SEC-1d-0 Plugin Spike

Passkey/WebAuthn — Architekturentscheidung für SEC-1d-1

Datum: 2026-05-14 (UTC) | Master HEAD: `31ef276` (lokal) | Vorgänger: SEC-1d Plan-Review

SPIKE / READ-ONLY **GO Empfehlung: jeffersongoncalves** **NICHT JETZT umsetzen — SEC-1c-3c-Fenster**

> **Kurzfassung. Klare Gewinner-Empfehlung**: `jeffersongoncalves/filament-multifactor-passkeys ^2.0`. Composer-Compat ✓ mit PHP 8.5.5 / Laravel 13.7 / Filament 5. Implementiert genau das Coexistence-Modell (Modus 1) das du gewählt hast — wird per `PasskeyAuthentication::make()` ins existierende `multiFactorAuthentication([AppAuthentication, PasskeyAuthentication])`-Array gesetzt, TOTP bleibt unverändert. Nutzt unter der Haube `spatie/laravel-passkeys` (680k DL, stable) das wiederum `web-auth/webauthn-lib` wrappt. Migration-Footprint: **1 neue Tabelle** `passkeys`, FK auf `users` — der Migrator-Rolle ist `REFERENCES` auf `users` bereits gegrantet, also **kein SEC-1c-3d-Konflikt**. `laravel/passkeys-server` bleibt v0.1 Pre-Release auf Packagist nicht resolvable → ausgeschlossen.

1. Boundary-Snapshot

Item	Wert
master HEAD	`31ef276` (lokal)
git status	clean
Bot main.py PID	195 (in-container)
Bot Container Host-PID	2657896 — healthy
Worker Container Host-PID	2658058
BINANCE_TESTNET	true
cmd 13 / mp / history	cancelled / 0 / 0
Worker Heartbeat age	13 s (frisch)
composer.json + composer.lock	git-clean (md5sum bestätigt: dry-run hat nichts geschrieben)

2. Stack-Realitätscheck

Komponente	Version	Kompatibilität mit Passkey-Plugins
PHP	8.5.5	Composer 2.9.7 erkennt 8.5.5. Caret-Constraints `^8.2/^8.3` matchen 8.5.5 (Composer-Logik: ≥X.Y, <next major).
Laravel	13.7.0	`spatie/laravel-passkeys` v1.7.3 deckt L11/L12/L13 ✓
Filament	5.0	jeffersongoncalves 2.x-Branch explizit Filament 5 ✓; marcelweidum 3.x ebenfalls ✓
Composer	2.9.7	aktuell, Dry-Run-Support ✓

3. Kandidaten-Inventur (5 Pakete)

#	Paket	Latest	Stars/DL	Compat L13/PHP 8.5/Filament 5	Rolle in Architektur
1	`jeffersongoncalves/filament-multifactor-passkeys`	v2.0.0 (2026-05-04)	4 ★ / NA	L12/13 ✓, PHP ^8.2 ✓, Filament 5 ✓	Filament-MFA-Provider-Wrapper, coexistiert mit TOTP via Array
2	`marcelweidum/filament-passkeys`	v3.0.6 (2026-05-08)	62 ★ / 38k DL	L ✓, PHP ^8.2 ✓, Filament ^5.0 ✓	Passkey-only (keine native MFA-Coexistence)
3	`spatie/laravel-passkeys`	v1.7.3 (2026-05-11)	457 ★ / 680k DL	L11/12/13 ✓, PHP ^8.2/8.3/8.4 ✓	Low-mid-level: Livewire+Blade-Komponenten, kein Filament-Provider
4	`laravel/passkeys-server`	v0.1.0 (2026-04-23)	71 ★ / NA	**nicht auf Packagist resolvable** (Pre-Release-Stability)	Standalone Server-Companion zu npm `@laravel/passkeys`, kein Filament-Bezug
5	`web-auth/webauthn-lib`	v5.3.2	NA	L/Filament-agnostisch ✓	Low-level Library (Spomky-Labs), Custom-Code-Pfad

