TechWizard
Structuring Digital Complexity

EA-WIZARD · SECURITY

Security & sovereign multi-tenancy

Granular RBAC, Row-Level Security tested under attack, an immutable audit log, AES-256 everywhere, and a published performance certification. Built to pass audits, not avoid them.

May 2026 · Version 15

RFP-READY DOCUMENT

EA-Wizard delivers the multi-tenant security that banks and the public sector expect — and proves it with measured, published results rather than marketing claims.

340	23	0	2 099
RBAC permission codes	tenant isolation tests	leaks under attack	test methods

Access control

RBAC — 340 permission codes

- Pattern `module__resource__action`.
- Caffeine cache with 60-second TTL; `@CacheEvict` instant invalidation on role change.
- Live-probed via Spring Actuator.

Enterprise SSO

Full IAM integration with Keycloak, LDAP and SAML 2.0. `UserStatusFilter`, `DemandStatusPolicy` and `OrganizationResolutionFilter` are all tested under attack to block impersonation.

License validation — HMAC-SHA256

Signed keys in `TIER-ORGID-EXPIRY-MAXUSERS-HMAC` format. The frontend LicenseGate refuses out-of-scope features — with no client-side bypass.

Multi-tenant isolation

Tenant isolation is not an application convention. It is a boundary enforced by the database itself, through PostgreSQL Row-Level Security across the full schema.

- Dedicated `eaapp` role with `NOSUPERUSER` — even an authenticated developer cannot bypass RLS.
- 40+ parent tables and 60+ child tables covered; 4 orphan tables explicitly handled.
- 23 automated isolation tests (cross-tenant + Testcontainers RLS) running in CI.
- NULL-org leak audited and closed (V145 / V146).

Tested under attack — Gatling

METRIC	VALUE
Cross-tenant leak attempts	60
Rejected (HTTP 400)	60
Records exposed	0
Latency under attack (p95)	23 ms

These are not marketing lines — they are measured outcomes, committed to the repository as the `TenantIsolationSimulation`.

Audit & traceability

Immutable audit log

- PostgreSQL `BEFORE` trigger blocking `UPDATE` and `DELETE`.
- Tamper-proof by design — even a DBA cannot alter an audit event.
- Protection lives in the engine, not in the application; RLS tightened in V146 to prevent NULL-org leaks.
- CSV + PDF export, date-range filtered, aligned with European and Moroccan regulators' requirements.

Distributed observability

- Full OpenTelemetry auto-instrumentation: every HTTP request, SQL query and cache hit traced.
- Runtime-configurable from an admin GUI (sampling, endpoint) — no restart needed.
- Auto-disable on connectivity failure via an AtomicInteger probe counter.

Encryption

Uniform AES-256-GCM across six secret categories, through a single `AesEncryptionService`: OpenTelemetry headers, Jira and ServiceNow connector credentials, SMTP credentials, AI provider API keys, and EA Chat credentials. One algorithm, one master key, one audit point.

Performance certification

Reference **EAW-PERF-CERT-V12-2026-003** — measured and published.

METRIC	VALUE
Requests	34 476
Errors	0
p95 latency	136 ms
p99 latency	240 ms
Committed simulations	4

Production-tuned stack: Tomcat threads 300, accept-count 200, Hikari pool 25, 5 s connection timeout — sized for a 200-user spike.

Audit readiness

- 28 of 30 known CVEs remediated.
- Immutable audit log + full-schema RLS + live tenant-attack testing.

> **AVAILABLE ON REQUEST**
>
> For RFP responses: full RBAC permission catalog, RLS policy listing, audit-log schema and trigger source, Gatling simulation sources, the performance certification report, and the OWASP scan report.