ENCRYPT IT!

For those who love encryption

Our story

Team Name: Encrypted

How we started: we want to enrcypt in web3.

“Can I use your eth pub address?”

3 days later...

State of Encryption in Ethereum

- EIP5630 and other failed efforts
- App level references
  - DM3, (Status / Waku) do encrypt
- Encryption handled in Application.
- Security not in the domain of the wallet.

Existing EIPs:

Signatures:
- EIP-191 and EIP 712

Authentication:
- SIWE-EIP 4361

Encryption/Decryption
- N/A

Problem: no standard, not easy.

What we found -> tl;dr

Level 1: Do NOT encrypt with the wallet keys.

Level 2: Use safe encryption keys (ECC with DH or RSA)

Level 3: securely? derive keys from BIP-44 m / / / ? 😱

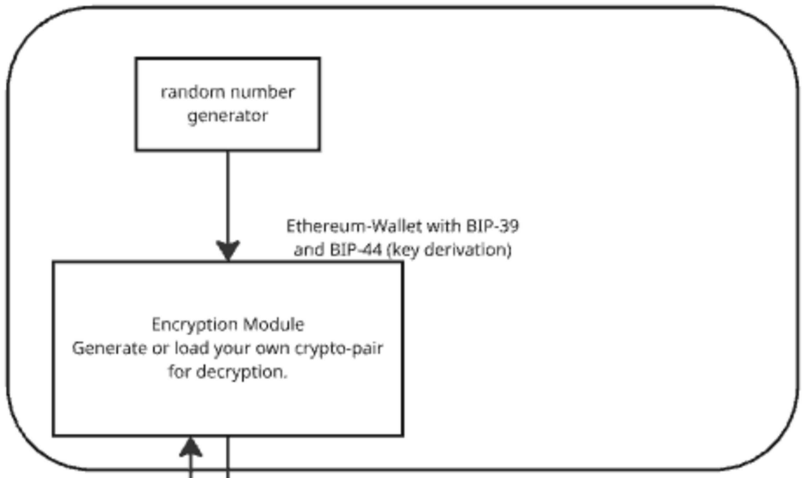
Level 4: Post-Quantum w ECC with AES256

Current impl: ECDH from OpenPGP based on RFC 9580.

PoC DEMO

Next steps?

- Build prod implementation
- Find support - join us!
- Propose standardization: EIP / WIP’
- Build trust
- Adoption through the ref impls



- Request symmetric key
- send pubkeys for encryption
- send cipher for decryption

Decryption API potential security vulnerability. But there are ways to do that.

Log-Term goal - having an embedded solution.

Public Keys
Are stored in a smart contract public key - wallet association.

Web-Browser

Existing EIPs:

Signatures:
- EIP-191 and EIP 712

Authentication:
- SIWE-EIP 4361

Encryption/Decryption
- N/A

DRAFT for Standard

Talk to us!

Formalize

Standardize