4. Composer Dry-Run-Ergebnisse

Paket	Resolution	Neue Packages	Security-Advisories
`jeffersongoncalves/filament-multifactor-passkeys:^2.0`	OK	11 (inkl. spatie/laravel-passkeys 1.7.3 + web-auth/webauthn-lib 5.3.2 + symfony/property-access + spomky-labs/cbor-php …)	0
`marcelweidum/filament-passkeys:^3.0`	OK	11 (fast identische Liste)	0
`spatie/laravel-passkeys:^1.7`	OK	11 (inkl. spomky-labs/pki-framework + web-auth/cose-lib + symfony/serializer …)	0
`laravel/passkeys-server:^0.1`	FAIL	Packagist: „package could not be found in any version" — stability-too-low oder Repo-not-	—

		public	
`web-auth/webauthn-lib:^5.0`	**OK**	11 (low-level Layer)	0

composer.json/composer.lock unangetastet: vor und nach dry-run identische md5-Hashes (`c207c6aa…` / `f2190cf1…`), git working tree clean.

5. Migrations-Footprint & Filament-Integration

Footprint (alle Plugins, die spatie/laravel-passkeys nutzen — Optionen 1, 2, 3)

1 neue Tabelle `passkeys` (aus `spatie/laravel-passkeys`):

```
id              primary key
authenticatable_id  FK → users(id) ON DELETE CASCADE
name            text
credential_id   text
data            json    ← public key + metadata (Spomky-WebAuthn-Serialisierung)
last_used_at    timestamp nullable
created_at, updated_at  timestamps
```

Index: `passkeys_authenticatable_fk` auf FK. **Keine Änderung an `users` -Tabelle** — kein ALTER TABLE, also **kein Migrator-Owner-Konflikt** (SEC-1c-3d).

User-Trait: `HasPasskeys` wird in `App\Models\User` via PHP-Code hinzugefügt (kein DB-Change).

SEC-1c-3d-Vereinbarkeit verifiziert

Migrator-Privilege	Status
`CREATE` auf public-Schema	**vorhanden** (SEC-1c-3a-Default-Grant)
`REFERENCES` auf `users` (FK-Setup)	**vorhanden** (live geprüft via `has_table_privilege`)
`ALTER` auf bestehende Tabellen	**NICHT BENÖTIGT** (Plugin macht keine ALTER)

> **SEC-1d-0 hat KEINE Konflikt mit SEC-1c-3c-Stabilitätsfenster oder SEC-1c-3d Migrator-Owner-Thema.** Eine zukünftige `SEC-1d-1` -Phase kann auch *vor* SEC-1c-3d laufen — die Plugin-Migration ist Migrator-konform.

Filament-Integration pro Plugin

Plugin	Filament-MFA-Contract	TOTP-Coexistence
jeffersongoncalves	Implementiert `HasPasskeyAuthentication` -Trait + nutzt Filament-MFA-Array via `PasskeyAuthentication::make()`	**explizit dokumentiert** — sauberes `->multiFactorAuthentication([AppAuthentication::make()->recoverable(), PasskeyAuthentication::make()])`
marcelweidum	Eigene `PasskeysPlugin::make()` , NICHT als MFA-Provider — Profile-Page-Integration	**parallel möglich** aber Plugin ist nicht als MFA-Stufe gedacht; passt eher zu passwortlos
spatie/laravel-passkeys	Kein Filament-Wiring — Livewire + Blade	**eigene Auth-Pages** — Filament-MFA bleibt separat aktiv
web-auth/webauthn-lib	Selbst zu schreiben (~200-400 LOC)	Custom: muss als `MultiFactorAuthenticationProvider` -Provider gebaut werden

