Supplement S2: Requirements

to Securing the Semantic Supply Chain: Meaning as a Foundation of Trust Infrastructure

Supplement to the research article

Dr. Carsten Stöcker
Spherity GmbH
carsten.stoecker@spherity.com
ORCID 0009-0003-7417-8872

Version 1.0, 16 November 2026 doi:10.5281/zenodo.24293613



Except where otherwise noted, this work is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). © 2026 Dr. Carsten Stöcker.

Contents

Legend **3**

S2.1 Governance and authority of meaning (GOV) **4**

S2.2 Producing meaning (PRD) **5**

S2.3 Keys and release (KEY) **7**

S2.4 Distribution (DST) **8**

S2.5 Verification and use (VER) **11**

S2.6 Decision and accountability (DEC) **15**

S2.7 Monitoring and response (MON) **21**

S2.8 Interoperability and conformance (INT) **24**

S2.9 Performance and availability (PRF) **25**

S2.10 Privacy (PRV) **26**

S2.11 Summary **28**

What is new, in one list **29**

S2.12 From this table to the Community Group's first drafts **30**

S2.13 Regulation to architecture (full table) **31**

Numbers in square brackets refer to the reference list of the article.

This supplement belongs to the article *Securing the Semantic Supply Chain: Meaning as a Foundation of Trust Infrastructure* (C. Stöcker, 2026).

Objectives and use cases. The objectives OBJ-1 to OBJ-11 are defined in the article, §3, and the use cases UC1–UC4 in the article, §7. UC5 (the article, §7) states open problems and adds no requirements. UC6 (the article, §7.6), verifiable business-partner records, applies the requirements and adds none.

Requirements. 91 requirements in 10 groups. The table is offered as **our proposed requirements baseline** for the W3C *High Assurance Profile for W3C VCDM 2.0* Community Group (proposed 11 November 2026; launched 12 November 2026); the group has not adopted it. The **Profile** column says which requirements belong in a W3C profile, in which module, and which belong to other bodies.

Legend

Column	Values
Novelty	★ **NEW**: introduced by the article (as far as the prior-art searches of 12–13 and 16 November 2026 found (S4)). ◐ **REFINED**: extends or sharpens an existing requirement; the basis is named. ◯ **BASELINE**: restates an existing requirement needed for completeness
Basis	Prior art, standard or regulation the requirement starts from. PoS = *Proofs over Statements* v1.3 (Stöcker, 9 Nov 2026); WP = *The Semantic Supply Chain* working paper (Stöcker, 7 May 2026)
Class (conformance class)	**I** issuer · **H** holder/wallet · **V** verifier · **P** semantic-artefact publisher · **D** distribution or registry operator · **E** ecosystem or governance authority
Profile	**Core**: normative for every implementation of the profile. **Core (if . . .)**: normative whenever the named feature is used or claimed (for example compressed carriers, replayable receipts). **Opt: module**: an optional module; MUST statements apply to implementations that claim the module. **Ref**: the profile references another body (ETSI ESI, IETF, SLSA, TUF). **Dep**: informative deployment guidance; contains no MUST
Obj	Objective(s) OBJ-1–OBJ-11 (authority, integrity, freshness, rollback, consistency, completeness, bounded processing, safe interpretation, privacy, accountability, conditional availability)
Lvl	Minimum semantic assurance level (WP levels): L2 profiled, L3 high assurance, L4 qualified/regulated
UC	1 Battery Passport and label · 2 e-commerce shipment · 3 edge verifier · 4 AI agent
Mech	Mechanisms M1–M31 (the article; S1) · HW-* (identifiers of the planned Paper B profile; not yet published)
Ev	Evidence: WE-1 to WE-5 (harness v0.3.0; for corrected mechanisms this is evidence about the predecessor, see the article, §4), experiments X1–X14, model checks MC-1–MC-6, a theorem in parentheses, or —

Identifiers of the form R2-nn and R3-nn in the Basis and Ev columns name review findings; S5 records them.

S2.1 Governance and authority of meaning (GOV)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
GOV-1	Each semantic-artefact release MUST identify its publisher, authority record and exact namespace/type scope. Verifier authorisation is specified separately by GOV-7.	◐	CIR (EU) 2025/1569 Art. 8 (catalogue); SD-JWT VC Type Metadata publishers; WP	P	Core	1	L3	all	M8, M29	—
GOV-2	Before acceptance, the verifier MUST establish issuer authorisation for the credential type and selected rulebook version using the authenticated authorisation snapshot selected by the recorded decision-time policy.	◐	WP check 4; SD-JWT VC; HAIP §3.4 (out of scope there)	V	Core	1	L3	1, 2	M22, HW-K3	—
GOV-3	An ecosystem claiming L4 publisher assurance MUST define an authenticated trust anchor and a supervised register schema that binds publisher identity, authority scope, keys, status and effective times.	★	ETSI TS 119 612/602 (issuers only)	E	Ref (ETSI profile; L4 only)	1	L4	1, 2	M29	—
GOV-4	In the reviewed-release module, each semantic release MUST have recorded approval of its exact source/release digest by two distinct authorised reviewers before release signing.	○	SLSA 1.2 Source track	P	Opt: reviewed release	1, 10	L3	all	M1	—
GOV-5	Semantic artefacts SHOULD identify the legal text and version they model, using an official identifier and effective date where available.	★	WP layer model	P	Opt: legal linkage	10	L4	1, 2	M3	—
GOV-6	Conformance testing and access to the normative specification MUST NOT require enrolment with a designated private platform operator.	○	WP §4.4	E	Core	1	all	all	P1	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
GOV-7	Before accepting a semantic release, the verifier MUST validate its publisher authorisation against the selected authenticated root: all delegation signatures and thresholds, namespace/type constraints, role separation, validity intervals, root version and revocation state must satisfy the profile's authorisation predicate.	◐	TUF delegations; X.509 name constraints; formal model T17	V	Core	1	L3	all	M8, M29	— (T17)

