ARS-1

Agentic Remittance Standard

Working Paper v0.2 — Draft for Comment

Published by	Kadikoy Limited, Bermuda (Reg. 202302362)
Date	16 May 2026
Status	Draft — open for public comment
Version	0.2 — supersedes v0.1 (16 May 2026)
Companion to	AIS-1 Agent Identity Standard (ais-1.org); AAS-1 Agent Auditability Standard (aas-1.org)
Contact	info@aiagentsservices.net
Repository	github.com/Kadikoy1/ars-1
Website	ars-1.org
License	Creative Commons CC0 — no rights reserved

v0.2 KEY CHANGES FROM v0.1

NEW “In Essence” front-matter section — the standard in five paragraphs
PROMOTED ISO 20022 envelope mechanic — now Section 4
NEW Addressability via AIS-1 — Section 5
NEW Settlement-Layer Independence — Section 6
EXPANDED Operator profiles — three deployment patterns — Section 13
TIGHTENED Prose throughout; sharper assertions; removed hedging
RETAINED All v0.1 schemas, definitions, message classes, purpose codes

ABSTRACT

ARS-1 is the open protocol for agent-mediated value transfer. It is the action-protocol complement to AIS-1 (which gives agents identity) and AAS-1 (which gives agents an audit trail). Where AIS-1 outputs a verifiable identity card and AAS-1 outputs signed action records, **ARS-1 outputs messages** — structured, signed JSON documents that one party hands to another to instruct, execute, confirm, condition, or reverse a value transfer.

ARS-1 rides inside ISO 20022. A Class I instruction is a valid pain.001 message with the agentic payload carried in the `<SplmtryData>` extension envelope. Existing banking infrastructure routes the message without modification; ARS-1-aware operators unwrap the envelope and execute the agent-mediated logic. The standard is dual-readable from day one, settlement-rail agnostic, FATF Travel Rule-native, and globally addressable via AIS-1 DIDs — the universal address scheme that replaces N² operator-to-operator integration with a single integration to the standard.

v0.2 retains all v0.1 schemas and adds clarifying structure: explicit sections on the ISO 20022 envelope, AIS-1 addressability, and settlement-rail independence; named deployment-pattern profiles for the three classes of use case now in scope — institutional disbursement, commercial remittance, and state-to-citizen.

CONTENTS

IN ESSENCE

One. ARS-1 outputs messages. Five classes — Instruction (I), Transfer (T), Receipt (R), Conditionality (C), Reversal (V). Each is a structured, signed JSON document. The message is the artefact, parallel to the AIS-1 identity card and the AAS-1 audit record. One remittance lifecycle produces one Class I instruction, one or more Class T transfers, one Class R receipt, and — where conditions govern release — one or more Class C conditionality blocks. If something must be undone, a Class V reversal.

Two. Every party in a message is addressed by AIS-1 DID. A DID such as `did:ais1:base:recipient-agent-example` resolves, anywhere in the world, against the public AIS-1 registry to return the agent's keys, jurisdiction, sponsor, and AML status. The DID is the universal address. No operator maintains its own recipient directory. There is no bilateral integration. ARS-1 + AIS-1 are to value transfer what DNS + HTTP are to the web — one global address space, one shared protocol on top.

Three. ARS-1 rides inside ISO 20022. The Class I instruction is a valid pain.001 message. The agentic payload — identities, conditionality, compliance, onward delivery — sits inside the standard's `<SplmtryData>` extension envelope. To a bank running normal ISO 20022 infrastructure, the message is a perfectly conforming pain.001 it can route, log, and report on. To an ARS-1-aware operator, the same message contains the full agent-mediated transaction. The standard is dual-readable. It does not require banks to upgrade to carry it.

Four. Settlement is rail-agnostic. The underlying movement of value — USDC on Base, EURC on Avalanche, a Bermuda-issued ISA stablecoin on Hedera, a CBDC on a private rail, an MT103 over correspondent banking — is plug-replaceable. The ARS-1 message does not change. The on-chain transaction hash, or the bank settlement reference, is carried as one evidence entry inside the message. The ledger answers *did value move?* The message answers *why, under whose authority, with what compliance, against what conditions, with what proof of delivery?* The two are complementary, not alternative.

Five. Multiple deployment patterns coexist on the standard. The **institutional** profile handles multilateral and sovereign flows — programmatic disbursement, agentic loan facilities, conditional and parametric transfers, oversight-heavy programmes. The **commercial** profile handles private-sector remittance — diaspora and B2B flows, volume-driven, lighter conditionality. The **state-to-citizen** profile handles sovereign welfare disbursement to a state's own citizens. All three speak ARS-1; all three address recipients by the same AIS-1 DID; all three emit AAS-1 records on every action. A recipient agent does not care which operator initiated a given transfer. That is the network effect ARS-1 unlocks.

---

1. Motivation and the Stranded Agent Problem

The agentic economy is now executing value transfer at scale. Stablecoin rails settled approximately USD 33 trillion in 2025, exceeding the combined annual volume of Visa and Mastercard. A growing share of those flows is being initiated, intermediated, and received by AI agents — disbursement agents at multilateral institutions, settlement agents at operators, recipient agents holding identity and onward-delivery instructions for natural-person principals.

Yet the rails on which agents move value are operator-specific. Every operator implements its own message format, conditionality grammar, compliance overlay, addressing scheme, and reversal protocol. Agents and the value they carry are stranded on whichever rail they were issued on. We term this the **Stranded Agent Problem**.

The consequences are concrete:

- **N² integration.** With N operators, every pair needs bilateral integration. The economics do not work past a handful of partners.
- **Closed recipient networks.** A citizen with a recipient agent on one operator cannot easily receive from another. Switching cost falls on the citizen — typically a person in a development corridor least able to bear it.
- **Regulator blindness.** Each operator builds its own telemetry. A regulator wanting cross-operator visibility must build N separate adapters and reconcile across N data models.
- **No portable conditionality.** “Release on verified vaccination” means a different thing in every operator’s system. Programmatic flows cannot move across rails.
- **No portable audit.** Audit firms cannot form opinions on flows that span operators because no shared evidentiary format exists.
- **No common reversal semantics.** What “cancel” means, when it is permitted, and who can issue it differs per operator. Counterparties have no shared expectation of finality.

