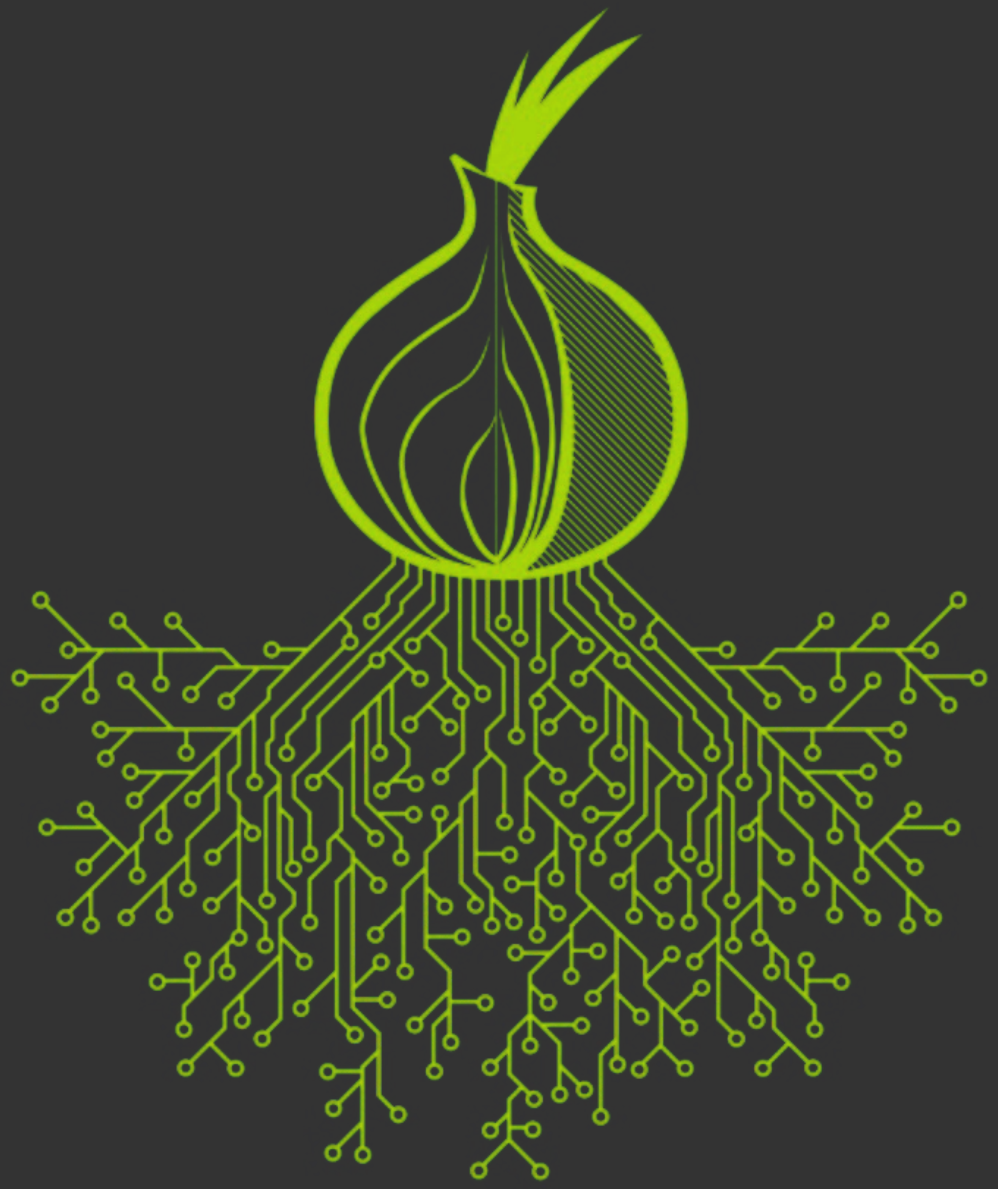
Tor et ses .onion

Un système d'adressage « privacy by design »

Journée du Conseil scientifique de l’Afnic
11 juillet 2016

Lunar
lunar@torproject.org
0603 CCFD 9186 5C17 E88D 4C79 8382 C95C 2902 3DF9

The Tor Project



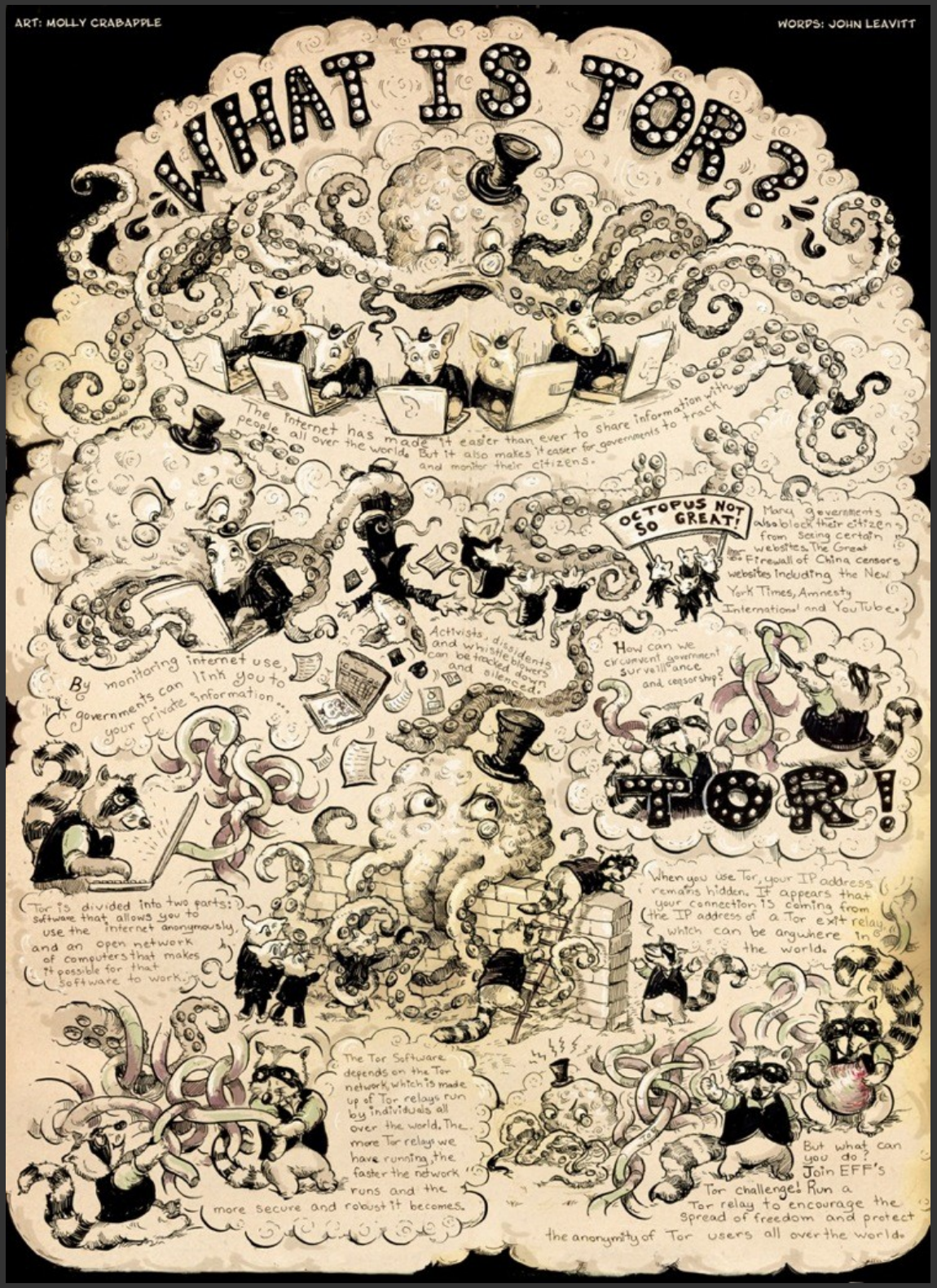
Our mission is to advance human rights and freedoms by creating and deploying free and open privacy and anonymity technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding.

