Jade - Virtual Secure Element

SatoshiSpritz Treviso
25 Marzo 2026

Tutto (o quasi) quello che c’è da sapere

Cos'è il Secure Element (SE)

In parole povere

Un chip a microcircuito resistente alle manomissioni (tamper-resistant) progettato per ospitare applicazioni sicure e conservare dati riservati (es: chiavi private)

Isolato

Il chip è fisicamente separato dal processore principale del dispositivo.

Se il processore principale viene compromesso da un malware, il SE rimane isolato

Crittografia Hardware

Genera e conserva le chiavi private internamente; le chiavi non "escono" mai dal chip in chiaro.

Resistenza agli attacchi fisici

È progettato per resistere a tecniche di hacking avanzate come

- **Side-channel attacks**: misurazione del consumo energetico per indovinare il PIN
- **Fault injection**: causare picchi di tensione per bypassare i controlli di sicurezza

Il paradosso del Secure Element

Una scatola nera

Nonostante siano sicuri, bisogna fidarsi dei produttori di SE

1. **Sorgente chiuso** (proprietario): I chip sono coperti da brevetti e segreti industriali. Se un ricercatore di sicurezza volesse verificare l'affidabilità di questi chip, non potrebbe farlo legalmente o tecnicamente.

2. **Fiducia nel Produttore**: Devi fidarti che il produttore non abbia inserito "backdoor".

Il Virtual Secure Element (VSE)

Nessun SE fisico

La sicurezza del chip, senza il chip

1. **Concetto chiave**: Jade non utilizza un chip fisico proprietario per proteggere le chiavi, ma un protocollo crittografico che ne emula le funzioni.

2. **Obiettivo**: Ottenere la stessa resistenza agli attacchi fisici (come il fault injection) pur rimanendo un dispositivo 100% Open Source.

3. **Il segreto**: La chiave privata non è salvata “in chiaro” nella memoria flash del dispositivo, ma è criptata con una chiave AES-256 e richiede un fattore esterno per essere sbloccata.

Funzionamento

Per decriptare i dati sul Jade, il dispositivo deve comunicare con un server remoto (l'Oracolo) tramite un’app che vede passare dati cifrati senza possibilità di aprirli.

1. L’utente sblocca il Jade con il PIN (questo non lascia mai il dispositivo)
2. Il Jade utilizza il PIN per derivare una chiave temporanea che stabilisce un canale cifrato con l'oracolo.
3. L’oracolo, che conserva una parte della chiave di decrittazione, invia il “pezzo mancante” al Jade.
4. Il Jade può ora firmare con la sua chiave privata.

Perché blind (cieco)

L'oracolo **NON** conosce le chiavi, il saldo o il PIN; ma un segreto univoco che serve a decriptare i dati salvati sulla memoria flash del Jade.

L’oracolo è solo un “serratura crittografica” remota.

Protezione antifurto

Se un ladro tenta di indovinare il PIN sul dispositivo fisico, **dopo 3 tentativi errati** l'oracolo cancella la sua parte di chiave di decrittazione, rendendo i dati sul Jade permanentemente illeggibili.

Questo NON comporta la perdita dei fondi, perché può essere usata la frase mnemonica per ripristinare il wallet.

Chi è l'oracolo?

L’oracolo nei server Blockstream

Blockstream può conoscere il mio indirizzo IP?

- Di default l’app di Blockstream si connette ai server gestiti direttamente da loro.
- Blockstream può conoscere l’IP dal quale ci si connette, ma non sapere chi tu sia (all’oracolo non vengono passati PIN, chiavi pubbliche/private, transazioni, ecc.).
- Si può comunicare con l’oracolo esclusivamente tramite la rete Tor.
- Si può installare l’oracolo in un server personale e connettersi direttamente a lui.

Sitografia

- https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf
- https://help.blockstream.com/hc/en-us/articles/13745404122265-Why-doesn-t-Jade-have-a-secure-element
- https://help.blockstream.com/hc/en-us/articles/15884462476953-Jade-security-model-FAQs
- https://help.blockstream.com/hc/en-us/articles/12800132096793-Set-up-a-personal-blind-oracle