S2.2 Producing meaning (PRD)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRD-1	A release claiming the reproducible-build profile MUST provide verifiable provenance identifying reviewed source, complete pinned build inputs and deterministic build parameters, together with an independent rebuild producing the release digest.	◐	SLSA 1.2; in-toto (software only)	P	Ref (SLSA / in-toto profile)	2	L3	all	M1	—
PRD-2	Every release MUST publish a compatibility assessment containing L2 and L3 semantic diffs against the preceding release over a declared versioned corpus; detected or otherwise known incompatible changes MUST use a new immutable version identifier.	★	ROBOT/Bubastis diff; EBSI and eProcurement versioning rules	P	Core	4, 10	L3	all	M2	—
PRD-3	The publisher MUST publish an authenticated canonical dependency manifest covering the complete supported context-resolution closure and every L3 dependency, including shape severity/openness and parent versions.	◐	PoS L1(c); SHACL security (Chiem Dao & Debruyne)	P	Core	6	L3	1, 2	M3	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRD-4	For each claimed pair of representation formats, the publisher MUST supply a versioned transformation specification and conformance vectors showing equal canonical RDF or equal defined application outputs, whichever equivalence the profile claims.	★	YAML-LD tests (isomorphism only)	P	Core (if cross-format equivalence is claimed)	2, 6	L3	1	M4	—
PRD-5	The publisher MUST declare an admitted input language, maximum sizes and deterministic work-budget semantics, and publish conformance vectors covering its admitted production boundary and adversarial cases.	★	RDFC-1.0 §7.1; Fujie & Suzuki	P	Core	7	L3	2, 3	M1, M19	WE-4
PRD-6	Verifiers claiming this JSON-LD authoring-format module MUST accept only the authenticated built representation as a runtime semantic input, rather than processing YAML-LD source during verification.	◐	YAML-LD §6	V	Opt: JSON-LD authoring	2, 7	L3	all	M6	—
PRD-7	In the machine-generated-source module, each release containing machine-generated semantic source MUST carry provenance identifying that source and an authorised human approval of its semantic changes before signing.	★	AI Act Art. 50 covers specific content categories only; this is the profile's own control	P	Opt: machine-generated source	1, 10	L3	2, 4	M7	—
PRD-8	Each published crosswalk MUST identify pinned source and target vocabulary versions and carry an authenticated versioned mapping specification with declared relation semantics, loss conditions and conformance vectors.	◐	SSSOM; Health-RI mapping governance	P	Opt: crosswalks	2, 6	L3	2	M28	—
PRD-9	A verifier using a compiled context MUST authenticate its compiler/profile version and source-closure digest and verify the profile-required evidence that its processing semantics match that source closure.	★	Ruby json-ld preloaded contexts (unsigned)	P, V	Opt: compiled contexts	2, 7	L3	3	M5	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRD-10	Every closure offered for blank-node-free admission MUST carry a signed certificate binding its complete source/compiled closure digest, admitted document grammar, processor semantics/options, certificate-checker version and the sound admission property established by the named certification procedure.	★	Review finding R2-14; formal model T9.2	P	Core (if blank-node-free admission)	7	L3	all	M5, M18	— (T9.2)

S2.3 Keys and release (KEY)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
KEY-1	Publisher release keys MUST be generated and used within an approved key-protection boundary whose certified or attested configuration prohibits plaintext key export.	○	eIDAS QTSP practice	P	Ref (key-protection profile)	1	L3	all	M10	—
KEY-2	In the policy-gated-signing module, the signing service MUST refuse release signatures unless it has authenticated all gate evidence required by a pinned policy and bound that evidence to the exact release digest and signing request.	★	Kritis Signer (outside HSM); DiVerify	P	Opt: policy-gated signing	1, 2	L3	all	M10	—
KEY-3	In the independent-build threshold module, release signing MUST require the declared threshold of independently administered builders to contribute shares bound to the identical release digest after verifying their own reproducible-build results.	★	apt-transport-in-toto, repro-threshold (client-side)	P	Opt: independent-build threshold	1, 2	L4	1, 2	M11	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
KEY-4	Each role's authenticated key-lifecycle policy MUST specify rotation, revocation effective time, compromised-key recovery, trust-anchor transition and the treatment of previously signed artefacts.	◯	TUF	P, D	Ref (TUF-style profile)	1, 4	L3	all	M8, M10	—
KEY-5	Every signing and verification role MUST enforce a versioned authenticated algorithm policy that specifies allowed algorithms/key sizes, effective dates, verification horizons and downgrade rules, including state-management rules for any stateful hash-based scheme.	◐	NIST SP 800-208; RFC 9964; PoS §8.6	P, I, V	Core	1	L3	1	M12, HW-C4	—
KEY-6	Random seeds used for keys, nonces, salts or randomised assignments MUST satisfy the named entropy/RBG profile, with the profile-required source, health-test and generation evidence; deterministic derivations MUST use the separately specified approved construction. The same applies to whichever actor generates a hiding-commitment salt, including holders, and the salt MUST be encoded as fixed-length octets; this row is mandatory wherever M31 commitments are claimed.	★	NIST SP 800-90A/B/C; BSI AIS 20/31	I, P, H, V	Opt: entropy profile (mandatory with M31 commitments)	2, 9	L3	1, 2	M13, M31	—