Deep Dark Marina Abyssal Web

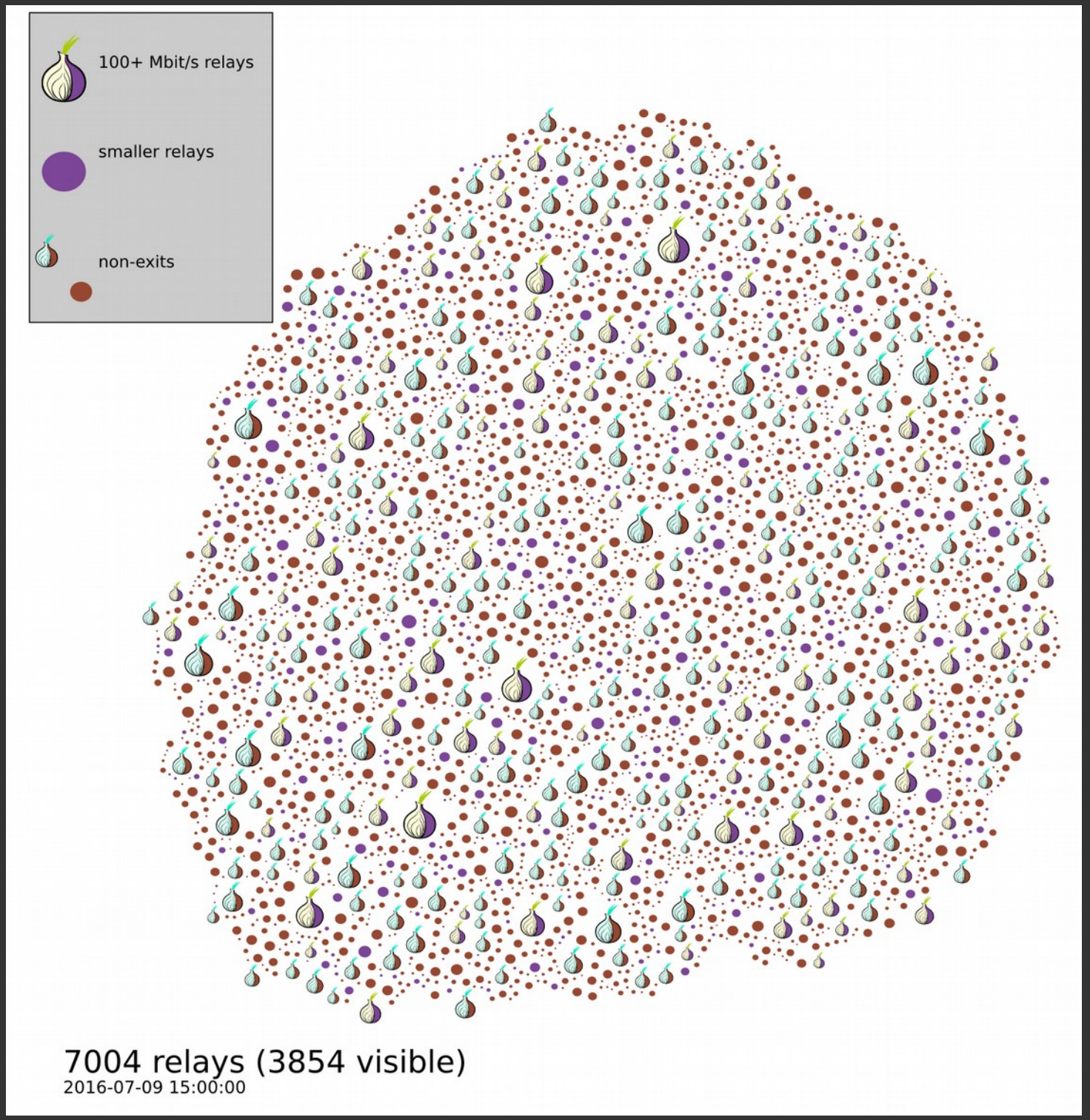
JOSEPH COX SECURITY 06.18.15 7:00 AM

THE DARK WEB AS YOU KNOW IT IS A MYTH

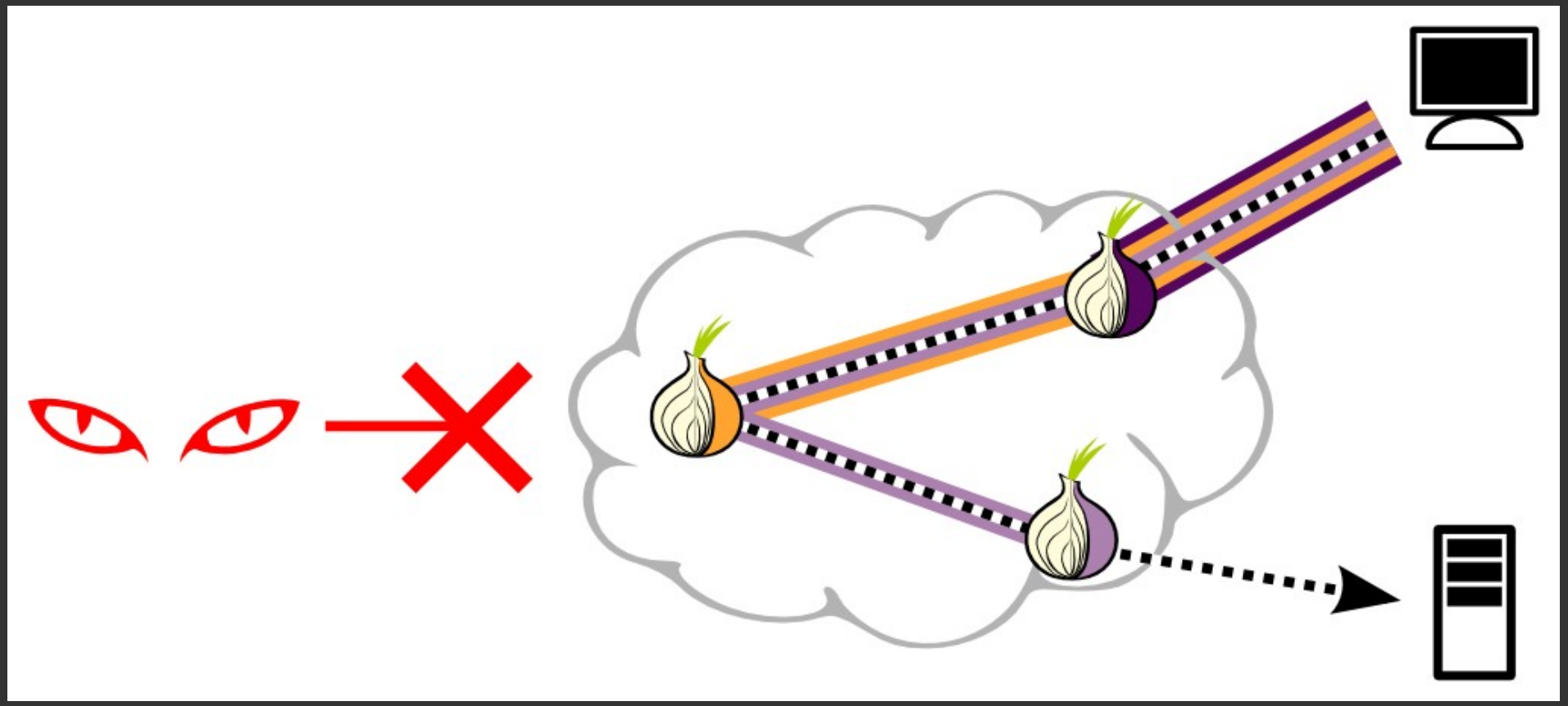
... **<u>NOT</u>** about the **Dark Web**



- Online Anonymity
  - Open Source
  - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization


100+ Mbit/s relays
smaller relays
non-exits
7004 relays (3854 visible)
2016-07-09 15:00:00

Usual Tor connections



Blog Stéphane Bortzmeyer: Mon blog dans les oignons - Navigateur Tor

Blog Stéphane Bortz…

7j3ncmar4jm2r3e7.onion/blog-tor-onion.html

Mon blog

Autres trucs

Accueil

Seulement les RFC

Seulement les fiches de lecture

Ève

Mon blog dans les oignons

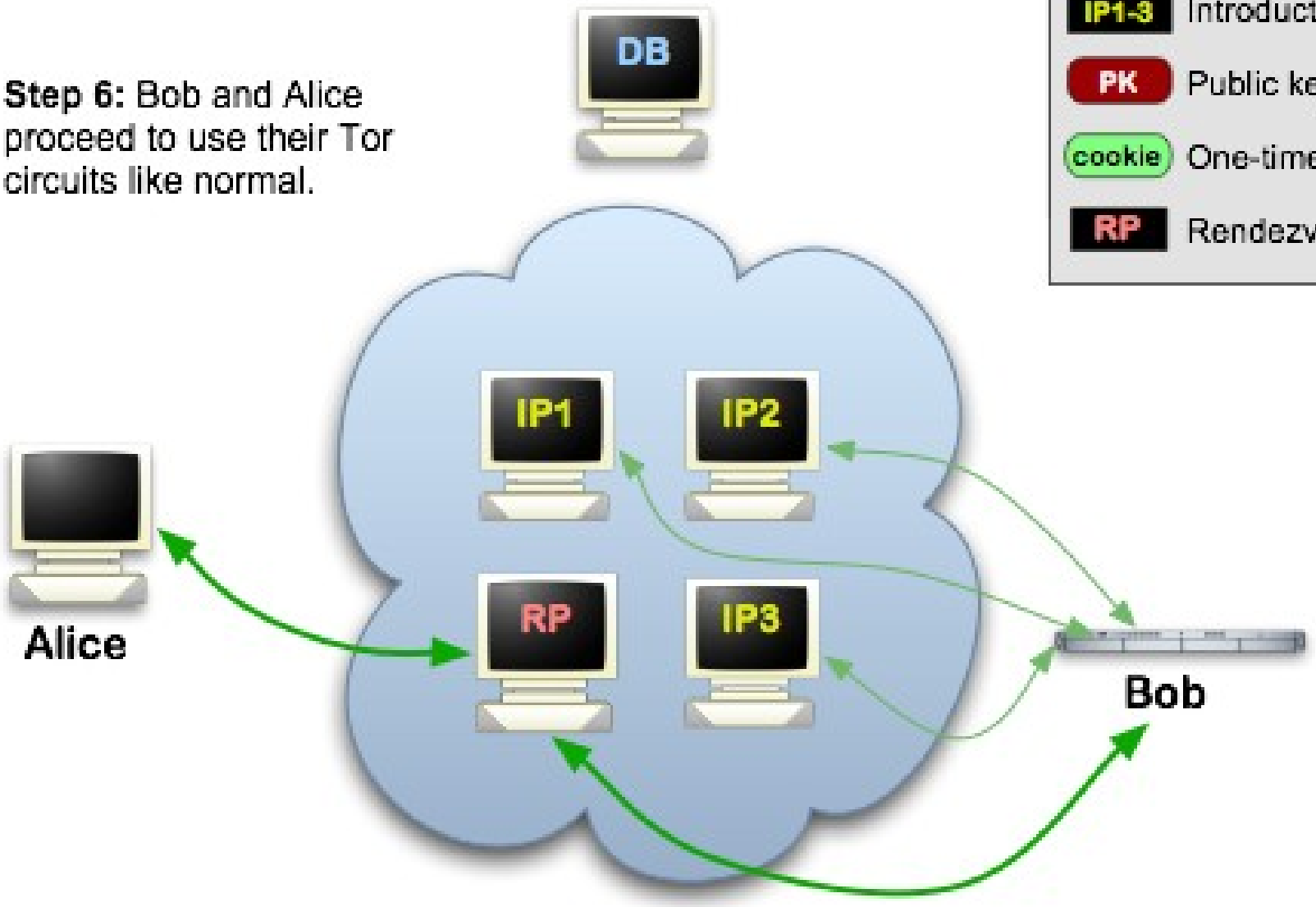
Première rédaction de cet article le 15 janvier 2015
Dernière mise à jour le 25 février 2015

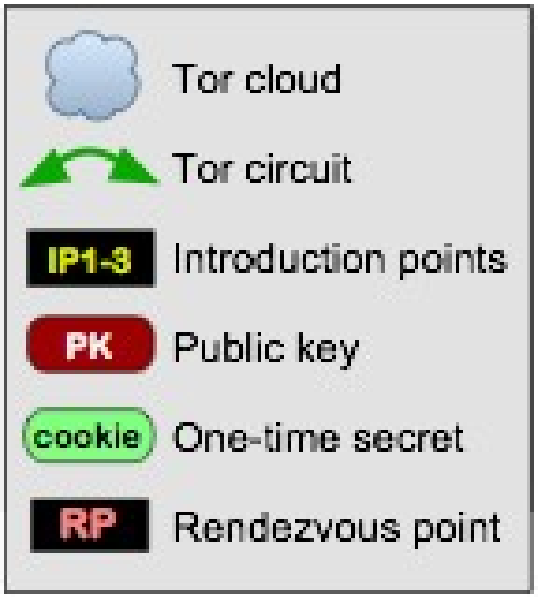
Cela faisait longtemps que je voulais m'amuser avec cela, donc, désormais, ce blog est désormais également accessible en *Tor hidden service*, c'est-à-dire avec un nom de domaine en `.onion`.

Quel est l'intérêt de faire cela ? Le réseau Tor est connu pour permettre une connexion aux services de l'Internet qui soit anonyme (attention à votre sécurité toutefois : aucune technique n'est parfaite et rien n'est jamais complètement anonyme) et qui résiste à la censure. Tor assure ce service en **relayant** chaque requête par plusieurs nœuds Tor. Seul le premier connait le client initial (il ne

Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.