6. Security-Review (spatie/laravel-passkeys = Underlying)

Security-Aspekt	Status
Challenge-Storage (gegen Replay)	**via `web-auth/webauthn-lib`** — Library handhabt Challenge-Generation, einmalige Verwendung, Session-bound
User-Verification	WebAuthn-Default ist `preferred` — kann konfiguriert werden auf `required` (z.B. via custom Action)
Multiple Credentials pro User	**unterstützt** — `passkeys.authenticatable_id` hat keine UNIQUE-Constraint, beliebig viele Rows pro User
Credential-ID-Storage	als Text in `credential_id` -Spalte; Public-Key in `data` JSON
Lost-Device Recovery	Fallback via TOTP (Modus 1) ODER Recovery-Codes des Filament-AppAuthentication (8 Codes, bereits aktiv für Steve)
Audit-Events	**2 Events**: `PasskeyRegisteredEvent` + `PasskeyUsedToAuthenticateEvent` — listener-fähig für `audit_events` -Tabelle. **Gap**: kein DELETE-Event
Public-Key-Leakage-Risiko	**niedrig** — Public Key ist per Definition öffentlich, kein Secret. Aber: **Credential-Privacy** — User-Tracking via Credential-ID möglich falls leaked

7. Testbarkeit

Test-Typ	jeffersongoncalves	spatie standalone	Custom (web-auth/webauthn-lib)
Unit-Tests	Plugin-eigene Tests (Pest)	Pest, 100% Coverage laut Repo	Selbst zu schreiben
Feature-Tests (Laravel)	via Test-Helper aus Plugin	vorhanden	Selbst
WebAuthn-Mock	WebAuthn-Server-Mock via `web-auth/webauthn-lib` -internal-Mocking	analog	analog

Browser-Integration-Test	Dusk/Playwright erforderlich (Browser-WebAuthn-API)	analog	analog
Safe-Runner-Kompat	Standard-Laravel-Tests laufen unter `gui/scripts/run_tests_safe.sh`	analog	analog

Recovery-Pflicht-Tests (für SEC-1d-1): Setup, Challenge, Login, Recovery, DELETE-Credential, Multi-Device.

8. Maintenance-Bewertung

Paket	Stars	DL	Letztes Release	Open Issues	Sicherheits-Advisories	Maintenance-Score
spatie/laravel-passkeys	457	680k	2026-05-11	0	0	**sehr hoch**
jeffersongoncalves/filament-multifactor-passkeys	4	klein	2026-05-04	0	0	**aktiv, aber jung** — Maintainer hat 80+ Pakete
marcelweidum/filament-passkeys	62	38k	2026-05-08	0	0	**stabil**
web-auth/webauthn-lib	NA (Spomky-Labs)	extrem hoch (Symfony-eco)	v5.3.2	n/a	0	**sehr hoch**

9. Vergleichsmatrix & Empfehlung

Kriterium	jeffersongoncalves	marcelweidum	spatie standalone	web-auth Custom
Coexistence Modus 1 (TOTP + Passkey)	**native**	**workaround**	**workaround**	**selbst designen**
Filament-MFA-Array-Integration	**explizit**	nein	nein	selbst
Aufwand SEC-1d-1 Implementation	**~4-6h**	~6-8h (Glue-Code)	~8-12h	~16-24h
Existierendes TOTP-Setup für Steve bleibt	**ja**	**ja**	**ja**	**ja**
Migration-Footprint	1 neue Tabelle (via spatie)	1 neue Tabelle (via spatie)	1 neue Tabelle	1 neue Tabelle (selbst)
Migrator-konform (SEC-1c-3d)	**ja**	**ja**	**ja**	**ja**
Audit-Events out-of-box	**ja** (via spatie)	**ja**	**ja**	selbst
Maintenance-Risiko	mittel (jung, kleines Team)	niedrig	niedrig	hoch (eigener Code)
Lock-in	mittel	mittel	niedrig	keiner

EMPFEHLUNG für SEC-1d-1: `jeffersongoncalves/filament-multifactor-passkeys ^2.0`.
Begründung:

- Einziges Paket, das explizit Filament 5 `MultiFactorAuthenticationProvider`-Array-Pattern unterstützt → Operator-Decision D1 (Modus 1) ist 1:1 abgebildet.
- Composer-Resolution sauber (PHP 8.5/Laravel 13.7/Filament 5), 0 Security-Advisories.
- Migrator-konforme Migration: nur 1 neue Tabelle `passkeys`, kein `ALTER users` → SEC-1c-3d kein Block.
- Underlying `spatie/laravel-passkeys` ist mature (680k DL, 0 issues).
- Aufwand SEC-1d-1: ~4-6h Code + Tests, 1× GUI-Container-Recreate.