S2.4 Distribution (DST)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DST-1	A verifier MUST load each semantic dependency from bytes matching the authenticated closure manifest selected for the recorded decision context.	◐	VCDM 2.0 `relatedResource`; vc-data-integrity #272 resolution (verifier side only)	V	Core	2	L3	all	M8, HW-S3	WE-1 E
DST-2	A verifier MUST refuse definitive acceptance unless every indispensable object in its authenticated metadata/status chain has valid signatures and hash/version links and is unexpired under the profile's trusted-time rule.	★	TUF timestamp role (software only)	V	Core	3	L3	all	M8	—
DST-3	Before each use, the verifier MUST enforce the scoped rollback predicate: metadata is at least its durable high-water mark; the artefact version is at least its durable high-water mark unless explicitly authorised by a valid scoped downgrade; and the artefact is absent from its permanent withdrawal set.	★	TUF / Uptane (software only)	V	Core	4	L3	3	M8, M14	MC-1
DST-4	A verifier requiring witnessed transparency MUST accept a release only with an inclusion proof under a checkpoint consistent with its retained checkpoint and cosigned under the profile's common, stateful, honestly intersecting witness-quorum policy.	★	RFC 9943 (architecture); witness cosigning with intersecting quorums (T7)	V	Ref (transparency profile)	5	L3	1, 2	M9	—
DST-5	The publisher MUST publish each release's status through an authenticated state machine in which withdrawal is a terminal, threshold-authorised event identifying the exact affected version and scope.	★	— (TS11 catalogue has no status field)	P	Core	3, 10	L3	all	M8, M25	WE-3 E
DST-6	A verifier MUST enforce a profile-declared maximum clock error ε throughout each freshness decision and refuse definitive acceptance when it cannot establish that bound.	◯	RFC 3161; Roughtime	V	Core	3	L3	3	M8, M14	MC-1 (T4)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DST-7	An offline verifier MUST cease definitive acceptance at the earlier of the declared offline deadline and expiry of any indispensable supporting evidence, and label further outcomes unknown or subject to a separate authorisation policy.	◐	Uptane; US 12579272 (policies)	V	Opt: offline	3	L3	3	M14	—
DST-8	An archive operator supporting a long-lived carrier MUST retain and make retrievable by digest all manifest-specified decoding and interpretation inputs through the carrier profile's declared retention end date.	★	ESPR data carriers; Battery Regulation (passport from 18 Feb 2027)	D	Core (if long-lived carriers)	10	L3	1	M15	**WE-2 S6**
DST-9	A compressed-carrier verifier MUST use the profile-specified authenticated binding to the complete decoding manifest in DST-12 and MUST consume only the output authenticated by the selected profile: signed-envelope deterministic decoding for B, or verified inner RDF graph for I-RDFC.	★	CBOR-LD 1.0 WD; VC Barcodes; T10	I, V	Core (if compressed carriers)	2, 6	L3	1	M15	**WE-2 S3, S5, S7**; X4, X7, X8; MC-4
DST-10	Under the declared network-observer model, the distribution protocol MUST make observable retrieval/update traces independent of the processed credential, except for explicitly declared leakage; conformance MUST test the specified trace-equivalence property.	◯	SD-JWT VC privacy considerations; WP	V, D	Core (if resolution privacy is claimed)	9	L3	all	M8, M20	—
DST-11	A distribution profile MUST specify the authenticated object that asserts current status, its maximum lifetime Δ_status, its honest-signing/compromise assumptions, the checked metadata chain and the resulting cessation bound Δ_status + ε; outer timestamps MUST NOT refresh the validity of expired or stale underlying status evidence.	◐	TUF timestamp/snapshot/targets expiries; review finding R2-04	E, D, V	Core	3	L3	all	M8	MC-5

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DST-12	A compressed-carrier manifest MUST bind every decoding input that can affect output: registry and decoder/processing-model identifiers and versions, codec implementations or normative semantics, type and URL codecs, tables, transitive contexts, base/processing options and canonicalisation/normalisation rules.	★	CBOR-LD 1.0 WD (registry entries, codecs); review finding R2-13	I, P	Core (if compressed carriers)	2, 6	L3	1	M15	MC-4; X7
DST-13	A transparency deployment claiming conflict detection MUST specify and operate an honest monitor that eventually retrieves all leaves through accepted checkpoints and checks a declared conflict relation over publisher, namespace, identifier, version, epoch and status.	◐	Certificate Transparency monitors; RFC 9943	D, E	Ref (transparency profile)	5	L3	1, 2	M9	— (T7)

S2.5 Verification and use (VER)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
VER-1	In the authenticate-first module, the verifier MUST validate an approved lexical/envelope authentication gate binding the exact input before invoking JSON-LD expansion or RDF canonicalisation. A standalone RDF proof requires an independently specified bounded-processing profile or an additional gate; it does not conform to this module by itself.	◐	PoS §5.4 (cheap pre-checks; residual: forged proof naming an allowed issuer); Fujie & Suzuki	V	Core (if authenticate-first module)	7	L3	2, 3	M17	**WE-4**; X10, X11

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
VER-2	For the RDF module, the securing mechanism MUST bind the accepted RDF dataset to the issuer-authenticated canonical dataset or its signed commitment, with the processing profile identified. Closure archival and L3 interpretation MUST separately satisfy the closure requirements.	◐	PoS L1, L3(iii); vc-jws-2020 (historical)	I, V	Core (if RDF module)	2, 6	L3	all	M17	**WE-1 B, D, F**
VER-3	The verification cell MUST have no network capability and MUST accept external dependencies only through the authenticated, integrity-checked snapshot interface.	◯	DI 1.0 §5.14 (network requests not required; defensive fetching allowed) — this is a stronger rule; Fujie & Suzuki (SSRF)	V	Core	2, 9	L3	all	M20	WE-1 I
VER-4	A verifier claiming the blank-node-free RDF profile MUST reject inputs outside its normative admission grammar and MUST use a closure certificate tied to the complete closure digest, processor/options and grammar version, whose certification establishes that every admitted input expands without blank nodes.	◐	PoS A1; F5 (lists with repeated values); review finding R2-14	I, P, V	Opt: blank-node-free RDF	7	L3	all	M18	**WE-4**; X1, X5, X9
VER-5	A verifier MUST derive any definitive budget-exceeded rejection from the profile's deterministic metering semantics; a wall-clock or resource interruption MUST yield unknown/retryable, not a cryptographic-invalid verdict.	★	PoS §9.1 (time limit with interrupt); rdf-canonize, rdf-canon limits	V	Core	7, 10	L3	2, 4	M19	**WE-5**
VER-6	When an authenticated representation is transformed into the application view, the verifier MUST reject loss of an authenticated, interpretation-relevant member except for omissions explicitly permitted by the selected transformation profile.	◐	DI 1.0 §2.4.3 (securing transformations); PoS L1	I, V	Core	6	L3	all	M17	WE-1 G

