Wild and cultivated .onions

A ground survey + recipes & planting tips

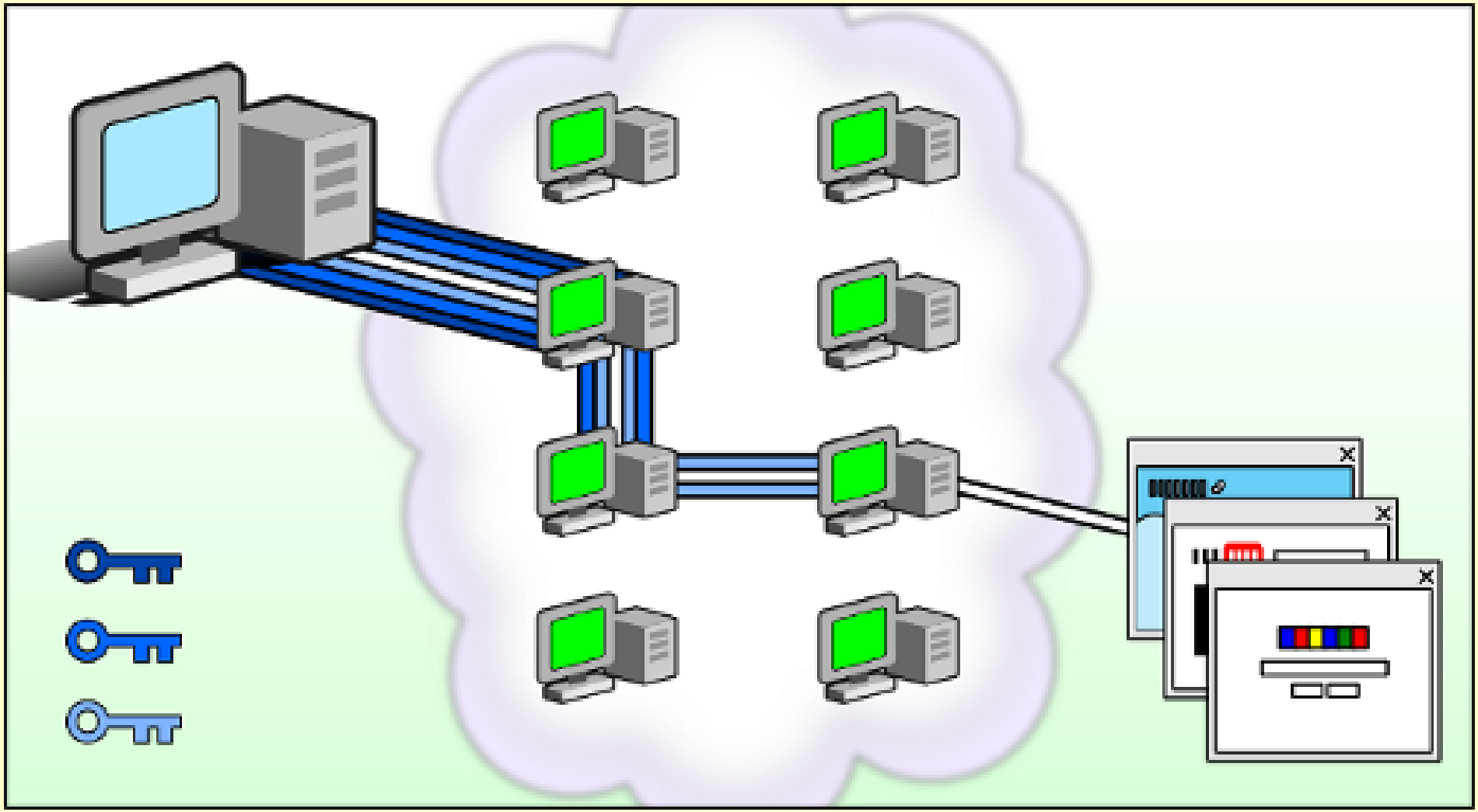
by: Dave the Onion Eater

whoami

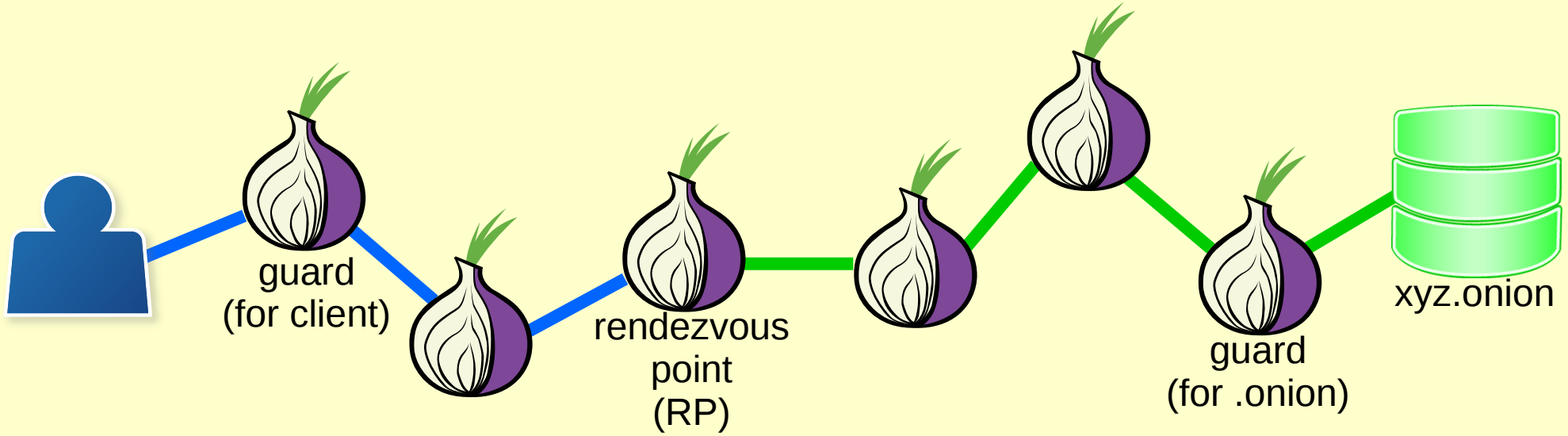
- “Daily” TorBrowser user (main browser)
- Common Tor user beyond the browser
- `.onion` eater
- Privacy advocate
- Independent security impostor, amateur 

Disclaimer:
This presentation is produced independently from the Tor® anonymity software and carries no guarantee from The Tor Project about quality, suitability, or anything else.

