

The complete identity and trust platform for autonomous AI agents.

AI Agent Identity and Trust Platform

CyberSecAI Ltd · London, United Kingdom · agentpass.co.uk

01 At a glance

EXECUTIVE SUMMARY

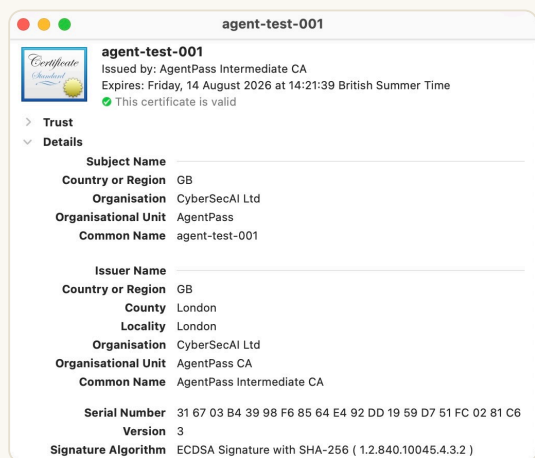
AgentPass is the first platform to combine a **purpose-built Certificate Authority for AI agents** with graduated trust enforcement, per-action cryptographic signing, real-time sanctions screening, and a tamper-evident evidence ledger. A complete stack. No sidecars. No proxies. One API call.

- ✓ **Purpose-built CA.** Short-lived X.509v3 agent certificates, auto-issued and auto-rotating, instantly revocable.
- ✓ **Sovereign, region-bound.** Jurisdiction is signed into the certificate. The agent operates only within its authorised region.
- ✓ **Real-time sanctions.** 19,129 OFAC SDN entries screened before execution, not after.
- ✓ **Behavioural XDR (AEBA).** Anomaly detection even with valid credentials. Kill switch built in.
- ✓ **Standards-aligned.** RFC 5280, FIPS 186-5, SPIFFE v1.0, EU AI Act, eIDAS 2.0.
- ✓ **Trust built into the certificate.** The L0-L4 trust level is signed into every cert. Earned sequentially, no self-promotion.
- ✓ **Per-action signing (MCPS).** Every action ECDSA P-256 signed. Non-repudiable, court-admissible.
- ✓ **Evidence ledger.** SHA-256 hash-chained, tamper-evident, exportable for auditors and courts.
- ✓ **CA-agnostic.** Issue from the AgentPass CA or your regional CA. Your CA issues identity, AgentPass enforces trust.
- ✓ **Protected.** PCT international patent, 21+ UK filings, 9 IETF drafts, IANA OID 66339.

02 Certificate Authority

Root CA	AgentPass Root CA (CyberSecAI Ltd)
Intermediate	AgentPass Intermediate CA
Algorithm	ECDSA P-256 (FIPS 186-5)
Signatures	SHA-256 (ecdsa-with-SHA256)
Certificate	X.509 Version 3 (RFC 5280)
Validity	1-day ephemeral, auto-rotating
Identity	SPIFFE v1.0 workload ID (URI SAN)
Trust Level	L0-L4 (signed extension)
Jurisdiction	Region-bound (OID ...66339.2.*)
OID Arc	1.3.6.1.4.1.66339 (IANA PEN)
Chain	Agent → Intermediate → Root · VERIFIED
Key Usage	Digital Signature + Client Auth

LIVE CERTIFICATE · VALID



A live AgentPass-issued agent certificate, inspected in macOS Keychain. Issued by AgentPass Intermediate CA, ECDSA with SHA-256, X.509 v3. Chain resolves to the AgentPass Root CA.

Every AI agent receives an ephemeral certificate at creation, automatically issued and rotated. **No manual provisioning. No long-lived credentials. No shared secrets.**

1-day

Ephemeral certificate validity. Auto-issued, auto-rotating, instantly revocable.

L0-L4

Graduated trust levels, earned sequentially with a full audit trail.

19,129

OFAC SDN sanctions entries screened in real time, before execution.

03

Trust enforcement

L0 IDENTITY	Identity only Agent exists, cryptographic identity issued
L1 READ	Read / Query Agent can read data and query systems
L2 WRITE	Write / API Agent can call APIs and modify data
L3 FINANCE	Financial Agent can execute payments - sanctions screened
L4 CRITICAL	Critical Agent requires hardware-backed human approval

Agents earn trust sequentially. Cannot skip levels. Cannot self-promote. Admin-only promotion, with a full audit trail.