Existing standards do not close this gap. ISO 20022 is the modern payments message standard adopted by SWIFT, SEPA, Fedwire, and major RTGS systems, but it assumes bank-to-bank flows and does not specify agent-action, identity-binding, or conditionality semantics. FATF Recommendation 16 prescribes the data that must accompany a cross-border transfer without prescribing the agent-native carrier for it. SWIFT gpi is closed to non-bank operators. CBDC pilots are sovereign and not cross-border interoperable. Crypto-native payment protocols — x402, Lightning, ERC-3009 — move value but carry no identity, no conditionality, and no compliance.

ARS-1 closes the gap by defining a portable agent-mediated remittance protocol, profiled on ISO 20022, integrating FATF Travel Rule data natively, binding to AIS-1 for identity and emitting to AAS-1 for audit.

A note on naming. ARS-1 is positioned as a *remittance* standard rather than a *payments* standard for three reasons. First, the payments standards space is crowded and dominated by ISO 20022; framing ARS-1 as an extension rather than a competitor opens the path to collaborative standardisation. Second, remittance is the harder case — identity binding for unbanked beneficiaries, last-mile delivery, FX hardship, conditional release, cross-border compliance — and solving the hard case incidentally solves easier ones (B2B settlement, agent-to-agent commerce). Third and most importantly, ARS-1 is not really about payments at all. Payments standards assume an account-to-account model: balances move between custodial accounts at financial institutions. ARS-1 assumes an *agent-to-agent* model: agents acting on behalf of principals communicate intent, and settlement on some underlying rail follows. The shift from accounts to agents is the architectural paradigm shift. Remittance is the most visible use case where that shift does meaningful work.

2. Definitions

2.1 Parties and Roles

Term	Definition
AI Agent	A software system that perceives its environment, makes decisions, and takes actions to achieve goals. As defined in AIS-1.
Originator	The legal or natural person initiating a remittance — multilateral, sovereign, NGO, employer, or natural-person sender.
Originator Agent	The AI agent acting on the originator’s behalf. Holds its own AIS-1 identity.

Operator	A licensed entity routing ARS-1 messages between originators and recipient agents. Operates one or more AIS-1-identified routing agents.
Routing Agent	The AI agent operated by an operator to execute Class T transfer messages.
Beneficiary	The natural or legal person ultimately entitled to the value.
Recipient Agent	The AI agent holding the beneficiary's AIS-1 identity, receiving the transfer, managing onward delivery.
Onward-Delivery Agent	The agent or interface executing the final conversion to local currency, bank credit, mobile-money credit, retail cash, or in-network spend.

2.2 Messages and Protocol Elements

Term	Definition
Remittance Message	A structured, signed, AIS-1-identified ARS-1 document. The atomic unit of the protocol.
Instruction (Class I)	The originator's initial remittance instruction. ISO 20022 pain.001 analog.
Transfer (Class T)	An operator-to-operator settlement message. pacs.008 analog.
Receipt (Class R)	Proof of delivery, signed by the recipient or onward-delivery agent. camt.054 analog.
Conditionality (Class C)	A portable conditionality block. Inline within a Class I or referenced by URI.
Reversal (Class V)	Cancellation, return, or recall. pacs.004 / camt.056 analog.
Purpose Code	Four-character categorisation. ARS-1 extends ISO 20022's `ExternalPurposeCode1Code`.
Travel Rule	FATF Recommendation 16. Originator and beneficiary information accompanying cross-border value transfers above defined thresholds.
Selective Disclosure	Cryptographic property by which a privacy envelope releases specific fields to authorised parties without revealing the full payload.
Hardship Adjustment	Operator policy that delays or paces onward conversion to local currency to soften FX shocks for the beneficiary.
Canonicalisation	Deterministic serialisation prior to hashing or signing. ARS-1 specifies JCS (RFC 8785) as default.
Timestamp Service	Auditable timestamping authority. Reuses the AIS-1 §3.4 primitive — technology-neutral and optional.

3. The ARS-1 Standard

3.1 The Remittance Message

ARS-1 defines the **remittance message** as the fundamental unit of agent value transfer. A remittance message is a structured, signed, AIS-1-identified document capturing one stage of a remittance lifecycle.

Messages are portable across operators. Any operator in possession of a message and the referenced AIS-1 identities can validate the signature, evaluate conditionality, screen against the compliance block, and act on the message — or reject it with a typed reason. Messages compose: a single lifecycle typically begins with a Class I instruction, generates one or more Class T

transfers, is governed by zero or more Class C conditionality blocks, and terminates in a Class R receipt. In error, any party may issue a Class V reversal.

Every ARS-1 message MUST emit an AAS-1 Class A action record at issuance. The audit trail is automatic — no additional instrumentation required.

3.2 Class I Instruction Attributes

A Class I message comprises a set of identity and amount fields (the core of any payment instruction) and a set of agentic-extension fields (conditionality, compliance, delivery, audit). Both sets are normative for v0.2.

3.2.1 Core Fields

Attribute	Description	Required
ars	Standard version. v0.2.	Yes
messageId	ULID or UUID, unique within the originator.	Yes
class	Message class. “I” for Instruction.	Yes
originatorRef	AIS-1 DID of the originating institution or natural person.	Yes
originatorAgentRef	AIS-1 DID of the originator’s disbursement agent.	Yes
beneficiaryRef	AIS-1 DID of the beneficiary.	Yes
recipientAgentRef	AIS-1 DID of the recipient agent.	Yes
operatorRef	AIS-1 DID of the routing operator.	Yes
amount	`{ currency, value, issuer }` object. ISO 4217 or stablecoin symbol with issuer DID.	Yes
purposeCode	Four-character code. ISO 20022 list or ARS-1 extension per §8.	Yes
valueDate	RFC 3339 date on which value becomes available to the beneficiary.	Yes
timestamp	RFC 3339 timestamp of instruction issuance.	Yes
iso20022Profile	ISO 20022 profile in use (e.g. “pain.001.001.10”).	Yes

3.2.2 Extended Fields

Attribute	Description	Required
conditionality	Inline Class C block, or URI to a referenced block.	Optional
compliance	Compliance block per §3.4. Mandatory for cross-border or Travel-Rule-qualifying transfers.	Yes
onwardDelivery	Onward-delivery instructions per §12.3.	Optional
privacyEnvelope	Selective-disclosure envelope per §11.2.	Optional
timestampServiceRef	URI of timestamping authority.	Optional
aas1RecordRef	URI of the AAS-1 Class A action record emitted at issuance.	Yes

signature	Signature object over the canonicalised message.	Yes
notes	Free-text issuer notes.	Optional

3.3 The Conditionality Block

The conditionality block expresses programmable release rules. Portable across operators, evaluable by any party in possession of the referenced oracles or attestations, and emits an AAS-1 record on every evaluation.