Onion Service Properties

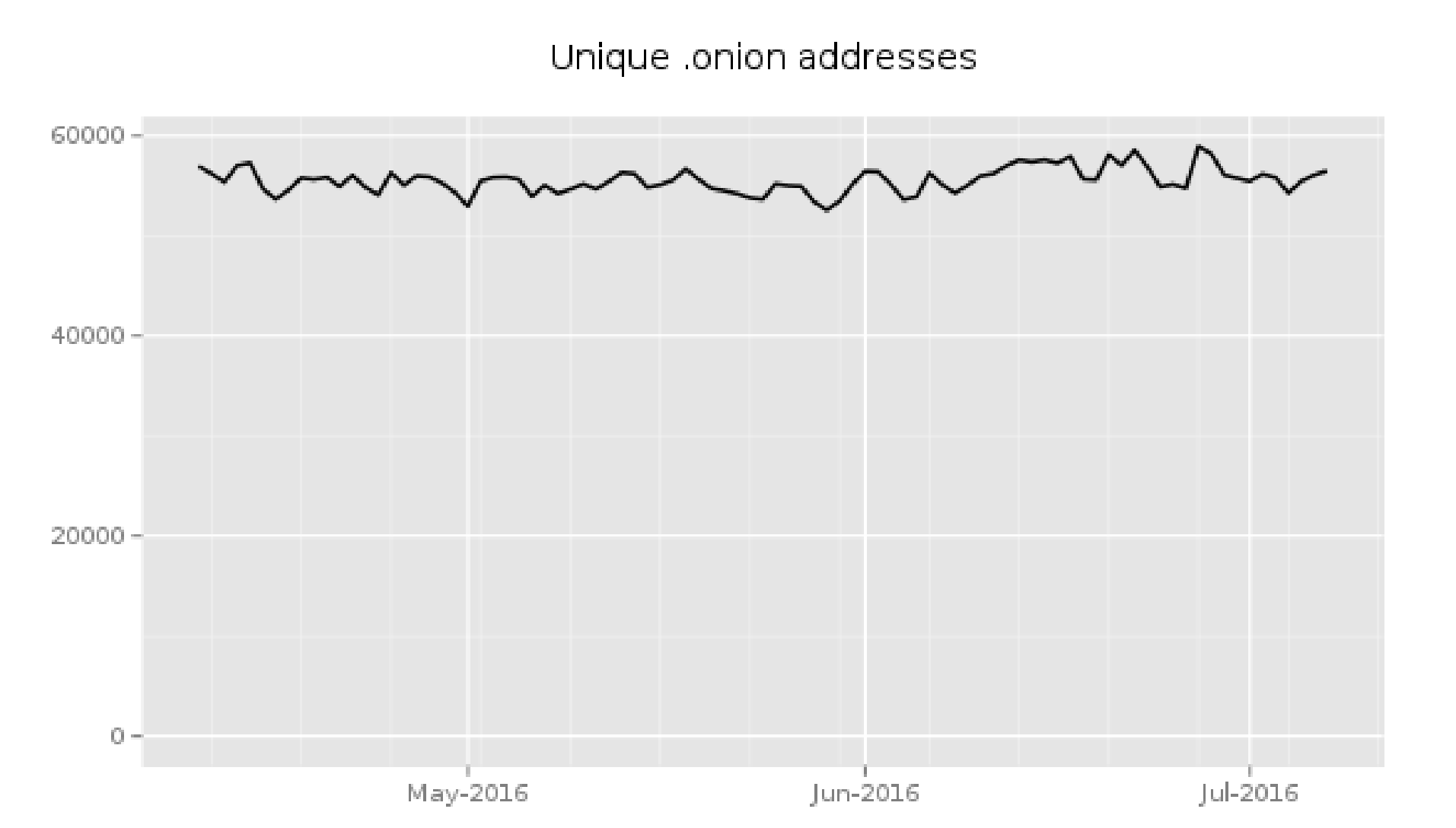
Self authenticated

Distributed directory

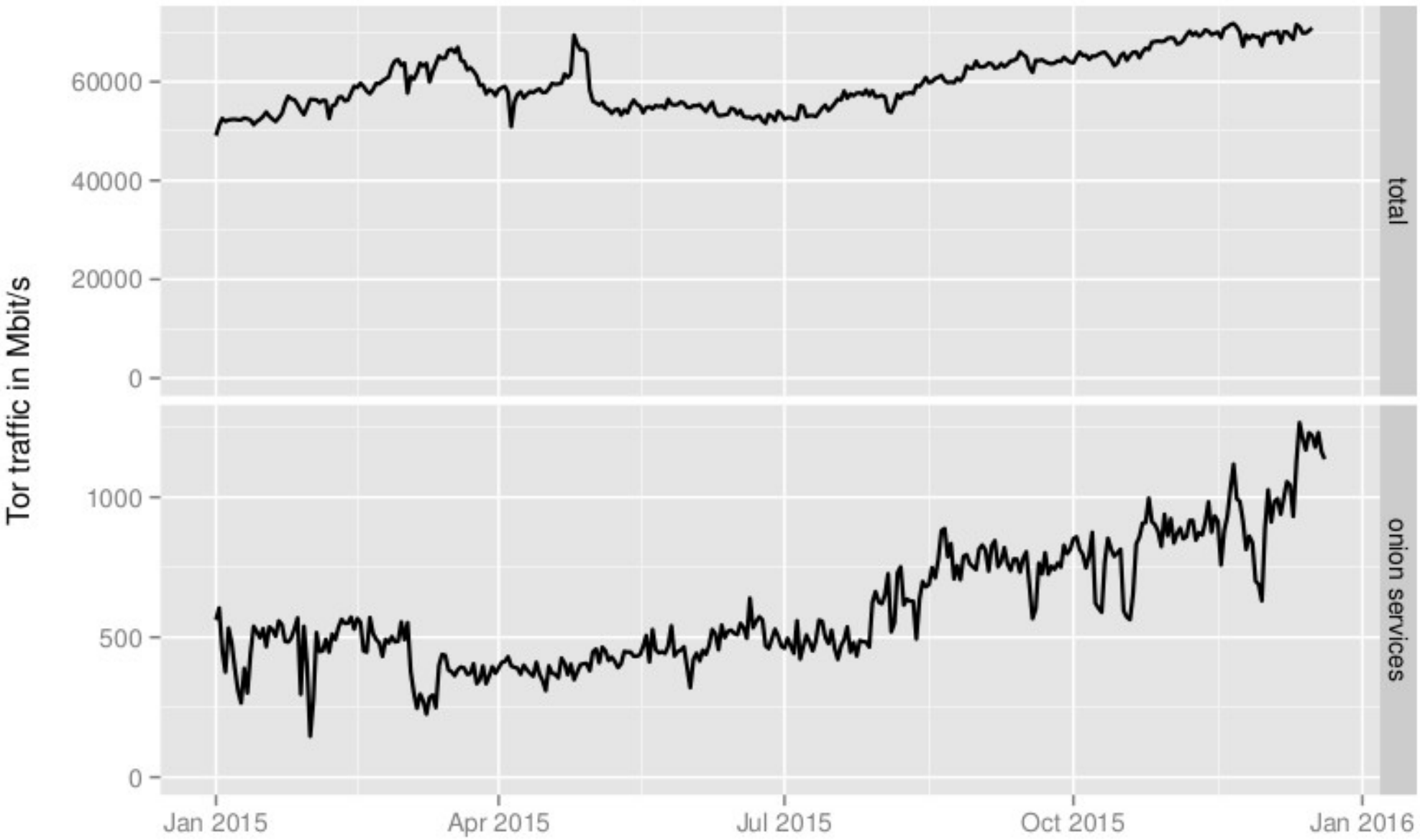
End-to-end encrypted

NAT punching

Unique .onion addresses



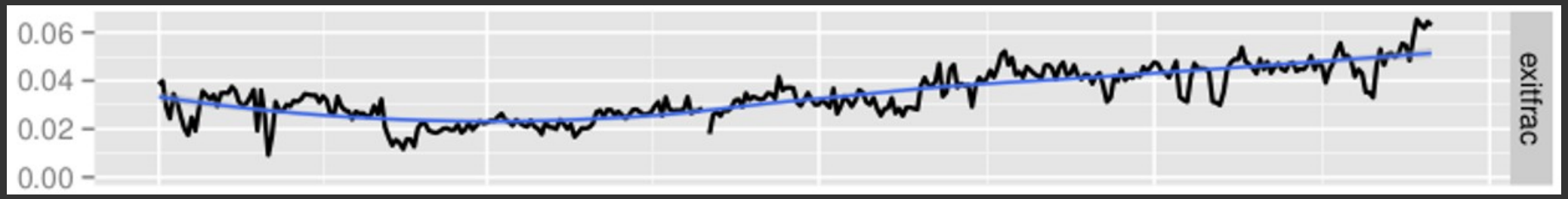
Estimated Traffic



Estimated Traffic

As of December 2015,

~5% of client traffic is HS

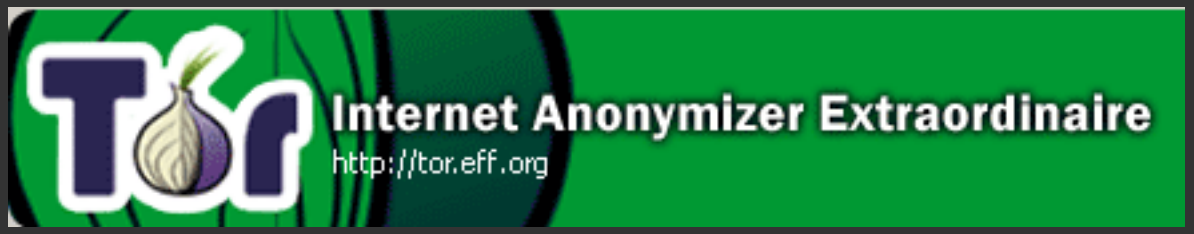


Statistics

Proposal 238

https://research.torproject.org/techreports/extrapolating-hidserv-stats-2015-01-31.pdf

Birth - 2004



ChangeLog file entry:

```
Changes in version 0.0.6pre1 - 2004-04-08
  o Features:
    - Hidden services and rendezvous points are implemented. Go to
      http://6sxoyfb3h2nvok2d.onion/ for an index of currently available
      hidden services. (This only works via a socks4a proxy such as
      Privoxy, and currently it's quite slow.)
```

Early use case - 2006

Souce: wikipedia.org

Wikileaks - 2007

Wikileaks:Tor

(Redirected from Tor)

The following method requires some technical ability. If you are used to installing new software and configuring proxy servers you should have the required skills, otherwise you may wish to use one of our other submission methods. Don't let the technology defeat you!

Tor or The Onion Router is a cryptographic technique first implemented by US navy research to permit intelligence agents to use the internet without being traced, by encrypting and routing communications through many different internet servers. Subsequently Tor has been developed by US University MIT and the California internet rights watchdog the Electronic Frontier Foundation and subsequently incorporated into Wikileaks.

Using our anonymous access package (see below) you can prevent internet spies knowing that your computer has connected to Wikileaks.

Most Wikileakers willl not need this extra security and there are simpler and possibly safer alternatives for once-off high-risk leaks (see Submissions). But for those who are at risk and want to access Wikileaks from the comfort of their homes or offices or need to bypass Internet Censorship, Tor (Onion Routing) is an excellent solution.

When you have installed our Tor access package (see below), you may then connect to Wikileaks via our anonymous address (the ".onion" is short for "Onion Routing", but you do not need to be concerned with this detail).

Then whenever you want to establish an encrypted anonymous (even to internet spies) connection to Wikileaks goto our magic link:

> http://gaddbiwdftapglkq.onion/
> (**this link will only work once you have installed and configured Tor**)

To upload a document anonymously using tor:

> http://gaddbiwdftapglkq.onion/wiki/Special:Leak
> (**this link will only work once you have installed and configured Tor**)

Unless your memory is superb you may wish to write that address down, but make sure you discard the paper after you are finished with it.

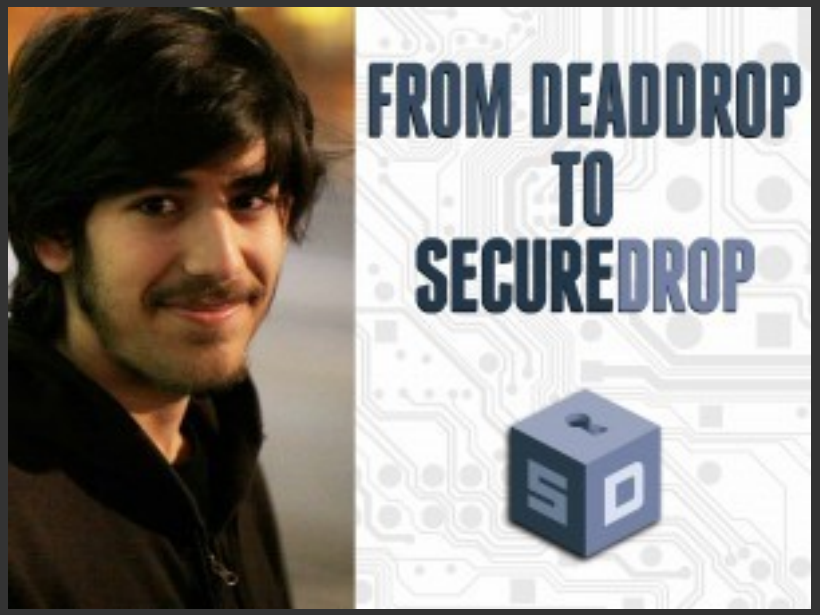
Without Tor, when you access a Wikileaks site the usual way, e.g via https://wikileaks.org/ all your data is encrypted, but internet spies maybe able note how long your computer spent talking to Wikileaks servers. See Connection Anonymity for further discussion.

