Onion Plan

2023 Tor Meeting

Raya, Rhatto, your-name-here

2023.Q2

Onion Support and Working Group - The Tor Project

Intro

Session goals

1. Inform the community about what we've done, what we plan to do, the challenges ahead and the open questions about Onion Services.
2. And then get some input from people :)

Onion Plan?

- **What**: The Onion Plan is an *applied research* to *help and facilitate* Onion Services improvement.
- **Why**: discussions often gets easily dispersed and buried; there's a need to keep track of many options and how to translate those into funding projects.
- **How**: collecting and analyzing proposals; building roadmap scenarios.
- **Who**: it's a multi-team effort and everyone can collaborate. Currently it's happening mostly on Community and Network teams.
- **When**: discussions on Onion Service improvements happens for years and years; we started organizing it during 2022.

Retrospective

Technology timeline

Year	Technology
2003	Onion Services v2 spec (rendezvous)
2013	Proposal 224 (Next Generation of Onion Services)
2014	HTTPS certificates (facebook)
2014	Vanity addresses (facebook)
2015	Onion Services v3 initial development (Tor 0.3.0.1-alpha)
2016	Proposal 279
2017	Onion Services v3 spec
2018	Onion Services v3 release (Tor 0.3.2.9)
2018	Alt-Svc (cloudflare)
2020	Onion-Location (TBB 9.5)
2020	Onion Authentication (TBB 9.5)
2020	Onion Names for SecureDrop (TBB 9.5)
2021	Onion Services v2 final deprecation (v2 deprecation timeline)
2023	20 years of Onion Services! Congrats everyone involved!

Updates

The Limerick session (2022.Q3)

Four tracks:

1. Network Layer (formely *Health*).
2. Usability.
3. Tooling.
4. Outreach.

Recent changes

Since the Limerick session, i.e, from 2022.Q4 to 2023.Q2:

- Tor Blog: Reflections on how we plant and grow onions.
- Onion Plan documentation was released: `https://tpo.pages.torproject.net/onion-services/onionplan/`.
- ACME for Onions got a draft spec: acmeforonions.org.
- Fundraising: The Onion Services Coalition has arrived! & other perspectives.
- Two full-time C & Rust developers joined the team and the Onion Services Working Group has formed.
- We did some online meetings about certificates and service discovery.
- Work included at the 2023 Tor Strategic Plan: *Goal 2 (product) - Objective 2 (any person on the planet be able to use Tor to access any online service) - KR 1 - Health of onion services its improved, onion names plan draft is concluded*.

Network Layer

Onion Services Coalition

...

Recent progress on PoW

...

Onion Services roadmap on Arti

...

Usability

Overview

Research is split in two efforts:

1. Tracking and discussion of existing proposals.
2. Building incremental roadmap scenarios.

It also aims for *coexistence between proposals*, which needs:

1. **Tech specs**: for writing and implementing proposals.
2. **Governance specs**: build criteria and decision making procedures to accept or reject proposals.

Sorting proposals

Proposals are currently grouped as:

1. Certificates.
2. Service Discovery (address translation and “pure” Onion Names).

Certificates

- Many non-conflicting proposals.
- ACME for Onions is currently the best option so far, since it opens two possibilities:
  1. Adoption by existing Certificate Authorities such as Let's Encrypt.
  2. Running an .onion-only CA!

Certificates - Effort

Amount of work involved for each level (initial assesment).

Proposal	Engineering effort	Operation effort	Governance effort	Overall assessment
Existing CA validation	None (already done)	None (already there)	None (already done)	None
ACME for .onion	High	Medium	High	
Self-signed X.509 for .onion	Very High	None	Very High	
Same Origin Onion Certificates (SOOC)	High	None	Very High	
DANE for .onion	High	None	Very High	
Onion-only CAs	Low	High	High	

Certificates - Challenge

Difficulty in solving open questions while implementing a given proposal (initial assesment).