Attribute	Description
conditionId	ULID or UUID.
predicate	The release predicate (see types below).
evidenceRequired	Array of AAS-1 evidence types required to satisfy the predicate.
fallback	Action if the predicate is not satisfied within the validity window.
validity	`{ notBefore, notAfter }` in RFC 3339.
evaluatorRef	Optional AIS-1 DID of the party authorised to evaluate. If absent, the operator's routing agent evaluates.

Predicate types defined in v0.2:

Type	Use
oracle	Reads a typed value from a declared external source.
attestation	Requires a Class A AAS-1 attestation from a named agent or party.
time	Time-based release (scheduled, recurring).
balance	Conditional on a stated balance or threshold at a referenced address.
manual	Requires a human-attested release via an AAS-1 `human` evidence entry.
composite	Boolean combination of nested predicates via `{ allOf, anyOf, not }`.

Fallback actions defined in v0.2: `return_to_originator` | `escrow_extend` | `release_to_alternate` | `null_and_audit`.

3.4 The Compliance Block

The compliance block carries the data required by FATF Recommendation 16, local AML/CFT rules, sanctions screening results, and capital-flow management metadata. Mandatory for any cross-border instruction and any domestic instruction above the operator's declared threshold.

Attribute	Description
travelRule	Travel Rule envelope per §11. In clear or under selective-disclosure wrapper.
sanctionsScreening	`{ result, listSetRef, screenedAt }`. Result one of: `clear` | `match` | `review`.
amlAssessment	`{ riskRating, basis, assessedAt }`.
capitalFlowTags	Array of jurisdiction-pair tags supporting regulator reporting.
beneficialOwnerRef	URI to a verifiable credential establishing beneficial owner, where required.

4. The ISO 20022 Envelope

ARS-1 is defined as the agentic profile of ISO 20022. Every ARS-1 message class maps to a corresponding ISO 20022 message type. This is the load-bearing design choice of the standard.

The mechanic. ISO 20022 messages include a `<SplmtryData>` element — an extension point officially designated for domain-specific data that does not fit in the core schema. ARS-1 uses this slot. The ARS-1 payload sits inside the supplementary-data envelope under the namespace `urn:ars-1:v0_2`. The core ISO 20022 fields carry canonical payment data: debtor, creditor, amount, value date, purpose.

The result. A Class I instruction is simultaneously:

- A valid ISO 20022 pain.001 message that any bank or payment processor running standard ISO 20022 infrastructure can route, log, screen, and report on.
- A valid ARS-1 instruction that any ARS-1-aware operator can unwrap and execute as an agent-mediated remittance.

Banks that do not speak ARS-1 do not need to. ISO 20022 conformance rules require them to preserve `<SplmtryData>` end-to-end without modification. The ARS-1 payload passes through correspondent-banking infrastructure unchanged. The agentic operator at the receiving end unwraps it and acts.

```
<pain.001.001.10>
  <GrpHdr>
    <MsgId>01HZ9D7XKQ4N5MJ2Y8VR3PTBFW</MsgId>
    <CreDtTm>2026-05-16T10:14:22Z</CreDtTm>
  </GrpHdr>
  <PmtInf>
    <Dbtr>                                <!-- Originator -->
      <Id><OrgId><Othr>
        <Id>did:ais1:sponsor:originator-example</Id>
        <SchmeNm><Prtry>AIS-1</Prtry></SchmeNm>
      </Othr></OrgId></Id>
    </Dbtr>
    <Cdtr>                                <!-- Beneficiary -->
      <Id><PrvtId><Othr>
        <Id>did:ais1:sponsor:beneficiary-example</Id>
        <SchmeNm><Prtry>AIS-1</Prtry></SchmeNm>
      </Othr></PrvtId></Id>
    </Cdtr>
    <InstdAmt Ccy="USDC">500.00</InstdAmt>
    <Purp><Prtry>PRAM</Prtry></Purp>   <!-- ARS-1 purpose code -->
    <SplmtryData>
      <Envlp xmlns="urn:ars-1:v0_2">
        <ars1Instruction>              <!-- Full ARS-1 JSON payload -->
          ...
        </ars1Instruction>
      </Envlp>
    </SplmtryData>
  </PmtInf>
</pain.001.001.10>
```

The dual-readable design gives ARS-1 a free path into existing infrastructure. The standard extends ISO 20022; it does not replace it.

5. Addressability via AIS-1

ARS-1 uses AIS-1 DIDs as the universal addressing scheme. Every party in every ARS-1 message — originator, originator agent, beneficiary, recipient agent, operator, onward-delivery agent — is identified by an AIS-1 DID.

The problem this solves. Conventional remittance addressing is fragmented. Western Union has its directory of cash-pickup points; mobile-money operators have phone-number-keyed accounts; banks have IBAN/SWIFT/routing pairs; crypto wallets have chain-specific addresses. None is portable. Each provider maintains its own directory of who-to-pay. Each cross-provider integration is bespoke. The result is N^2 complexity at the network layer.

How AIS-1 collapses this. A DID like `did:ais1:base:recipient-agent-example` is globally resolvable. The AIS-1 §7.1 resolution algorithm returns a DID Document containing the agent's public keys, sponsor, jurisdiction, capability scope, AML status, and the verification methods needed to validate any signature the agent emits. Any party — anywhere — performs this resolution against the public AIS-1 registry.

When a multilateral institution sends to a recipient under an institutional-profile operator, the Class I message writes the recipient's AIS-1 DID into `recipientAgentRef`. When a diaspora sender uses a commercial-profile operator, the same recipient is addressed by the same DID. When the recipient's own government disburses welfare under a state-to-citizen profile, again the same DID. The DID is the address. There is no operator-specific directory anywhere in the protocol.