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
VER-7	Issuers/publishers MUST authenticate a critical-extension declaration using the profile's scoped identifiers. Verifiers MUST reject unsupported critical extensions and MUST apply supported ones according to that profile; a closed-world profile MUST reject every unsupported extension.	◐	X.509 critical extensions; JOSE `crit`; W3C #218	I, P, V	Core	8	L3	all	M21	—
VER-8	A derived presentation MUST preserve the issuer-authenticated interpretation of each disclosed statement under the selected disclosure profile; the verifier MUST separately enforce the policy's required inputs and proofs. Selective disclosure of policy-irrelevant fields remains permissible once the complete required evidentiary basis is established; for compliance decisions, DEC-8 applies.	◯	PoS P2	I, H, V	Core (if selective disclosure)	6, 8	L3	1, 2	M21, M31	—
VER-9	Before applying a status entry, the verifier MUST validate its pinned status profile and authenticated evidence against the profile's maximum age and trusted-time rules; unavailable or stale status MUST yield unknown.	◐	Bitstring Status List; W3C #218; revocation series	I, V	Core (if status-bearing credentials)	3, 8, 9	L3	all	M21	—
VER-10	Raw-context caches MUST verify their content-addressed bytes. Processed-context caches MUST additionally key entries by all processing inputs, including effective/base URL, active context where relevant, processor/profile/options and trust domain.	★	jsonld.js #502, #537, PR #552 (functional bug, no security framing)	V	Core	2, 5	L3	2, 4	M20	WE-1 H
VER-11	Applications MUST consume the immutable authenticated view or the output of a pinned, approved derivation from that view.	◯	PoS Def. 5.2, P4	V	Core	6	L3	all	M17, M21	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
VER-12	Render metadata MUST NOT alter machine validation semantics unless explicitly admitted as a semantic dependency by the profile. Human-decision interfaces MUST identify and integrity-check any template on which the presented interpretation relies.	◐	VC Render Method WD (digest optional)	I, H, V	Opt: rendering	1, 8	L3	2	M21	—
VER-13	Verifiers MUST derive L3 interpretation solely from the pinned vocabulary/rule closure and the identified interpretation engine/configuration, including built-in mappings and inference rules.	★	PoS L1 (contexts only); formal model T2 (LFSC binds L2, not L3)	V	Core	2, 6	L3	all	M3, M22	—
VER-14	JSON inputs MUST satisfy the declared I-JSON/JCS profile on raw UTF-8 text, including unique names, permitted Unicode, finite binary64 parsing and specified rounding; exact decimal quantities outside that model MUST use a specified string/typed-value representation. The authenticated parsed value MUST be passed immutably onward.	◐	RFC 7493; RFC 8785 (assumes I-JSON); formal model T16	V	Core (if JSON input)	2, 8	L3	all	M17, M18	—
VER-15	Before accepting a credential proof, the verifier MUST establish from authenticated, current local authorisation evidence that the exact verification method is authorised by the credential's authenticated issuer for the required purpose and scope.	◯	VC Data Integrity 1.0 (verification method and controller)	V	Core	1, 2	L3	all	M17	X10

VER-16	Before semantic acceptance, the verifier MUST verify that every dependency actually used by expansion/interpretation is present in the authenticated closure manifest, including nested/scoped/imported contexts, relevant loader metadata, processor options and interpretation configuration; undeclared resolution MUST fail closed.	★	JSON-LD 1.1 embedded and scoped contexts; review finding R2-02	V	Core	2, 6	L3	all	M3, M17, M22	X2; X12

S2.6 Decision and accountability (DEC)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-1	Every replayable receipt MUST cryptographically bind the outcome and a manifest identifying the reconstructible decision context, including executable/configuration semantics and decision-relevant state, by authenticated digests. A replayable action receipt MUST also bind its profile and key epoch, request or challenge, subject, action and scope, audience and purpose, and role-labelled dependencies in one injective encoding; honest approval MUST be keyed to these exact bytes, and single-use actions MUST enforce consumption or equivalent idempotency.	★	AI Act Art. 12 (record-keeping, where applicable)	V	Core (if replayable receipts)	10	L3	all	M22, M24	— (T11′, T14)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-2	A time-scoped decision MUST bind the selected historical/current closures, selection rule and authenticated time evidence. If certification time selects meaning, use the validated TSA generation time or trusted bounded log-inclusion time bound to the evidence digest; issuer-asserted event time alone MUST NOT select it.	★	Bi-VAKs, Temporal RDF (data, not decisions); HS 2028 (1 Jan 2028)	V	Opt: temporal decisions	10	L3	2	M27	—
DEC-3	Retained evidence SHOULD support the selected format's standalone proof re-verification. A long-term preservation profile MUST specify evidence renewal, algorithm migration and validation-material retention before relevant trust expires.	◯	PoS Def. 5.1 (requirement); LFSC-G is a new means	I, V	Opt: long-term preservation	10	L3	1, 2	M17	v0.3.0: **0.18 ms**
DEC-4	In the agent-authority module, admission tokens MUST bind the action, closure and authority epoch; accepting an applicable withdrawal MUST advance the epoch durably.	★	Revocation series (authority epoch for mandates)	V	Opt: agent authority	6, 10	L3	4	M22, M25	WE-3 E (relying party)
DEC-5	When required meaning or its verification evidence is unavailable, stale or indeterminate, the verifier MUST return unknown and MUST NOT authorise the action through that verification path; any escalation MUST use a separately authorised, recorded policy.	◐	Revocation series ("stale is unknown"); AI Act Art. 14	V	Core	3, 7	L3	all	M19, M22	WE-5

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-6	For the declared replay-retention period, the receipt custodian MUST preserve and retrieve by authenticated digest every dependency required to reconstruct the claimed decision, including executable semantics/configuration and relevant state; privacy/access restrictions MUST be part of the preservation profile.	◐	RFC 4998 / RFC 6283 evidence records	V, D	Core (if replayable receipts)	10	L3	all	M22	— (T14)
DEC-7	An agent commit MUST atomically validate the token's action/closure authorisation against the current durable epoch and freshness/withdrawal state at the external effect's defined linearisation point. Where an effect depends on a co-signed receipt, it MUST NOT occur before that receipt is valid and these checks pass at that point; a provisional decision MUST NOT authorise the effect.	◐	Revocation series (authority epoch)	V	Opt: agent authority	6, 10	L3	4	M25, M24	MC-2; MC-6

