Privacy-Preserving Names: A Stealth Address Standard and Dev Kit for ENS

Scope

What problem is this work solving?

Today, most ENS names resolve to a single, public address. Every transaction sent to that name creates a permanent, onchain link between sender, recipient, and the entire history of the recipient's address.

But there is a simple solution: ENS is the perfect identity layer for stealth addresses. A static ENS identity can return privacy-preserving, one-time-use addresses, combining a simple user experience with much stronger privacy for end-users.

Fluidkey has demonstrated that this experience is possible in production today, with over $900M transacted by 20,000+ users to date.

There is, however, no simple way for other developers to enable stealth addresses with ENS in their product. This proposal builds a standardized architecture for secure stealth address resolution by unifying the ENS identity layer with the ERC-6538 standard, along with a plug-and-play toolkit for secure stealth address resolution.

A core design goal is that the ENS manager interface itself and any other wallet UI can adopt stealth-address registration without significant additional engineering. By keeping the standard wallet-agnostic, the resolver interface minimal, and the verifier permissionless, the broadest distribution channel for stealth addresses on ENS becomes ENS itself.

What is the approach?

Five interlocking deliverables, all of them public goods:

1. **ENS as the source of truth for stealth address resolution** - an ENSIP defining stealth-meta-address resolver standards: defining the storage of the ERC-5564 meta-address directly within standard ENS user text records and the resolution-and-verification flow against the stored value in an ERC-6538 compliant flow. This eliminates fragmented state and redundant key storage. Authored, submitted to ensdomains/ensips, and advanced through community discussion.

2. **ERC-6538 bridge smart contract** - a custom ERC-6538 compatible registry contract. This contract will not store state internally, instead its core function is to act as a dynamic read proxy pointing to ENS stealth records. Audited and deployed to mainnet.

3. **Onchain resolver with verification module** - a smart contract that calls into the ERC-6538 smart contract, verifies a stealth address, and reverts on mismatch, so resolution cannot be silently corrupted. This ensures users do not need to trust an offchain resolver, each stealth address is verified onchain. Audited and deployed to mainnet.

4. **Resolver kit** - a typescript stealth address resolution library extending the fluidkey-stealth-account-kit and a reference implementation so developers and agents can implement stealth address resolution in minutes. Published under the MIT license.

5. **Reference deployment in Fluidkey** - Fluidkey integrates the standard end-to-end across two user flows:

    - **Subname issuance** for new users: ENS subnames issued under a Fluidkey-controlled parent, with stealth resolution active by default.

    - **Bring-your-own ENS domain** for users who already hold a .eth name: connect the existing name, set the stealth-capable resolver, register the meta-address inside the user ENS domain.

What does success look like at the end of the cycle?

1. All 4 items in the previous section are completed, live, and publicly accessible

2. +30,000 ENS names use the stealth address verification module, verifiable onchain, by month 12 - this estimate is based on Fluidkey users alone

3. We will actively engage the ENS labs team and wallets to integrate stealth address support - by solving the current lack of privacy with ENS, one of the biggest pain points for power users, we expect a strong positive impact on professional ENS use cases

Milestones

Q1

Deliverable	Verification method	Expected date
Public RFC posted to the ENS forum for community feedback	Forum post link	Month 1

ENSIP for stealth address resolution submitted to `ensdomains/ensips` and opened for community discussion	PR link and assigned ENSIP number	Month 2
ERC-6538 bridge smart contract architecture specification published	Markdown spec in public Fluidkey repo	Month 3
Verifier contract architecture specification published	Markdown spec in public Fluidkey repo	Month 3

Q2

Deliverable	Verification method	Expected date
ENSIP advanced to Last Call (or beyond), subject to community process	ENSIP status in `ensdomains/ensips`	Month 4
Resolver kit beta published to npm (extends `fluidkey-stealth-account-kit` with the ENSIP-compliant resolver interface)	npm package link	Month 6
ERC-6538 bridge smart contract deployed to testnet	Etherscan link to verified contract	Month 6
Onchain verifier deployed to testnet	Etherscan link to verified contract	Month 6

Q3

Deliverable	Verification method	Expected date
Audits complete, public report released	Audit report	Month 9
ERC-6538 contract deployed to mainnet and L2s	Etherscan link to verified contract	Month 9
Verifier deployed to mainnet	Etherscan link to verified contract	Month 9

Fluidkey reference integration live across both flows - subname issuance and bring-your-own .eth domain - with stealth resolution and onchain verification enforced in production	Product release notes, live demo, on-chain evidence	Month 9
Integration guide published	Docs link	Month 9

Q4

Deliverable	Verification method	Expected date
Adoption report published: subnames issued, BYO .eth names connected, stealth-resolved transactions, kit installs and forks	Public forum report with raw numbers	Month 12

Prior delivery record

Prior ENS grants

The origin of Fluidkey was the **ETH Rome 2023 ENS hackathon**, which our submission won and which ultimately became the first version of our product. We have since been a **three-time recipient of ENS retroactive grants**:

- ETH Rome submission: https://taikai.network/ethrome/hackathons/ethrome-23/projects/clnga7i8400oswu016ugm1nk3/idea
- ENS retroactive grant #1: https://discuss.ens.domains/t/term-4-grants-summary/17624/6
- ENS retroactive grant #2: https://discuss.ens.domains/t/term-5-grants-summary/18921/4
- ENS retroactive grant #3: https://discuss.ens.domains/t/term-6-grants-summary/20320/8

Links to public evidence

- Main product: fluidkey.com
- Open source repos:
  - https://github.com/fluidkey/fluidkey-stealth-account-kit (audited by Dedaub)
  - https://github.com/fluidkey/fluidkey-earn-module (audited by Ackee)

Other relevant work

Founded Walletbeat - a public good project that brings transparency to the Ethereum wallet ecosystem. We are connected with many wallets through this and will actively promote the ENS stealth address libraries.

Budget

Total requested: USD 339,716

Line item	Amount	Justification
Engineering	USD 266,844	1.5 FTE average monthly contribution over 12 months - led by Fluidkey CTO with support of senior developers covering ENSIP authorship, resolver kit extension, verifier contract development, and the docs/example repo. Note: the Fluidkey reference integration is not budgeted and will be covered separately by the company.
Smart contract audit	USD 50,000	One external audit of the ERC-6538 bridge and verifier contracts by a reputable firm prior to mainnet deployment.
Distribution, Operations & Overhead	USD 22,872	0.2 FTE average monthly contribution over 12 months - led by Fluidkey CEO. Integrator engagement, community engagement, ENSIP iteration through the standards process, quarterly forum reporting, and project management.

The budget is deliberately scoped to the public-goods work. Fluidkey's product-specific UI and customer-facing integration costs are excluded and remain self-funded.