The analogy. AIS-1 + ARS-1 are to value transfer what DNS + HTTP are to the web. DNS gave every resource on the internet a universal name. HTTP gave every server a shared protocol for serving content against that name. Together they killed the era of incompatible online services and unlocked the web. AIS-1 gives every agent in the world a universal identifier. ARS-1 gives every operator a shared protocol for transferring value against that identifier. The network effect that follows is structural, not contingent.

The cost of integration for an operator is *integration with the standard, once*. After that, the operator can transact with every recipient agent in the world that has an AIS-1 identity. N^2 becomes N.

6. Settlement-Layer Independence

ARS-1 is rail-agnostic. The settlement of value — the actual transfer of fungible units from one account to another — happens on whatever underlying rail the operator pair chooses. ARS-1 does not specify the rail.

Supported settlement modes in v0.2:

Mode	Settlement event	Carried in ARS-1 as
Stablecoin on public chain	On-chain transaction	`hash_anchor` evidence with chain ID and tx hash
Stablecoin on private chain or consortium ledger	Ledger entry	`log` evidence with ledger reference
CBDC (where available)	CBDC system event	`attestation` evidence with CBDC operator signature
Real-time gross settlement (Fedwire, RTGS)	pacs.009 settlement message	`log` evidence with settlement reference
Correspondent banking (MT103)	SWIFT MT confirmation	`log` evidence with MT103 reference
In-network rebalancing	Operator internal ledger	`log` evidence; operator attestation

The principle. The ARS-1 message does not change with the settlement mode. A Class I instructing USDC-on-Base settlement and a Class I instructing CBDC-via-private-rail settlement have the same structure, the same fields, the same signatures. Only the settlement reference inside the evidence array differs. This means an operator can change rails without re-integrating with counterparties, regulators, or audit firms.

Why messages even on public ledgers. A reasonable question: if the value moves on a public blockchain, both parties can read the same ledger — why send a message at all?

Because the on-chain transfer alone is *incomplete*. A USDC transfer on Base is a movement of tokens between two addresses. That is all it is. No purpose code, no conditionality evaluation, no Travel Rule data, no AML assessment, no identity binding, no onward-delivery instruction, no audit reference, no signature chain of authorisation. For consumer crypto this minimalism is acceptable. For institutional, regulated, or programmatic flows it is not. The ARS-1 message is the envelope of meaning around the settlement event. The ledger answers *did value move?* The message answers *why, under whose authority, with what compliance, against what conditions, with what proof of delivery, and how do we know?* The two together are the complete record.

Every serious crypto compliance system — Chainalysis, TRM, Elliptic — is effectively trying to reconstruct ARS-1-shaped metadata after the fact from on-chain forensics. ARS-1 puts the metadata at the front, signed and structured, at the moment of transfer. The on-chain transaction hash, where present, is one piece of evidence inside the ARS-1 message. It is necessary but not sufficient.

7. Message Classes

Class	Name	Issuer	Purpose	v0.2 Status

I	Instruction	Originator agent	Initial remittance instruction. pain.001 analog.	Schema published
T	Transfer	Operator routing agent	Operator-to-operator settlement message. pacs.008 analog.	Schema published
R	Receipt	Recipient or onward-delivery agent	Proof of delivery to beneficiary. camt.054 analog with agent-action semantics.	Schema published
C	Conditionality	Originator or operator	Portable conditionality block. Inline or referenced.	Schema published
V	Reversal	Any party	Cancel, return, or recall. pacs.004 / camt.056 analog.	Schema published

8. Purpose Codes

ISO 20022 maintains the external purpose-code list `ExternalPurposeCode1Code`. ARS-1 implementations MUST honour the ISO 20022 list and MAY emit codes from the ARS-1 supplementary set below. Operators MUST NOT define proprietary codes outside the `ARS:` namespace prefix.

Rationale for the supplementary codes. ARS-1's additions to the ISO 20022 list cluster around three areas where the existing codes do not capture distinctions that matter to regulators and operators. *Programmatic-flow codes* (`PRAM`, `COND`, `HLTH`) categorise transfers whose release is governed by oracle-evaluated or attestation-evaluated conditions; central banks reporting on national accounts increasingly need to distinguish programmatic flows from discretionary disbursements, and AML systems risk-score them differently. *Agent-native disbursement codes* (`DTCT`, `UBAA`) cover patterns that did not exist before the agentic recipient model — direct-to-citizen institutional disbursement and recurring agent allocations — and have no banking-era analog. *Commercial remittance codes* (`RMSP`, `RMBP`, `RMTB`) classify by payer category, which matters for AML risk scoring because a diaspora send from an individual carries a different risk profile from a corporate payroll. The remaining codes (`SCHL`, `HMRT`, `CLIM`, `DIAS`, `AGLN`, `AGRP`) are convenience codes for development-relevant flows; implementations MAY also use the existing ISO 20022 codes `STDY`, `CHAR`, `FAMI`, `LOAN`, `LOAR` where they apply. New codes that survive comment will be submitted to the ISO 20022 Registration Authority through the formal Request for Purpose Code process; the codes in this section are proposed, not yet ratified.

Code	Name	Description	Primary profile
DTCT	Direct-to-Citizen Transfer	Institutional disbursement directly to a citizen agent.	Institutional
COND	Conditional Cash Transfer	Funds released against an agent-verified condition.	Institutional
PRAM	Parametric Disaster Response	Funds released by oracle on parametric trigger.	Institutional
SCHL	Scholarship Disbursement	Education-targeted, typically conditioned on enrolment.	Institutional
HMRT	Humanitarian Emergency Relief	Time-critical relief disbursement.	Institutional
CLIM	Climate Resilience Payment	Adaptation, mitigation, or just-transition payment.	Institutional
HLTH	Health-Conditional Transfer	Health-programme transfer.	Institutional
DIAS	Diaspora Coordinated Remittance	Pooled diaspora flow matched with multilateral co-funding.	Commercial, Institutional
AGLN	Agentic Loan Drawdown	Drawdown under an agentic loan facility.	Institutional

AGRP	Agentic Loan Repayment	Repayment under an agentic loan facility.	Institutional
UBAA	Universal Basic Agent Allocation	Recurring base allocation under a UBA scheme.	State-to-Citizen
RMSP	Sender-Pays Personal Remittance	Diaspora or family P2P remittance.	Commercial
RMBP	Business-Pays Personal Remittance	Employer payroll, gig payout, marketplace settlement.	Commercial
RMTB	Treasury / B2B Remittance	Cross-border B2B payment with full agentic envelope.	Commercial

9. Schema Specification

9.1 JSON Schemas

Schemas for Class I, T, R, C, and V are published as JSON Schema 2020-12 at `github.com/Kadikoy1/ars-1/blob/main/schemas/`. All five are normative for v0.2.

