OnlyKey Duo Configuration Strategy

Table of Contents

Overview

This document describes a comprehensive security strategy for using an OnlyKey Duo hardware security key to protect two password managers (Bitwarden and KeePassXC), SSH access to GitHub, and GPG-based email encryption. The goal is to ensure that a lost or stolen laptop or mobile device remains secure, provided the OnlyKey Duo itself is not compromised.

Understanding the OnlyKey Duo's Capacity

The OnlyKey Duo provides the following capability:

- **2 profiles**: Profile 1 (primary) and Profile 2 (plausible deniability)
- **12 slots per profile**: 6 slots per page, 2 pages
- **ECC/RSA key slots**: For SSH private keys and GPG subkeys
- **FIDO2/WebAuthn support**: Hardware-backed, supports unlimited site registrations
- **HMAC-SHA1 challenge-response**: Compatible with KeePassXC and similar tools
- **Self-destruct PIN**: Wipes the device after a configurable number of wrong PIN attempts

---

Requirements Mapped to OnlyKey Features

Bitwarden

Bitwarden supports **FIDO2/WebAuthn** natively, making this the cleanest integration.

Configuration steps:

1. Register the OnlyKey Duo as a FIDO2 security key in Bitwarden's *Two-Step Login* settings.
2. Retain the Bitwarden master password in memory (never store it on the device).
3. The Duo becomes the required second factor on every login.

Security outcome:

On a stolen laptop or phone, an attacker has neither the master password nor the physical Duo. Access is fully blocked.

> Warning
>
> Register a **backup FIDO2 key** (a second OnlyKey or another FIDO2 device) for Bitwarden and store it securely offline. Without this, losing the Duo locks you out of Bitwarden permanently.

KeePassXC

KeePassXC supports **HMAC-SHA1 challenge-response**, which the OnlyKey Duo provides in YubiKey-compatible mode.

Configuration steps:

1. In the OnlyKey configuration app, assign one slot as **HMAC-SHA1 challenge-response**.
2. In KeePassXC, enable *Challenge-Response* as an additional database protection factor (under *Database* > *Database Security*).
3. Opening the database will now require both the master password and a physical tap on the Duo.

Security outcome:

A stolen laptop with the KeePassXC database file cannot be opened without the Duo present.

> Warning
>
> The HMAC-SHA1 challenge-response secret is stored on the Duo and is included in the **encrypted OnlyKey backup**. If the Duo is lost and no backup exists, the KeePassXC database becomes permanently inaccessible. Always maintain an up-to-date backup.

SSH Access to GitHub

Two options are available. Option B is recommended for GitHub specifically.

Option A — Store SSH Private Key on the OnlyKey

- Load an Ed25519 or NIST P-256 private key into one of the OnlyKey's **ECC key slots**.
- The private key never exists in usable form on the laptop's filesystem.
- SSH operations are performed by the OnlyKey; the private key cannot be extracted.
- Configure `~/.ssh/config` to use the `onlykey-agent` or the PKCS#11 interface.

Option B — FIDO2 SSH Resident Key (Recommended)

- GitHub natively supports FIDO2 SSH keys using the `sk-ssh-ed25519` key type.
- Generate a resident FIDO2 SSH key stored directly on the Duo:

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

- Upload the resulting public key to GitHub as usual.
- No separate key management is required; the Duo holds the credential.
- Physical presence (tap) is required for every SSH authentication.

Security outcome:

A stolen laptop has no usable private key for GitHub. Authentication requires the physical Duo.

GPG / Email Encryption

The OnlyKey Duo acts as an **OpenPGP smart card**, holding GPG subkeys for signing, encryption, and authentication.

Configuration steps:

1. Generate a GPG master key on an **air-gapped machine** (never on the laptop or the Duo).
2. Generate three GPG subkeys from the master key:
    - **[S]** Signing subkey
    - **[E]** Encryption subkey
    - **[A]** Authentication subkey
3. Load each subkey into an **ECC key slot** on the OnlyKey Duo.
4. Export and upload the public key to a keyserver or share directly.
5. GPG operations (signing, decrypting) now require the Duo to be present and tapped.

> **Important**
>
> The GPG **master certification key** must remain in cold storage (air-gapped machine, encrypted offline backup, or printed paper key). It should **never** be stored on the Duo or on an internet-connected device. The master key is required to add subkeys, revoke keys, or extend expiry — losing it means losing control of your GPG identity.