Tor: onion routing

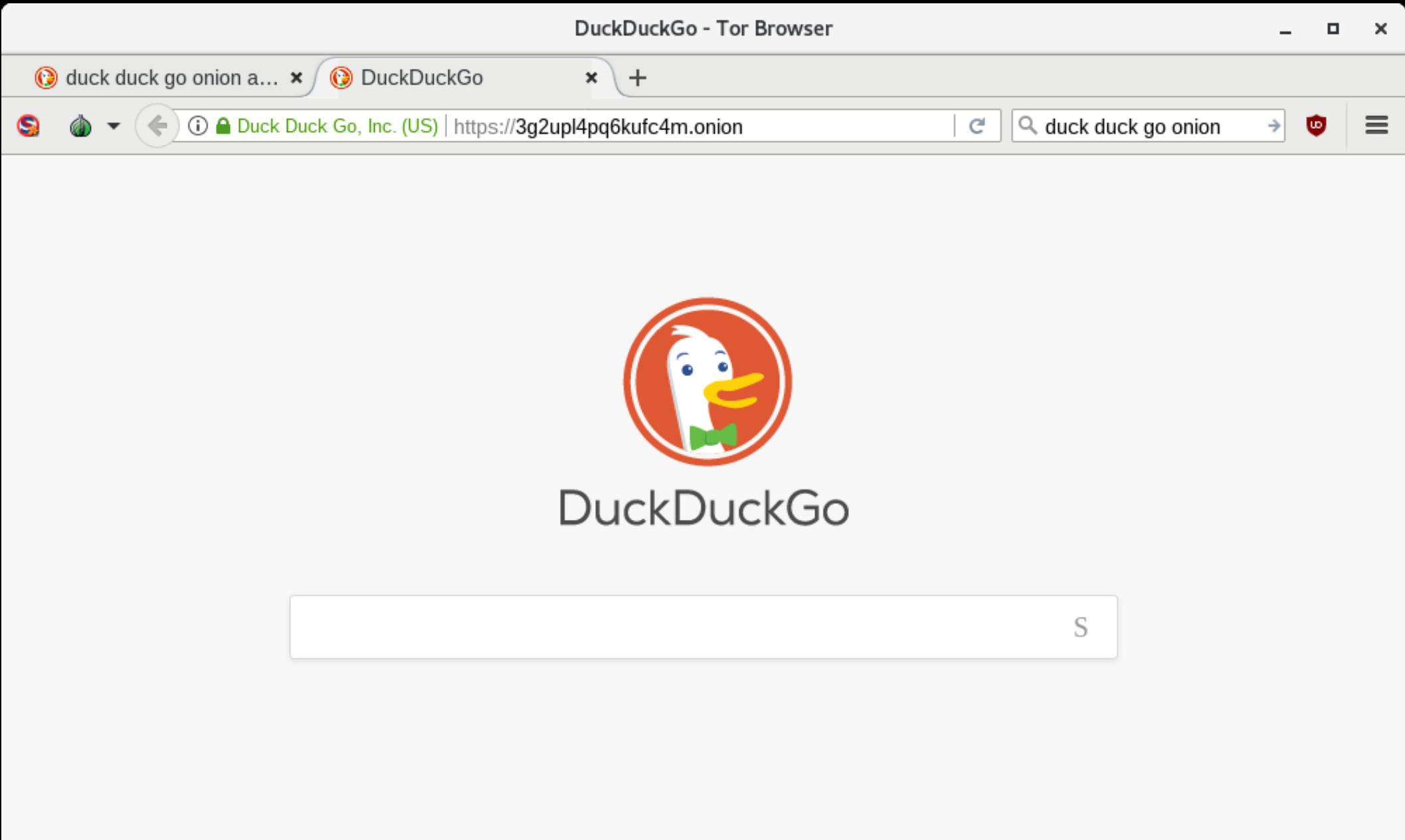


Onion Services – Intro



- User visits xyz.onion without exiting the Tor network (e.g. no IP resolution)
- Originally called “Hidden Services”

In the browser...



Onion Services – History/Future

- 2004 – first added to tor
- ~2006 – “Hidden services” notoriety started perhaps by leak for ethics of pharm. company

- Dec 2007 – switch to decentralized Onion Services directory (distributed hash table / DHT)
- …
- Nov 2013 – first draft of proposal for next-generation Onion Services (prop 224)
- …
- Sep 2015 – RFC 7686 approved; reserves .onion
- …
- Dec 2017 – anticipated next-generation uplift ready for Tor stable

{ scope }

- tor .onion on Linux
  - public, non-anonymous
  - private
- .onion user (any common OS, Debian easiest)

- **NOT** public + anonymous AKA “hidden”
- not much on next-generation

“This is not only *decentralised* and *distributed*, it is ***disintermediated*** communication: there’s no DNS-name to be censored, nor spoofed nor hijacked, there’s no fixed network route to be blocked, there’s no firewall to be bypassed nor a single big ISP router to be DDoSed by some attacker.

In short: *Tor is a very attractive proposition for secure networking*.”

– Alec Muffett

https://medium.com/@alecmuffett/tor-is-end-to-end-encryption-for-computers-to-talk-to-other-computers-34e41d81c9e2

