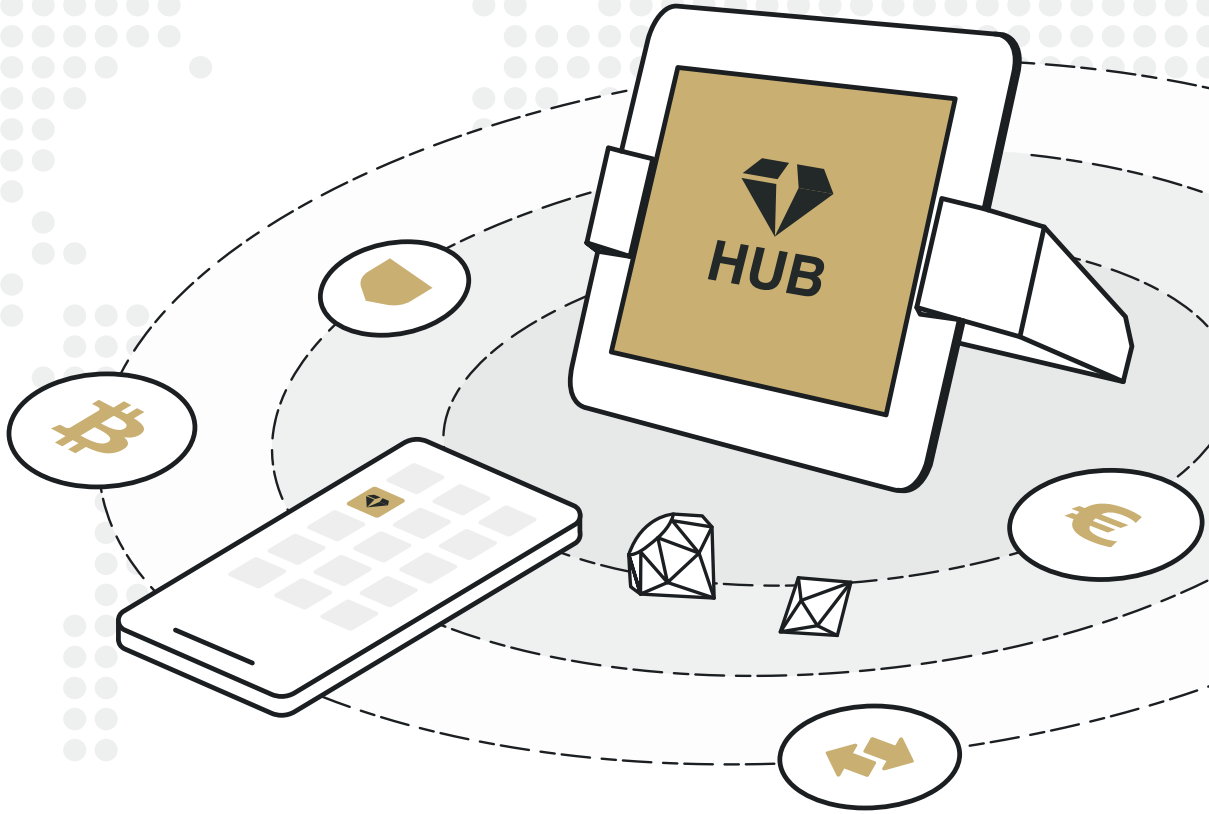
JUWELIS
Digital Systems

JUWELIS HUB Security

Die nächste Generation von
Krypto- und FIAT-Zahlungen



www.juwelis.digital

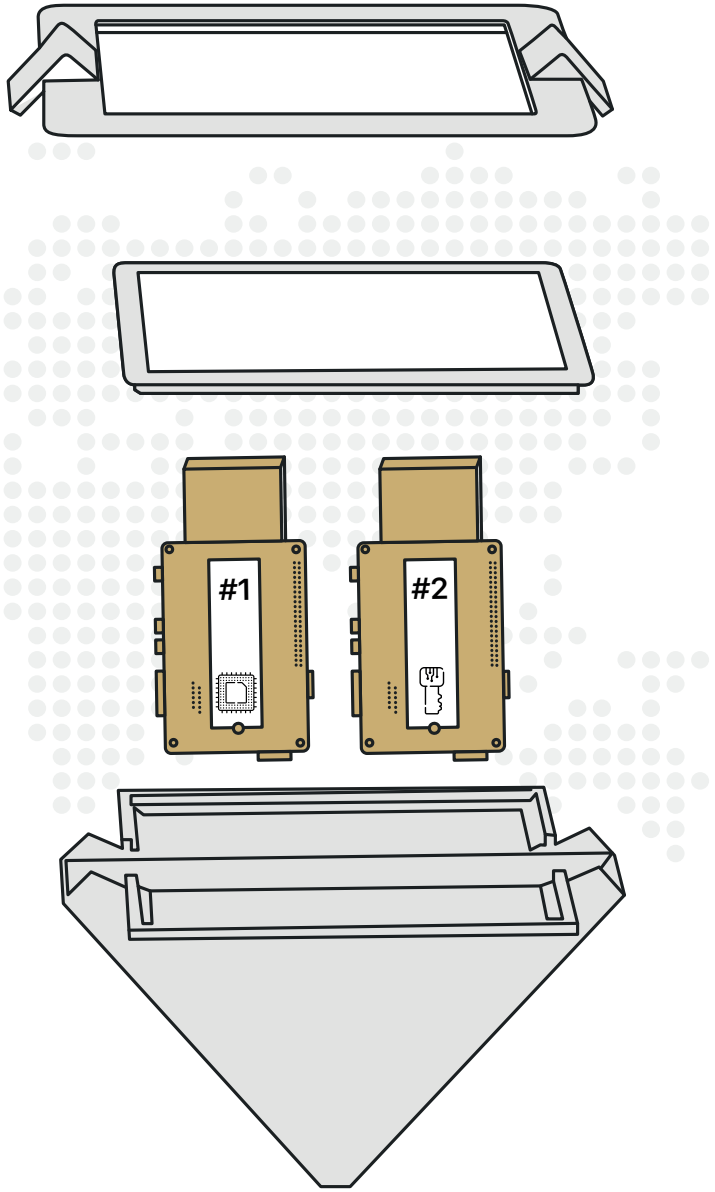
JUWELIS
HUB Security

Das Innenleben des JUWELIS Hubs beherbergt zwei technische Komponenten.

Komponente 1 ist die Hauptkomponente des JUWELIS Hubs. Es ist der Main Computer, auf dem die Software des Hubs integriert ist. Alles, was der User auf dem Display des Hubs sieht und bedient, läuft primär über den User Computer. Diese Hauptkomponente ermöglicht zudem die Internetverbindung, die für alle grundlegenden Funktionen des Hubs benötigt wird. Dazu gehören unter anderem:

- Zugang zur JUWELIS Exchange