9.2 Canonicalisation and Hashing

Messages MUST be canonicalised before hashing or signing. v0.2 specifies JCS (RFC 8785) as the default canonicalisation, matching AAS-1 §6.2. Hash algorithm declared per-message in the signature object; SHA-256 default. Implementations MAY use other algorithms by setting `hashAlg`; verifiers SHOULD reject unknown algorithms unless in a published registry.

9.3 Signature Object

Field	Description
alg	Signature algorithm (EdDSA, ES256K, etc.).
hashAlg	Hash algorithm. Default SHA-256.
canonicalisation	Canonicalisation method. Default JCS.
keyRef	Verification method identifier within the issuer's AIS-1 identity document.
value	Signature value, base64url-encoded.

Structurally identical to AAS-1 §6.3 — shared verification tooling.

10. AIS-1 and AAS-1 Binding

Every ARS-1 message MUST reference AIS-1 identities for all named parties, and MUST emit an AAS-1 Class A record at issuance.

10.1 Identity Binding

A verifier dereferences each AIS-1 DID using the AIS-1 §7.1 resolution algorithm and obtains the DID Document containing verification methods, agent class (`ala` or `soa`), sponsor, and AML status. A verifier MAY call `verifyBond(bondId)` on the AIS-1 contract to confirm the bond is active.

10.2 Audit Emission

At issuance, the message issuer MUST emit an AAS-1 Class A action record:

- `agentRef` is the issuer's AIS-1 identity.
- `principalRef` is the issuer's principal per AIS-1.
- `action.type` is `transaction` for Class I/T/R/V, `policy_check` for standalone Class C evaluations.

- `action.inputsHash` and `action.outputsHash` are computed over the canonicalised ARS-1 message and its evaluation result.
- `materiality` carries the ARS-1 `amount`.
- `evidence` includes at minimum a `signature` entry; SHOULD include `hash_anchor` for high-materiality flows.

The resulting AAS-1 `eventId` is recorded as `aas1RecordRef` on the ARS-1 message — bidirectional link.

10.3 Verification Flow

```
        const msg = await ars1.fetch(messageId);

        // 1. Resolve AIS-1 identities for all named parties
        const orig    = await ais1.resolve(msg.originatorRef);
        const origAg  = await ais1.resolve(msg.originatorAgentRef);
        const recipAg = await ais1.resolve(msg.recipientAgentRef);
        const op      = await ais1.resolve(msg.operatorRef);

        // 2. Validate the message signature against the originator agent's key
        assert(verifySignature(msg, origAg.verificationMethod));

        // 3. Confirm bonds are active
        for (const id of [origAg, recipAg, op]) {
          const bond = await ais1.verifyBond(id.bondId);
          assert(bond.valid && bond.amlStatus === 'cleared');
        }

        // 4. Verify the corresponding AAS-1 record
        const aasRec = await aas1.fetch(msg.aas1RecordRef);
        assert(aasRec.agentRef === msg.originatorAgentRef);

        // 5. Evaluate the compliance block
        assert(msg.compliance.sanctionsScreening.result === 'clear');

        // 6. Evaluate conditionality if present
        if (msg.conditionality) {
          const result = await ars1.evaluateConditionality(msg.conditionality);
          if (!result.satisfied) return reject('conditionality_unsatisfied', result);
        }

        // 7. Accept for routing
        return accept(msg);
```

11. FATF Travel Rule Integration

ARS-1 treats FATF Recommendation 16 as a first-class protocol element rather than an external overlay.

11.1 Originator and Beneficiary Information

The Travel Rule envelope carries the fields required for transfers above the operator's declared threshold (USD/EUR 1,000 by default, or as set by local regulator):

Field	Source
originatorName	AIS-1 Sponsor Card `legal_name`.
originatorAccount	AIS-1 `agent_did` + settlement-rail account.
originatorAddress	AIS-1 Sponsor Card `jurisdiction` + registered address.
originatorIdentifier	AIS-1 Sponsor Card `registration_number` or national ID.
beneficiaryName	AIS-1 identity of the beneficiary.
beneficiaryAccount	AIS-1 `agent_did` + settlement-rail account.

Where AIS-1 Verified or Sovereign tiers are in use, originator and beneficiary information is already verified by the issuing authority; the Travel Rule envelope references the AIS-1 identity rather than restating the data. This is the privacy-preserving mode.

11.2 Selective Disclosure

Compliance block fields MAY be carried as commitments (salted hashes) with the underlying values held by the operator. The operator releases specific fields to specific counterparties by role:

- Receiving operator sees fields necessary for sanctions screening and onward routing.
- Home regulator of either party sees fields necessary for AML/CFT supervision.
- Beneficiary's principal sees fields confirming the originator's identity to the extent permitted.
- Third parties see nothing without an explicit authorisation chain.

Implemented using the AIS-1 Assurance Container (AIS-1 §10.3) mechanism. Reference cryptographic envelopes specified in v0.3.

11.3 Three-Checkpoint Screening

Sanctions screening occurs at three checkpoints:

1. **Pre-instruction**, by the originator agent against its declared list set, before issuing Class I.
2. **Pre-transfer**, by the routing operator against the operator's declared list set, before issuing Class T.
3. **Pre-receipt**, by the recipient or onward-delivery agent against the recipient jurisdiction's list set, before issuing Class R.

Each screening produces a `sanctionsScreening` block embedded in the relevant message and emits an AAS-1 record of type `policy_check`. A `match` or `review` result halts the lifecycle pending human disposition.

