Estrategia de configuración de OnlyKey Duo

Tabla de Contenidos

Descripción General

Este documento describe una estrategia de seguridad integral para usar una llave de seguridad de hardware OnlyKey Duo con el fin de proteger dos gestores de contraseñas (Bitwarden y KeePassXC), el acceso SSH a GitHub y el cifrado de correos electrónicos mediante GPG. El objetivo es garantizar que una laptop o dispositivo móvil perdido o robado permanezca seguro, siempre que el propio OnlyKey Duo no se vea comprometido.

Capacidades del OnlyKey Duo

El OnlyKey Duo ofrece las siguientes funcionalidades:

- **2 perfiles**: Perfil 1 (principal) y Perfil 2 (negación plausible)
- **12 ranuras por perfil**: 6 ranuras por página, 2 páginas
- **Ranuras de llaves ECC/RSA**: Para llaves privadas SSH y subllaves GPG
- **Soporte FIDO2/WebAuthn**: Respaldado por hardware, admite registros ilimitados de sitios
- **Desafío-respuesta HMAC-SHA1**: Compatible con KeePassXC y herramientas similares
- **PIN de autodestrucción**: Borra el dispositivo tras un número configurable de intentos de PIN incorrectos

---

Requisitos Mapeados a las Funcionalidades del OnlyKey

Bitwarden

Bitwarden soporta **FIDO2/WebAuthn** de manera nativa, lo que lo convierte en la integración más sencilla.

Pasos de configuración:

1. Registrar el OnlyKey Duo como llave de seguridad FIDO2 en los ajustes de *Inicio de Sesión en Dos Pasos* de Bitwarden.
2. Conservar la contraseña maestra de Bitwarden en la memoria (nunca almacenarla en el dispositivo).
3. El Duo se convierte en el segundo factor obligatorio en cada inicio de sesión.

Resultado de seguridad:

En una laptop o teléfono robado, un atacante no tiene ni la contraseña maestra ni el Duo físico. El acceso queda completamente bloqueado.

> Warning
>
> Registrar una **llave FIDO2 de respaldo** (un segundo OnlyKey u otro dispositivo FIDO2) para Bitwarden y guardarla de forma segura sin conexión. Sin esto, perder el Duo te bloqueará permanentemente de Bitwarden.

KeePassXC

KeePassXC admite el **desafío-respuesta HMAC-SHA1**, que el OnlyKey Duo proporciona en modo compatible con YubiKey.

Pasos de configuración:

1. En la aplicación de configuración del OnlyKey, asignar una ranura como **desafío-respuesta HMAC-SHA1**.
2. En KeePassXC, habilitar *Desafío-Respuesta* como factor de protección adicional de la base de datos (en *Base de datos > Seguridad de la base de datos*).
3. Abrir la base de datos requerirá tanto la contraseña maestra como una pulsación física en el Duo.

Resultado de seguridad:

Una laptop robada que contenga el archivo de base de datos de KeePassXC no puede abrirse sin la presencia del Duo.

> Warning
>
> El secreto de desafío-respuesta HMAC-SHA1 está almacenado en el Duo y se incluye en la **copia de seguridad cifrada del OnlyKey**. Si se pierde el Duo y no existe una copia de seguridad, la base de datos de KeePassXC quedará permanentemente inaccesible. Mantené siempre una copia de seguridad actualizada.

Acceso SSH a GitHub

Hay dos opciones disponibles. La opción B es la recomendada para GitHub específicamente.

Opción A — Almacenar la llave privada SSH en el OnlyKey

- Cargar una llave privada Ed25519 o NIST P-256 en una de las **ranuras de llave ECC** del OnlyKey.
- La llave privada nunca existe en forma utilizable en el sistema de archivos de la laptop.
- Las operaciones SSH son realizadas por el OnlyKey; la llave privada no puede ser extraída.
- Configurar `~/.ssh/config` para usar `onlykey-agent` o la interfaz PKCS#11.

