Protocolo de Custodia de Llaves

Compromisos públicos del protocolo: quórum configurable, separación de funciones, llave de acceso obligatoria, sobres cifrados, enfriamiento, vigilante de custodia y recuperación solo por quórum.

Qué protege el protocolo

Estado: Disponible

El Protocolo de Custodia de Llaves gobierna las operaciones críticas del producto —firma de versiones, activación de licencias y recuperación— mediante una ceremonia por quórum. Ninguna persona, por sí sola, puede ejecutar esas operaciones ni reconstruir una llave protegida.

Este documento recoge solo los compromisos públicos del protocolo. El diseño completo se facilita bajo confidencialidad en sesión de evaluación, según consta en el documento de confidencialidad de esta biblioteca.

Compromisos públicos

Quórum por secreto compartido de Shamir

La llave protegida se reparte mediante el esquema de secreto compartido de Shamir sobre GF(256), con **quórum configurable** y con posibilidad de fragmentos ponderados. Los fragmentos jamás se almacenan en el sistema: solo se conservan sus metadatos y su huella. La llave reconstruida existe únicamente durante la ceremonia y para el acto autorizado.

Separación de funciones

La ceremonia aplica separación de funciones: quien solicita una operación no es quien aporta los fragmentos que la autorizan. Las funciones de solicitante y de aportante son disjuntas por diseño.

Llave de acceso obligatoria para todo participante

Toda participación en una ceremonia exige una **llave de acceso WebAuthn** (passkey) del participante. Sin ella no se opera. Opcionalmente, un fragmento puede sellarse al hardware del autenticador de su custodio.

Sobres cifrados

Los fragmentos y los sobres de recuperación se protegen con derivación **Argon2id** y cifrado **AES-256-GCM**. Los códigos impresos que intervienen en la ceremonia residen en el sistema únicamente como huellas unidireccionales con sal; sus valores en claro no existen en ninguna base de datos.

Ceremonia registrada en bitácora

Cada ceremonia queda registrada en la bitácora, con sus participantes y su resultado, y su acta se firma digitalmente dentro de la plataforma.

Periodo de enfriamiento en la recuperación

Toda recuperación está sujeta a un **periodo de enfriamiento** y al aviso a todos los custodios antes de completarse. Durante ese periodo la recuperación puede detenerse. La existencia de este mecanismo es pública; sus parámetros operativos no se divulgan.

Mecanismos de protección del custodio

El protocolo incorpora mecanismos de protección del custodio. Su detalle forma parte del diseño que se facilita bajo confidencialidad en sesión de evaluación.

Marca forense documental

Los documentos impresos de custodia incorporan una **marca forense** cuya finalidad es atribuir filtraciones de documentos de custodia. Su existencia y su finalidad son públicas; su formato no se divulga.

Vigilante de custodia

Existe un **vigilante de custodia** cuya función es detectar la pérdida o la degradación de las custodias y alertar de ello. Su existencia y su función son públicas; sus parámetros operativos no se divulgan.

Sin quórum no hay recuperación

Sin quórum, la llave no se recupera, por diseño y sin puertas traseras, incluidas las del proveedor. Esta no es una limitación operativa: es la propiedad central del protocolo.

Las dos formas

Forma	Custodia
Gobierno	El proveedor **no retiene ningún fragmento** de las llaves institucionales. La recuperación es posible únicamente por quórum de los custodios de la propia institución.
Comercial	El proveedor retiene un **fragmento de recuperación ponderado**, que por sí solo no reconstruye nada: la recuperación sigue exigiendo el quórum con los custodios.

Ejercicio propio del proveedor

Como evidencia de ejercicio —no como parámetro de ninguna instalación de cliente—, el proveedor ejerce este protocolo sobre su propia llave de firma de versiones con un quórum **2 de 3**, con ceremonia real ejecutada y registrada. El quórum de cada instalación lo define esa instalación.