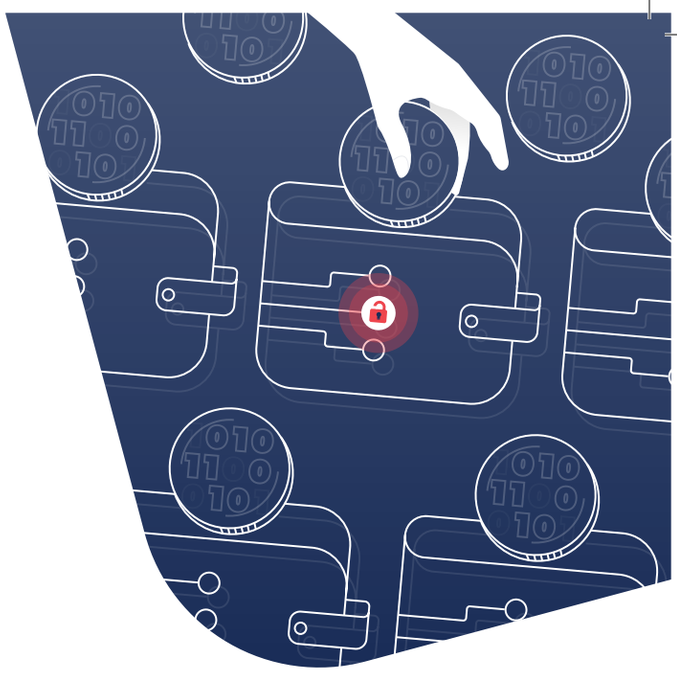
KUDELSKI IOT THINGS



Crypto Wallet
Security Assessment

The security of crypto wallets depends directly on the components used and the implementation of their hardware, software, and communication protocols. Independent, third-party validation and advice by security experts is therefore critical to ensure that crypto wallets are robust against relevant threats.

According to Allied Market Research, the global hardware wallet market size will grow at a compound annual growth rate of 24.0 % from 2021 to 2028.

Both custodial and non-custodial wallet solution developers need to secure their business and build user confidence in how their crypto assets are protected. We can give you that confidence.

MISSION

We help companies build secure, validated crypto wallet solutions

Our experience

We ensure the security and robustness of crypto wallet products based on more than 25 years of research, analysis, development, and operational excellence in security. We have a unique portfolio of services and solutions that give wallet manufacturers critical insights and proven technologies to help you meet quickly evolving regulatory and customer expectations around security.

How we work together

We work with you to assess your security threats and opportunities and help you create a crypto asset wallet - whether it's a physical one, an app, or a service - that protects keys for cryptocurrency transactions. We provide security designs, security assessments and pre-certification support for government schemes like CSPN.

APPROACH

3-Steps to a secure crypto wallet

THREAT ASSESSMENT

We identify attack vectors, followed by evaluation of threats based on likelihood, complexity, and business impact. This results in a comprehensive view of risks that should be protected against.

ARCHITECTURE REVIEW

We validate the presence and efficacy of security controls. We highlight any security risks associated with the architecture and with the implementation of critical features.

LAB EVALUATION

We provide concrete proposals for threat mitigation measures. We review the security of source code for software wallets and conduct pen tests on virtual ledgers and apps. We perform hardware attacks on secure elements for hardware cold Personal Security Devices.

METHOD

Main focus areas to secure crypto wallets

1. Security of identification and end-user authentication mechanisms (e.g. PIN, user interface).
2. Confidentiality, integrity and availability of the wallet, crypto assets and secret keys (e.g. plausible deniability, genuine PSD, deterministic RNG, seed generation, transaction signature).
3. Robustness of cryptographic primitives implementation (e.g. side-channel attacks due to bias in key handling algorithms).
4. Connectivity, communication patterns and protocols, offline constraints.
5. Security lifecycle (e.g. provisioning, secure software / firmware updates, decommissioning / revocation).

CORE INGREDIENTS

Building a secure solution, from design to operations

Threat Assessment & Risk Analysis, Architecture Review

System- and device-wide market-specific threat analysis

Security Target Definition, listing of critical security controls

Classification of assets, risk, probabilities of attack vectors and impact

Validation of efficiency of security controls

Cryptographic schemes review and implementation analysis

Identification of non-addressed security risks

Evaluation in our IoT Security Lab

Remediation analysis to validate the effectiveness of countermeasures and security controls

Non-invasive low-costs attacks, advanced electrical, EM and multi-locations laser fault injection, multi-temporal hardware attacks

State of the art side-channel attacks, DPA, using deep machine learning

Application penetration testing

Source code security review

Compliance validation against standards, such as BIP32, BIP39, BIP44

CLIENT REFERENCES

The following customers have depended on the Kudelski Group for our expertise in ensuring the security of their products and services.

LEDGER · crypto.com · INPUT | OUTPUT · tangem · SOLANA

 V1.2

www.kudelski-iot.com