

zk Stealth

EthBerlin 2024

Sembrestels


May 26, 2024

Independent developer

1. Stealth Addresses and Zero Knowledge Proofs
2. zk Stealth



Stealth Addresses and Zero Knowledge Proofs



FluidKey is great!







zksteve.fkey.eth
A privacy-preserving fluidkey.com profile
[zksteve.fkey.id](#)



Addresses

 0x671...21FEb 



 0x3Dc...23De0 


 0x2Aa...BeCee 

 0x00f...9558e 

 0xc59...ee871 



Ownership → [View](#)



expiry **no expiry**  parent **fkey.eth** 







zksteve.fkey.eth
A privacy-preserving fluidkey.com profile
[zksteve.fkey.id](#)



Addresses

 0x4F6...5A656 



 0xddf...9321b 


 0xB37...dE846 

 0x75F...2f41d 

 0xF6f...c79e2 



Ownership → [View](#)



expiry **no expiry**  parent **fkey.eth** 







zksteve.fkey.eth
A privacy-preserving fluidkey.com profile
[zksteve.fkey.id](#)



Addresses

 0ecc5...D6555 


 0x04E...606E7 

 0x0E0...F6670 

 0xF97...D6177 



 0xa57...7C1E6 



Ownership → [View](#)







zksteve.fkey.eth
A privacy-preserving fluidkey.com profile
[zksteve.fkey.id](#)



Addresses

 0x9e2...3429C 

 0x78B...FE8e3 

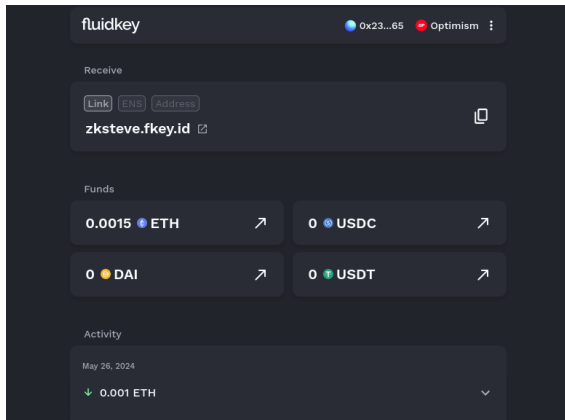
 0x382...2a9d3 

 0x342...230dC 

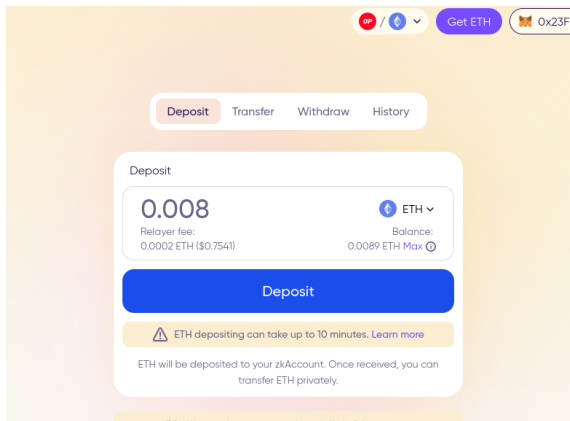
 0x482...7eB08 

Ownership → [View](#)

FluidKey is great!



zkBob is great too!



The screenshot shows the zkBob web interface for depositing ETH. At the top, there's a navigation bar with a red 'OP' button, a blue lightning bolt icon with a dropdown arrow, a purple 'Get ETH' button, and a wallet address '0x23F1...'. Below this is a tabbed menu with 'Deposit', 'Transfer', 'Withdraw', and 'History'. The 'Deposit' tab is active, showing a large input field with '0.008' and an 'ETH' dropdown. Below the input field, it shows 'Relayer fee: 0.0002 ETH (\$0.7541)' and 'Balance: 0.0089 ETH Max'. A large blue 'Deposit' button is centered below the input field. At the bottom, a yellow warning box states: '⚠ ETH depositing can take up to 10 minutes. [Learn more](#)'. Below the warning, a note says: 'ETH will be deposited to your zkAccount. Once received, you can transfer ETH privately.'

OP / ⚡ ▼ Get ETH 0x23F1...

Deposit Transfer Withdraw History

Deposit

0.008 ⚡ ETH ▼

Relayer fee: 0.0002 ETH (\$0.7541) Balance: 0.0089 ETH Max ⓘ

Deposit

⚠ ETH depositing can take up to 10 minutes. [Learn more](#)

ETH will be deposited to your zkAccount. Once received, you can transfer ETH privately.

Two complementary privacy technologies

This project combines two complementary and powerful privacy technologies:

- **Stealth Addresses:** We can generate virtually unlimited addresses where users can receive funds.
 - We do not need the collaboration of the user to generate a new address, we can derive as much as we want from a single stealth address published on ENS.
 - They provide a convenient way to receive funds offering privacy to the sender.
- **Zero Knowledge Proofs (ZKP):** We can prove to a smart contract pool that we own a specific address without revealing our identity.
 - They allow us to combine the funds received from a stealth address into a single address.
 - Hence, they provide a private way to receive funds.

zk Stealth

Let's get the best of both worlds!

Hello Anon

NONCE	STEALTH SAFE ADDRESS	SIGNER PRIVATE KEY	ETH BALANCE
0	0x459a394a778ab2bedd6daf4820b6707b3275219e	0xfef8bfa3...ec40	0 ETH
1	0xed758f7ed675180c1e71b44101564f566f13a3ab	0x77f2d172...a8a2	Send 0.0005 ETH to zkBob
2	0xa6f19c7a6e306f1bf8380181890222413200024d	0x3cd844ca...0f06	0 ETH
3	0xc73b35f6c8ff22f411f0f8d6c4d1fabe7036864b	0xa29aea92...cd2c	0 ETH
4	0x5d1755acf01d4b55599245cfb7865cf7d7112e60	0xc369eb15...679f	0 ETH

<https://github.com/sembrestels/zkstealth>

Thank You

Questions?