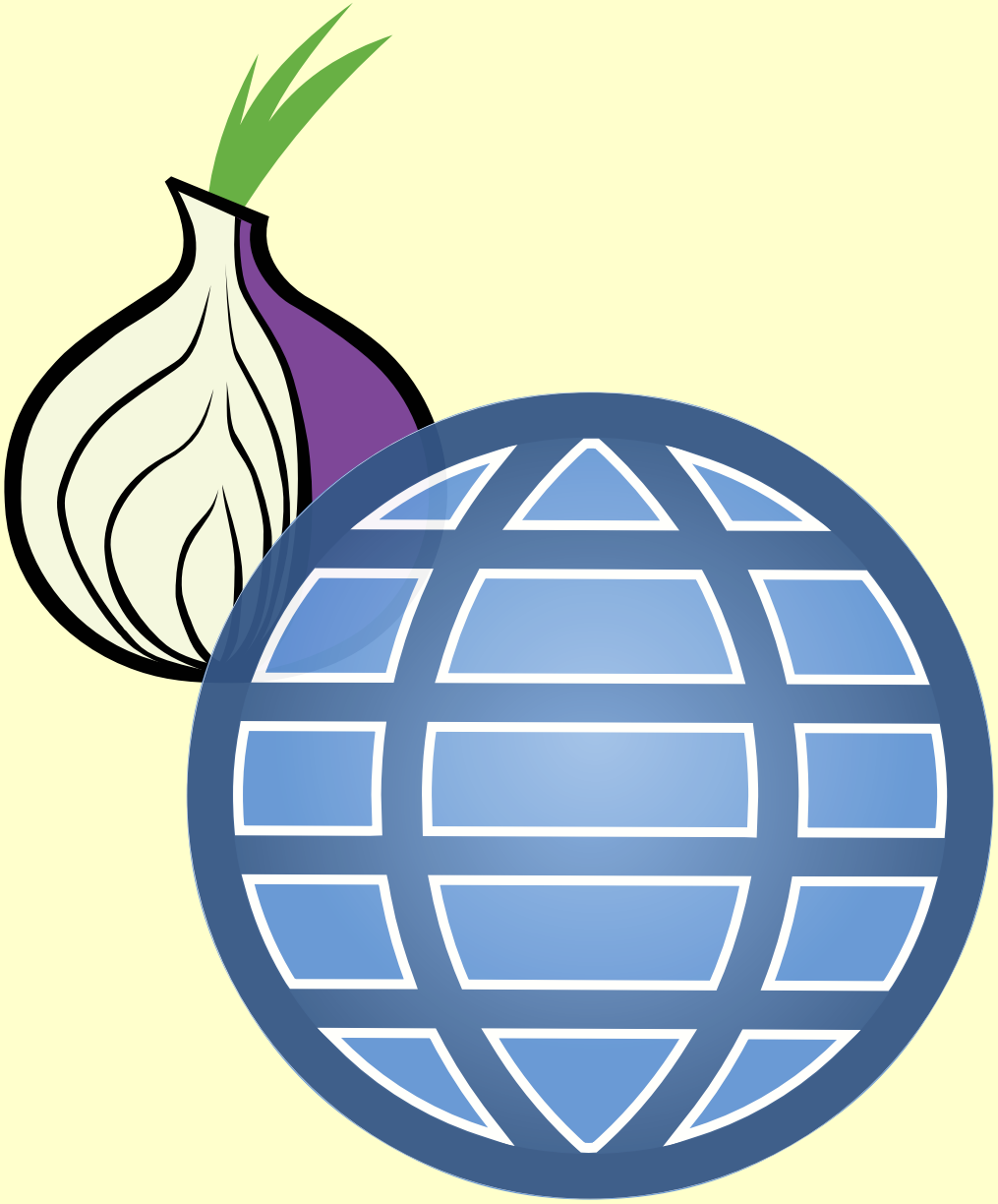
.onion properties

- address is self-authenticating ***to key***
- NAT piercing =>
  - reduce attack surface
- onion-to-onion encryption with PFS *(perfect forward secrecy)*
- ~DDoS protection
- censorship resistance

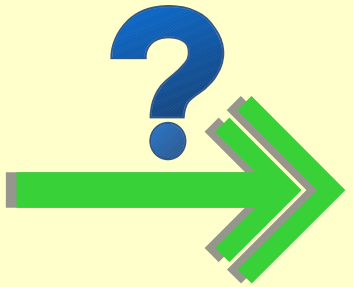
- avoid exit node =>
  - **security**: defeat MITM, BGP hijacking, bad CAs, bad DNS, ...
  - **performance**: reduce load on exits... (potentially) faster, scales better
  - **privacy**: avoid protocol leaks
  - **...**

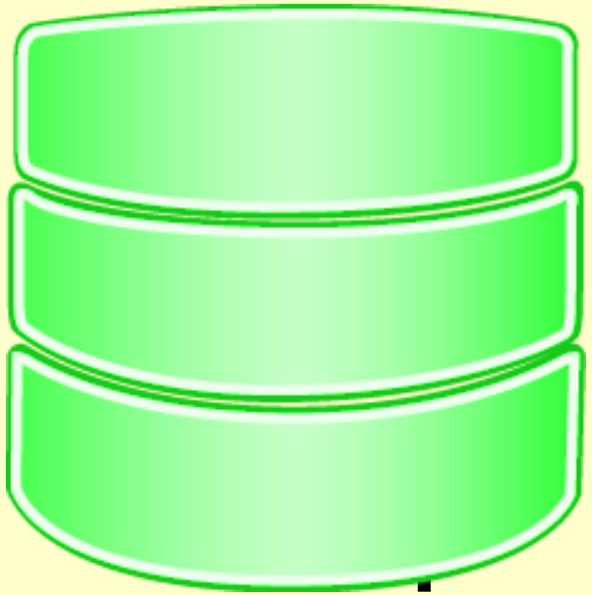
DEMO TIME

ground survey: public



Bootstrapping?
Discoverability?