Opción B — Llave SSH residente FIDO2 (Recomendada)

- GitHub admite de manera nativa llaves SSH FIDO2 usando el tipo de llave `sk-ssh-ed25519`.
- Generar una llave SSH residente FIDO2 almacenada directamente en el Duo:

```
ssh-keygen -t ed25519-sk -O resident -C "github-onlykey"
```

- Subir la llave pública resultante a GitHub de la manera habitual.
- No se requiere gestión de llaves separada; el Duo almacena las credenciales.
- Se requiere presencia física (pulsación) para cada autenticación SSH.

Resultado de seguridad:

Una laptop robada no tiene ninguna llave privada utilizable para GitHub. La autenticación exige el Duo físico.

GPG / Cifrado de Correos Electrónicos

El OnlyKey Duo actúa como una **tarjeta inteligente OpenPGP**, almacenando las subllaves GPG para firma, cifrado y autenticación.

Pasos de configuración:

1. Generar una llave maestra GPG en una **máquina sin conexión a internet** (nunca en la laptop ni en el Duo).
2. Generar tres subllaves GPG a partir de la llave maestra:
    - **[S]** Subllave de firma
    - **[E]** Subllave de cifrado
    - **[A]** Subllave de autenticación
3. Cargar cada subllave en una **ranura de llave ECC** del OnlyKey Duo.
4. Exportar y subir la llave pública a un servidor de llaves o compartirla directamente.
5. Las operaciones GPG (firma, descifrado) requieren ahora que el Duo esté presente y sea pulsado.

> **Important**
>
> La **llave maestra de certificación GPG** debe permanecer en almacenamiento en frío (máquina sin conexión, copia de seguridad cifrada sin conexión o llave en papel impreso). **Nunca** debe

almacenarse en el Duo ni en un dispositivo conectado a internet. La llave maestra es necesaria para agregar subllaves, revocar llaves o extender la fecha de vencimiento — perderla significa perder el control de tu identidad GPG.

Resultado de seguridad:

El descifrado y la firma de correos electrónicos requieren la posesión física del Duo. Un dispositivo robado no puede suplantar la identidad del propietario ni descifrar el correo recibido.

Plan de Asignación de Ranuras (Perfil 1)

La siguiente tabla muestra una asignación de ranuras recomendada para el perfil principal:

Ranura	Uso
Ranura ECC 1	Llave privada SSH (GitHub) o llave SSH residente FIDO2
Ranura ECC 2	Subllave de cifrado GPG [E]
Ranura ECC 3	Subllave de firma GPG [S]
Ranura ECC 4	Subllave de autenticación GPG [A]
Ranura HMAC	Desafío-respuesta KeePassXC
FIDO2	Bitwarden + todos los demás sitios WebAuthn/FIDO2
Ranuras 1–3	OTP / contraseñas estáticas para cuentas adicionales si es necesario

El Perfil 2 puede reservarse para un conjunto de credenciales de negación plausible o dejarse vacío.

Análisis del Escenario de Robo de Dispositivo

Con esta configuración, las siguientes protecciones se aplican si una laptop o dispositivo móvil se pierde o es robado:

Bitwarden
: Bloqueado. El segundo factor FIDO2 requiere el Duo físico.

KeePassXC
: Bloqueado. La base de datos no puede abrirse sin pulsar el Duo.

GitHub SSH
: Bloqueado. La llave privada reside en el Duo; la copia en el sistema de archivos es inutilizable.

GPG / Correo electrónico
: Bloqueado. Las subllaves están en el Duo; el descifrado y la firma requieren pulsación física.

La superficie de ataque restante es el **PIN del OnlyKey Duo** en sí mismo. Mitigá este riesgo:

- Usando un PIN fuerte (6 o más dígitos).
- Habilitando la función **PIN de autodestrucción** para borrar el dispositivo tras un número configurado de intentos incorrectos.
- Nunca compartir ni registrar el PIN junto al dispositivo.

