Environments
`exp` — token expiration time claim

Speaker reference: an explanatory map, not a claim that every rail is already cryptographically chained