Requiems API — API Authentication & Security Policy

Effective February 1, 2026 · Bobadilla Technologies

1. Purpose and Scope

This document defines the authentication mechanisms, access controls, and security procedures governing the Requiems API API platform. It applies to all API consumers and governs Requiems API's obligations with respect to API access security.

2. API Key Issuance

- Each registered account is issued a unique, cryptographically random API key
- Keys are generated using a high-entropy random source — not derived from account data
- Keys are transmitted to the user once at creation time over TLS 1.3 encrypted channels
- Keys are stored in our system as hashed values — the plaintext key is never stored
- Key format: high-entropy alphanumeric string, minimum 32 characters

3. API Key Usage

- All API requests must include the API key in the Authorization header: Bearer <key>
- TLS 1.3 is required on every request — HTTP connections are rejected
- Keys must not be embedded in client-side code, public repositories, or URLs
- Keys should be stored in environment variables or secrets management systems

4. Key Revocation

- API keys can be revoked instantly via the user dashboard
- Revocation takes effect within seconds at the authentication layer
- Users should revoke keys immediately upon suspicion of compromise
- Revoked keys cannot be recovered — a new key must be generated
- Multiple keys per account are not currently supported; users must regenerate to rotate

5. Transport Security

- TLS 1.3 enforced on all API endpoints — no TLS 1.2 or lower accepted
- Cipher suites: TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256
- TLS termination handled by Cloudflare before reaching origin servers
- HSTS (HTTP Strict Transport Security) enforced
- Certificate validity monitored and auto-renewed via Cloudflare

6. Rate Limiting & Abuse Prevention

- Rate limits enforced at the Cloudflare edge layer before requests reach origin
- Limits are applied per API key — not per IP, preventing shared-IP false positives
- Exceeding rate limits returns HTTP 429 with Retry-After header
- Cloudflare WAF rules block malformed requests, known attack patterns, and injection attempts
- DDoS mitigation active at all times — volumetric attacks absorbed before reaching API

7. Origin Security

- Origin servers are not exposed directly to the internet
- Caddy requires a Cloudflare Origin Pull client certificate before proxying
- Server firewall rules whitelist only Cloudflare IP ranges for inbound traffic
- SSH access to servers is key-authenticated only — no password authentication

8. Data Handling During Authentication

Authentication is validated at the middleware layer before any request payload is processed. If authentication fails, the request is rejected immediately and no payload processing occurs. Successful authentication does not result in any logging of the request payload — only the API key hash, endpoint, response code, and timestamp are recorded for usage metering.

9. Incident Response Procedures

- Security incidents are triaged within 4 business hours of detection
- Affected API keys are revoked immediately upon confirmed compromise
- Affected customers notified within 72 hours of confirmed incident
- Post-incident review conducted within 7 days
- Security contact: eliaz@bobadilla.tech

10. Policy Review

This policy is reviewed at minimum annually and updated as required when the authentication infrastructure changes. The current effective date is February 1, 2026. For the latest version, visit requiems.xyz/en/security