GlobaLeaks - 2011

Today, more than 30 projects use GlobaLeaks

https://en.wikipedia.org/wiki/GlobaLeaks#Implementations

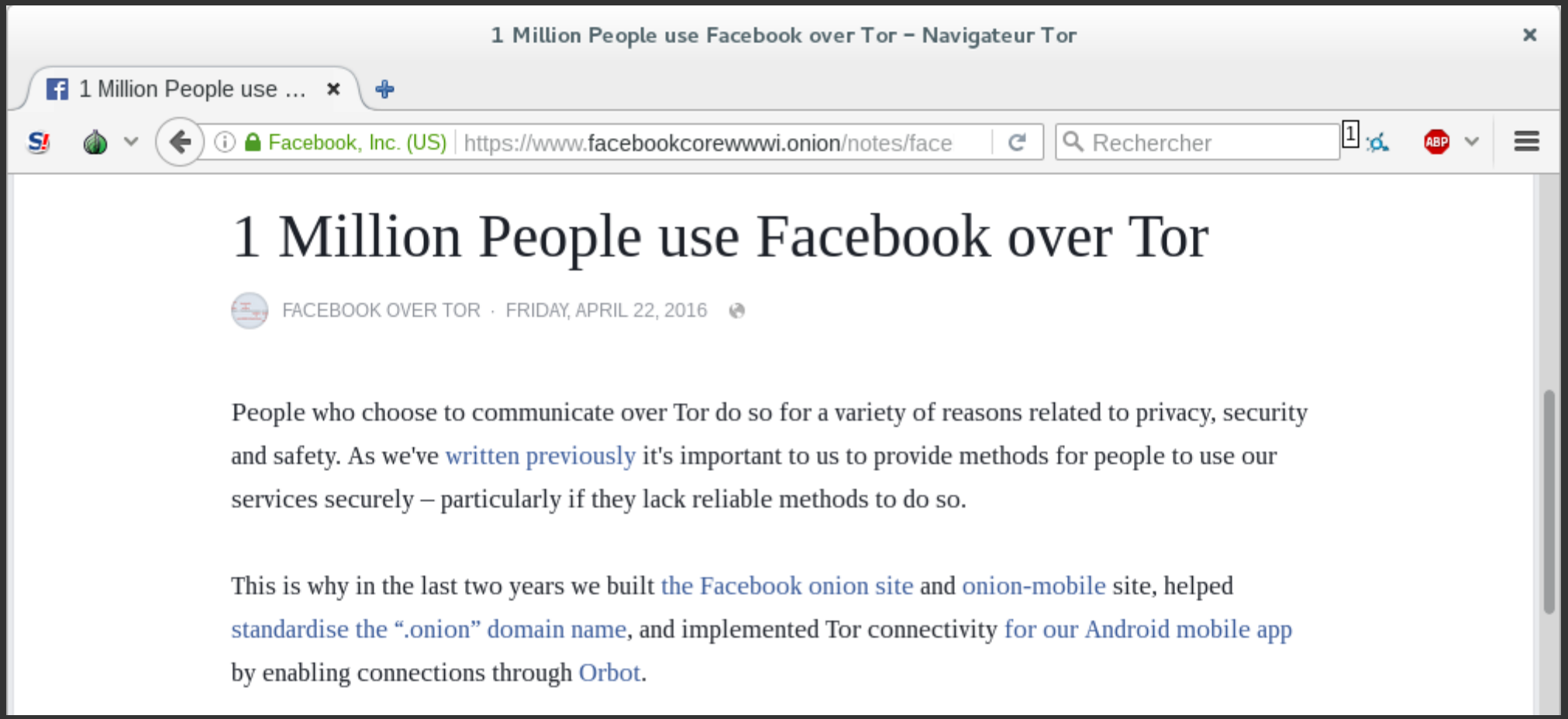
SecureDrop - 2013



Today, 22 organizations use SecureDrop

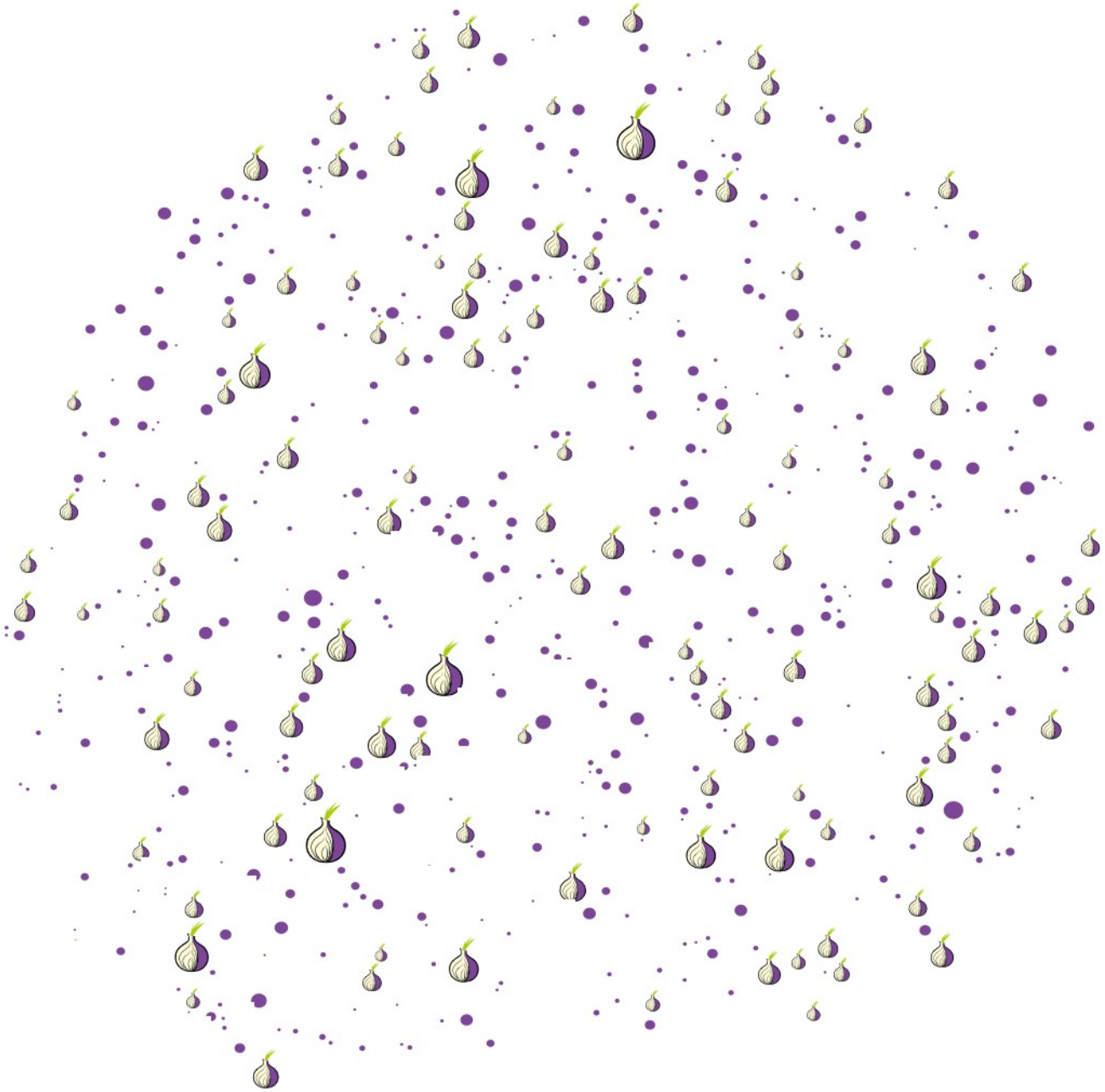
https://securedrop.org/directory

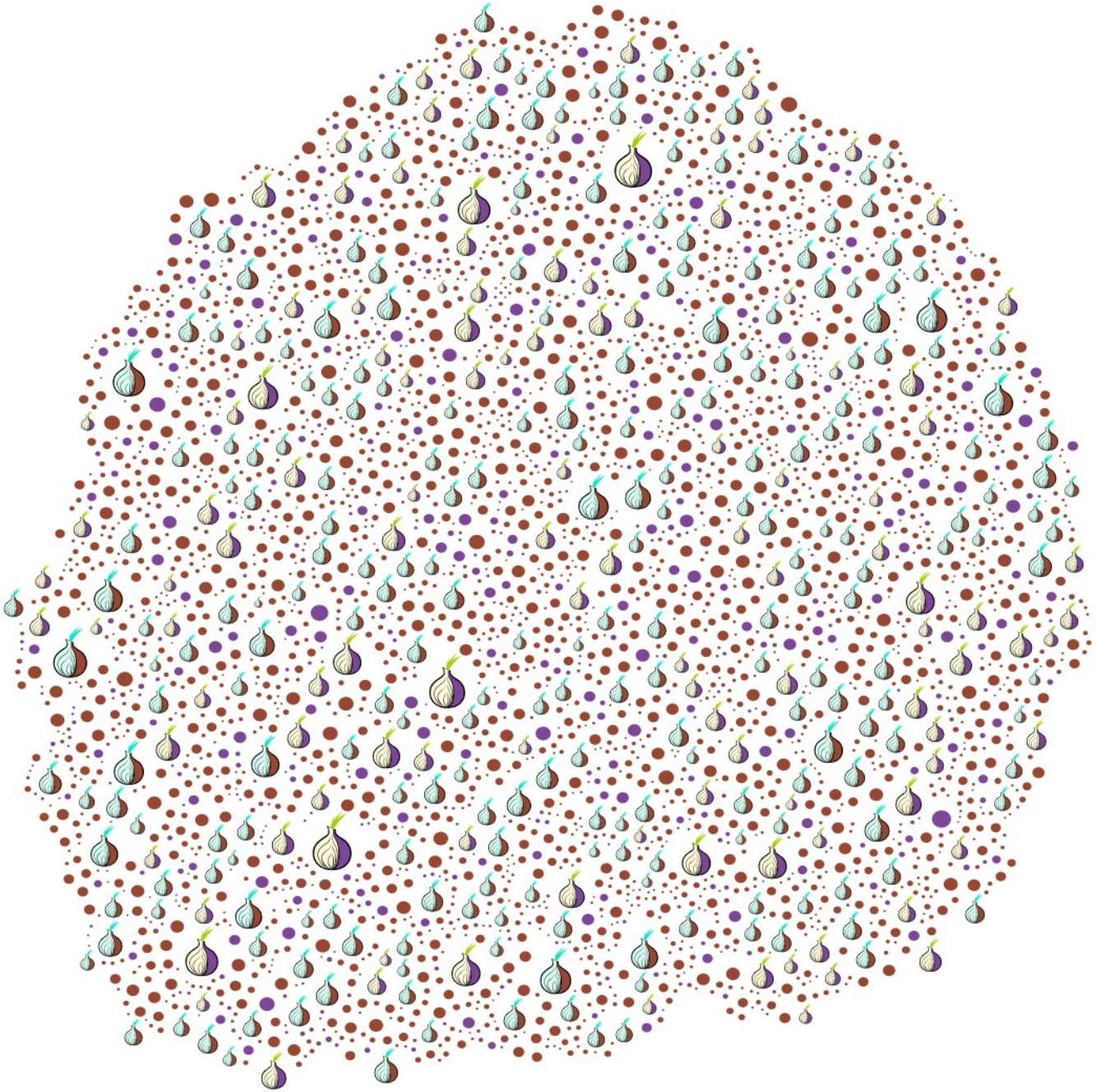
And Facebook Too - 2015



And Facebook Too - 2015

- No more worrying about **bad** certificate authorities
- Avoids exit relay contention, traffic **never leaves** the network!



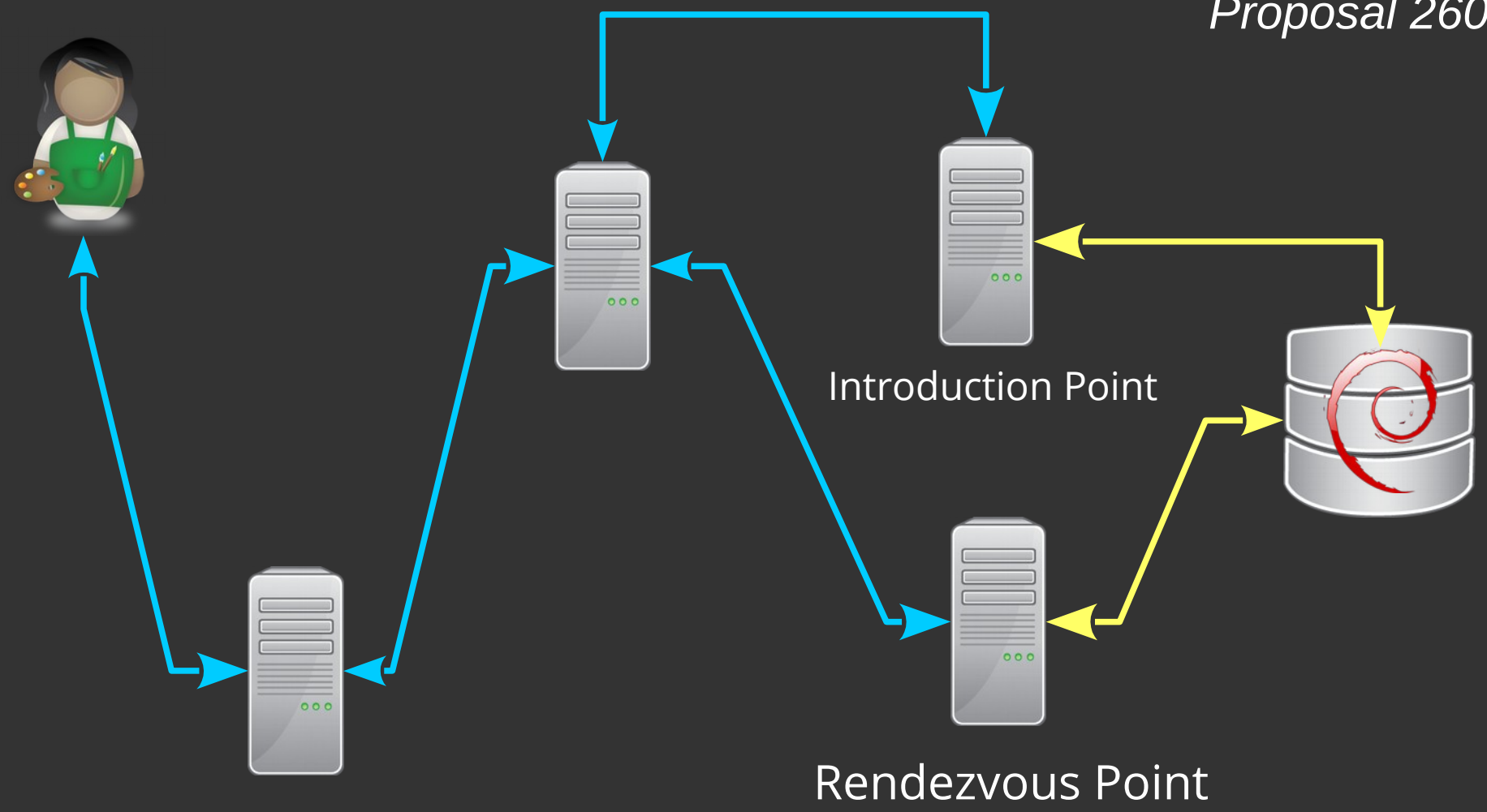


And Facebook Too - 2015

- No more worrying about **bad** certificate authorities
- Avoids exit relay contention, traffic **never leaves** the network!
- Ultimately it could be **faster** than reaching Facebook with a normal Tor circuit