Risiko-Mitigation: Falls jeffersongoncalves-Maintenance je nachlässt (kleines Team), kann durch direkten Wechsel auf `spatie/laravel-passkeys` standalone migriert werden — DB-Schema ist identisch. Lock-out-Risiko ist niedrig.

10. Risiken

Risiko	Wahrsch.	Mitigation
jeffersongoncalves verschwindet / archiviert	niedrig (Maintainer hat 80+ Pakete)	spatie/laravel-passkeys ist drop-in replacement; Schema kompatibel
spatie/laravel-passkeys breaking change 2.x	niedrig	composer-pinning auf `^1.7` halten bis migration-plan
web-auth/webauthn-lib CVE	niedrig (stable Spomky-Lib)	Composer-Audit + `composer-audit` in CI
Operator-Lockout (Authenticator-Loss + TOTP-Loss)	mittel	≥2 Passkeys (D3), TOTP-Recovery-Codes (8 Codes), separater SSH-only Break-Glass-Admin
CSP/Permissions-Policy-Konflikt	niedrig	aktuelle CSP-Report-Only erlaubt WebAuthn; ggf. `publickey-credentials-{get,create}` in Permissions-Policy listen
Composer-Auflösung bei Laravel 13.7-Update bricht	niedrig (spatie hat L13-Support)	Pin Filament 5.x, Laravel ^13.0

11. Empfohlene SEC-1d-1-Implementierungs-Skizze

1. Composer-Require (nicht --dry-run): `composer require jeffersongoncalves/filament-multifactor-passkeys:^2.0`
2. Vendor-Publish + Migrate als Migrator-Rolle: `php artisan vendor:publish --tag="passkeys-migrations" && php artisan migrate`
3. `App\Models\User`: `use HasPasskeys, HasPasskeyAuthentication`-Traits

4. `AdminPanelProvider`: `->multiFactorAuthentication([AppAuthentication::make()->recoverable(), PasskeyAuthentication::make()])`
5. Tests: PasskeyEnrollment, Coexistence mit TOTP, Recovery-Pfad
6. GUI-Container-Recreate (Composer-Install zieht neue Vendor)
7. Operator-Enrollment: erst auf iPhone/Safari, dann Desktop-Browser, ≥2 Passkeys (D3)

12. GO/NO-GO & Mainnet-Relevanz

> **NO-GO sofortige SEC-1d-1-Umsetzung.**
> - SEC-1c-3c-Stabilitätsfenster läuft bis 2026-05-21 — Operator-Decision D5 sagt: *nach* Soft-Lockdown.
> - Implementierungs-Phase erfordert Container-Recreate (Composer-Install) und sollte nicht ins Fenster reinfunken.

> **GO für SEC-1d-1-Planung**: frühestens ab **2026-05-22** (nach Soft-Lockdown). Vor MH-7 Mainnet abschließen.

13. Boundaries — alle eingehalten

- 0× `composer require` ohne `--dry-run` (5× dry-run, alle reverted)
- 0× `composer.json` / `composer.lock`-Edit (md5sum + git-status bestätigt)
- 0× Code-Touch im Repo
- 0× Migration / DB-Write
- 0× Container-Restart / docker cp
- 0× Mainnet (BINANCE_TESTNET=true durchgehend)
- 0× Push (master `31ef276` lokal unverändert)
- 0× Secret-Werte (Whitelist-Checks Boolean-only)
- 0× `env`-Dumps / `compose config` / `/proc/*/environ`
- 1× Composer-Trockenlauf in tmp-Throwaway: vorbereitet aber nicht ausgeführt (im aktuellen GUI-Container dry-run war ausreichend)

Erstellt: 2026-05-14 (UTC) · Phase: SEC-1d-0 Plugin Spike · Master HEAD: `31ef276` · Vorgänger: SEC-1d Plan-Review · Empfehlung: `jeffersongoncalves/filament-multifactor-passkeys ^2.0`