

Trusted agent execution

Inspectable authority, work and evidence

Discussion draft for the November 9–11, 2026 TBM Conference. DPF-originated work; no foundation endorsement, certification or completed cross-platform conformance is claimed.

The proposal

An agent can produce persuasive reasoning while acting under stale policy, excessive authority or an unqualified operating profile. A prompt review cannot show whether a business effect was permitted or whether its evidence was sufficient.

The project proposes a portable contract for the harness around an AI model. It connects the actor, its versioned operating profile, job qualification, accountable policy, bounded effects and attributable results. Model recommendations inform decisions; they do not grant permission.

Four responsibilities

TAK mediates effects through current authority, data, oversight and evidence controls. **GPP** models the capability envelope admitted by a scoped decision for a work stage, subject and validity period. TAK enforces that envelope. **GAID** connects identity, active profile, claims, lifecycle status and receipts. **TAK-JSI** defines qualification for a job and operating context, including change and revalidation.

A qualification does not grant authority. A GPP binding narrows available authority. A permission does not prove competence.

DPF binds platform, organization and profession decisions through WWMD, WWWD and WSID. Other platforms need equivalent accountable scopes, not those acronyms. Platform engineering cannot silently decide an organization's expense policy.

Model the execution chain

Requirement → work shape → scoped decision → GPP envelope → TAK-mediated effect → receipt → assessment and revalidation.

The proposed MBSE profile composes existing approaches: SysML for requirements and interfaces, process/state views for progression, DMN for decision dependencies and provenance for evidence relationships. Added semantics connect the decision's owner to the execution boundary and result. No new general modeling language or achieved interchange conformance is claimed.

Normative ownership remains with the standards family; the contribution roadmap retains venue allocation. This packet adds no requirements.

Evidence before adoption

Two contexts, one contract

The first specimen uses DPF software-development work. The second, selected by the operator, approves a synthetic expense using fabricated records and an isolated destination. It cannot make payments or access banking services. The finance owner must establish the specimen's policy, evidence rules and thresholds before assessment.

Both specimens should expose policy ownership, scope, qualification, tool mediation and receipts. Proposed vectors cover a permitted action, missing evidence, exceeded authority, revoked permission, stale policy, replay and material profile change. Expected outcomes are not execution results.

Independent Hermes Agent and Cursor reproductions remain programme work. An external participant must control at least one implementation or assessment before independence is claimed. A static walkthrough explains the proposed path if a qualified runtime demonstration is unavailable; it cannot satisfy live assessment.

Measure acceptable work

Cost per accepted outcome = attributable cost for the complete evaluated cohort ÷ accepted outcomes in that cohort.

Include unsuccessful attempts, retries, supervision and rework. Define acceptance independently and compare equivalent work, quality, data and operating conditions. With no accepted outcomes, report the ratio as undefined alongside total cost and failures. Also track exceptions, unauthorized effects and recovery after material change. This packet reports no measured savings.

Bounded-output inference, including TypeSafe Jev, is a component candidate. Typed output does not establish truth, calibration or permission. No provider adoption, inference run or performance claim is made.

The collaboration request

Review the narrow execution contract and its negative tests; identify overlap with existing work; help recruit one independent implementer and one assessor. Agree on a versioned evidence package that includes limitations, supervision and rework before discussing adoption.

Working-group review, project hosting and formal standardization are different decisions. License, patent, asset-transfer, membership and submission choices remain with the owner. No outreach or commitment has occurred through producing this packet.

Sources and current limits

Primary sources checked October 16, 2026: TBM Conference; OMG SysML 2.0 and DMN 1.5; W3C PROV-O; TypeSafe Jev; AAIF project intake and lifecycle policy. See the linked source register for exact URLs. The accompanying gap sheet separates source artifacts from uncompleted runtime and independent assessment.

Primary links: [TBM](#) | [SysML](#) | [DMN](#) | [PROV-O](#) | [AAIF policy](#) | [Jev](#)