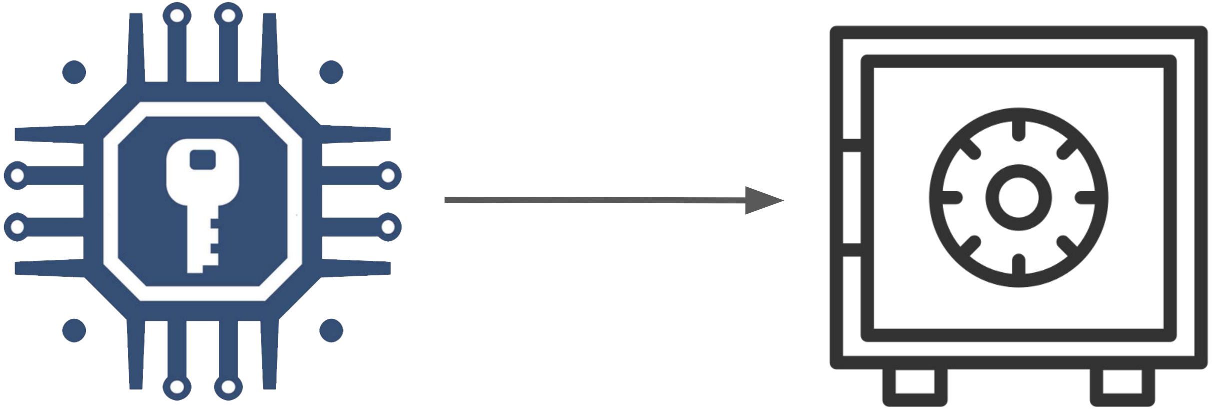
inblockio

2. PKC Wallet Security / Separation of concerns

Author :Tim Bansemer 17th November 2021 License CC BY 4.0

Separation of Concerns



Wallet

Data Vault

Key

Value

Wallet / Data-Vault

Wallet’s ONE JOB: KEEP KEYS SAFE!

- Should be stupid, simple, safe
- Operations:
  - Signing
  - De- / Encrypt
  - Publishing transactions to service (e.g. witness networks)
- Ability to choose “high level of assurance”
- Takes care of key recovery mechanisms

Data-Vault - KEEP DATA SAFE!

- Air Gapped on local machine
- All actions authorized though wallet
- General data governance (maximum flexibility -> we use mediawiki)
- Encrypt / Protect data
- Strong access control
  - Share / Publish private data
- Backup / Recovery

Authentication assurance levels (AAL)

How safe are the wallets to used?

