



REALNODE PROTOCOL

Infraestructura de Confianza y Gobernanza de Hardware

Libro Blanco Técnico

Autor: EMKAY LABS

Documento Público

Rev. 1.0 — Junio 2026

Resumen Ejecutivo

*Este Libro Blanco define las especificaciones fundamentales del protocolo **RealNode**, una infraestructura de confianza asimétrica diseñada específicamente para proteger los flujos de venta de entradas de alta demanda (Ticketing) y Ventas Flash contra la reventa masiva automatizada (mass-scalping). Al trasladar la validación de la capa de aplicación al determinismo de hardware, RealNode introduce un método de atestación transparente que detiene instantáneamente las compras automatizadas por bots, garantizando el acceso a los verdaderos fans.*

Objetivos Estratégicos:

- **Protección de Inventario (Anti-Scalping):** Asegurar las ventas flash para garantizar que cada entrada sea comprada por una entidad humana orgánica y certificada, no por un bot.
- **Inclusión Digital Universal:** Compatible con todos los terminales a través de estándares criptográficos (FIDO2 / WebAuthn).
- **Eficiencia Económica (Edge Security):** Reducción masiva de la carga del servidor durante los picos de venta — hasta un **60 %** de ahorro en procesamiento.

Estructura de la Oferta: El protocolo se estructura en tres niveles de integración (**RN Insight**, **RN Sentinel**, **RN Vault**), permitiendo a las plataformas de ticketing calibrar la seguridad según la demanda — desde la auditoría pasiva hasta la atestación criptográfica absoluta de hardware.

1 Los Límites de la Seguridad Adaptativa en Ticketing

1.1 El Colapso del Modelo de “Confianza Relativa” en Ventas Flash

En 2026, la industria del ticketing de alta demanda se enfrenta a un nivel de profesionalización sin precedentes en las redes de reventa automatizada. Cuando se abren las ventas de un concierto muy esperado, los bots de scalping vacían un stock de 50.000 entradas en segundos, mucho antes de que los verdaderos fans puedan siquiera ingresar a la cola virtual. Las soluciones tradicionales — CAPTCHA, Scoring de IP, WAF — intentan calibrar la seguridad usando modelos probabilísticos y fracasan.

- **Los Límites del CAPTCHA:** Los desafíos visuales son cada vez más superados por redes neuronales adversarias. Este enfoque añade fricción al proceso de compra del fan legítimo sin garantizar una barrera absoluta contra la automatización avanzada.
- **Evasión de Colas Virtuales:** Los scripts de scalping utilizan miles de proxies para saltarse la cola y asegurar el inventario instantáneamente.

1.2 La Filosofía RealNode: Determinismo Binario

A diferencia de los enfoques basados en la incertidumbre permanente, *RealNode* adopta una postura de **Seguridad Determinista**. *“El hecho de que un comprador sea humano no es una probabilidad algorítmica — es un estado verificable tanto material como matemáticamente.”*

Este principio rige cada capa del protocolo: no se autoriza ninguna compra de entrada a menos que se haya establecido criptográficamente una prueba de identidad irrefutable vinculada al hardware.

1.3 Estandarización Criptográfica: Autenticación Cross-Device

Para garantizar un acceso universal sin comprometer la seguridad, *RealNode* confía en primitivas matemáticas asimétricas (Ed25519) definidas por consorcios abiertos:

- **Delegación de Atestación:** El smartphone del usuario se utiliza como autenticador universal mediante su componente de hardware seguro (Secure Enclave / TPM), aprovechando los protocolos FIDO2.
- **Ejecución de Alto Rendimiento:** Tras una atestación exitosa, el acceso se concede en menos de **200ms** a través de un clúster de evaluación distribuido en memoria.