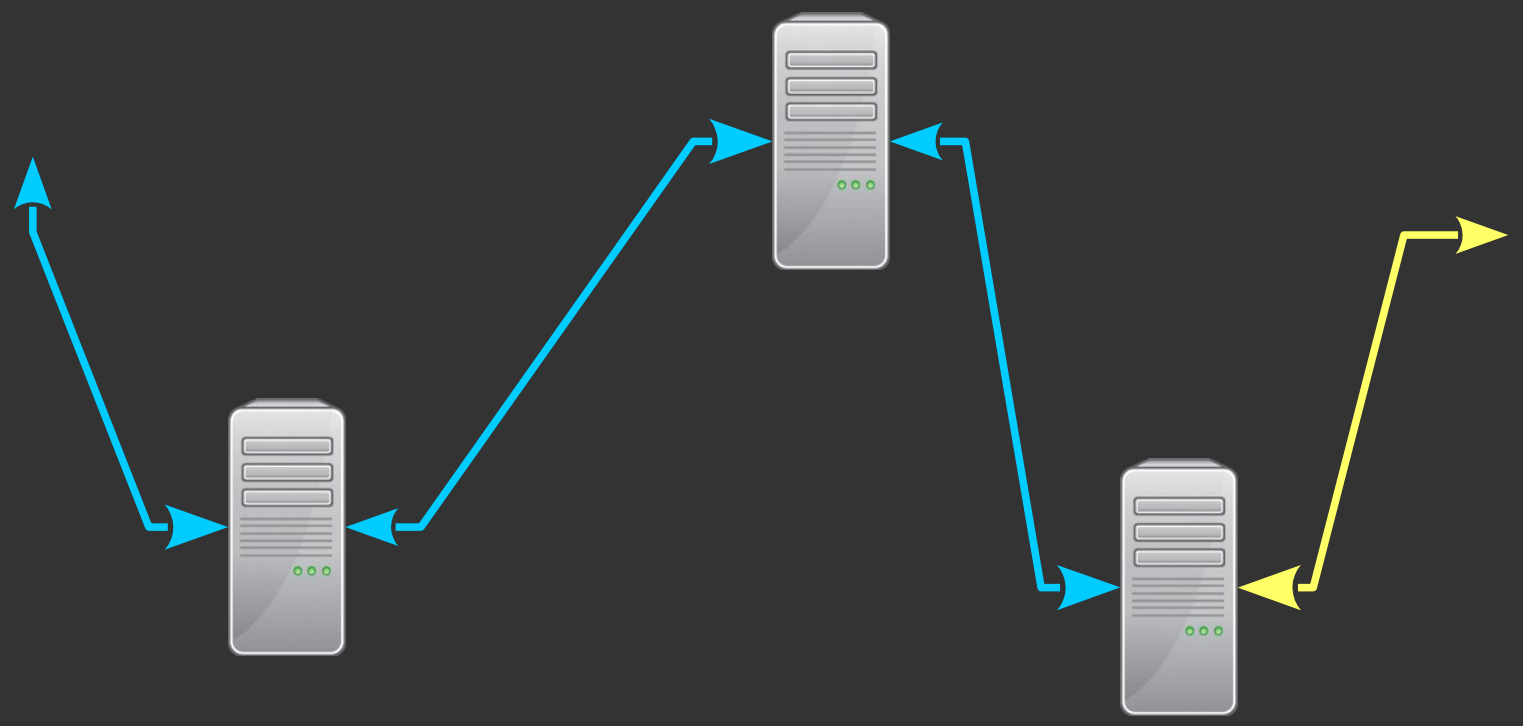
Rendezvous Single Onion Services (RSOS)

Proposal 260



Single Onion Services (SOS)

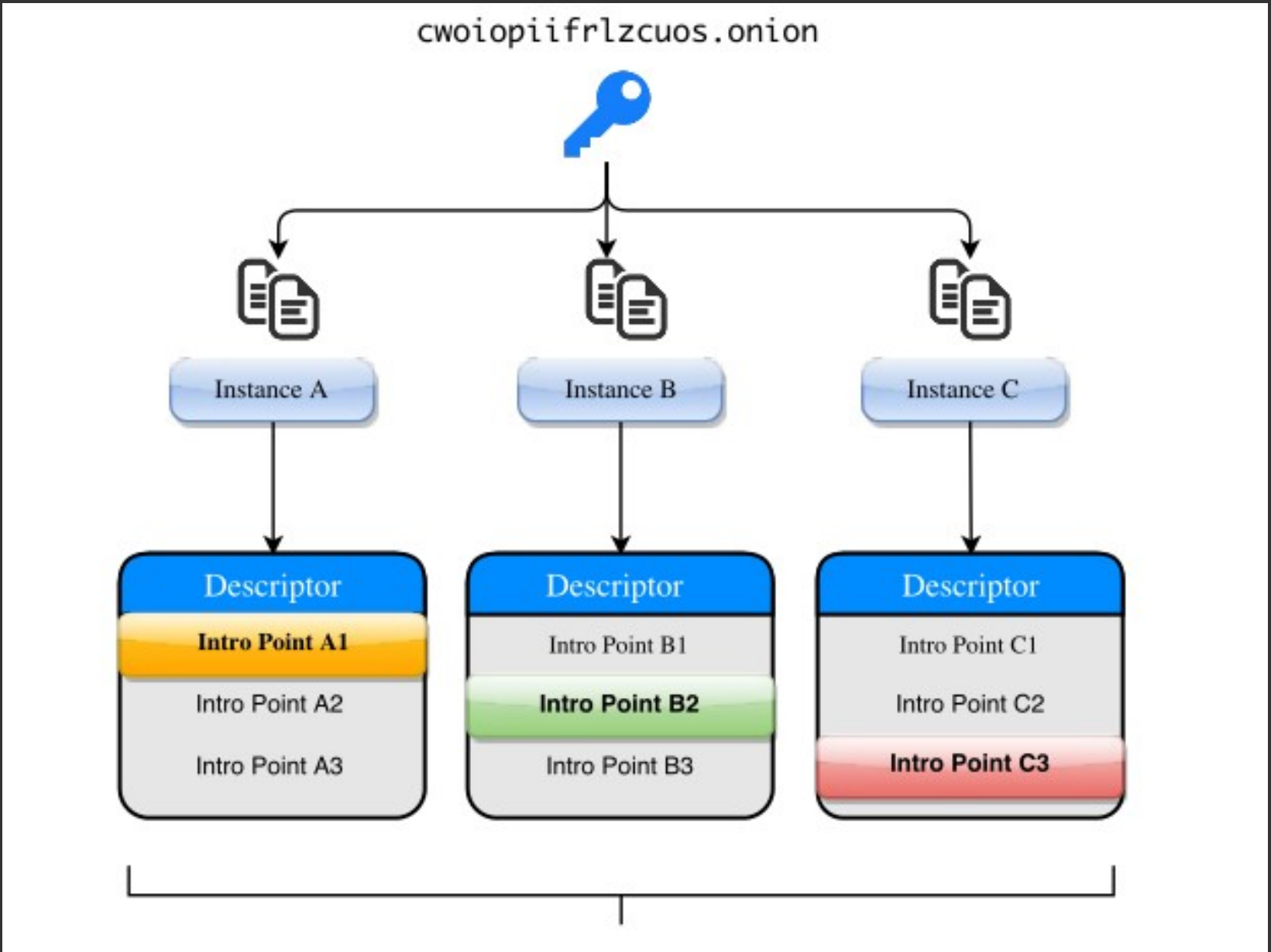
Proposal 252



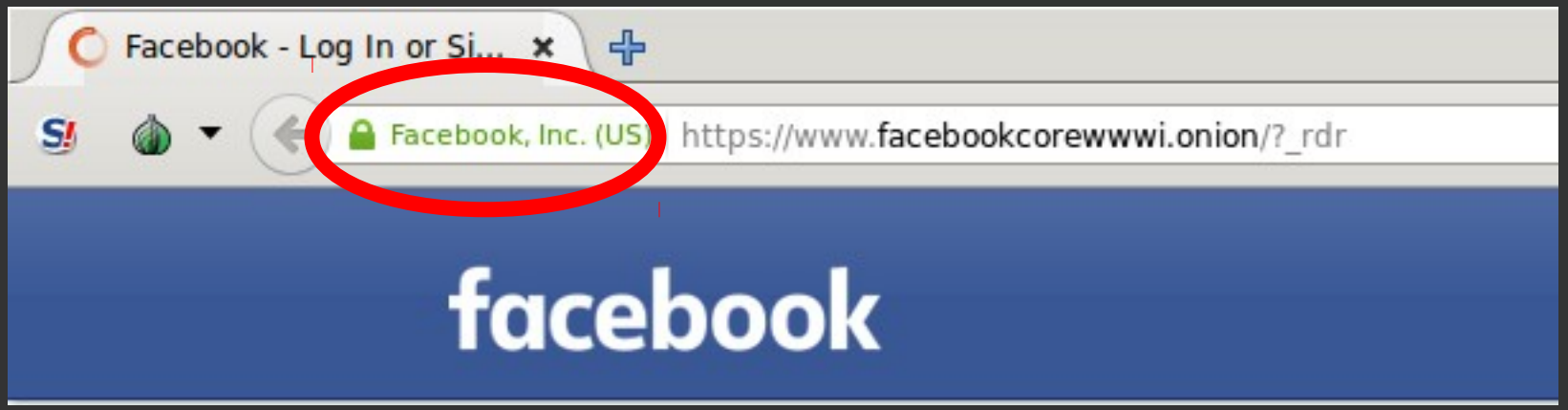
The circuit is **extended** to the service.
No Introduction nor Rendezvous.

OnionBalance - TSoP

https://onionbalance.readthedocs.org



.onion and EV cert



- Browsers know to treat cookies/etc like **TLS**
- Server-side does **not** need to treat `.onion` specially
- With an EV cert, the browser shows the user that it's **really** Facebook

Subdomain support

Proposal 204

`www.facebookcorewwwi.onion`

connects to

`facebookcorewwwi.onion`

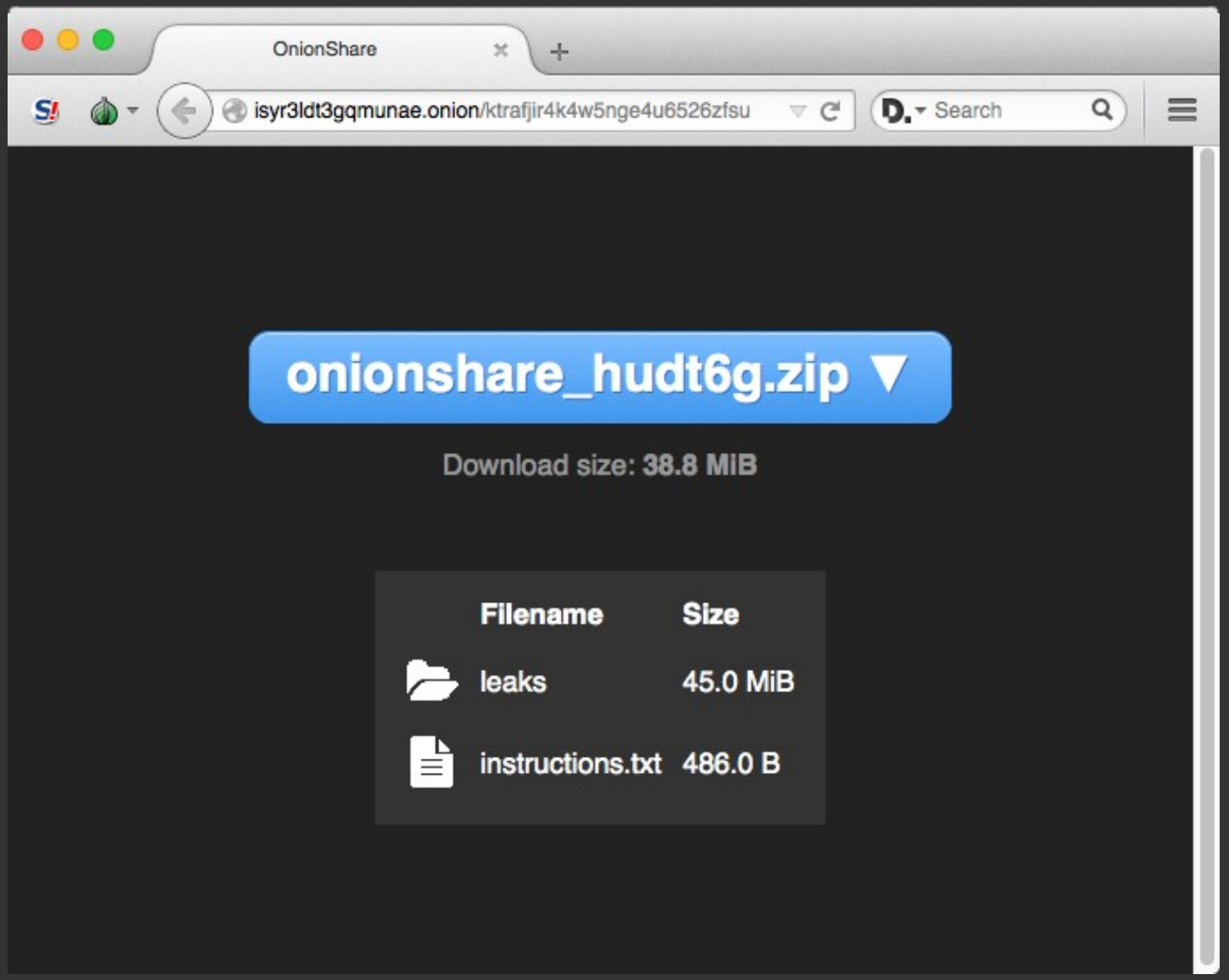
Magic of .onion EV certs!

