GSN – Revisión de Seguridad y Arquitectura (Versión Expandida)

Resumen Ejecutivo

GSN (Global Security Netguard) es una red descentralizada y stateless de validación criptográfica diseñada para proporcionar autenticación segura sin almacenar identidades ni historiales de actividad.

Su propósito es convertirse en una capa global de confianza para Internet, del mismo modo que DNS resolvió el direccionamiento y TLS aseguró las comunicaciones.

Principios Fundamentales

Una única identidad digital activa por persona. No existen múltiples dispositivos simultáneos asociados a la misma identidad, lo que minimiza la superficie de ataque.

No existe recuperación de credenciales; únicamente nuevas altas que sustituyen a la anterior.

La red valida autenticidad, pero no conserva registros de transacciones.

Analogía Operativa

GSN funciona como un portero que verifica si una persona está autorizada a entrar, pero no anota quién pasó ni a qué hora. Solo certifica autenticidad en ese instante.

Proceso de Alta

El usuario se identifica con biometría, factor físico (NFC/RFID) y clave privada. El sistema genera un hash único que se convierte en la única identidad activa.

Pérdida o Robo

Un organismo autorizado utiliza un dispositivo desactivador para suspender temporalmente el hash comprometido tras verificar la identidad del usuario mediante documentación y biometría.

Suspensión y Sustitución

El hash puede permanecer suspendido durante 15 días. Una vez generado el nuevo alta, el hash anterior se elimina definitivamente.

Modelo de Privacidad

La red procesa únicamente solicitudes de validación y devuelve una respuesta sí/no. No almacena identidad real, historial ni metadatos persistentes.

Modelo de Amenazas

Protege frente a phishing, robo de credenciales, suplantación y compromisos de proveedores centralizados. Los principales riesgos residuales son el compromiso del hardware y el abuso de dispositivos desactivadores.

Niveles de Seguridad

Se pueden definir niveles según el contexto: huella, iris, ADN u otros factores, con distintos requisitos criptográficos y de hardware.

Hardware y Certificación

Los dispositivos incorporan chips certificados y sellados por fabricantes autorizados por la alianza, que actúan como raíz de confianza.

Gobernanza

GSN sería gestionado por una asociación internacional sin ánimo de lucro inspirada en modelos como CERN, Linux Foundation y FIDO Alliance.

Licenciamiento Abierto

La licencia recomendada para la versión abierta del white paper es CC BY 4.0, que permite reutilización y adaptación con atribución.

Valor Diferencial

GSN no compite con FIDO o SSI, sino que los integra dentro de una arquitectura global neutral, interoperable y orientada a la privacidad radical.

Conclusión

GSN es técnicamente plausible, conceptualmente elegante y estratégicamente ambicioso. Su mayor reto no es técnico, sino institucional y de adopción global.