12. Conditionality, FX, and Onward Delivery

12.1 Conditionality Grammar

Conditionality is ARS-1's programmable layer. Every conventional payment standard treats conditions on release as out-of-band agreements between counterparties, enforced by humans reading contracts. Conditional cash-transfer programmes today verify vaccination, school attendance, or proof of life through human-mediated workflows that delay disbursement by weeks. ARS-1 brings conditions into the protocol, with formal semantics that any operator can evaluate, any auditor can re-evaluate, and any regulator can read. The conditionality block is a portable JSON document, not a chain-specific smart contract — it does not require a particular ledger or execution environment, and its fallback grammar makes it safe for production use in a way that smart-contract conditionality often is not.

Specified in §3.3. Implementations MUST support the six predicate types. Operators MAY support implementer-defined predicate types under a reverse-DNS namespace; receiving operators MAY reject unknown types.

Every conditionality evaluation emits an AAS-1 record of type `policy_check` carrying the conditionId, evaluator's AIS-1 identity, evaluation result, and all evidence consulted.

12.2 Hardship and FX Policy

A recipient agent typically receives value in a settlement currency (most commonly a stablecoin denominated in USD or EUR) and must convert to local currency for onward delivery. In stable corridors this is a trivial step. In corridors where the local currency is volatile or undergoing a run — historically Argentina, Lebanon, Venezuela, Turkey, Egypt at various periods — the *timing* of conversion materially affects what the beneficiary receives. A disbursement converted in the morning may be worth substantially more or less than the same disbursement converted in the afternoon. Hardship adjustment is the operator's published policy for protecting beneficiaries from this timing exposure.

For Class I messages with currency mismatch between the settlement leg and the onward-delivery leg, the operator MAY apply one of the following policies:

- **Hold-in-stablecoin**: defer onward conversion when local-currency volatility exceeds a declared threshold.
- **Rate-locked window**: lock the FX rate at instruction time for a stated window; beneficiary receives the better of locked rate or spot.
- **Run-protection**: pause onward conversion during a local-currency run, releasing automatically on stability signal from a declared oracle.

Hardship policies MUST be declared in the operator's published policy URI and referenced in `policyRefs` on the emitted AAS-1 record. Critically, policies MUST NOT operate to the detriment of the beneficiary versus a no-policy baseline as evaluated at the close of the validity window. The protection runs to the citizen, not to the operator's spread.

12.3 Onward Delivery Handoff

Channel	Reference Carried
Bank credit	IBAN, BIC, or local clearing reference.
Mobile money	Provider identifier and customer wallet.
Retail cash agent	Cash-out partner identifier and authorisation token.
In-network spend	Reference to a network of merchant agents accepting on the recipient agent's identity.
Hold-in-rail	No onward delivery; value remains on rail under recipient agent's control.

Onward-delivery agents issue Class R receipts on completion, signed under their own AIS-1 identity.

12.4 Reversal and Recovery

Class V reversal may be issued by:

- The originator, within a declared cancellation window before Class T issuance.
- Either operator, on sanctions match, fraud indicator, or oracle-attested error.
- The recipient agent, on mistaken-send or beneficiary repudiation.

Recovery scenarios — beneficiary mortality, key loss, controller change — are handled at the AIS-1 layer through the AIS-1 Verification Method change procedure, and at the ARS-1 layer through a Class V reversal followed by a fresh Class I to the corrected recipient agent.

13. Operator Profiles

ARS-1 supports three named deployment-pattern profiles in v0.2. Each is a published reference profile with declared purpose codes, conditionality predicates, onward-delivery channels, and licensing posture. An operator MAY claim conformance with one or more profiles. The standard does not endorse or name specific commercial operators; conformance is a matter of meeting the published criteria for the relevant profile.

13.1 Institutional Disbursement Profile

Deployment pattern for institutional-payer flows: multilateral disbursements (IMF, World Bank, regional development banks), sovereign-to-citizen aid programmes, parametric disaster response, conditional cash transfers, agentic loan facilities (`AGLN` / `AGRP`), scholarship and humanitarian programmes. Originators are AIS-1 Sovereign tier. Recipient agents are AIS-1 Verified, typically issued in the field by an authorised onboarding partner. Conditionality is heavily used — oracle-driven for parametric flows, attestation-driven for conditional programmes. Operators are licensed under a jurisdiction-appropriate digital-asset framework.

13.2 Commercial Remittance Profile

Deployment pattern for commercial value transfer: diaspora P2P remittance, employer payroll, marketplace settlement, B2B cross-border. Originators are AIS-1 Verified or Basic tier individuals and small businesses. Recipient agents are AIS-1 Verified, typically issued via a partner network (mobile-money operators, diaspora associations, retail remittance agents). Conditionality is light or absent. Volume-driven, lower per-transaction margin. Operators are licensed as money transmitters, payment institutions, or digital-asset businesses in their home jurisdiction.

13.3 State-to-Citizen Profile

Deployment pattern for sovereign welfare and public-sector disbursement: social benefits, pensions, tax refunds, public-sector salaries. The originator is a state entity. Recipient agents are AIS-1 Sovereign tier, issued by the national registry of the originating state. Settlement may be in CBDC, central-bank-issued stablecoin, or domestic fiat rail. Conditionality may include eligibility predicates verified against government attestations.

13.4 Profile Interoperability

The three profiles share the protocol. A recipient agent provisioned under one profile can receive transfers under another. A citizen who first received institutional disbursement aid can subsequently receive commercial remittance from a diaspora relative, and welfare from her own government — all to the same AIS-1 recipient agent, all in the same protocol format. The recipient agent is profile-agnostic; the operator is profile-specific. This is the network effect ARS-1 unlocks.

14. Comparison with Existing Frameworks

Framework	Scope	Gap addressed by ARS-1
ISO 20022	Modern payments message standard	No agent-action semantics; no conditionality grammar; assumes bank-to-bank flows. ARS-1 extends, does not replace.
SWIFT gpi	Cross-border payment tracking	Closed to non-bank operators; no agent identity binding.
FATF Recommendation 16	Travel Rule data requirements	Prescribes data, not the agent-native protocol carrying it.
ERC-20 / ERC-3009	Token transfer on EVM chains	No identity, no conditionality, no compliance.
x402 (HTTP-payable)	Agent-to-agent micro-payment	No conditionality, no Travel Rule, no remittance lifecycle.
Lightning Network	Bitcoin micropayments	Bearer instrument; no identity; no compliance.
W3C Verifiable Credentials	Claims about an entity	No value-transfer semantics.
AIS-1	Agent identity (companion)	Identity only; no protocol for value transfer.
AAS-1	Agent auditability (companion)	Audit only; no protocol for value transfer.
ARS-1 (this standard)	Agent-mediated remittance protocol	First open standard for portable, compliant, conditional agent value transfer.