Relevant in relationship to BSI report

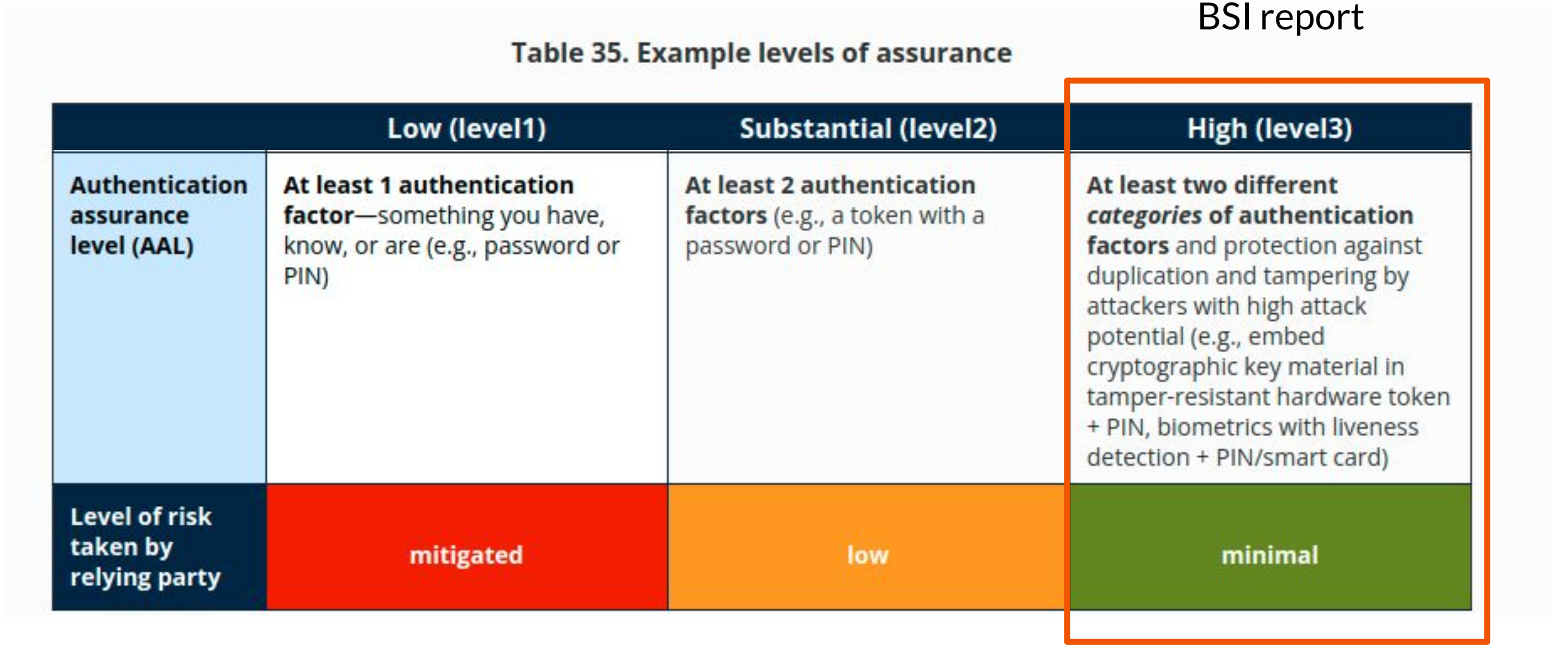


Table 35. Example levels of assurance

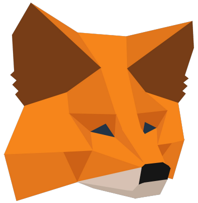
	Low (level1)	Substantial (level2)	High (level3)
Authentication assurance level (AAL)	**At least 1 authentication factor**—something you have, know, or are (e.g., password or PIN)	**At least 2 authentication factors** (e.g., a token with a password or PIN)	**At least two different *categories* of authentication factors** and protection against duplication and tampering by attackers with high attack potential (e.g., embed cryptographic key material in tamper-resistant hardware token + PIN, biometrics with liveness detection + PIN/smart card)
Level of risk taken by relying party	mitigated	low	minimal

Wallet Assurance - Level 1 -

The Metamask web-wallet alone has a low (level 1) level of assurance.

MetaMask is the most common browser blockchain wallet applications on the web and their developer teams strive for increased security to keep crypto-assets of their 10 Million+ Users safe.

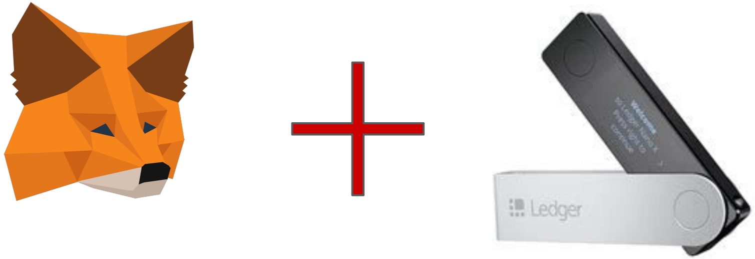
- MetaMask requires a password to be unlocked