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-8	For a decision under an authenticated compliance-evidence profile, the verifier MUST accept an evidentiary basis only when the profile's required input sufficiency, coverage (DEC-9) and computation guarantees are established: verified complete sufficient key claims, a valid certificate (DEC-10, DEC-11), or disclosed claims or proofs whose sufficiency for the exact policy, closure and required decision guarantee is established. Holder choice over policy-relevant evidence MUST NOT determine the outcome.	★	T19; VER-8; PoS P2; customs H1/H7 data sets (Rukanova et al. 2026); WCO Data Model	V	Core (if compliance-evidence module)	8, 10	L3	1, 2	M31, M22	— (T19.1–T19.5)
DEC-9	The governing compliance-evidence profile MUST identify the subject, action and purpose; the authoritative evidence domains and sources; identifier resolution and query or push coverage; the snapshot or cut-off; source authority and status; and the positive or absence evidence sufficient for every policy-relevant dependency. These choices MUST be authenticated independently of the holder, and missing, stale or inconsistent coverage MUST yield unknown.	◐	T19.5; WCO Data Model; customs data requirements; audit completeness assertion	E	Core (if compliance-evidence module)	6, 10	L3	1, 2	M31	— (T19.5)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-10	A certificate issuer MUST validate the profile-required authenticated evidence and coverage, recompute the hiding commitment, evaluate the pinned policy, and sign a canonical core binding the outcome, privacy-preserving input, coverage and context bindings, closure and policy digests, scope, authorisation reference and retention manifest. Indeterminate required coverage MUST yield unknown. Trusted time MUST be external evidence over the signed core.	◐	Conformity-assessment certificates; RFC 3161; RFC 4998	I, V	Core (if issuing evidence-graph certificates)	2, 10	L3	1, 2	M31, M27	— (T19.4)
DEC-11	A relying party MUST check the certificate's proof, the issuer's authorisation for the decision class, an authorising outcome, the selected certificate, its subject, action, purpose, audience and time scope against the request, the applicable closure and policy, and the required certificate, issuer and dependency status. Missing or stale required evidence MUST yield unknown; effect authorisation MUST satisfy the applicable commit-point rule (DEC-7).	◯	X.509 path validation and certificate policies (RFC 5280)	V	Core (if relying on evidence-graph certificates)	1, 10	L3	1, 2	M31	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-12	A certificate lifecycle profile MUST index certificates by every decision-relevant dependency (policy, closure, inputs, status) and define invalidation, suspension, replacement and historical-replay rules. After an invalidating event, including a policy-only correction with an unchanged closure, current reliance MUST cease within the declared freshness bound until re-evaluation with current inputs succeeds; replacement MUST preserve and link the prior record.	◐	Revocation series; RFC 5280 revocation	E, I, V	Core (if evidence-graph certificates)	3, 10	L3	1, 2	M31, M25, M27	—
DEC-13	Before treating a certificate as replayable, the verifier MUST validate a custodian acknowledgement of a verified deposit of the complete archive manifest, opening and recovery material bound to the certificate core. The custodian MUST demonstrate reconstruction on deposit and at profile-defined intervals, under defined continuity, access, retention and release rules.	◐	RFC 4998; provable data possession; proofs of retrievability	V, D	Core (if replayability claimed)	10	L3	1, 2	M31, M22	—
DEC-14	A dispute report MUST report separately the authenticity of the certificate and evidence, the validity of the opening, the reconstructibility of the context and the equality of the outcome. Missing evidence, inconsistent openings and computation mismatch MUST be distinct results, and any attribution of fault or statement of substantive correctness MUST name the additional evidence it relies on.	◐	RFC 4998; forensic reporting practice	V, D	Core (if dispute reporting claimed)	10	L3	1, 2	M31	— (T19.4)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
DEC-15	A profile claiming one authoritative evidence snapshot per scope and epoch MUST define an authenticated selection and supersession rule and enforce or detect conflicting selections through its consistency mechanism; verifiers MUST bind reliance to the selected snapshot.	◐	Transparency logs (M9; RFC 9943)	E, I, D, V	Core (if a single authoritative snapshot is claimed)	5, 10	L3	1, 2	M31, M9	— (T19.4)

S2.7 Monitoring and response (MON)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
MON-1	An implementation selecting the semantic-inventory module MUST produce a signed inventory of loaded closure/configuration digests. Operators SHOULD run a declared differential corpus against those versions and record divergences.	★	CycloneDX data components (static); EBSI conformance header	V, H, E	Opt: semantic inventory	5, 6	L3	2, 3	M23	—
MON-2	An implementation claiming execution-bound attested decisions MUST enforce an isolated decision runtime and exclusive authorisation of its certified receipt key, bind receipts to the exact executed context and relying-party challenge, and enforce current engine authorisation across upgrade/restart. Replay-validated receipts are a separate claim governed by MON-6 and MON-7.	★	Linux IMA CRITICAL_DATA (SELinux policy); RATS, EAT	V	Opt: attested engine	2, 10	L4	3, 4	M24	**WE-3** (v0.3 design, qualified); MC-3

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
MON-3	Publishers MUST issue authenticated advisories under the designated advisory/withdrawal role with affected immutable identifiers, action, scope and publication time. Verifiers MUST process them according to the pinned advisory policy and freshness rules.	★	CRA Arts. 13–14 (software); VEX	P, V	Core	3, 10	L3	all	**M30**	WE-3 E
MON-4	Agent deployments SHOULD compare the admitted closure digest with the closure used for each action and reject or re-admit on mismatch; semantic-change diagnosis requires a separate differential analysis.	★	KG/RAG poisoning (instance level); OWASP MCP03	V	Dep	6, 10	L3	2, 4	M26	—
MON-5	The attested-engine module MUST specify and enforce authenticated engine/key-policy updates, version rollback protection, revocation, state recovery and register/index lifecycle, with relying-party appraisal tied to the same policy version.	◐	TPM 2.0 PolicyAuthorize; RATS reference values	V, E	Opt: attested engine	1, 2, 10	L4	3, 4	M24	MC-3

