Agent Passport Standards Series
APS 1001 (2026), revision 5
Series 1000: Payment Rails
Category: Proposed Industry Standard
Team Agent Passport
Cambridge, United Kingdom
8 September 2026

APS 1001

Agent Passport Standard: Delegated Authority of AI Agents on Payment Rails

Status of this Memo

APS 1001 specifies the procedure by which an AI agent proves, before a payment executes, that it acts within a current, human-granted authority, and by which the bank that executes the payment records evidence of what it verified. It is a proposal for an industry standard, demonstrated on synthetic data. It does not describe a current legal requirement, and no regulator has approved it. Distribution is unlimited.

Revision 3 replaced the authority approval of revision 2 with a bank-operated model: an industry register records AI products, each bank decides which registered products its customers may delegate to, and the regulator receives evidence through normal supervisory processes without operating or approving anything.
Revision 4 adds assurance levels on filings, currency and velocity limits and account-type tiers on mandates, replay protection by nonce, two classes of refusal, and a check of payees against the public company register.
Revision 5 adds the enumerated payment intent a product is filed for, which bounds every admission and mandate on it, and the UK data protection declaration with completeness check F.7.

Abstract

An AI agent that can be identified can still act beyond what its principal allowed. This document separates identity from authority. An Agent Passport is an envelope of three signed claims, each made by the only party entitled to make it: the bank, which admitted the AI product to its list; the customer, which deployed an agent on that product; and the same customer, which signed the mandate the agent must stay within. Behind them stands a register on which the product's provider filed its identity, an accountable principal, insurance and Independent Assurance Evidence. The bank verifies the envelope and the signed instruction with an ordered, deny-by-default procedure and answers ALLOW, ESCALATE or DENY with a rule citation and a signed receipt. Authority may be delegated but never expanded. Revocation is a list lookup. Every decision is replayable, and every passport can be exported as one

self-verifying evidence bundle.

1. Introduction

Firms delegate invoice payment to AI agents. A bank receiving an instruction cannot determine which agent sent it, whether it was permitted to, or who answers for it. Since 2024, UK banks bear the loss when a misdirected payment is authorised. HM Treasury's 2026 consultation on modernising payment services regulation asks how authentication, consent and liability provisions should adapt to agentic payments. This standard gives the bank one verification call that answers those three questions before money moves, and gives a supervisor complete evidence afterwards without requiring it to inspect agents, products or transactions in advance.

The key words MUST, MUST NOT, SHOULD and MAY are to be interpreted as described in RFC 2119.

2. Terminology

Register
: An industry-operated record of AI products. It records identity and accountability. It does not certify that AI agents are good; it guarantees that someone is accountable when they are bad.

Provider
: The company that files an AI product on the register.

AI product
: A named, version-pinned AI system filed by a provider.

Independent Assurance Evidence
: A benchmark or audit report from a party other than the provider that the product meets the minimum assurance requirements for a stated use case. It is attached at filing and assessed by each relying bank, never by the register.

Assurance level
: One of three declared with the evidence: self-declared, independently verified, independently audited. It describes the evidence provided; nobody certifies it.

Bank
: The relying party that executes payment instructions. It admits products to its list and verifies every instruction.

Customer
: The legal person whose funds an AI agent moves.

AI agent
: The customer's deployment of an admitted product: a private key, a configuration, a mandate.

Supervisor
: A regulator that receives evidence through supervisory or incident processes. It operates no part of the infrastructure.

Passport
: The envelope defined in Section 4. A passport that satisfies Sections 3 to 7 is APS 1001-conformant.

3. Registration and Admission

3.1 A provider MUST file an AI product on the register before any bank admits it. A filing MUST name the legal entity, an accountable principal with a signed declaration that the filing is accurate, insurance in force at or above the minimum cover, the product and its pinned model version, the location of its documentation, Independent Assurance Evidence naming the use case it covers, the assurance level declared with that evidence, the payment intent the product is filed for (one of an enumerated list: supplier invoices, salaries and contractors, recurring subscriptions, tax and duties, customer refunds, card and wallet top-ups), and a UK data protection declaration: compliance with the UK GDPR and the Data Protection Act 2018, the provider's ICO registration number, the retention period for personal data the product processes, and any data protection impact assessment reference. A filing MUST NOT name a customer or contain any mandate content.