- Minting-Funktion
- Handel und Transaktionen von Assets
- Verbindung zur Smartphone-Wallet
- Software Updates

Komponente 2 ist eine Sicherheitskomponente im JUWELIS Hub. Der sogenannte Key Guard ist ein kleinerer Computer, welcher den Private Key des Nutzers sicher verwahrt. Der Key Guard ist, durch ein Air Gap, physisch und logisch vom Main Computer getrennt und somit NICHT mit dem Internet verbunden.

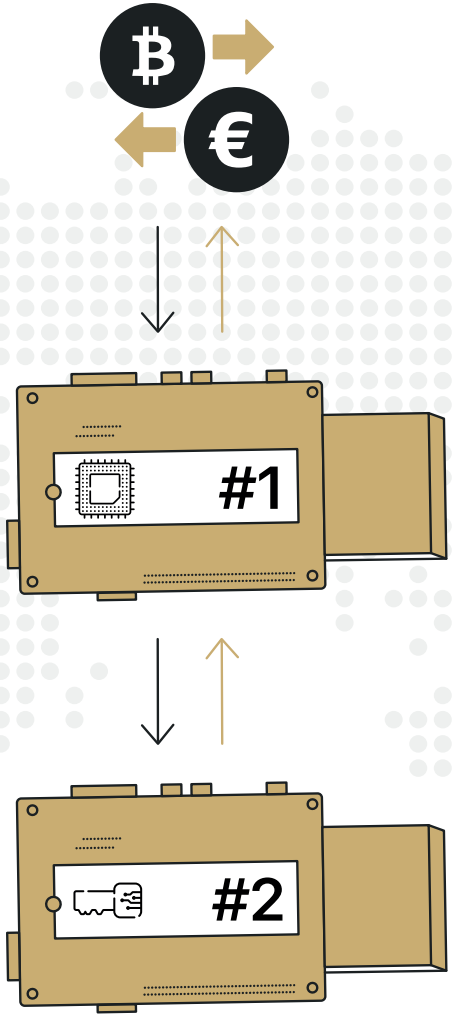


Transaktionsprozess

Krypto-Transaktionen werden am Main Computer des JUWELIS Hub in Auftrag gegeben. Sie benötigen dann die Unterschrift mittels Private Key, der sich auf dem Key Guard befindet. Ohne Unterschrift erfolgt keine Transaktion.