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
MON-6	A replay co-signer MUST authorise only the exact canonical receipt message whose committed input and context it has authenticated, found admissible under the independently anchored request policy (authorised closure, current authority epoch and status, declared clock tolerance), and evaluated to the proposed definitive outcome; an unresolved dependency or an unknown outcome MUST NOT authorise a share.	◐	Hyperledger Fabric endorsement; CoSi witness cosigning	I, V	Opt: replay-validated receipts	2, 10	L4	3, 4	M24	MC-3 V6, V6x; MC-6
MON-7	A replay-signing profile MUST identify the threshold scheme, its security and corruption game, the authenticated group key, participant authorisation and key epoch, and MUST enforce the scheme's key-generation, nonce and session, restart, share-protection, rotation and revocation conditions; adaptive or mobile corruption claims require their own proof.	◯	RFC 9591 (FROST); threshold-signature security models	E, I	Opt: replay-validated receipts	1, 2	L4	3, 4	M24	— (T11′)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
MON-8	Before current reliance on an execution-bound or replay-validated receipt, the verifier MUST reject it unless an authenticated enrolment record from a governance-recognised authority satisfies the M24 acceptance predicate for the exact receipt key or group configuration, key epoch, claimed participant or device, approved engine and key-policy versions, responsible legal person and authorised scope at the defined use or commit point.	◐	RATS (RFC 9334); IEEE 802.1AR; TCG TPM 2.0 device-identity keys; RFC 8995; eIDAS Art. 35 (seals); agent–owner credentials [26]; NIST NCCoE agent-identity concept paper (2026); harness WE-3 E3; review record (S5)	V	Core (if execution-bound or replay-validated receipts)	1, 10	L4	3, 4	M24, M29	— (proposed; WE-3 E3 demonstrates only the key-certification limit)

S2.8 Interoperability and conformance (INT)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
INT-1	The profile specification SHALL define format-neutral security objectives and a requirements-applicability matrix for each supported format, with equivalent evidence and test obligations where mechanisms differ.	○	WP	E	Core (specification)	all	L2	all	all	WE-1, WE-2
INT-2	Each conformance module MUST publish positive and negative vectors for every applicable attack class, identify unsupported/untested classes, and define the expected outcome and applicable role.	◐	OpenID HAIP conformance; Fujie & Suzuki vectors	E	Core	all	L3	all	M1, HW §15	harness
INT-3	A conformance claim MUST identify the profile version, applicable format/modules, role, requirements satisfied and evidence for any declared assurance level.	○	WP levels 0–4	E	Core	all	L2	all	P1	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
INT-4	A technical conformance claim MUST NOT assert legal recognition or cross-jurisdiction equivalence unless separately established under the identified legal framework.	◯	PoS C2	E	Core	10	all	2	M27, M28	—

S2.9 Performance and availability (PRF)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRF-1	The authenticate-first module MUST specify maximum input/field sizes and an auditable preauthentication operation/memory budget; under the stated cost model, total preauthentication work MUST be O(n log n) or better plus the declared bounded number of cryptographic operations.	★	Fujie & Suzuki (problem); PoS §5.4 (residual)	V	Core (if authenticate-first module)	7	L3	2	M17, M18	v0.3.0: **WE-4 ≤ 0.33 ms**; X11
PRF-2	A verifier MAY cache results only after binding the request to the exact authenticated input and all decision-relevant dependencies; cache reuse MUST satisfy PRF-5.	◐	PoS T2, L3 (cache policy)	V	Opt: caching	7	L3	2, 4	M17	v0.3.0: **0.25 ms**; X13
PRF-3	The issuer MUST verify that the complete encoded carrier payload, including signatures, bindings, version/algorithm identifiers and error-correction overhead, fits the declared carrier/profile capacity.	◯	ESPR data carriers	I	Core (if carriers)	2	L3	1	M15	v0.3.0 128-bit configuration: **+23 bytes**
PRF-4	Agent deployments SHOULD declare hardware, workload/adversary envelope, latency percentile and overload behaviour, and measure the selected verification profile against that budget.	◯	Agent-kernel paper	V, E	Dep	7	L3	4	M17, M22	—

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRF-5	A cached result MUST be reused only while its authenticated input, processing/configuration, issuer-key authorisation, trust/policy/status snapshots and time-dependent predicates remain valid; negative or unknown entries MUST have bounded lifetime/storage and MUST NOT suppress re-evaluation after a relevant dependency changes.	◐	PoS caching (T2, L3); review finding R2-15	V	Opt: caching	2, 3, 7, 10	L3	2, 4	M17	X13
PRF-6	A profile claiming availability MUST specify its admitted input/workload and resource envelope, dependency-reachability assumptions and retention horizon, and demonstrate the declared bound to a definitive result under those conditions, with explicit overload/partition outcomes. Where decisions depend on replay co-signing, the envelope MUST include a reachable, willing qualified quorum ($n - f \geq t$), coordinator and progress assumptions, terminating deterministic evaluation and permitted context access, and its tests MUST distinguish safe refusal or deferral from completion.	◐	Review finding R2-11 (availability objective OBJ-11)	V, D, E	Opt: availability	11	L3	all	M8, M15, M24	— (T4); MC-6