3.2 The register MUST run completeness checks and record each result next to the entry:

- F.1 provider matches the companies register
- F.2 accountable principal named, with a signed declaration
- F.3 insurance evidenced, cover at or above the minimum, in force
- F.4 product documented with a pinned model version
- F.5 Independent Assurance Evidence attached, with its assurance level, covering the registered use case
- F.6 product not already on the register
- F.7 UK data protection declared: compliance stated, ICO registration number well formed, retention period given (the declaration is the provider's; the register verifies nothing about compliance)

F.1 SHOULD be answered from the public company register (Companies House in the UK), which reports what companies filed and verifies nothing itself.

The register MUST sign a receipt for the filing. The register MUST NOT review, approve or rank filings.

3.3 A bank MUST decide for itself whether its customers may delegate payments to a registered product. The decision is the bank's; it MAY use any assessment it chooses, including its own evaluation of the Independent Assurance Evidence against the question "does this product meet the minimum assurance requirements for this use case". Automated review MAY recommend; a named officer MUST decide.

3.4 An admission MUST state the ceilings that every mandate on the product at that bank must satisfy (maximum per-payment

limit, maximum rolling limit per payee account, maximum payments per day, maximum validity, permitted actions, which MUST NOT exceed the payment intent filed, currency) and a hold condition (an amount above which the bank holds the instruction for a named person, at the bank or at the customer, to approve or decline with a note). A bank MAY require a minimum a
MAY scale its ceilings by the level declared.

3.5 A bank SHOULD tier its ceilings by the type of account the AI agent operates on and by customer class, as it already does for other payment channels. An AI agent is a payment channel on the account: every mandate MUST sit at or below the lower of the product ceiling for that account type and the admission ceiling for the product.

3.6 An admission MAY be suspended or withdrawn by the bank. Either act MUST cascade to every passport issued on the product at that bank.

4. The Passport

A passport MUST consist of three signed tokens (JWT, RFC 7519; EdDSA, RFC 8037) and an identifier:

admission	signed by the BANK: the admitted product (registration reference, name, identifier, version, hash of the register's receipt), the assurance level declared, ceilings, hold condition, validity, list pointer, and the hash of the agent_identity it was issued for.
agent_identity	signed by the CUSTOMER: agent name, the product it runs on, agent public key (cnf, RFC 7800), proof of possession, configuration hash, key custody.
mandate	signed by the CUSTOMER: permitted actions, currency, payee allow-list by account with the public-register record of each payee where one was checked, per-payment limit, rolling limit per payee account, maximum payments per day, expiry, and the account type and customer class the limits derive from, as an authorization_details object (RFC 9396).

No party MAY alter a claim it did not sign. A passport carries permission, not personal data.

5. Issuance

5.1 A customer registers an AI agent inside its bank's own channel by choosing an admitted product, generating a key pair, proving possession of the private key by signing the bank's challenge, and signing agent_identity. This creates an agent record. It is not a passport.

5.2 The customer writes its mandate. Before signing, the bank MUST check that every limit sits within the lower of the product's admission ceilings and the account-type tier (containment). A mandate outside them MUST NOT be signed. Where a payee is identified by company number, the bank SHOULD read the public company register and record the legal name, status and registered office in the mandate. The register holds no bank accounts; the account is the customer's statement, and payment goes only to that account.

5.3 On signature of a contained mandate the bank's system MUST sign the admission, assign the passport identifier, set the list status to ACTIVE and, where a purpose-bound rail is in use, mirror the mandate on it. No further review takes place at issuance. The first instruction under each mandate version is held for the customer's own confirmation (R.9); later instructions inside the mandate flow without a person.

6. Verification Procedure

The AI agent MUST sign every instruction with the key named in agent_identity, over the canonical instruction including a nonce used once. The bank MUST evaluate the following in order and stop at the first failure:

```
R.1  admission signature verifies (bank key)
R.2  passport ACTIVE and unexpired (list lookup)
R.3  agent_identity verifies (customer key) and is bound to
     this admission
R.4  instruction signed by the agent key in agent_identity,
     and its nonce not accepted before (a repeat is a replay)
R.5  mandate present, customer-signed, unexpired, not revoked
R.6  action and currency permitted; payee account on the
     allow-list
R.7  amount within the per-payment limit
R.8  amount plus the bank's own rolling total within the
     limit per payee account; payments in the rolling day
     within the mandate's count
R.9  amount above the hold condition, or the first
     instruction under this mandate version   -> ESCALATE
else                                            -> ALLOW
```

A failed check MUST NOT execute. The bank MUST either refuse it (DENY) or hold it for a named person to approve or decline with a note (ESCALATE), and in both cases MUST cite the failed rule. The reference implementation holds every failed check for review, so that a person, not a rule, has the last word on money that did not move; the failed rule and its class (fraud indicator, or the agent's own error) travel with the hold.