Damit eine Transaktion durchgeführt werden kann, müssen die beiden Komponenten also miteinander kommunizieren können. Dies ermöglicht eine eingeschränkte Schnittstelle zwischen den beiden Rechnern, welche nur vorprogrammierte Nutzerdaten austauschen kann. Jede Transaktion wird somit vom Hauptrechner zum Key Guard gesendet, um dort signiert zu werden.

Auf diese Weise bleibt der Private Key des Nutzers stets OFFLINE und kann den Key Guard nicht verlassen.

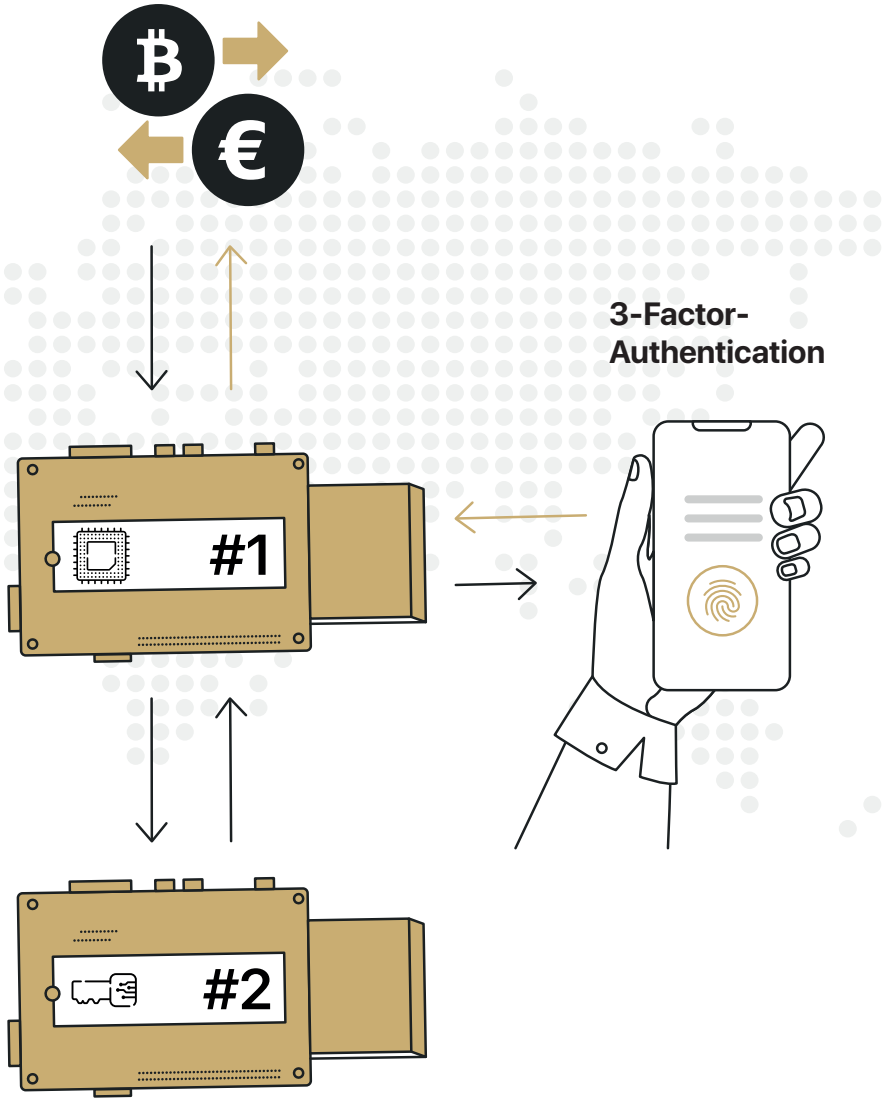


Drei-Faktor-Authentisierung

Nachdem eine Transaktion vom Main Computer in Auftrag gegeben und vom Key Guard signiert wurde, wird eine Benachrichtigung an das Smartphone des Nutzers gesendet.