Estrategia de Respaldo Crítica

> !DANGER!
>
> Omitir los respaldos es el error más común y más catastrófico. Perder el Duo sin una copia de seguridad puede bloquearte permanentemente fuera de todos los servicios y datos protegidos.

Los siguientes respaldos deben mantenerse:

1. **Copia de seguridad cifrada del OnlyKey** Exportar una copia de seguridad cifrada completa del Duo usando la aplicación OnlyKey. Guardarla en un lugar seguro sin conexión (por ejemplo, una USB cifrada en una caja fuerte física, o un código QR impreso guardado de forma segura). Esto preserva los secretos HMAC, las ranuras de llaves ECC y la configuración OTP.
2. **Segunda llave FIDO2 para Bitwarden (y otros sitios WebAuthn)** Registrar una llave de hardware FIDO2 de respaldo para cada servicio protegido por FIDO2. Guardar la llave de respaldo separada del Duo principal.
3. **Copia de seguridad de la base de datos KeePassXC** Mantener una copia almacenada por separado de la base de datos, accesible solo con la contraseña maestra (sin desafío-respuesta) para recuperación de emergencia. Guardar esta copia en un lugar que esté bien protegido.
4. **Almacenamiento en frío de la llave maestra GPG** La llave maestra de certificación GPG debe almacenarse en una máquina sin conexión a internet o en medios cifrados sin conexión. Sin ella, no es posible emitir certificados de revocación ni extender la fecha de vencimiento de las subllaves.
5. **Documentación de la asignación de ranuras** Documentar las asignaciones de ranuras del Duo y guardar el registro dentro de tu bóveda de Bitwarden (una vez configurada) u otro lugar seguro.

Orden de Configuración Recomendado

Seguí esta secuencia para garantizar siempre acceso funcional a las credenciales antes de agregar capas adicionales de protección:

1. **Definir el PIN del OnlyKey Duo y la frase de contraseña de respaldo** primero. Sin esto, nada más puede recuperarse.
2. **Configurar la ranura HMAC** y establecer el desafío-respuesta de KeePassXC. Verificar que la base de datos se abra correctamente, luego exportar una copia de seguridad del OnlyKey.
3. **Generar las llaves GPG** en una máquina sin conexión. Cargar las subllaves en las ranuras ECC del Duo. Verificar que la firma y el descifrado funcionen mediante GPG. Almacenar la llave maestra sin conexión.
4. **Generar una llave SSH FIDO2** para GitHub (`ssh-keygen -t ed25519-sk`). Agregar la llave pública a tu cuenta de GitHub. Probar el acceso SSH.
5. **Registrar el Duo en Bitwarden** como llave FIDO2. También registrar una llave FIDO2 de respaldo en la misma sesión. Probar el inicio de sesión en un segundo dispositivo.
6. **Exportar y guardar una copia de seguridad cifrada final del OnlyKey** ahora que todas las ranuras están completamente configuradas.

Este orden garantiza que el acceso a las contraseñas esté asegurado antes de comenzar el endurecimiento de SSH y GPG, minimizando el riesgo de bloqueo durante la configuración.

Resumen

El OnlyKey Duo está bien adaptado a este caso de uso. Al combinar FIDO2 para Bitwarden, desafío-respuesta HMAC para KeePassXC, ranuras de llaves ECC para subllaves GPG, y ya sea llaves residentes FIDO2 o ranuras ECC para SSH, todos los secretos principales se eliminan de los sistemas de archivos de la laptop y el teléfono. La posesión física del Duo (y el conocimiento de su PIN) se convierte en el único factor de control para el acceso a todo el ecosistema de credenciales.

El punto más débil de cualquier estrategia de llave de hardware es el procedimiento de respaldo. Invertí tiempo en establecer y probar los respaldos antes de completar la configuración.

Documento generado en abril de 2026. El firmware y el software del OnlyKey Duo pueden evolucionar; verificá el número actual de ranuras y las funcionalidades en la documentación oficial del OnlyKey en https://docs.onlykey.io