Onion SSL Certificates have a **magic extra feature**,

The only EV SSL Certs which can use wildcards!

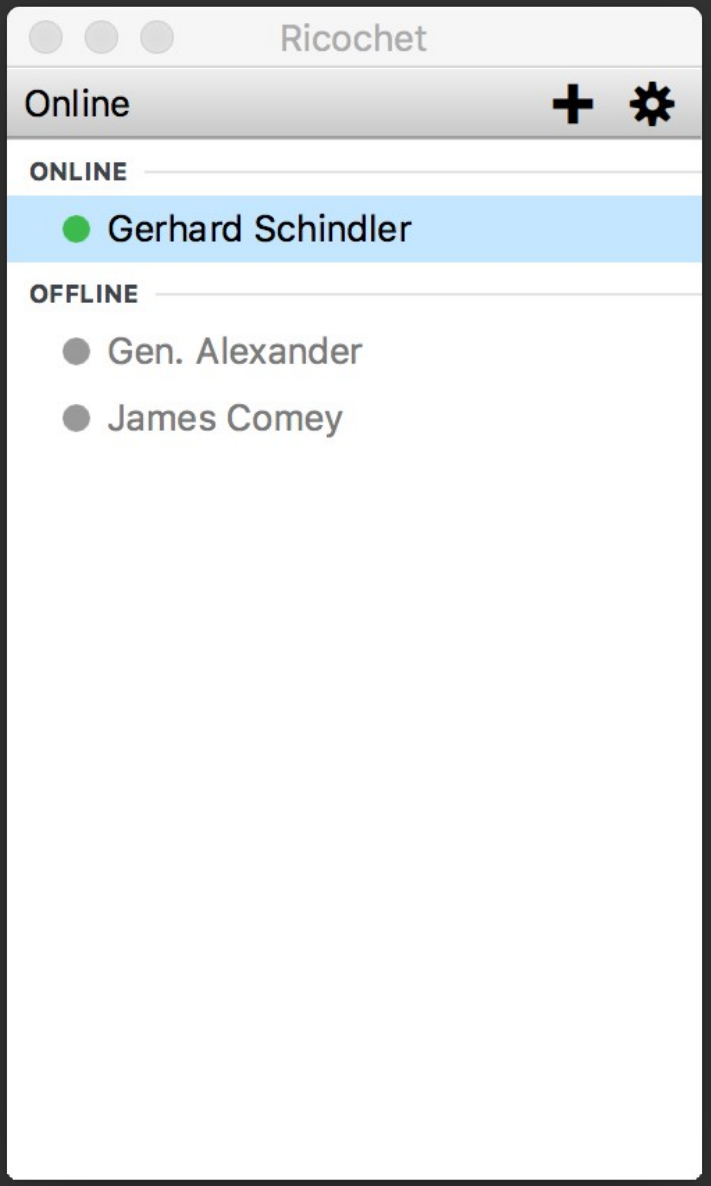
OnionShare

https://onionshare.org/



Ricochet

https://ricochet.im



RFC7686 - 2015

```
Internet Engineering Task Force (IETF)                      J. Appelbaum
Request for Comments: 7686                       The Tor Project, Inc.
Category: Standards Track                                  A. Muffett
ISSN: 2070-1721                                               Facebook
                                                           October 2015


                 The ".onion" Special-Use Domain Name

Abstract

   This document registers the ".onion" Special-Use Domain Name.
```

Setup

```
# apt-get get install tor
# cat << EOF
HiddenServiceDir /var/lib/tor/blog/
HiddenServicePort 80 127.0.0.1:80
EOF
# killall -HUP tor
# cat /var/lib/tor/blog/hostname
7j3ncmar4jm2r3e7.onion
```

⚠ Watch out for leaks! e.g. `/server-status/`

Access control

Proposal 121

Sur le serveur :

`HiddenServiceAuthorizeClient stealth` *`user`*

Sur le client :

`HidServAuth ww2ufwkgxb2kag6t.onion`
☛ `ErQPDEHdNNprvWYCA2vTLR`

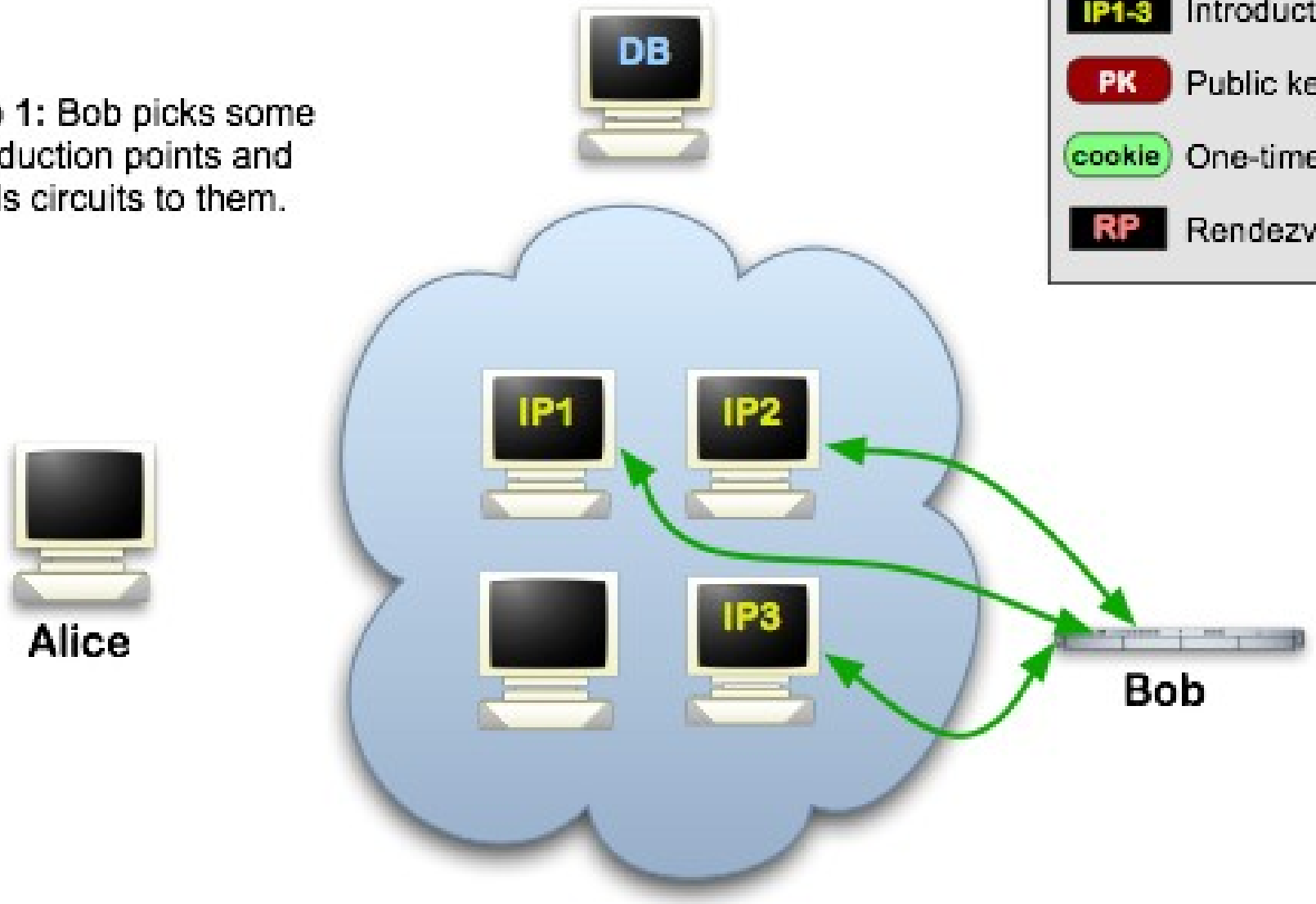
La clé se trouve dans `Tor/Data/hostname`

Current Security Problems

- Onion identity keys are **too short**!
- You can choose relay identity keys to **target** a particular onion service
- You can run relays to **harvest** onion addresses
- **Sybil** attacks remain an issue for Tor in general
- Guard **discovery** attack (proposal 247)
- Website **fingerprinting** for onion services?

Hidden Services: 1

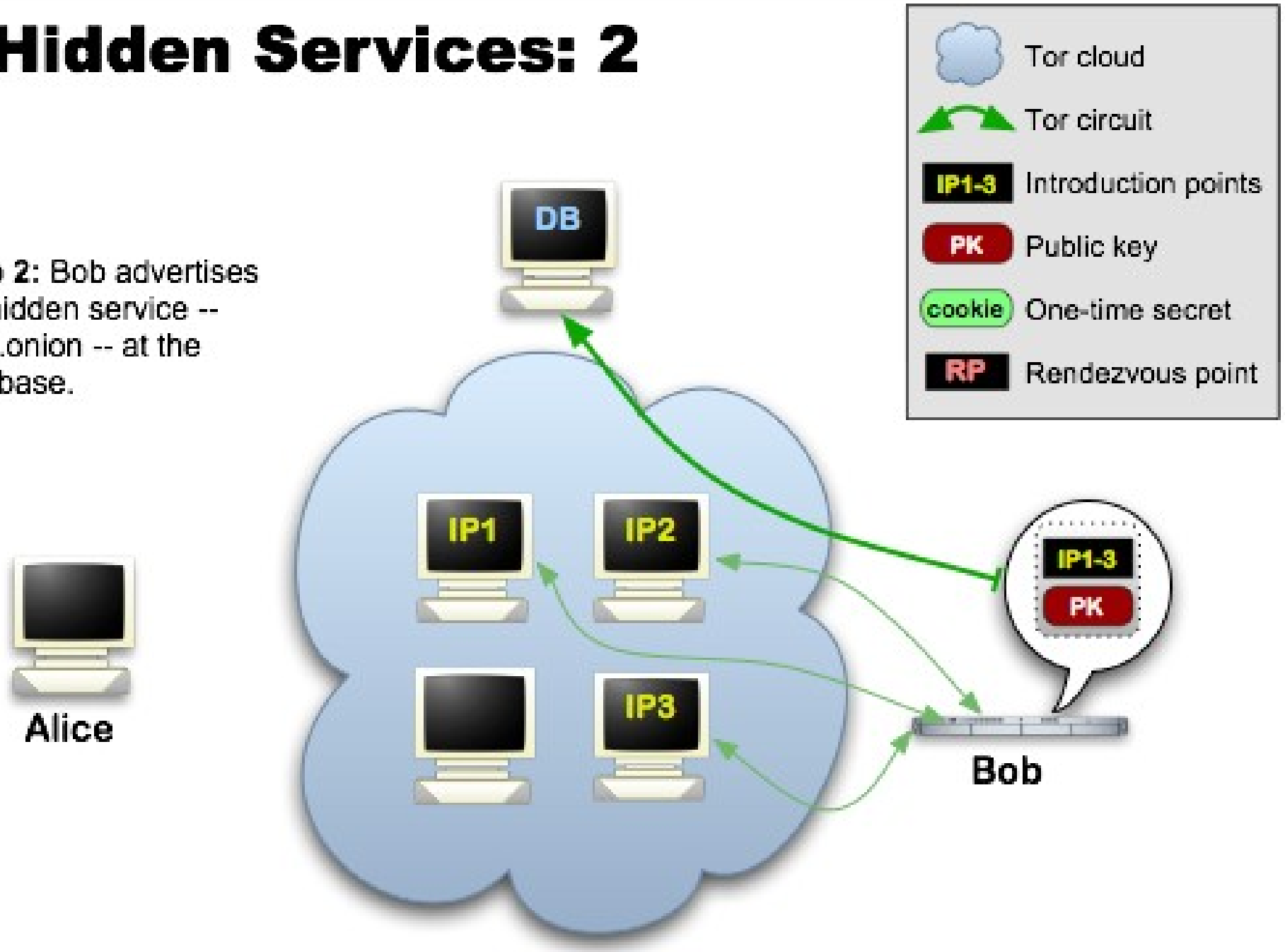
Step 1: Bob picks some introduction points and builds circuits to them.



- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

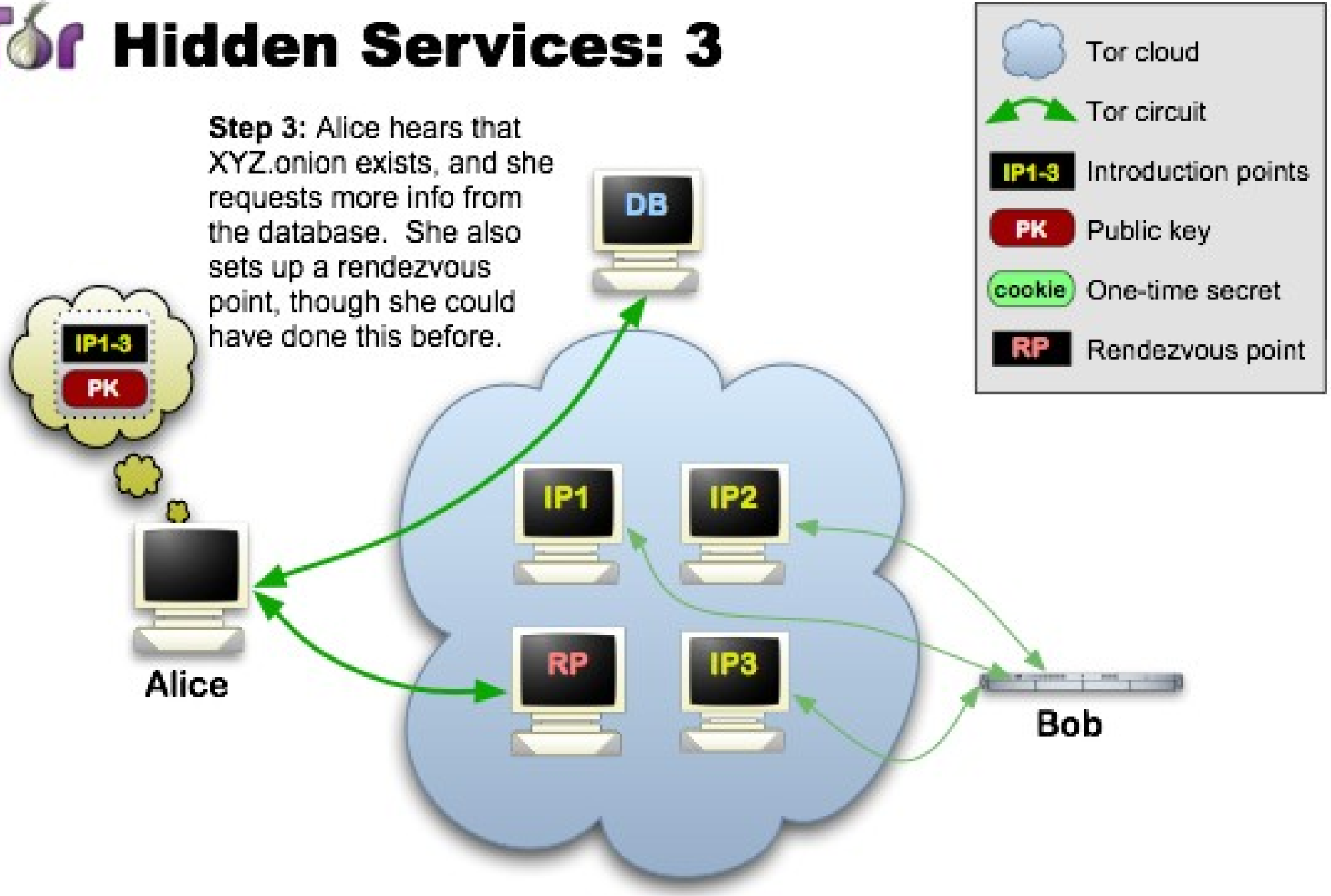
Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



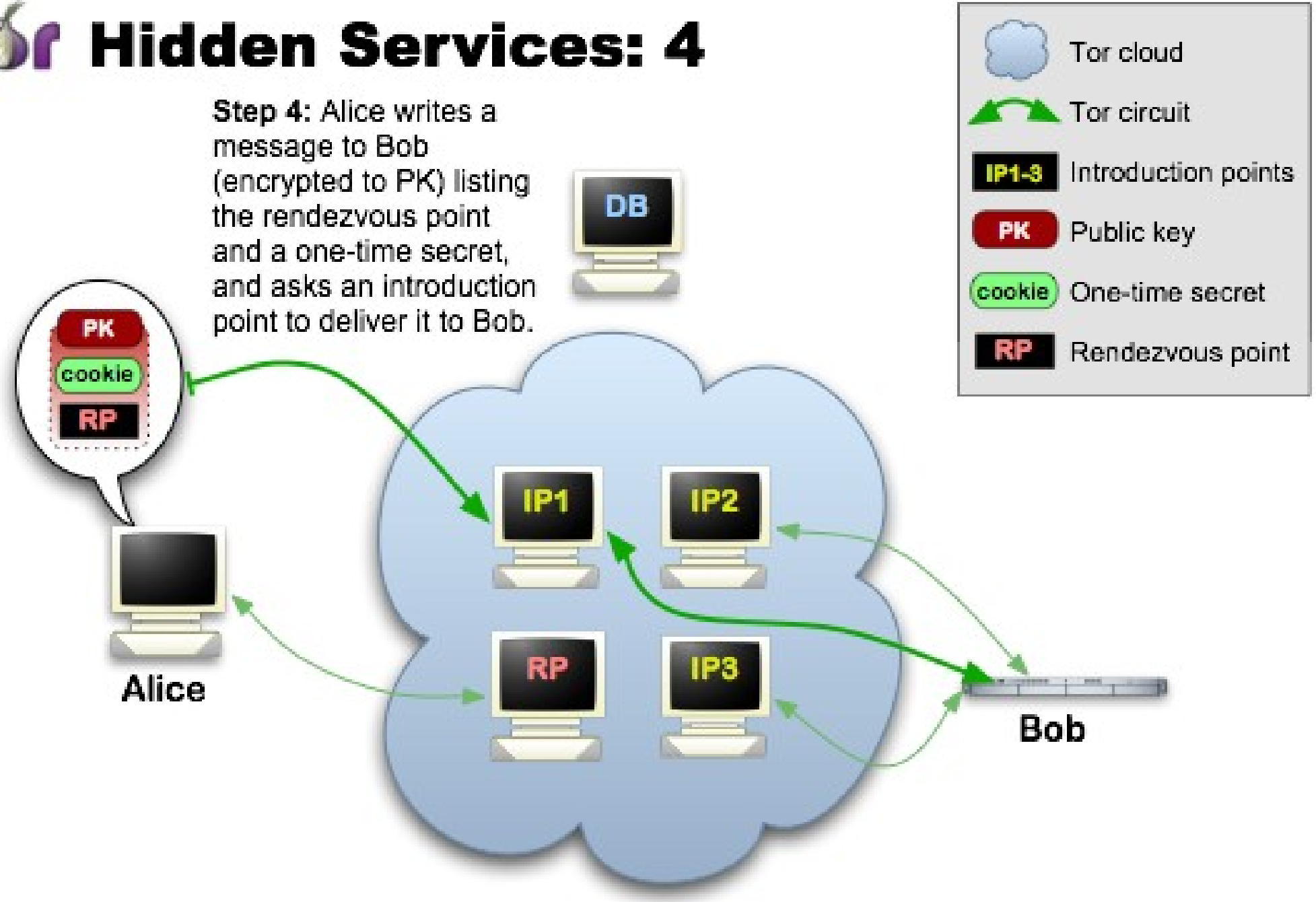
Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



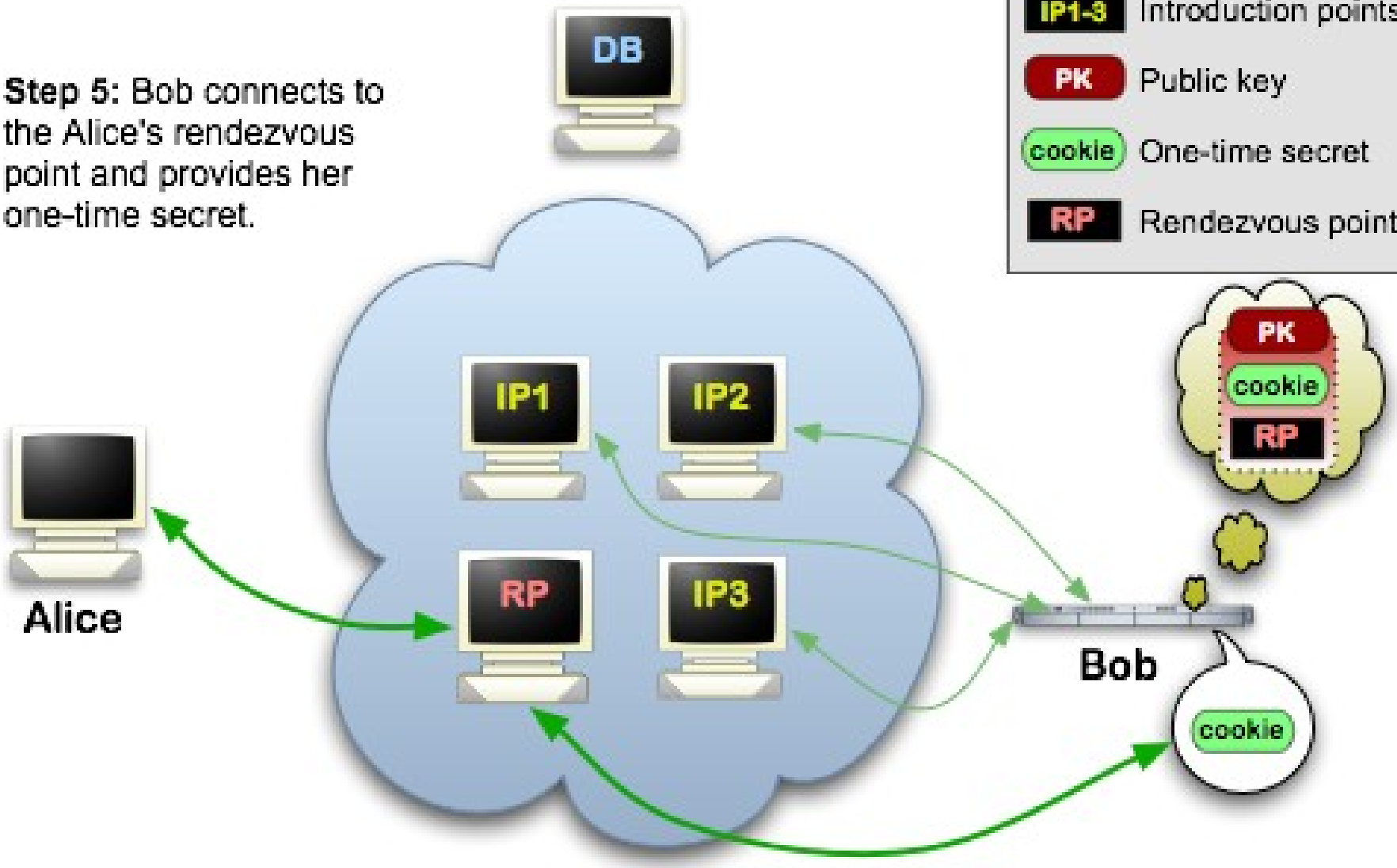
Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