The result MUST cite the rule that decided it and MUST be accompanied by a receipt signed by the bank. Limits live in the mandate; running totals live at the bank.

7. Delegation

Where an AI agent delegates to another, the delegation MUST be signed by the delegating key, and for scopes S0 (mandate), S1 ... Sn:

    Sn is a subset of ... S1 is a subset of S0, and
    the action is an element of Sn.

Delegation MAY narrow authority. It MUST NOT expand it.

8. Evidence

8.1 Every filing, admission, signature, lifecycle change, verification and incident MUST be recorded in an append-only, hash-chained log. Every verification MUST be reproducible from its recorded inputs.

8.2 Every failed check MUST be recorded with the instruction, the rule, the reason, its class and, where a document produced the instruction, the extraction that produced it. Two classes MUST be distinguished: a fraud indicator (the instruction points at a destination, key or record the customer never authorised: redirection, a copied passport, a replay, a forged claim) and an agent error (a wrong amount, currency, action or frequency inside the agent's own remit, an operational quality event for the agent's owner). A repeated refusal of the same rule SHOULD raise an alert at the bank. Nothing in this standard reports a refusal to an authority; evidence is available on request (8.4).

8.3 Each party sees only what its role requires: the customer, and conceptually the provider, its own agent's error pattern; the bank its instructions, checks and verdicts; a supervisor evidence on request.

8.4 For any passport the bank MUST be able to produce one evidence bundle: the register filing and receipt, the admission, the agent identity, the mandate, every verification with its inputs and receipt, the refusals, and the chain segment, verifiable with the published public keys. A supervisor MAY request such a bundle through normal supervisory or incident processes. The export MUST itself be recorded.

9. Lifecycle

File	A provider files an AI product (Section 3.1).
Admit	A bank runs its own assessment and admits the product with ceilings and a hold condition (Sections 3.3, 3.4).
Issue	A customer registers an AI agent and signs a contained

	mandate; the passport is issued at signing (Section 5).
Act	The bank verifies each instruction (Section 6).
Detect	Every refusal is recorded; patterns raise alerts.
Revoke	The bank sets the list status of a passport or of a product. The next instruction fails at R.2 on every rail that mirrors the mandate.
Evidence	Any passport can be exported as one bundle (Section 8.3).

10. Governance

APS 1001 is written for adoption by an industry body on the precedent of the Open Banking Implementation Entity: the body maintains the standard and the register, banks adopt it through commercial schemes because they carry the fraud loss and the customer relationship, and regulators set guardrails and receive evidence without building, operating or approving the technology. Nothing in this standard requires or implies regulatory approval of any AI product.

11. Security Considerations

A copied passport is useless without the agent's private key (R.4). A forged or altered claim fails its signature (R.1, R.3, R.5). A manipulated agent that requests payment to an account the customer never listed fails R.6 regardless of how genuine the invoice appeared. A mandate cannot exceed the product's ceilings at that bank (Section 5.2). Compromise of the bank's key, and attestation of the running software, are out of scope.

12. What APS 1001 Does Not Specify

Settlement. Know-your-customer, sanctions or funds checks. Whether a payment is wise. Whether an AI product is good: the register records accountability and the bank makes its own assessment. Liability of the provider for an agent's conduct beyond the accuracy of its filing and the insurance it declared. Any judgement by a model: models read and draft; rules decide; humans sign.

13. References

APS 1002 (delegation chains, reserved), APS 2001 (tax rails, reserved), RFC 2119, RFC 7519 (JWT), RFC 7800 (cnf), RFC 8037 (EdDSA), RFC 9396 (Rich Authorization Requests), W3C Verifiable Credentials (JWT profile), NIST NCCoE 2026 (agent identity and authorization), FATF 2025 (AI and AML/CFT), HM Treasury (2026) Modernising Payment Services Regulation, section 3.2 and question 15; the Open Banking chapter of the same consultation.

Authors' Addresses

Team Agent Passport, Cambridge, United Kingdom. Developed alongside

Cambridge academic and industry partners.
Reference implementation: https://cdir.agenticworld.uk
Source: https://github.com/cvikl/agent-passport