VLS

SILICON SALON 2

Validating Lightning Signer

https://vls.tech/

VLS

What is VLS?

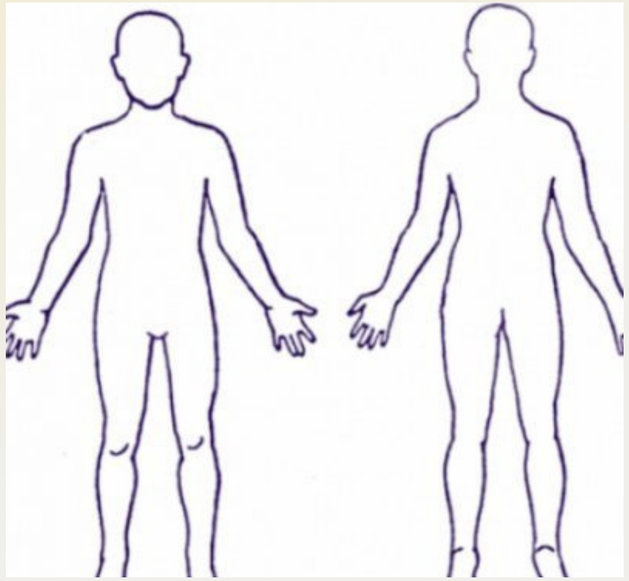
We're an open-source project, not a company.

Software can be run in a wide variety of use cases:

- in HSMs to secure enterprise scale lightning nodes
- ensure custody on an inexpensive consumer device

VLS

Our Team



DEVRANDOM
CO-FOUNDER

KEN SEDGWICK
CO-FOUNDER

JACK RONALDI
PRODUCT MANAGER

VLS

Unmet Need

Lightning nodes more challenging to secure than Bitcoin wallets:

- lightning funds must be "hot", with network connected private key
- large attack surface with lots of code and rapid feature development

Signing

More challenging for lightning. If remote signer is not carefully considering channel state, can be tricked into approving a transaction which steals funds from the node. See Blind Signing Considered Harmful for more ...

Policy Controls

VLS software enforces a comprehensive set of policy controls which protect the node's funds even if the node is entirely compromised.

Custody

VLS = secrets + state --> Protect lightning funds & Simple way to provide custody:

On an inexpensive consumer device it is sufficient to run VLS to maintain custody of the funds; the node itself can be run in the cloud as a Lightning Service Provider (LSP).

VLS

Embedded Device Requirements

Code

- VLS written in rust
- Core VLS code is built using no_std to facilitate running on embedded hardware.

Current Devices

- Wasm
- STM32F412,413
- ESP32-C3

Requirements

Base Requirements:

- Flash: 828.00 KiB (release build for STM32F413)
- RAM: Estimated 1KB per active channel
- NVStorage: Same as RAM, (excluding historical payment hashes)
- Capable of secp256k1 ECDSA and Schnorr

VLS can be used by integrating developers in a wide range of solutions:

- Tamper-proof hardware might be needed
- Boot and firmware update security might be needed
- Supply chain security might be needed
- A wide range of cost sensitivity is likely (consumer <-> enterprise)

VLS

Sponsors

Spiral

Blockstream

VLS

Connect With Us!

https://vls.tech/

Main Code Repository