3.1

Sovereign AI, bound at the certificate

The trust level and the jurisdiction are signed into every certificate. The agent is cryptographically bound to operate only within its authorised region. Sovereign AI, enforced at the certificate, not by policy.

Jurisdiction	Signed X.509 extension under OID 1.3.6.1.4.1.66339.2.* - agents are region-locked at issuance.
Regions	EU · UK · LATAM · APAC · US · MEA - each region carries its own trust anchor and legal standing.
Trust level	The L0-L4 level travels inside the certificate, so every relying party reads it from the cert itself.

04 Core capabilities



Per-action signing

MCPS PROTOCOL

Every action an agent takes is cryptographically signed with a unique nonce, timestamp, and ECDSA P-256 signature. Not the channel - **the action itself**. Tamper with any field and the signature breaks. Non-repudiable. Court-admissible.



Sanctions screening

REAL TIME · BEFORE EXECUTION

Financial actions are screened in real time against **19,129 OFAC SDN sanctions entries** before execution. Not after. Before. Blocked actions are logged with the screening result.



Evidence ledger

SHA-256 HASH-CHAINED

Every decision - allow, block, promote, revoke, screen - lands in a SHA-256 hash-chained evidence ledger. Tamper-evident. Exportable for auditors, regulators, and courts. **Every action your agent ever took, provable and permanent.**



Behavioural analytics

AEBA-XDR

An ML ensemble (Bayesian + Random Forest) monitors agent behaviour against learned baselines. Detects anomalies **even when the agent has valid credentials and certificates**. 6 detection packs, 36 rules. Kill switch: detect, revoke, preserve evidence.

05 Integration

Zero Code	Claude MCP server - one config file
REST API	Any language, any framework, any cloud
Python SDK	pip install agentpass-sdk
Gateway	Drop-in enforcement proxy - 7 checks, fail-closed
Frameworks	LangChain, CrewAI, Bedrock, AutoGen (roadmap)

06 Standards compliance

STANDARD	SCOPE	STATUS
RFC 5280	X.509 PKI certificate profile	COMPLIANT
FIPS 186-5	ECDSA P-256 digital signatures	COMPLIANT
SPIFFE v1.0	Workload identity framework	COMPLIANT
RFC 6125	DNS-based identity representation	COMPLIANT
IANA PEN	Private Enterprise Number 66339	REGISTERED
OWASP AISVS	AI Security Verification Standard	CO-AUTHORED
EAIS v1.0	Enterprise AI Standard (104 controls)	AUTHORED
EU AI Act	Articles 9-17 (effective Aug 2026)	COMPLIANT
LGPD	Brazil data protection	COMPLIANT
CMN 4,893	Brazil cybersecurity governance	COMPLIANT
eIDAS 2.0	EU digital identity framework	ALIGNED

07 IETF Internet-Drafts

draft-sharif-mcps-secure-mcp

draft-sharif-x509-agent-identity-profile

draft-sharif-agent-payment-trust

draft-sharif-attp-agent-trust-transport

draft-sharif-openid-agent-identity

draft-sharif-agent-audit-trail

+ 3 additional drafts (9 authored)

08 Intellectual property

THE MOAT

PCT International Patent	PCT/GB2026/051351
	157 countries
UK Patents filed	21+
IANA OID (CyberSecAI Ltd)	1.3.6.1.4.1.66339
Trademark	UK00004362551

09 CA-agnostic by design

AgentPass issues certificates from its own CA by default. For regulated industries requiring local legal standing, AgentPass integrates with regional Certificate Authorities:

LATAM	ICP-Brasil accredited trust providers
APAC	Nationally accredited G-PKI providers
Europe	eIDAS Qualified Trust Service Providers
Global	Any X.509-compliant CA

Your CA issues the identity. AgentPass enforces the trust. Together, that is a complete solution. Separately, a certificate is just a piece of paper.

10 Deployment

The platform runs on **LAInux**, a hardened secure Linux distribution built by CyberSecAI specifically for AI workloads. Runtime enforcement at every layer, from the operating system to the agent action.

Cloud GCP, AWS, Azure, on-premise

Monitoring Prometheus metrics, deep health checks

CONTACT

CyberSecAI Ltd
4th Floor, 205 Regent Street
London W1B 4HB
United Kingdom

GET IN TOUCH

agentpass.co.uk
cybersec.ai.co.uk
contact@cybersec.ai.co.uk