wikipedia.org

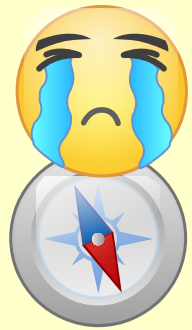
xyz.onion

here be dragons

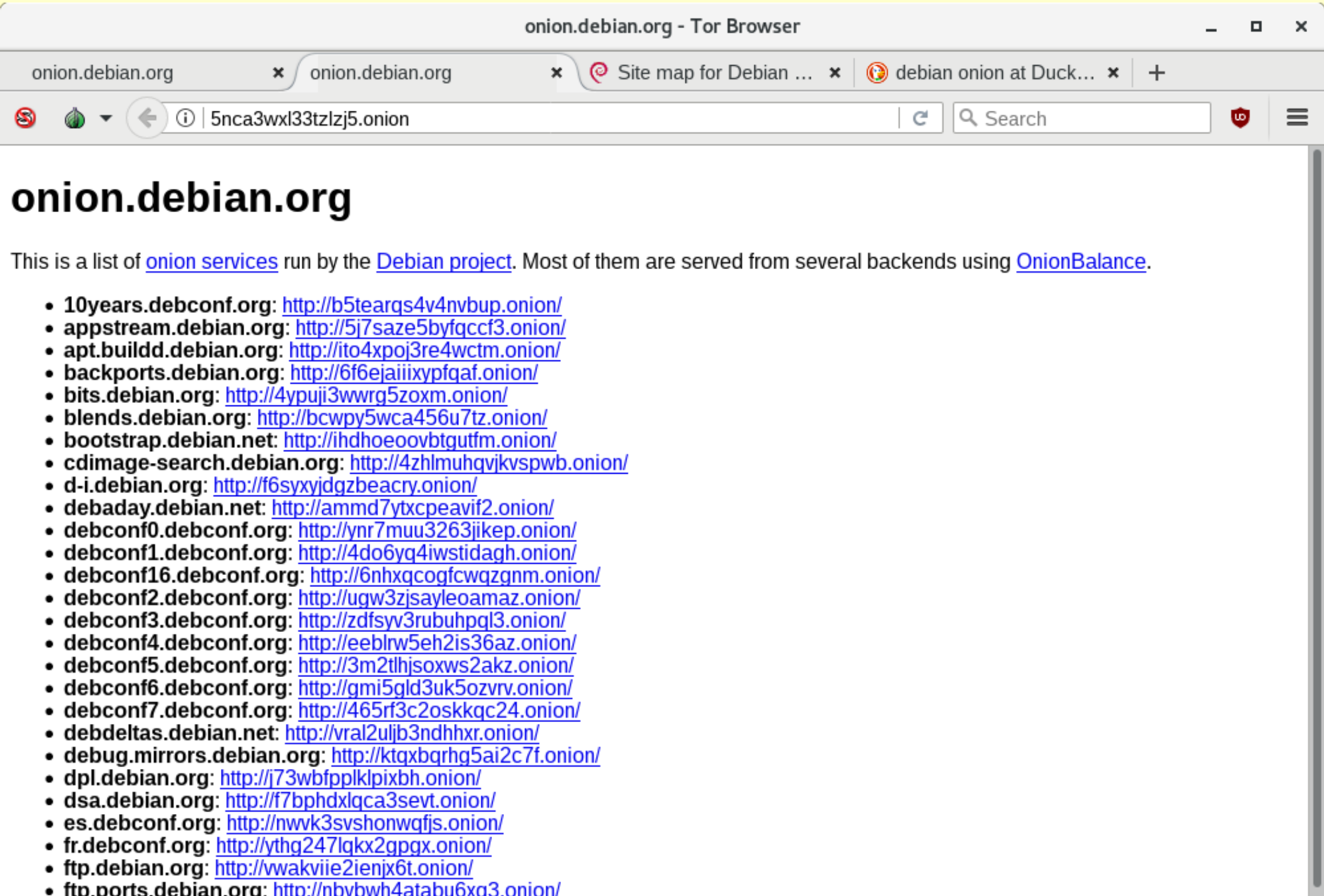
Bootstrapping? Discoverability?

