

Onion Plan

2022 Tor Meeting

Rhatto and Raya

2022.Q3

Onion Support Group - The Tor Project



About

- Who we are: The Onion Support Group!
- What do we want: More Onions Por Favor! :)
- Our goal: **increase Onion Service adoption** by offering an **enhanced experience** both for **users** and service **operators**.
- Our common feeling: **the moment is similar** to when the privacy-aware internet was **moving from HTTP to HTTPS**, but now with Onion Services!
- What we can do: help organizing and facilitating the process.

Retrospective

- Discussion about Onion Service usability is happening for years.
- It's a difficult topic, especially because no "perfect" solution was found for each problem.
- This and the lack of people working full time in this area yields to a stalled roadmap.

How to move again?

How to move again?

1. Get a step back, and organize what we have (notes, discussions, proposals. . .).
2. Try to set a feasible roadmap.
3. Translate/fit it into a fundraising project.

What to prioritize?

What to prioritize?

A suggestion, in order of importance:

1. Health (DoS protections, performance improvements etc).
2. Usability (Onion Names, Tor Browser improvements etc).
3. Tooling (Onionbalance, Onionprobe, Oniongroove etc).
4. Outreach (documentation, support, usage/adoption campaigns etc).

Fundraising projects could integrate all or some of these items by proposing an **Onion Service Enhancement Package**.

1. Onion Services Health

1. Onion Services Health

- Overview: recent Onion Services DoS and PoW protection implementation.
- We're not the best people to talk about, so we'll leave this to the discussion.

2. Usability

2. Usability

There are many ways to sort all proposals, especially by what type of problems they try to solve. Our suggestion is to group by:

1. **Address translation:** links a “traditional” domain name with an Onion Service address. Examples: Onion-Location Header; Sauteed Onions; DNSSEC-based, Alt-Svc).
2. **Onion Names:** alternative schemes for human-friendly names linked with Onion Services. Examples: ruleset-based (like Secure Drop’s list); blockchain-based (like Namecoin); other P2P-based (like GNUnet’s LSD); etc.
3. **HTTPS certificates:** easier integration of CA-validated TLS certificates into Onion Services. Examples: ACME for .onion; X.509 for .onion (self-signed by the .onion address).

2. Usability: coexistence between proposals

2. Usability: coexistence between proposals

It's possible to make proposals to coexist, which needs:

1. **Tech specs**: for proposing and implementing “**pluggable discoverability**” methods with **opportunistic lookup** linking human-friendly names with Onion Service addresses.
2. **Governance specs**: build criteria and decision making procedures to accept or reject pluggable discoverability proposals?
3. **Namespace allocation**: for each Onion Naming implementation.

3. Tooling

3. Tooling

- Onion Services currently is not very integrated into DevOps solutions.
- Toolset and configurations are needed to make system administration life easier, including Onion Services' keys life cycle.
- In 2022 we created Onionprobe (test tool), Onionmine (key management tool), Onion Launchpad (landing page) and drafted the Oniongroove (DevOps stack) specs, but we can do more.

4. Outreach

4. Outreach

- 4.1. Resources
- 4.2. Support
- 4.3. Training
- 4.4. Usage/adoption campaigns

4.1. Resources

In 2022, we created a generic training resource to introduce onion services to human rights and media organizations[1]. We could and should do more, including add more printables for offline trainings[2].

- [1] <https://gitlab.torproject.org/tpo/community/training/-/raw/master/2022/onion-services/intro-onion-service-2022.odp?inline=false>
- [2] <https://community.torproject.org/outreach/kit/>

4.2. Support

- We're supporting media organizations with deploying Onion Services but it's a top-down approach (doing what's required by the sponsor).
- The retention rate is uncertain, i.e. whether the Onion Services will continue to be maintained and used beyond sponsor work.
- It would be good to also build conversations with organizations that are already expressing a need for secure and private browsing and information sharing alternatives.

4.3. Training

- In 2022 we trained journalists about Tor and Onion Services (high level understanding).
- We could do more to better communicate the benefits of Onion Services and frame these benefits based on the audience in front of us.

4.4. Usage/adoption campaigns

- We're reaching out to groups and organizations that we believe can benefit from deploying Onion Services, but there's no documented process and it's not part of a campaign.
- But all this depends on what the future (near or far) of Onion Services will look like: will Onion Services become a norm (e.g. how the web has moved to HTTPS) or mainly reserved for specific use cases (e.g. whistleblowing, file sharing)?

Exercises

Exercise 1: The “Six What’s”

Organizing a short/mid-term roadmap, taking into account:

1. What we can implement ourselves (Tor Developers)?
2. What depends in other people/groups/community?
3. What depends on discussing/consensus due to different “world views” at Tor?
4. What depends on little-Tor implementation (specially due to arti’s current prioritization)?
5. What significantly increases the Tor Browser package size and then should be considered with care?
6. What is most important?
7. What could be included in a next Sponsor 123 phase (the sponsor work directly dealing with Onion Services)?

See spreadsheet companion for details.

Exercise 2: Tech specs

See spreadsheet companion for details.

Exercise 3: Governance specs

See spreadsheet companion for details.

Exercise 4: Namespace allocation

See spreadsheet companion for details.

Wrapping up

Wrapping up

- Conclusions.
- Next steps.