S2.10 Privacy (PRV)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRV-1	A profile claiming presentation unlinkability MUST use presentation-specific identifiers supported by its authenticated disclosure/re-randomisation scheme and MUST demonstrate that exposed identifiers/proofs do not enable linking under its stated observer model.	◐	`ecdsa-sd-2023` HMAC relabelling (identifiers stable per credential); review finding R2-03	I, H, V	Opt: unlinkability	9	L3	1, 2	M18	—
PRV-2	A status-index privacy module MUST define its assignment distribution, adversary knowledge, audit relation and permitted leakage, and provide a specified proof/audit procedure that verifies assignment policy without revealing protected mappings.	◐	Bitstring Status List ("SHOULD assign randomly")	I, E	Opt: status-index privacy	9	L3	all	M13	—
PRV-3	A masking profile MUST identify an immutable version of its cover-entry lifecycle rules and conformance vectors; its documentation MUST state the residual correlation/leakage and MUST NOT claim privacy from cover entries alone.	○	W3C #218 (author's proposal, not adopted text)	I, P, V	Opt: masked status lists	9	L3	all	M21	—
PRV-4	Shared evidence deployments SHOULD minimise exposed identifiers and commitments under a declared observer/data-protection model, use access-controlled indirection and appropriately hiding commitments where needed, and apply retention/access/deletion policy to pointers as well as payloads.	○	GDPR; PoS UC2	I, V, E	Dep	9	all	2	(PoS)	—
PRV-5	A resolution-privacy profile MUST declare the observer/permitted leakage and ensure credential-dependent identifiers, cache misses, message sizes, timing, failures and retries do not influence exposed resolution traffic beyond that leakage.	◐	Oblivious HTTP (RFC 9458); OCSP stapling; review finding R2-20	V, D	Core (if resolution privacy is claimed)	9	L3	all	M20	— (T18)

ID	Requirement	Novelty	Basis	Class	Profile	Obj	Lvl	UC	Mech	Ev
PRV-6	An evidence-certification profile claiming confidentiality MUST specify the permitted leakage of the entire public certificate, presentation, status and locator transcript, and MUST bind private inputs in public digests only through hiding bindings; personal-data processing MUST define purpose-specific necessary inputs, recipient and custodian access, and retention. Any unlinkability claim MUST use a supported presentation scheme and an observer-model test.	◐	GDPR Art. 5(1)(c); review findings R2-27 and R3-12	E, I, H, V, D	Core (if certificate confidentiality is claimed)	9	L3	1, 2	M31	— (R3-12 reproduction)

S2.11 Summary

	★ NEW	◐ REFINED	◯ BASELINE	Total
GOV	2	3	2	7
PRD	6	4	0	10
KEY	3	1	2	6
DST	7	4	2	13
VER	4	8	4	16
DEC	4	9	2	15
MON	4	3	1	8
INT	0	1	3	4
PRF	1	3	2	6
PRV	0	4	2	6
Total	**31**	**40**	**20**	**91**

Profile	Count	Meaning for the Community Group
Core	29	Normative for every implementation
Core (if . . .)	26	Normative when the named feature is used or claimed: RDF module, authenticate-first module, JSON input, compressed or long-lived carriers, selective disclosure, status lists, replayable receipts, execution-bound or replay-validated receipts (their attribution, MON-8), resolution privacy, blank-node-free admission, cross-format equivalence, compliance evidence (sufficiency, coverage, certificate issuance and reliance, lifecycle, archive deposit, dispute reporting, snapshot selection, transcript confidentiality)
Opt: module	27	Optional modules: reviewed release, legal linkage, JSON-LD authoring, machine-generated source, crosswalks, compiled contexts, policy-gated signing, independent-build threshold, entropy, offline, blank-node-free RDF, rendering, temporal decisions, long-term preservation, agent authority, semantic inventory, attested engine, replay-validated receipts, caching, availability, unlinkability, status-index privacy, masked status lists
Ref	6	The profile references ETSI ESI (L4 publisher registers, key protection), SLSA/in-toto, TUF-style key lifecycle, and a transparency profile with witnesses and monitors
Dep	3	Informative deployment guidance without MUST (MON-4, PRF-4, PRV-4)

What is new, in one list

1. **Meaning has a release lifecycle.** Signed, time-bounded distribution metadata; rollback protection; artefact status and withdrawal; split-view detection (DST-2 to DST-5).
2. **Producers carry obligations.** Expansion-level semantic diff with enforced versioning; attested cross-serialisation equivalence; declared processing bounds; signed compiled contexts; AI-generated semantics as untrusted source (PRD-2, 4, 5, 7, 9).
3. **Keys and randomness for meaning.** Signing gated inside the HSM or TEE; rebuild-gated threshold release; declared entropy class (KEY-2, 3, 6).
4. **Long-lived carriers.** Codec tables bound outside the compressed payload; lifetime archive by digest (DST-8, DST-9).
5. **Verification that is safe and replayable.** Deterministic bounds that decide *invalid*; content-addressed context caches; quasi-linear rejection; interpretation of IRIs only through pinned artefacts (VER-5, VER-10, VER-13, PRF-1).
6. **Decisions remember their meaning.** Closure digest in receipts; time-scoped meaning; withdrawal of meaning changes agent authority (DEC-1, 2, 4).
7. **Watching meaning.** Semantic BOM; measured semantics; semantic advisories; detection of definition-level poisoning (MON-1 to MON-4).
8. **Regulated anchor.** Trusted lists for publishers of meaning; legal-text linkage (GOV-3, GOV-5).
9. **Scoped authority, complete closures and safe reuse.** Scoped publisher authorisation (GOV-7); a certificate for blank-node-free closures (PRD-10); freshness anchored on the status-bearing object (DST-11); a complete decoding manifest for compressed carriers (DST-12); conflict monitoring (DST-13); issuer-key authorisation and a processing-aware closure, including contexts nested in the document (VER-15, VER-16); preservation for replay and atomic commit (DEC-6, DEC-7); engine lifecycle for attested decisions (MON-5); safe cache reuse and conditional availability (PRF-5, PRF-6); privacy of resolution traffic (PRV-5).
10. **Compliance decisions.** Compliance decisions rest on one view of the evidence: full disclosure of a standardised key-claim set, or a certificate over a committed evidence graph with replay in a dispute (DEC-8; its obligations are split by role in item 11).

11. **Compliance evidence as role-specific obligations.** A coverage contract independent of the holder (DEC-9), certificate issuance with source validation and external time (DEC-10), scope-checked reliance (DEC-11), lifecycle including policy-only changes (DEC-12), verified archive deposit (DEC-13), classified dispute results (DEC-14), snapshot selection (DEC-15) and transcript confidentiality (PRV-6); replay-validated receipts as their own module (MON-6, MON-7).
12. **Attribution of receipt keys.** Current reliance on an execution-bound or replay-validated receipt requires an authorised enrolment record (MON-8), normative whenever such receipts are used. Technical authentication of the exact receipt key or group configuration remains mandatory under T11 or T11′; organisational attribution is a separate property that MON-8 also requires whenever either receipt feature is used.