Der Nutzer wird dadurch auf einem zusätzlichen Kanal über die Transaktion informiert. Damit die Zusatz-Authentisierung nicht manipuliert werden kann, sendet der Key Guard die Benachrichtigung durch einen technischen „Tunnel“ im Main Computer an das Smartphone. So wird sichergestellt, dass die Benachrichtigung nicht am Main Computer unterbrochen oder verfälscht wird.

Nur wenn die Transaktion am Smartphone bestätigt wird, kann diese ausgeführt werden. Mit diesem Authentisierungsprozess werden unbefugte Zugriffe auf dem Hub zwecklos gemacht.



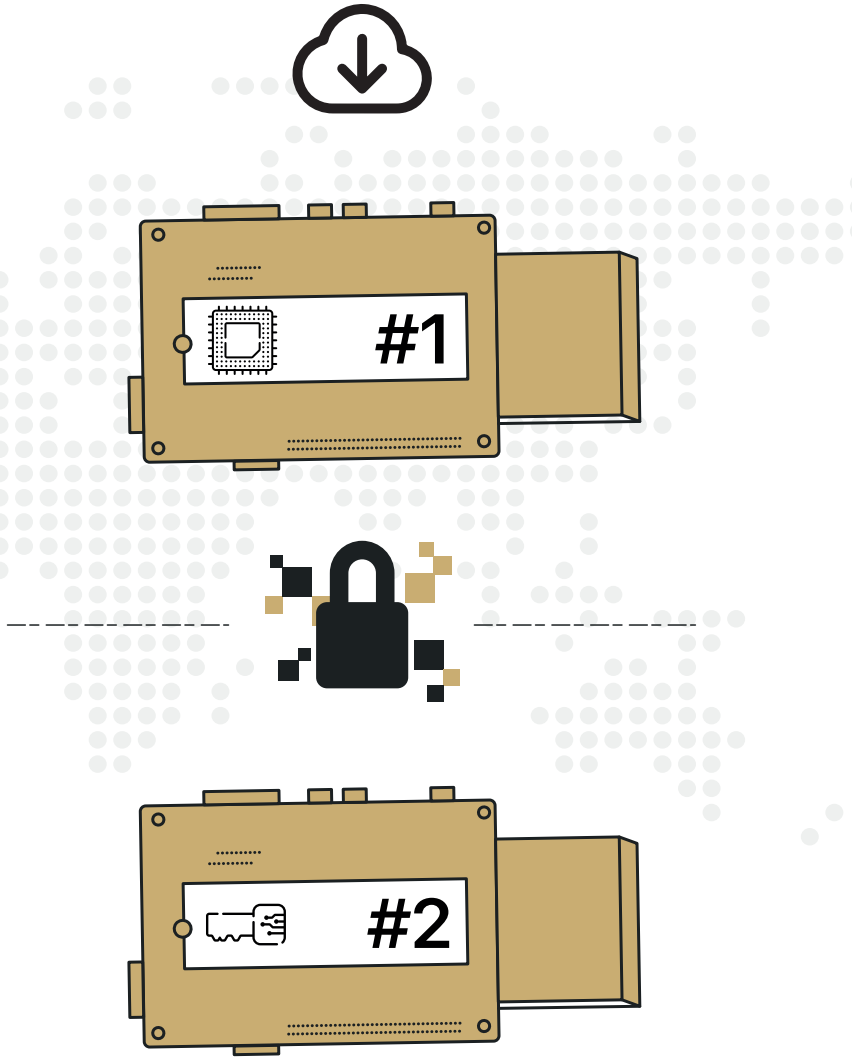
Sicherheit vor Schadsoftware

Die Internetverbindung einer Hardware-Wallet bietet die größte Angriffsfläche für Schadsoftware. Viele herkömmliche Wallets werden manuell über den eigenen PC oder Laptop upgedatet.

Dabei kann es passieren, dass Nutzer manipulative Schadsoftware von falschen Anbietern auf ihr Gerät laden, ohne dies zu bemerken. Potenzielle Cyberkriminelle können sich auf diese Weise Zugriff zum Private Key des jeweiligen Nutzers verschaffen.