15. Security Considerations

15.1 Message Integrity. Every ARS-1 message MUST be signed by the issuing agent using its AIS-1 verification method. Messages MAY include a `prevHash` field referencing the canonical hash of the preceding message in the same lifecycle.

15.2 Replay and Substitution. A signed message is bound to its `messageId`, `timestamp`, and AIS-1 identities. Replay under a different identity requires re-signing and is detectable.

15.3 Travel Rule Data Leakage. Travel Rule data carried in clear is visible to every operator on the routing path. Implementations SHOULD use the §11.2 selective-disclosure envelope.

15.4 Oracle Manipulation. Conditionality predicates that depend on oracles inherit the trust assumptions of those oracles. Implementations using oracle-dependent conditionality SHOULD require multiple independent sources, witness signatures, and a declared dispute-resolution path. Single-oracle conditionality is acceptable only where the oracle is itself an AIS-1-identified party operating under a published policy.

15.5 Sanctions Evasion. Three-checkpoint screening (§11.3) prevents naive sanctions evasion. Operators SHOULD additionally implement velocity checks, jurisdiction-pair limits, and structuring detection. ARS-1 carries the data needed for these checks but does not mandate their algorithms.

15.6 Conditionality Denial of Service. A conditionality predicate that cannot be evaluated within its validity window invokes the declared fallback. Operators MUST NOT design conditionality such that the fallback is materially worse for the beneficiary than the satisfied path.

16. Implementation Roadmap

Phase	Deliverable	Target
0.1	Specification; Class I JSON Schema; conditionality grammar; institutional-profile worked example.	May 2026
0.2 — This document	Class T/R/C/V schemas. Tightened prose. Operator profiles. ISO 20022 envelope and addressability sections promoted.	May 2026
0.3	Full ISO 20022 mapping annex. Selective-disclosure envelope. Travel Rule encryption profiles.	Q3 2026
0.4	Reference operator pilots across the three deployment profiles. Conformance criteria published.	Q4 2026
0.5	Conformance suite. Test vectors. Reference verifier and routing agent.	Q1 2027
1.0	Submission to ISO TC 68 / SC 8 (financial services). Convening with IMF, World Bank, BIS Innovation Hub. Stable schemas.	Q2 2027
1.1	Formal cross-mapping with the next ISO 20022 maintenance release. Joint conformance with SWIFT gpi successor.	Q3 2027
2.0	Generalisation to agent-to-agent commerce settlement: ARS-1 messages between operators acting for organisational and agent principals, beyond citizen-recipient flows.	2027

17. Request for Comment

ARS-1 v0.2 is published as a draft for public comment. Feedback is invited from multilateral institutions and development finance organisations (IMF, World Bank, IFC, regional development banks); central banks and supervisory authorities; FATF, FIUs, and AML/CFT regulators; remittance and money-transfer operators; ISO 20022 registration authorities and SWIFT; humanitarian and aid organisations; AI agent developers; legal, regulatory, and compliance professionals; enterprise deployers; and standards organisations including ISO TC 68, ITU-T, the BIS Innovation Hub, and the FSB.

Feedback may be submitted via:

- Feedback form: ars-1.org/#feedback
- Email: info@aiagentsservices.net
- GitHub: github.com/Kadikoy1/ars-1/issues

The comment period for v0.2 closes 31 August 2026. A revised draft will be published as v0.3.

18. Authors

Field	Value
Author	Kadikoy Limited, Bermuda
Affiliation	BDA Law; BDA AI Agent Services
Companions	AIS-1 Agent Identity Standard (ais-1.org); AAS-1 Agent Auditability Standard (aas-1.org)

Contact	info@aiagentsservices.net
Website	ars-1.org
Repository	github.com/Kadikoy1/ars-1
License	Creative Commons CC0. No rights reserved. Open for free implementation.

Appendix A — Class I Message — Worked Example

A multilateral institution (originator) instructs an institutional-profile operator to disburse USD 500 in USDC to a citizen agent in Saint Vincent and the Grenadines, conditional on a Category 3 or greater cyclone alert from a regional meteorological oracle within a 72-hour window. Travel Rule data carried by selective-disclosure reference; sanctions cleared; parametric-disaster purpose code; mobile-money onward delivery. The example uses placeholder identifiers — any conforming implementation would use its own AIS-1 identifiers and operator URLs.

```
{
  "ars": "0.2",
  "messageId": "01HZ9D7XKQ4N5MJ2Y8VR3PTBFW",
  "class": "I",
  "originatorRef": "did:ais1:sponsor:multilateral-originator-example",
  "originatorAgentRef": "did:ais1:base:originator-disbursement-agent-001",
  "beneficiaryRef": "did:ais1:sponsor:beneficiary-svg-example",
  "recipientAgentRef": "did:ais1:base:recipient-agent-svg-example",
  "operatorRef": "did:ais1:base:institutional-operator-example",
  "amount": { "currency": "USDC", "value": "500.00",
              "issuer": "did:ais1:sponsor:stablecoin-issuer-example" },
  "purposeCode": "PRAM",
  "conditionality": {
    "conditionId": "01HZ9D7Y2K3M4N5P6Q7R8S9T0V",
    "predicate": {
      "type": "oracle",
      "sourceRef": "https://oracles.example.org/caribbean-cyclone-feed",
      "field": "maxCategoryWithin72h",
      "operator": "gte",
      "value": 3,
      "asOfWindow": "PT72H"
    },
    "evidenceRequired": ["attestation", "hash_anchor"],
    "fallback": {
      "type": "expiry",
      "after": "2026-08-15T00:00:00Z",
      "action": "return_to_originator"
    },
    "validity": {
      "notBefore": "2026-05-16T00:00:00Z",
      "notAfter":  "2026-08-15T00:00:00Z"
    }
  },
  "compliance": {
    "travelRule": { "envelope": "selective-disclosure",
                    "ref": "https://compliance.example.org/envelope/01HZ9D7Y..." },
    "sanctionsScreening": {
      "result": "clear",
      "listSetRef": "https://compliance.example.org/lists/un-ofac-eu-2026-05",
      "screenedAt": "2026-05-16T10:14:22Z"
    },
    "amlAssessment": { "riskRating": "low", "basis": "verified-tier-sponsor",
                       "assessedAt": "2026-05-16T10:14:22Z" },
    "capitalFlowTags": ["US->VC", "multilateral-aid", "parametric"]
  },
  "onwardDelivery": {
    "channel": "mobile_money",
    "providerRef": "did:ais1:sponsor:mobile-money-operator-example",
    "customerWallet": "+1-784-XXX-XXXX",
    "currency": "XCD",
    "hardshipPolicyRef": "https://policies.example.org/hardship/v1"
  },
  "valueDate": "2026-05-16",
  "timestamp": "2026-05-16T10:14:22Z",
  "timestampServiceRef": "rfc3161:tsa.example.org",
  "iso20022Profile": "pain.001.001.10",
  "aas1RecordRef": "aas1:01HZ9D7Z3K4M5N6P7Q8R9S0T1V",
  "signature": {
    "alg": "EdDSA",
    "hashAlg": "SHA-256",
    "canonicalisation": "JCS",
    "keyRef": "did:ais1:base:originator-disbursement-agent-001#key-1",
    "value": "z7kQpNm9..."
  },
  "notes": "Institutional-profile parametric cyclone-response disbursement — illustrative reference flow."
}
```