Security outcome:

Email decryption and signing require physical possession of the Duo. A stolen device cannot impersonate the owner or decrypt received mail.

Slot Allocation Plan (Profile 1)

The following table shows a recommended slot assignment for the primary profile:

Slot	Purpose
ECC Key Slot 1	SSH private key (GitHub) or FIDO2 SSH resident key
ECC Key Slot 2	GPG encryption subkey [E]
ECC Key Slot 3	GPG signing subkey [S]
ECC Key Slot 4	GPG authentication subkey [A]
HMAC Slot	KeePassXC challenge-response
FIDO2	Bitwarden + all other WebAuthn/FIDO2 sites
Slots 1–3	OTP / static passwords for additional accounts if needed

Profile 2 can be reserved for a plausible-deniability set of credentials or left empty.

Device Theft Scenario Analysis

With this configuration, the following protections apply if a laptop or mobile device is lost or stolen:

Bitwarden
: Blocked. FIDO2 second factor requires physical Duo.

KeePassXC
: Blocked. Database cannot be opened without Duo tap.

GitHub SSH
: Blocked. Private key lives on the Duo; filesystem copy is unusable.

GPG / Email
: Blocked. Subkeys on Duo; decryption and signing require physical tap.

The remaining attack surface is the **OnlyKey Duo PIN** itself. Mitigate this risk by:

- Using a strong PIN (6 or more digits).
- Enabling the **self-destruct PIN** feature to wipe the device after a configured number of wrong attempts.
- Never sharing or recording the PIN alongside the device.

Critical Backup Strategy

> !DANGER!
>
> Skipping backups is the most common and most catastrophic mistake. Losing the Duo without a backup can permanently lock you out of all protected services and data.

The following backups must be maintained:

1. **OnlyKey encrypted backup** Export a full encrypted backup of the Duo using the OnlyKey app. Store this in a secure offline location (e.g., encrypted USB in a physical safe, or a printed QR code stored securely). This preserves HMAC secrets, ECC key slots, and OTP configuration.
2. **Second FIDO2 key for Bitwarden (and other WebAuthn sites)** Register a backup FIDO2 hardware key for every FIDO2-protected service. Store the backup key separately from the primary Duo.
3. **KeePassXC database backup** Maintain a separately stored copy of the database accessible with the master password alone (without challenge-response) for emergency recovery. Keep this copy in a location that is itself well protected.
4. **GPG master key cold storage** The GPG master certification key must be stored on an air-gapped machine or encrypted offline media. Without it, you cannot issue revocation certificates or extend subkey expiry.
5. **Slot assignment documentation** Document your Duo slot assignments and store the record inside your Bitwarden vault (once set up) or another secure location.

Recommended Setup Order

Follow this sequence to ensure you always have working access to credentials before adding additional layers of protection:

1. **Set OnlyKey Duo PIN and backup passphrase** first. Without this, nothing else is recoverable.
2. **Configure the HMAC slot** and set up KeePassXC challenge-response. Verify the database opens correctly, then export an OnlyKey backup.
3. **Generate GPG keys** on an air-gapped machine. Load subkeys into ECC slots on the Duo. Verify signing and decryption work via GPG. Store the master key offline.
4. **Generate a FIDO2 SSH key** for GitHub (`ssh-keygen -t ed25519-sk`). Add the public key to your GitHub account. Test SSH access.
5. **Register the Duo with Bitwarden** as a FIDO2 key. Also register a backup FIDO2 key in the same session. Test login on a second device.
6. **Export and store a final OnlyKey encrypted backup** now that all slots are fully configured.

This order ensures that password access is secured before SSH and GPG hardening begins, minimising the risk of a lockout during setup.

Summary

The OnlyKey Duo is well-suited to this use case. By combining FIDO2 for Bitwarden, HMAC challenge-response for KeePassXC, ECC key slots for GPG subkeys, and either FIDO2 resident keys or ECC slots for SSH, all major secrets are removed from the laptop and phone filesystems. Physical possession of the Duo (and knowledge of its PIN) becomes the single controlling factor for access to the entire credential ecosystem.

The weakest point of any hardware key strategy is the backup procedure. Invest time in establishing and testing backups before completing the configuration.

Document generated April 2026. OnlyKey Duo firmware and software capabilities may evolve; verify current slot counts and features against the official OnlyKey documentation at https://docs.onlykey.io