S2.12 From this table to the Community Group's first drafts

The **Core**, **Core (if . . .)** and **Opt** rows (82 requirements) map onto a profile document. A planned companion profile paper (Paper B) would draft most of them as HW-* requirements.

Proposed CG document	Content from this table	Status of our material
1. Use Cases and Requirements (CG Report)	UC1–UC4 + objectives + all 91 rows, with the Profile column deciding what is normative	This supplement (S2)
2. High Assurance Profile for VCDM 2.0 (CG Report, editor's draft)	Core, Core (if . . .) and Opt rows as conformance requirements per class (I, H, V, P, D, E)	planned Paper B (HW-*), plus the new rows (DST-2 to 6, 8, 9, 11, 12; VER-5, 10, 13–16; DEC-1, 6, 8–15; MON-3, 6, 7, 8; GOV-7; PRD-10; PRV-6)
3. Securing Mechanisms note	`ecdsa-lfsc-2026` (experimental), M15 CBOR-LD binding envelope	Harness v0.4.0 + the article, §6, and S1; v0.3.0 remains the source of historical measurements
4. Test suite	INT-2 negative vectors for every attack class; W3C vectors; the model checker	Harness v0.4.0 (Apache-2.0, with third-party notices); supported and untested classes are identified in its README
Liaison items (not CG documents)	Ref rows → ETSI ESI (TS 119 612/602, TS 119 472), IETF (SCITT profile), JSON-LD WG (CBOR-LD security considerations), VCWG (threat model DoS entries), OpenID DCP (W3C format identifiers, DCQL type binding)	Listed in the article, §8 (requests to other bodies)

Points to raise with the group:

1. **Name collision.** "HAIP" is OpenID's *High Assurance Interoperability Profile*. A distinct short name for the specification (for example *VCDM-HAP*) avoids confusion in EUDI and EBW discussions while keeping the group's name.

2. **IPR.** Community Group contributions fall under the W3C Community Contributor License Agreement, and final reports under the Final Specification Agreement. Both carry royalty-free commitments. This is consistent with publication without patents, but it means everything contributed is licensed royalty-free.
3. **Starting material.** The `eu-business-wallet/haip4w3c` repository (README skeleton and the May 2026 working paper) could move into the CG's GitHub organisation as its starting point.

S2.13 Regulation to architecture (full table)

The article (§8, Table 10) condenses this table. The full version adds the evidence artefact each mechanism produces and who verifies it. Legal statuses are as of 14–15 November 2026; the mapping is architectural, not legal advice.

Obligation or instrument (status, date)	Gap	Mechanism	Evidence artefact	Verified by
Battery Regulation (EU) 2023/1542, Art. 77: battery passport for LMT, industrial (> 2 kWh) and EV batteries from 18 Feb 2027	Restricted data relies on role meaning (the role-credential architecture is our proposal, not prescribed); labels outlive vocabulary versions	M15, M17, M22	Bound label envelope; receipt with closure digest	Passport provider; market surveillance
ESPR (EU) 2024/1781 (framework; product-specific requirements and dates follow in delegated acts) and the DPP Registry semantic data artefacts (30 Oct 2026)	Shapes and vocabularies sit in the evidence path; the published artefacts carry version metadata and a concept-level status, but no freshness or expiry metadata and no signed, artefact-level withdrawal (we did not audit the Registry protocol as a whole)	M3, M8, M9	Closure manifest; signed release metadata; transparency receipt	DPP service provider; market surveillance
eIDAS (EU) 910/2014 as amended. Catalogue of attributes and schemes, CIR (EU) 2025/1569 Art. 8: scheme status and version; authenticated inclusion and modification requests; governance including revocation mechanisms; a sealed catalogue. Arts. 6–9 apply from 19 Aug 2026; Art. 8 is unchanged by CIR (EU) 2026/1735. Qualified electronic ledgers: CIR (EU) 2025/2531, in force since 6 Jan 2026	Trusted lists cover who may *issue*, not who may *publish meaning*. Art. 8 does not itself specify catalogue-level withdrawal or deprecation transitions, or a maximum catalogue age for relying parties; we did not audit the catalogue specifications or operations	M8, M9, M29	Publisher entry in a trusted list; signed scheme status	Supervisory body; relying party
European Business Wallet proposal COM(2025) 838 (first reading; Council general approach 9 Jun 2026; Parliament's negotiating mandate confirmed 7 Oct 2026)	Legal-effect attestations across sectors and Member States rely on stable meaning	M22, M27	Receipt with closure digest and time-scoped selection	Relying party; auditor

Obligation or instrument (status, date)	Gap	Mechanism	Evidence artefact	Verified by
Cyber Resilience Act (EU) 2024/2847 (reporting obligations from 11 Sep 2026; main obligations from 11 Dec 2027)	Semantic artefacts in wallets and verifiers are undocumented components of covered products; no advisory process for meaning	M23, M30	Semantic BOM; signed semantic advisory (our proposed control)	Manufacturer; market surveillance
AI Act (EU) 2024/1689 as amended by the AI Omnibus (in force 27 Jul 2026): record-keeping (Art. 12) for high-risk systems, which apply from 2 Dec 2027 (Annex III) and 2 Aug 2028 (Annex I products), where the system is classified as high-risk	Logs record inputs, not the meaning applied to them; receipts with closure digests are our proposed implementation, not text of Art. 12	M22, M25	Decision receipt with closure digest and authority epoch	Deployer; supervisory authority
Union Customs Code reform, Regulation (EU) 2026/2108 (adopted 16 Sep 2026, in force, phased implementation); US CBP tests (DIDs and VCs for crude-oil pipeline data from 2 Jul 2026)	Automated risk analysis needs verifiable, semantically pinned data; holder-chosen disclosure of policy-relevant data would make the risk decision depend on the holder's choice	M17, M18, M27, M28, M31	Authenticated graph; time-scoped decision record; a sufficient data set with coverage evidence, disclosed in full or certified over a committed evidence graph	Customs authority