Proposal	Engineering challenge	Operation challenge	Governance challenge	Overall assessment
Existing CA validation	None (already done)	None (already there)	None (already done)	None
ACME for .onion	Low	Low	Medium (adoption)	
Self-signed X.509 for .onion	High	None	High	
Same Origin Onion Certificates (SOOC)	Low	None	High	
DANE for .onion	Low	None	High	
Onion-only CAs	High	High	High	

Certificates - Risk

Risk involved in the proposal not be successfully implemented in a given level (initial assesment).

Proposal	Engineering risks	Operation risks	Governance risks	Overall assessment
Existing CA validation	None (already done)	None (already there)	None (already done)	None
ACME for .onion	Low	Low	Medium	
Self-signed X.509 for .onion	High	None	?	
Same Origin Onion Certificates (SOOC)	Low	None	?	
DANE for .onion	High	None	?	
Onion-only CAs	Low	Medium	?	

Certificates - Next Steps

- Continue to pursuing ACME for Onions: trying to connect Q Missel with Let's Encrypt. This alternative has the minimal effort for Tor.
- Some Onion Service operators may not like to have their .onion addresses published into CT Logs, so having an alternative .onion-only Certificate Authority is also being considered, but that requires a lot more effort to implement beyond having an ACME for Onions implementation.

Service discovery

- There's a DRAFT proposal scenario towards *pluggable discoverability*.
- It still needs review and input before being ready for a concrete project.

Service discovery - DRAFT proposal - Phases

- **Phase 0**: current functionality.
- **Phase 1**: **accessing URLs** like `https://torproject.org` **directly** using Onion Services and HTTPS!
- **Phase 2**: **opportunistic discovery** of .onion addresses (increased censorship resistance).
- **Phase 3**: bringing "pure" **Onion Names** into Tor.

At any Phase, low-hanging fruit can be included, such as fixes and improvements to existing features like `Onion-Location`.

Service discovery - Phases comparison

Phase	Category	Method	Technology	Status
0	Addr. trans.	Onion-Location v1, Alt-Svc	HTTP	Done
1	Addr. trans.	DNS-based discovery	DNS	Planning
2	Addr. trans.	Sauteed Onions or other	CT Logs or other	Research
3	Onion Names	?	P2P/Blockchain	Research

Service discovery - Decentralization comparison

Phase	Technology	Decentralization
0	HTTP headers	Centralized (a single point of failure)
1	DNS	Very decentralized, but hierarchical
2	CT Logs?	Decentralized, less hierarchical, few nodes
3	P2P/Blockchain	Decentralized, non-hierarchical, many nodes

Service discovery - Censorship resistance comparison

Phase	Technology	Censorship resistance
0	HTTP headers	Does not work when the site is blocked
1	DNS	Even if site is blocked, not if DNS is
2	CT Logs?	Even if site/DNS blocked, not if CT Logs is
3	P2P/Blockchain	Should be fully censorship resistant

Service Discovery - Next Steps

- Need more research time to progress.
- Still need to discuss roadmap with the Arti (and maybe with the C Tor) team.

User Experience

- UX improvements for Tor Browser and mobile.
- Quality Assurance for Tor Browser regarding Onion Services.
- Input from UX and Applications Teams on what to include in the plan?

Tooling

Onionprobe improvements

- Onionprobe: a tool for testing and monitoring status of Tor Onion Services.
- There are many improvements towards making it kind of a swiss army knife for Onion Services testing and debugging.
- For 2023, the initial workload estimate for Onionprobe sums up to 1 month full time dedication.

Oniongroove roadmap

- Oniongroove: a suite for Onion Service deployment.
- Right now it's only an specification, and we hope to make a prototype still on 2023.
- Shall it be built with Arti from start?
- For 2023, the initial workload estimate for Onionprobe sums up to 2 months full time dedication.

Outreach

Onion Support work

Onion support work for organizations working on human rights:

- Trainings on using onion services (case of Sponsor 123).
- Trainings on deploying and maintaining onion services (case of T.).
- Hands-on support for deploying onion services (case of D.).

Online campaigns

- Online campaigns talking about onions, their features.
- A shift in the discourse: gathering arguments for promoting the technology: anonymity is only one of many interesting Onion Service properties.

Q&A

Q&A

:)