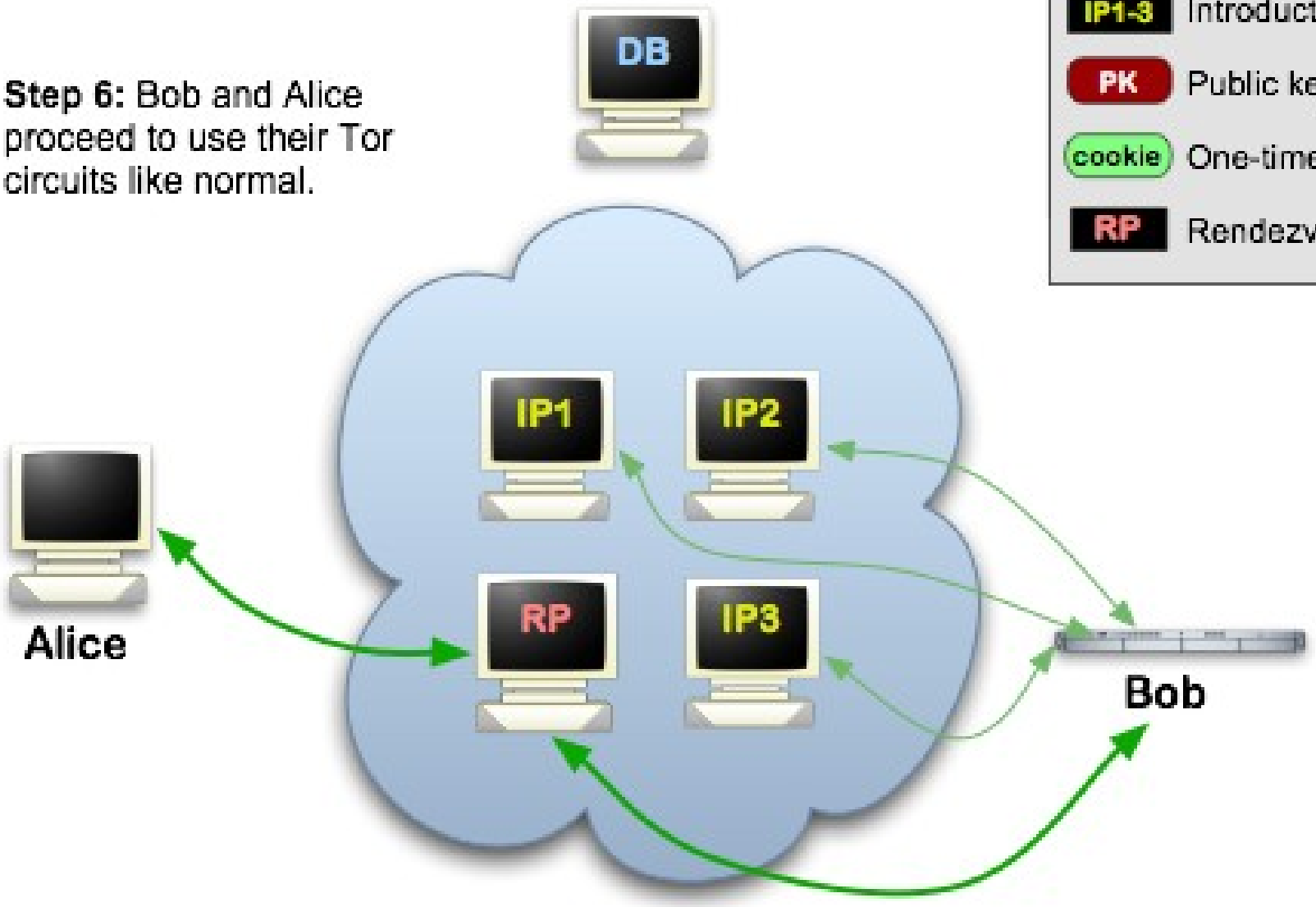
Hidden Services: 5

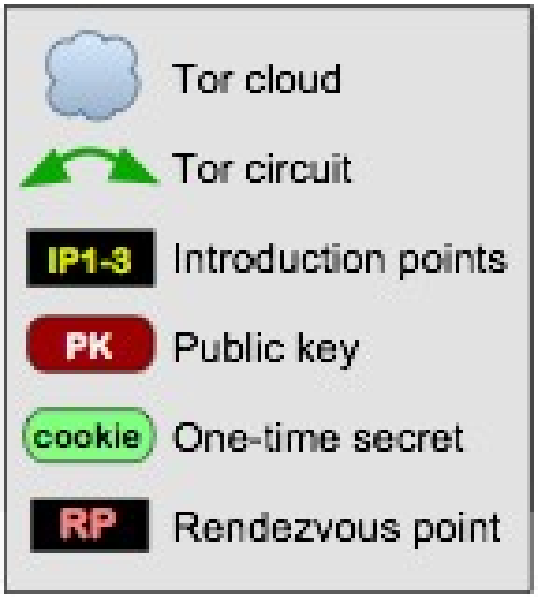
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Hidden Services: 6

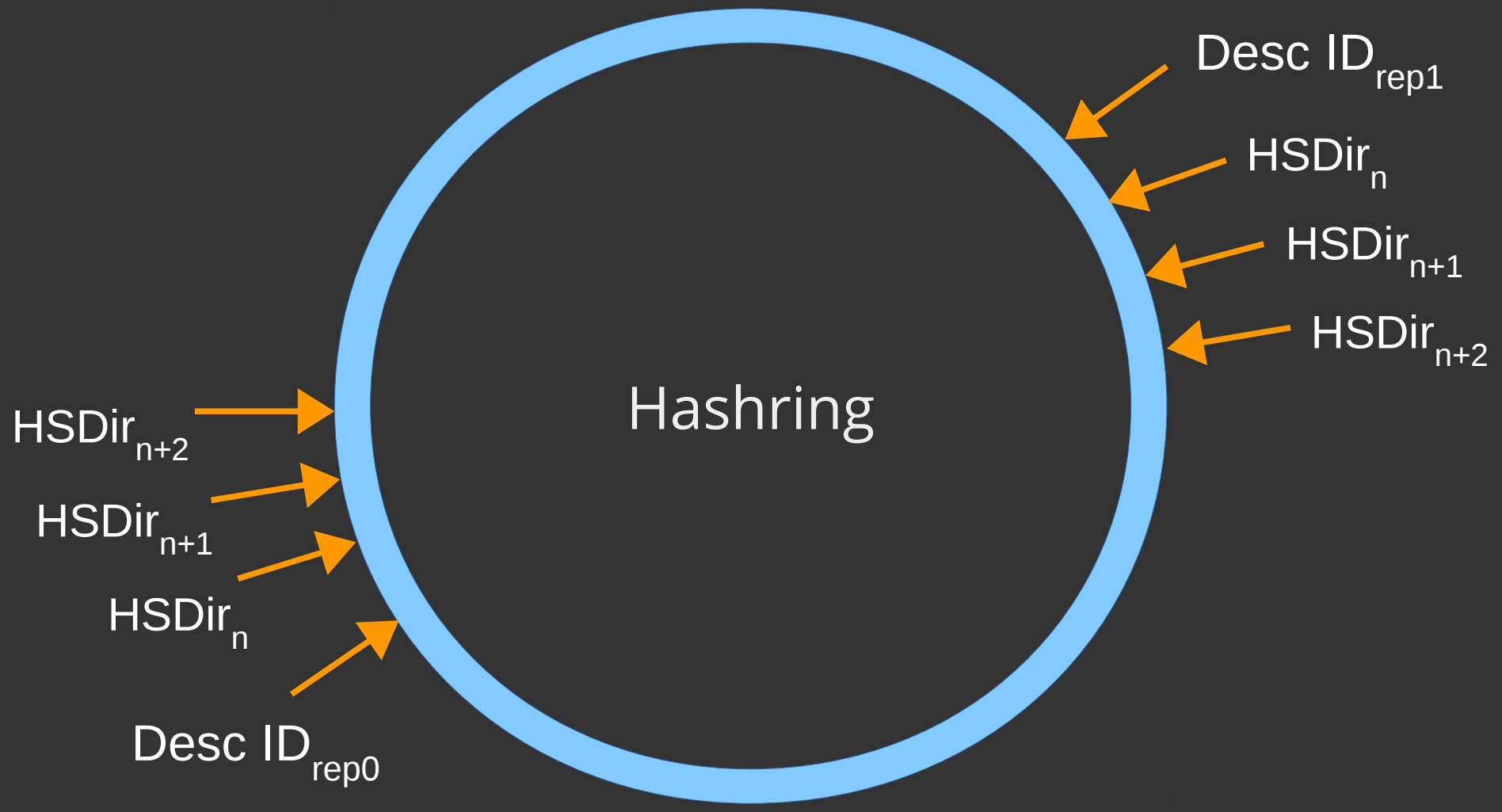
Step 6: Bob and Alice proceed to use their Tor circuits like normal.





HS Directory

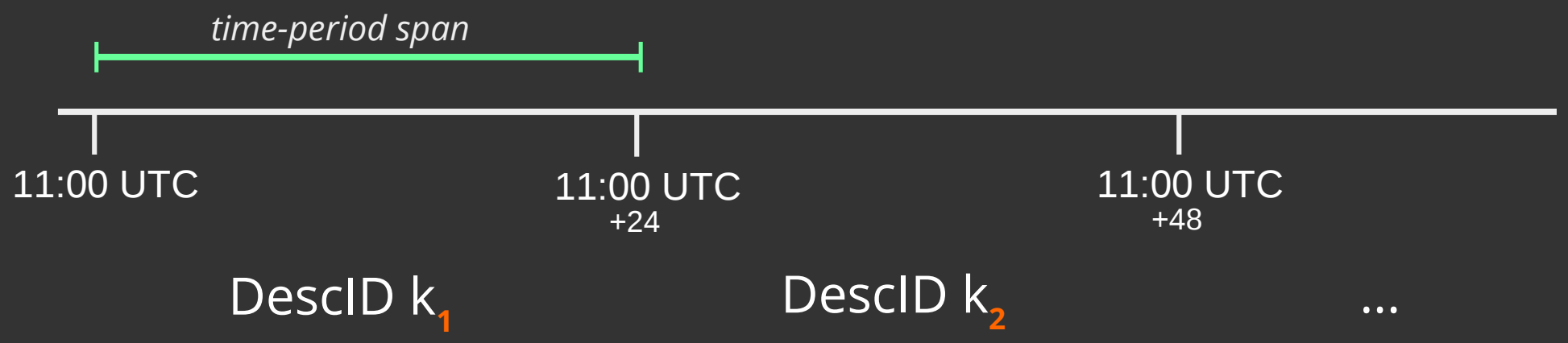
Desc ID = H(onion-address | H(time-period | descriptor-cookie | replica))



HSDir Predictibility

Desc ID = H(onion-address |
H(**time-period** | descriptor-cookie | replica))

Invariant



Next Generation Onion Service (NGOS)

Proposal 224

blob: 8dd30b0e95d4ff5695eebd7a73f894ce825bc587 (plain)

```
Filename: 224-rend-spec-ng.txt
Title: Next-Generation Hidden Services in Tor
Author: Nick Mathewson
Created: 2013-11-29
Status: Draft
```

Created: 2013-11-29

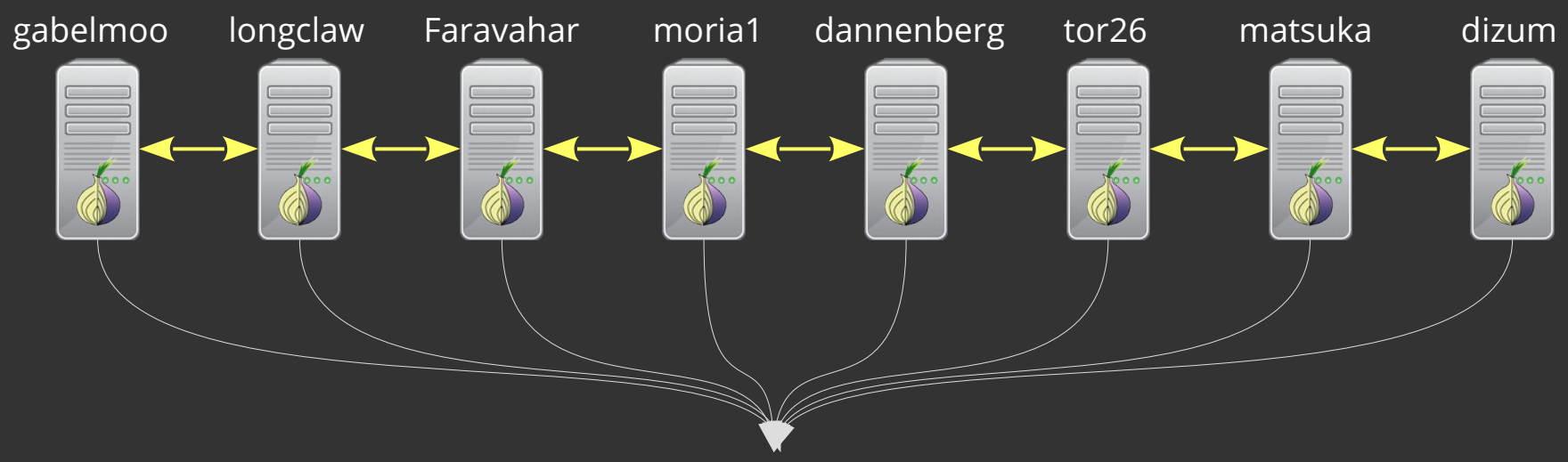
https://blog.torproject.org/blog/mission-montreal-building-next-generation-onion-services

Shared Randomness

Proposal 250

Desc ID = H(onion-address |
H(**time-period** | **random-value** | descriptor-cookie | replica))

Invariant



random-value

(new every 24h)

Better Crypto

Bigger Onion Address

From 16 characters:

`nzh3fv6jc6jskki3.onion`

... to 52 characters:

`a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rffdw9jmntwkdsd.onion`

(ed25519 public key base32 encoded)

... or maybe something else :
`correct-battery-horse-staple-chair-banana-table-river-pizza.onion`
... or another encoding...

Meaningful names for .onion?

Self-authentication is somewhat a lie...

- In DNS: `.onion` must be stored in TXT records (*unless you use the OnionCat trick / fake Ipv6)*
- Shareable address book(s)?
- Namecoin?
- OnioNS?
- Let's Encrypt!?

Onion services vs IP

Global routing requires common policy

- Hierarchical authorities
- Unauthenticated
- Metadata and payload visible to 3rd parties
- … ?

Onion services vs DNS

Human-meaningful

- Hierarchical, decentralized
- Partially authenticated (DNSSEC)
- Metadata and payload visible to 3rd parties
- … ?

Thanks!

Lunar
lunar@torproject.org

0603 CCFD 9186 5C17 E88D
4C79 8382 C95C 2902 3DF9