Almost no consistency, poor UX, poor assurance

- https://onion.domain.tld
  (e.g. https://onion.debian.org)
- 1st-party “clearnet” website
  - footer
  - notification for tor users – blocks “clearnet”
  - seamless HTTP redirect for tor users – blocks “clearnet”
  - GPG-signed list/info – freshness?
  - buried
  - wiki / forum posts / comments / etc.
- 3rd-party website(s), list(s), …



Bootstrapping? Discoverability?

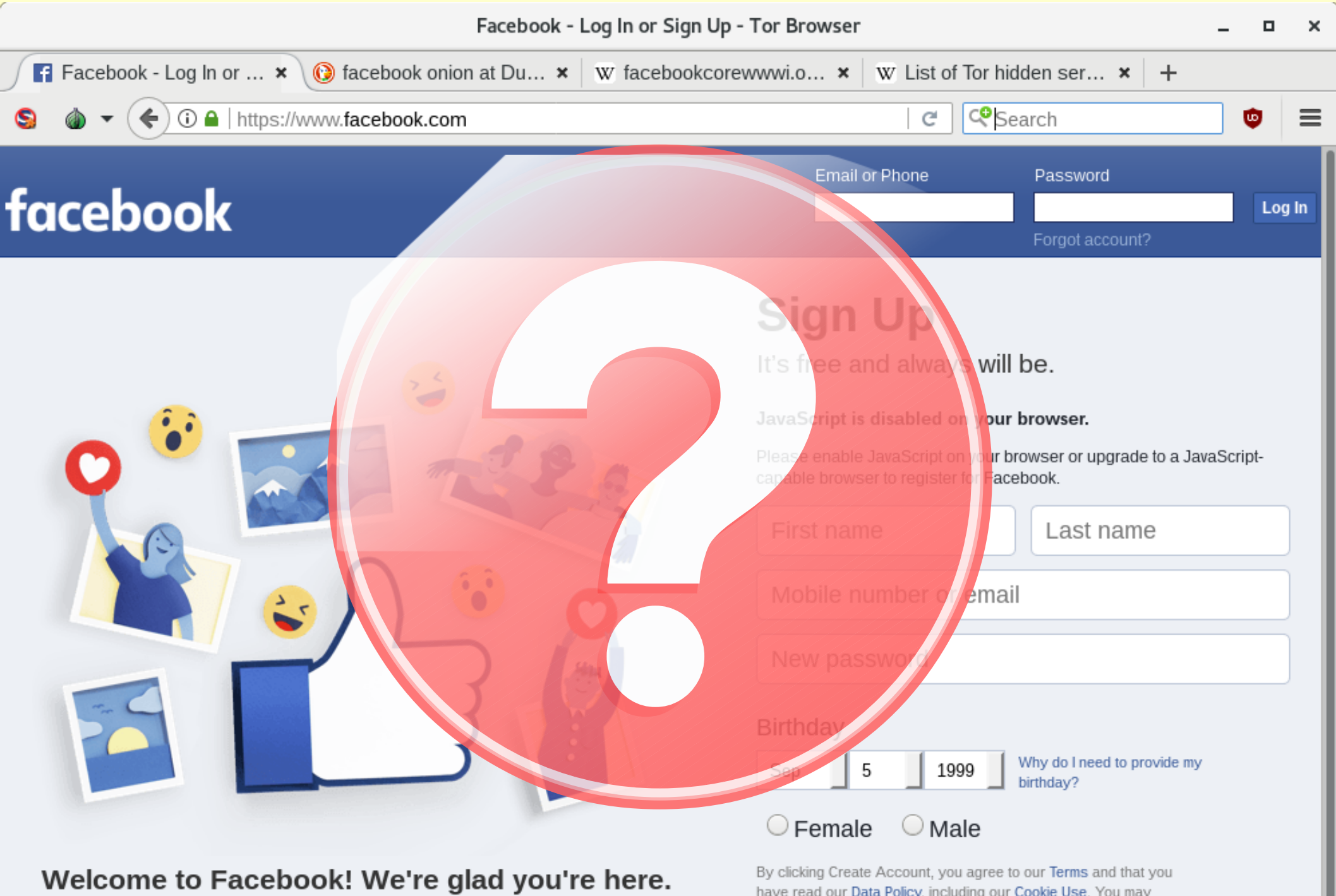


onion.debian.org

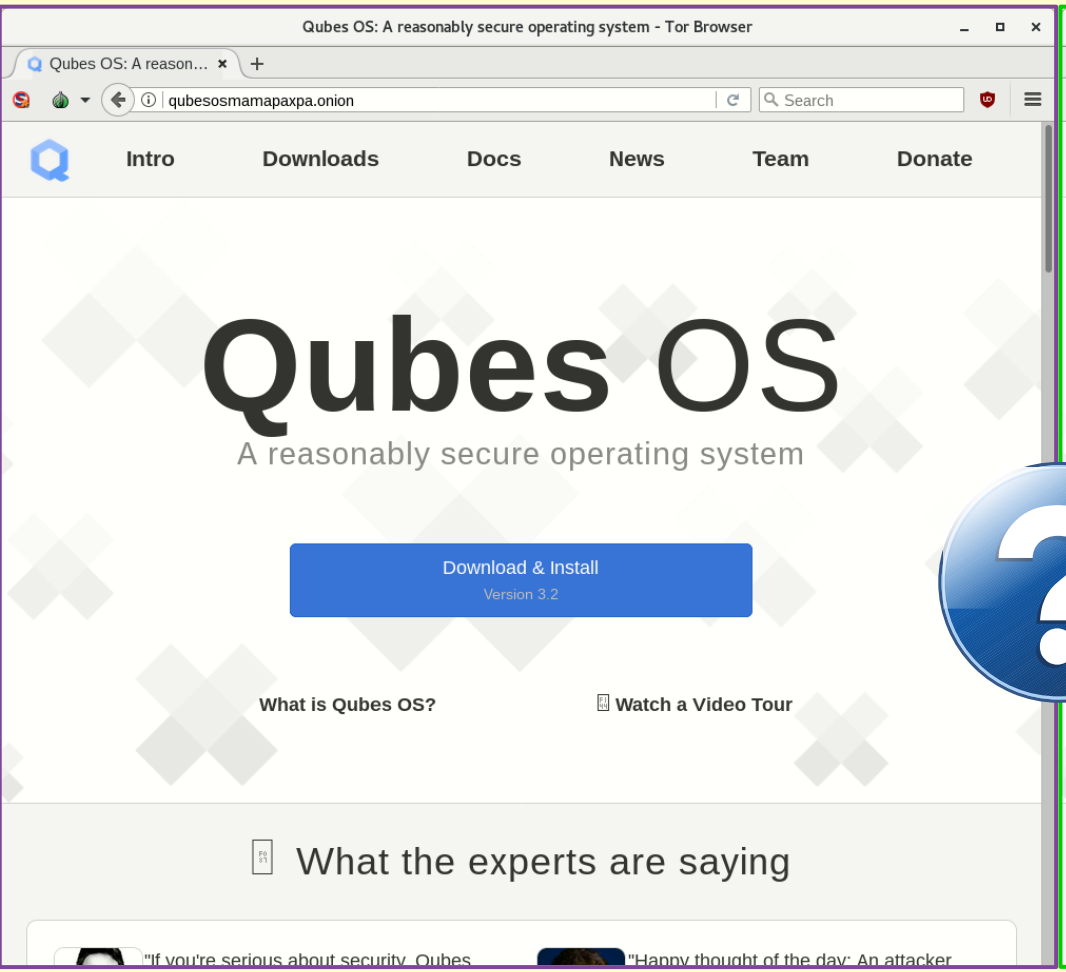
This is a list of onion services run by the Debian project. Most of them are served from several backends using OnionBalance.