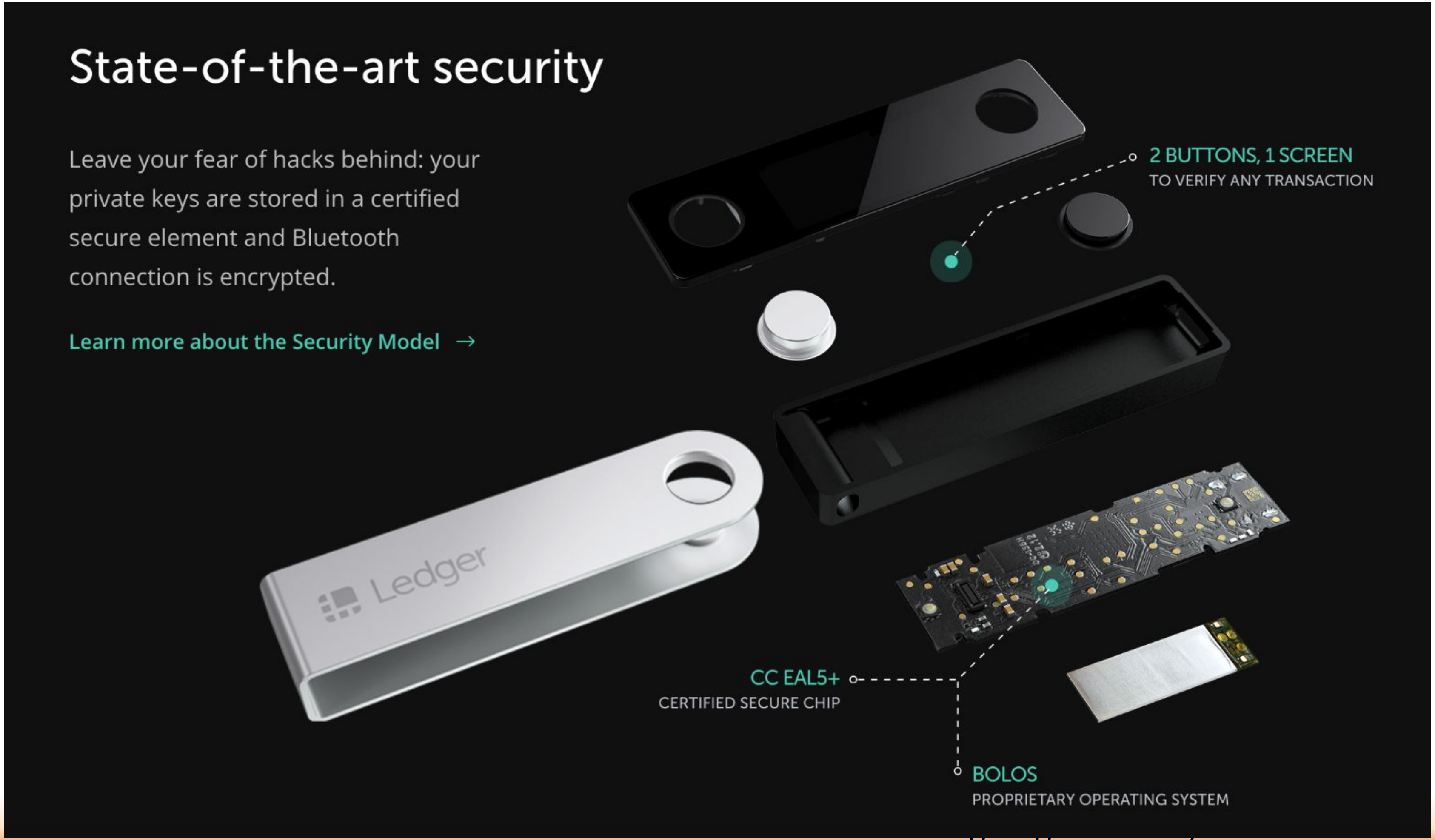
Wallet Assurance - Level 2 -

Metamask offers integration with Hardware-Wallets which raises the level of assurance by having at least 2 authentication factors:

- e.g. a token with a password or pin for min. level 2
- the hardware-tokens are build to be tamper proof (Ledger, Trezor)
    - E.g. Ledger X EAL5+ Certified (See Product-Page)



Product Page



State-of-the-art security

Leave your fear of hacks behind: your private keys are stored in a certified secure element and Bluetooth connection is encrypted.

Learn more about the Security Model →

Wallet Assurance - Level 3 -

Metamask with PW + Hardware-Wallet 8PIN + One-Time-Password (implemented by Data-Vault)

Wallet Assurance - Level 3 -

Other high security options

- Using multi-signature wallets
- Multi-signature wallets can be configured for extreme security
  - each security layer can be applied individually

Conclusion

1. We disagree with approaches taken by other wallet providers to **abuse wallets to store user-data**
2. We need to introduce **secure standard data vaults**
3. We showed how current technology gives us highest levels of assurance to manage data through data-vaults.