WHAT IS QODIQA

Authorize *first.* Execute second.

QODIQA is an **enforcement layer** between your applications and AI providers. A request reaches a provider only with a signed, single-use authorization that the gateway has verified, and every decision, allow or block, is recorded in a tamper-evident log that a third party can check offline.

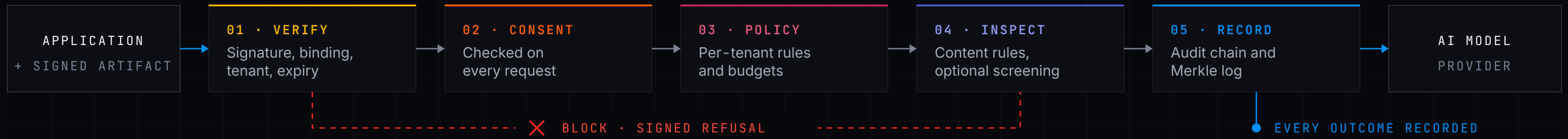
THE PROBLEM

AI decides in milliseconds. Compliance evidence is periodic.



THE EXECUTION PATH

A BLOCKED REQUEST NEVER REACHES THE MODEL. EVERY OUTCOME LEAVES A RECORD.



01 · Signed artifacts

Authorization you can check

Every request needs an Ed25519-signed artifact bound to one request and tenant. It expires within 60 seconds and works once.

02 · Tamper-evident record

A hash chain and a Merkle log

Each audit entry holds the hash of the previous one. A Merkle log proves an entry is included without revealing the others.

03 · Independent verification

Checked offline, by anyone

A separate verifier that imports none of the gateway code checks the evidence offline, with keys from another source.

WHO IT IS FOR

Teams that put AI in front of people, data or actions: **engineers** who integrate it, **security and compliance** owners who must show what was allowed, and **auditors** who verify it themselves.

MAPS TO · SUPPORTS EVIDENCE FOR

EU AI ACT · GDPR · HIPAA · ISO/IEC 42001 · ISO/IEC 27001 · NIST AI RMF · OECD AI PRINCIPLES

START HERE

WEBSITE	www.qodiqa.com	CONTACT	contact@qodiqa.com
SPECIFICATION	github.com/qodiqa/qodiqa		
QUICKSTART	github.com/qodiqa/qodiqa-gateway		
VERIFIER	github.com/qodiqa/qodiqa-verify		

Implemented: gateway v1.0.0 (Apache-2.0). **Specified separately:** QODIQA-STD-1.0 (CC BY 4.0). Technical evidence only: no certification, endorsement or partnership is implied, and this is not legal advice. **This page:** CC BY 4.0.