***Nota sobre la experiencia del usuario:** Esta arquitectura está diseñada para que la capa de seguridad no introduzca latencia perceptible. La autenticación se completa más rápido que una carga de página estándar, algo crucial para no ralentizar las ventas flash de entradas.*

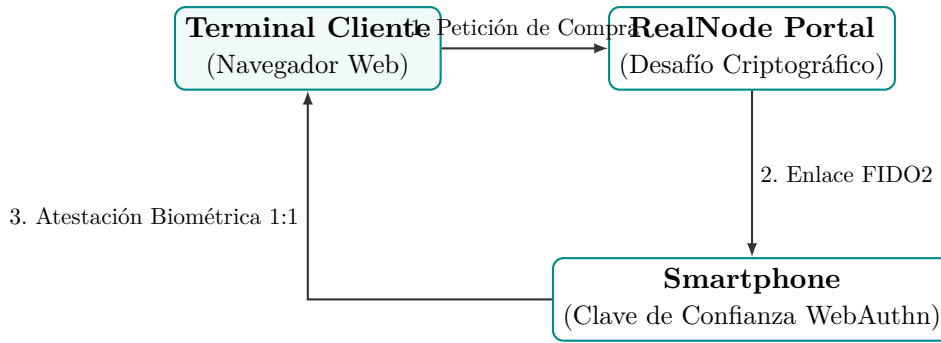


Figura 1: Relé biométrico entre dispositivos (Atestación asimétrica FIDO2 — no se transmite ni almacena ningún dato biométrico).

2 El Ecosistema RealNode: Arquitectura en Cascada

El protocolo *RealNode* ofrece tres niveles graduados de protección técnica, desde la observación inteligente hasta una barrera de hardware inviolable.

2.1 Matriz de Comparación Tecnológica

Indicador	RN Insight	RN Sentinel	RN Vault
Experiencia del Usuario	Fluida (Invisible)	Adaptativa	Registro Criptográfico
Mecanismo de Filtro	Analítico	Comportamental	Determinista (Secure Enclave)
Modo de Protección	Auditoría y Telemetría	Gobernanza Activa	Aislamiento Absoluto
Tasa de Falsos Positivos	Pasivo (no bloqueante)	Baja (con Fallback)	Casi cero

Cuadro 1: Evolución de los paradigmas de defensa en los niveles de integración.

2.2 RN Insight: Diagnóstico Pasivo y Telemetría

Este módulo emplea una arquitectura probabilística para clasificar el tráfico sin introducir latencia.

- **Detección de Bots Headless:** Identificación de bots automatizados a través del análisis de inconsistencias del DOM y huellas digitales de navegadores virtuales antes de que lleguen al carrito.

2.3 RN Sentinel: La Solución Absoluta contra el Mass-Scalping

Este módulo introduce una defensa adaptativa para proteger el inventario de entradas y las cuotas en tiempo real.

- **Cuotas Atómicas Distribuidas:** Los límites de compra dinámicos se aplican por sesión de hardware autenticada a través de contadores atómicos. Esta es la solución matemática definitiva contra el **mass-scalping**: Un revendedor ya no puede comprar 500 entradas con 500 direcciones IP falsas, porque el límite de compra está estrictamente ligado al dispositivo físico de hardware. Un dispositivo = una cuota de entradas autorizada.

- **Análisis Cinético vía Edge Computing:** El análisis cinético actúa como un filtro de telemetría de alto rendimiento. El puntaje cinético actúa como un disparador dinámico para escalar la verificación a niveles más altos (RN Vault) cuando se sospecha un comportamiento sintético.

2.4 RN Vault: Atestación de Hardware (Zero-Trust)

Este nivel representa el nivel más alto de seguridad para las ventas flash más demandadas.

- **Anclaje Físico:** La identidad digital está vinculada criptográficamente a una clave privada residente permanentemente en el *Secure Enclave* del procesador.
- **Vínculo Inviolable 1:1:** El sistema garantiza matemáticamente que un único dispositivo físico se mapea a un único fan real.
- **Registro Asimétrico:** El proceso de registro se ajusta a la especificación WebAuthn. La verificación de la raíz de confianza se realiza a través del FIDO Alliance Metadata Service.