Appendix B — Operator Verification Flow

How a routing operator verifies an inbound ARS-1 Class I message and issues a Class T transfer:

1. Receive the Class I message and, where present, the referenced Class C conditionality block.
2. Resolve `originatorRef`, `originatorAgentRef`, `recipientAgentRef`, and `operatorRef` via the AIS-1 §7.1 resolution algorithm.
3. Validate the message signature against the verification method declared in the originator agent's DID Document.
4. Confirm each AIS-1 bond is active by calling `verifyBond(bondId)`. Reject if any bond is suspended, revoked, or `amlStatus != cleared`.
5. Fetch the emitted AAS-1 Class A record at `aas1RecordRef` and verify it is consistent with the ARS-1 message (matching agent, principal, timestamp, materiality).

6. Evaluate the compliance block. If `sanctionsScreening.result != clear`, halt and route for human disposition.
7. Apply local sanctions screening as the receiving operator under §11.3 checkpoint 2. Emit an AAS-1 record of type `policy_check`.
8. If conditionality is present, evaluate the predicate per §12.1. If unsatisfied within the validity window, apply the declared fallback and halt. If satisfied, emit an AAS-1 record recording the evidence consulted.
9. Apply hardship/FX policy per §12.2.
10. Issue a Class T transfer message under the operator's AIS-1 identity, signed with the routing agent's verification method, with a fresh AAS-1 record emitted at issuance.
11. On receipt of a downstream Class R receipt from the recipient or onward-delivery agent, forward it back to the originator under the same operator signature.

Appendix C — ISO 20022 Mapping

How ARS-1 Class I fields populate ISO 20022 pain.001.001.10:

ARS-1 Class I field	ISO 20022 pain.001.001.10 location	Notes
messageId	`<GrpHdr><MsgId>`	Direct mapping.
timestamp	`<GrpHdr><CreDtTm>`	Direct mapping.
originatorRef	`<Dbtr><Id><OrgId><Othr><Id>` with `<SchmeNm><Prtry>AIS-1</Prtry>`	AIS-1 DID as proprietary identifier.
originatorAgentRef	`<DbtrAgt><FinInstnId><Othr><Id>`	Originator agent as proprietary FI.
recipientAgentRef	`<CdtrAgt><FinInstnId><Othr><Id>`	Recipient agent as proprietary FI.
beneficiaryRef	`<Cdtr><Id><PrvtId><Othr><Id>` or `<OrgId>`	Natural person (PrvtId) or entity (OrgId).
amount	`<PmtInf><CdtTrfTxInf><Amt><InstdAmt Ccy="">`	Direct. Stablecoin issuer reference in `<SplmtryData>`.
purposeCode	`<PmtInf><CdtTrfTxInf><Purp><Cd>` or `<Prtry>`	ISO codes in `<Cd>`, ARS-1 supplementary codes in `<Prtry>`.
conditionality	`<SplmtryData>` under `urn:ars-1:v0_2`	Inline or referenced.
compliance	`<SplmtryData>` under `urn:ars-1:v0_2`; Travel Rule core fields also in `<UltmtDbtr>` / `<UltmtCdtr>`	Dual carriage for non-agentic infrastructure interop.
onwardDelivery	`<SplmtryData>` under `urn:ars-1:v0_2`	Not natively expressible in pain.001.
valueDate	`<PmtInf><ReqdExctnDt><Dt>`	Direct mapping.
signature	`<SplmtryData>` carrying full ARS-1 signature object	ISO 20022 envelope signed separately under originator's standard regime.
aas1RecordRef	`<SplmtryData>` under `urn:ars-1:v0_2`	Cross-reference to AAS-1 audit record.

Appendix D — v0.2 Change Log

Change	Section	Description
In Essence section added	Front	The standard summarised in five paragraphs.
ISO 20022 envelope promoted	4	Was §8 in v0.1. Now a top-level section with rendered example.

Addressability via AIS-1 promoted	5	New top-level section. DNS analogy made explicit.
Settlement-Layer Independence	6	New top-level section. Addresses the question of why messages on public ledgers.
Operator Profiles expanded	13	Three deployment-pattern profiles explicit with conformance criteria.
Purpose codes extended	8	Added RMSP, RMBP, RMTB for commercial-profile flows.
Class T/R/V schemas	7, 9	Promoted from “schema in v0.2” to “schema published”.
Roadmap updated	16	Reference operators across three deployment profiles moved to Phase 0.4.
Prose tightened	Throughout	Removed hedging. Sharper assertions. Removed redundancy.
Grandfathering clause	n/a	v0.2 supersedes v0.1 in full; no in-flight messages exist to grandfather.