Software Updates für den JUWELIS Hub sind nicht „Open Source“ und können nur von JUWELIS selbst programmiert und durchgeführt werden. Die Updates werden automatisch am Gerät durchgeführt und müssen nicht manuell aus dem Internet heruntergeladen werden. Somit besteht keine Gefahr, dass Schadsoftware von falschen Identitäten auf das Gerät gelangt.

Der Key Guard spielt auch hier eine große Rolle. Entscheidend ist nämlich, dass dieser vom Main Computer getrennt und somit technisch unerreichbar für Schadsoftware ist. Der Private Key bleibt unter allen Umständen sicher auf dem Key Guard.

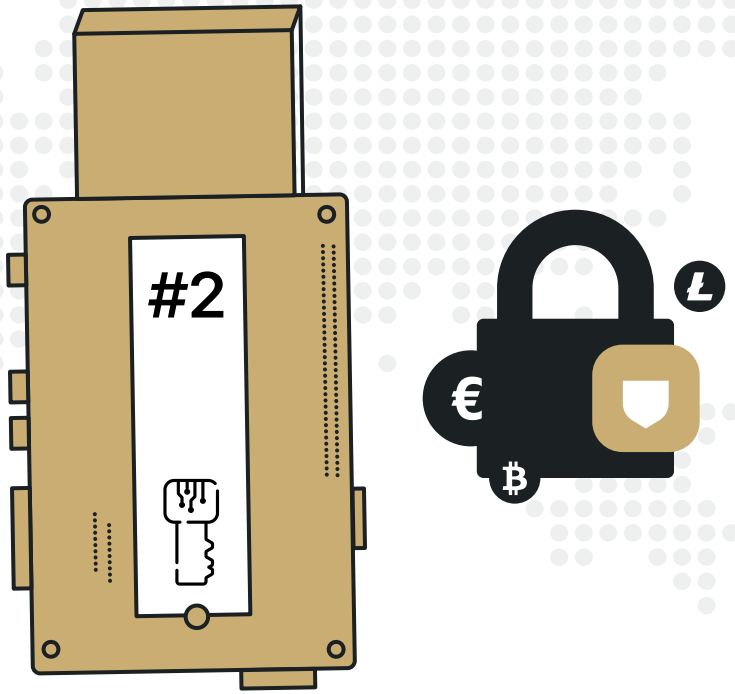


Fazit

Der JUWELIS Hub schafft mit seiner zusätzlich eingebauten Sicherheitskomponente einen noch nie dagewesenen Sicherheitsstandard für Krypto-Assets.

Die Isolierung des Key Guards vom Main Computer des Geräts schützt den Private Key vor unbefugten Zugriffen auf das Gerät, manuell oder via Malware. Der Main Computer agiert in diesem Sinne als die persönliche Bank des Nutzers.

Der Key Guard stellt praktisch einen technischen Hochsicherheitstresor dar, welcher den wertvollsten Besitz, den Private Key, verwahrt und niemals nach außen kommuniziert. Die Implementierung einer Zwei-Faktor-Authentisierung schützt die Assets des Besitzers zusätzlich vor unbefugten Zugriffen und macht diese obsolet.



Über die JUWELIS Digital Systems AG

Die JUWELIS Digital Systems AG hat es sich zur Aufgabe gemacht, einen einfachen, sicheren und vertrauenswürdigen Zugang zu digitalen Vermögenswerten zu schaffen. Oberstes Ziel ist es, Barrieren abzubauen, hohen Sicherheitsstandards zu entsprechen und dennoch Investitionen in digitale Anlagegüter so einfach wie möglich zu gestalten. Das Team setzt sich aus CEO Mag. Erwin Dokter, MBA, COO DDr. Michael Ofner, MBA, Steffen Bastian (Chairman of the Board), Evelyn Bernet (CAO) und Jan Bollmeyer (Chief Sales & Marketing Officer) zusammen.

Die JUWELIS-Gruppe investiert in Unternehmen, Organisationen und Fonds mit der Absicht, neben einer finanziellen Rendite, positive, messbare, soziale oder ökologische Auswirkungen zu erzielen. Die JUWELIS Digital Systems AG wurde im Jahr 2005 gegründet und 2019 neu strukturiert. Weitere Informationen finden Sie unter www.juwelis.digital

In Zusammenarbeit mit JUWELIS Asset Management GmbH, Firststrasse 6, 8835 Feusisberg, Schweiz, als Exklusiv-Vertrieb weltweit.

Feusisberg, den 02. Januar 2021