Guer

EXECUTIVE SUMMARY

WEB3 ENCRYPTION SUITE WITH CRYPTOGRAPHIC IDENTITY, DECENTRALIZED AUTHORITY AND ADVANCED SECURITY.

WHAT WE DO

Guer introduces the use of cryptographic identity (ETH keypairs) as the basis for three encryption protocols critical to the web:

- **Single Identity Encryption**, for secure remote data storage, from photos to NFTs
- **Shared Encryption**, for everything from end-to-end encrypted messaging to secured web connections
- **Proxy Re-encryption**, for licensing, digital rights management, and transerring digital assets

The protocols are completely decentralized, compatible with both emerging Web3 services and existing Web2 services, and completely open source.

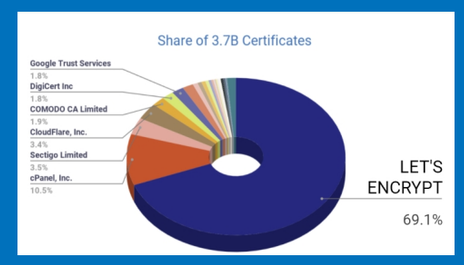
WHY WE DO IT

Web3 is decentralizing most web architecture, from web hosting to data storage to virtualization, but continues to use Web2 protocols for security. Internet security has not changed much since 1995, and is extremely centralized. This leaves our new infrastructure vulnerable to the same threats as Web2:

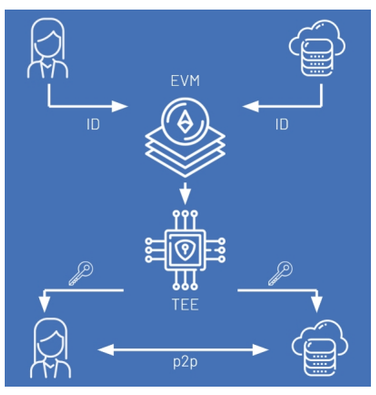
- **Internet Infrastructure Vulnerabilities**, such as Man-In-The-Middle Attacks
- **Device Vulnerabilites,** such as SIM swapping
- **3rd Party Vulnerabilities**, such as compromised cloud-based key management

Much of this infrastructure serves to add digital identity over location-based addressing, and in the process, increases attack surface.

94% of certificates from 10 orgs globally



HOW WE DO IT



Web3 is already built on cryptographic addressing - private/public keypairs. Our encryption suite uses this addressing as the root identity for encryption, security, and privacy.

- **Authority**: Identity and requests are handled by smart contracts and Web3 services such as ENS, eliminating DNS/Certificate Authority Risks
- **Key Generation and Distribution**: Securely generate keys, both locally and remotely (using networked TEEs), and safely distribute them across public networks such as blockchains
- **Encryption**: Our suite generates backwards compatible keys for encryption, allowing developers to use what's familiar, such as OpenSSL

The cryptography is tried and true: AES, ECDSA, and ECIES. Our suite focuses on modified libraries to take advantage of cryptographic identity.

FOR SOCIAL GOOD

Provides meaningful sovreignty over digital identity

Privacy-by-default, rather than Privacy-as-a-privelege

Enables useful alternatives to centralized services such as Big Tech

Digital business has an alternative to Surveillance Capitalism

Segments data, reducing quantity of high-value targets like databases

FOR THE COMMUNITY

100% Free & Open-source: Encourages adoption, fosters trust, and allows anyone to verify the code

DAO Foundation: Codebase, developer support, and governance managed by a community foundation

Sustainable Maintenance: Revenues from gas fees will go towards encouraging maintance and continued development of the suite

Backwards Compatibility: Build Web3 without breaking Web2

PROJECT STATUS

COMPLETED

- Encryption Suite, compiled in WASM
- Decentralized Authority 1.0 Smart Contracts deployed
- Use of Geth-compatible wallets
- APIs with IPFS, SKALE, Arweave, Eth Testnet
- Basic Public Docs + Demos

IN PROGRESS

- Ethers.JS/Web3.JS Wallet API
- Networked SGX Testing
- Decentralized Authority Contracts v2.0
- Additional APIs: OpenSSL, ENS, Opera/Brave
- Proxy Re-Encryption
- Revenue Collection