3 Posicionamiento Estratégico: ¿Por qué RealNode?

3.1 Diferenciación de los Estándares del Mercado

Mientras que la mayoría de las soluciones de seguridad se centran en el evento de inicio de sesión, RealNode establece una capa de confianza persistente durante toda la sesión de pago.

- **Eliminación de Fricción Cognitiva:** El protocolo reemplaza las pruebas de Turing visuales (CAPTCHA) — que penalizan a los fans reales — con atestaciones criptográficas transparentes en segundo plano ejecutadas en menos de 200ms.
- **Privacidad de Datos y Gobernanza:** Nunca se almacenan datos biométricos en bruto. La confianza se delega completamente en el identificador de hardware anonimizado (IDH).

4 Infraestructura: Resiliencia y Cumplimiento

4.1 Arquitectura de Persistencia Híbrida

- **Fast-Path In-Memory:** Para gestionar picos de tráfico masivos, la validación continua de acceso se ejecuta en clústeres en memoria con latencia sub-milisegundo. La atestación de hardware inicial, por su parte, se completa en menos de 200ms.
- **Aislamiento Multi-Tenant (RLS):** La capa de persistencia impone un estricto aislamiento de inquilinos mediante políticas de seguridad a nivel de fila (Row-Level Security) en la base de datos PostgreSQL.

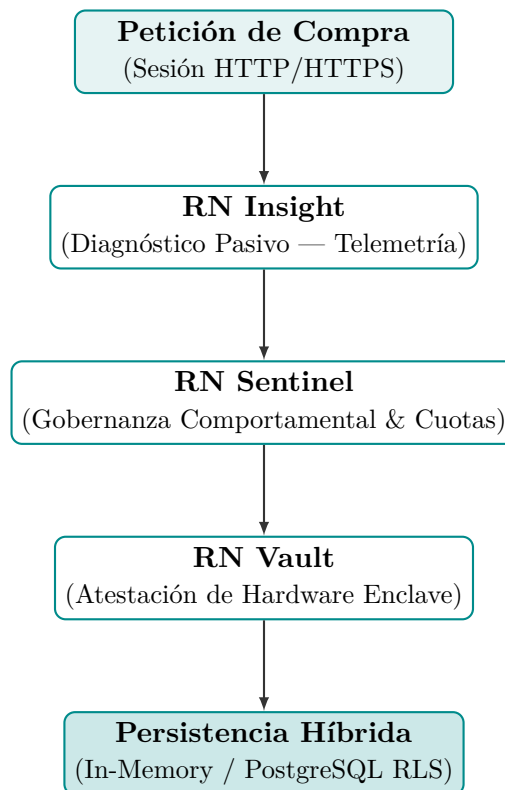


Figura 2: Arquitectura de resiliencia en cascada durante la venta de entradas.

4.2 Gobernanza de Privacidad (Privacy-by-Design / RGPD)

- **Sin Almacenamiento Biométrico Centralizado:** Los datos biométricos nunca abandonan el enclave seguro del dispositivo cliente.
- **Identificadores de Hardware Hasheados (IDH):** Los fans son rastreados exclusivamente a través de firmas de hardware anonimizadas y encriptadas.

5 Conclusión: Devolviendo el Mercado a los Fans

El protocolo *RealNode* no es simplemente una defensa perimetral; es una infraestructura soberana para un ticketing justo. Al restablecer un límite claro y matemáticamente fundamentado entre los fans genuinos y los revendedores automatizados, devuelve el control absoluto del inventario a las organizaciones que dependen de él.

¿LISTO PARA ASEGURAR SU INVENTARIO DE ENTRADAS?

Discutamos sus requisitos de protección y estrategia de integración.

Laboratorio: EMKAY LABS

Contacto Comercial: realnode@emkaylabs.tech

Contacto de Seguridad: security@emkaylabs.tech

Sitio Web: emkaylabs.tech