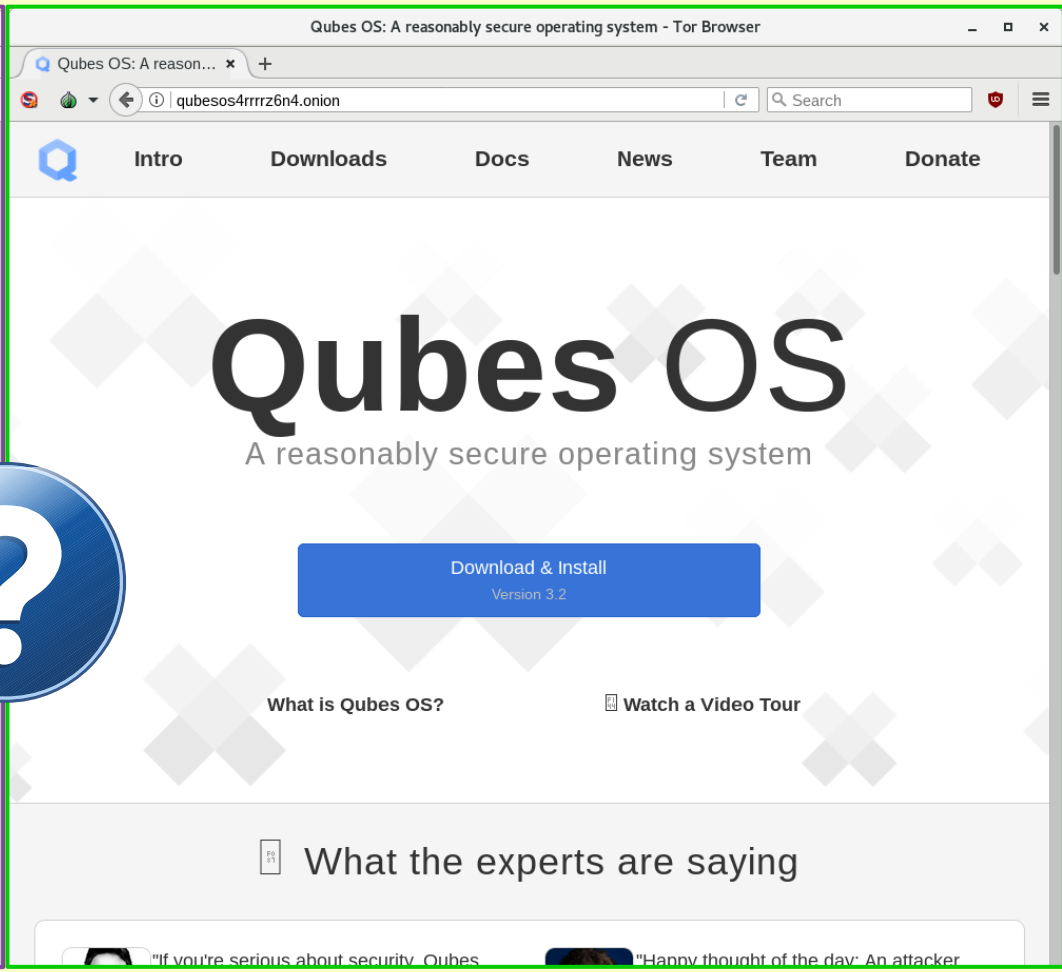
- **10years.debconf.org**: http://b5tearqs4v4nvbup.onion/
- **appstream.debian.org**: http://5j7saze5byfqccf3.onion/
- **apt.buildd.debian.org**: http://ito4xpoj3re4wctm.onion/
- **backports.debian.org**: http://6f6ejaiiixypfqaf.onion/
- **bits.debian.org**: http://4ypuji3wwrg5zoxm.onion/
- **blends.debian.org**: http://bcwpy5wca456u7tz.onion/
- **bootstrap.debian.net**: http://ihdhoeoovbtgutfm.onion/
- **cdimage-search.debian.org**: http://4zhlmuhqvjkvspwb.onion/
- **d-i.debian.org**: http://f6syxyjdgzbeacry.onion/
- **debaday.debian.net**: http://ammd7ytxcpeavif2.onion/
- **debconf0.debconf.org**: http://ynr7muu3263jikep.onion/
- **debconf1.debconf.org**: http://4do6yq4iwstidagh.onion/
- **debconf16.debconf.org**: http://6nhxqcogfcwqzgnm.onion/
- **debconf2.debconf.org**: http://ugw3zjsayleoamaz.onion/
- **debconf3.debconf.org**: http://zdfsyv3rubuhpql3.onion/
- **debconf4.debconf.org**: http://eeblrw5eh2is36az.onion/
- **debconf5.debconf.org**: http://3m2tlhjsoxws2akz.onion/
- **debconf6.debconf.org**: http://gmi5gld3uk5ozvrv.onion/
- **debconf7.debconf.org**: http://465rf3c2oskkqc24.onion/
- **debdeltas.debian.net**: http://vral2uljb3ndhhxr.onion/
- **debug.mirrors.debian.org**: http://ktqxbqrhg5ai2c7f.onion/
- **dpl.debian.org**: http://j73wbfpplklpixbh.onion/
- **dsa.debian.org**: http://f7bphdxlqca3sevt.onion/
- **es.debconf.org**: http://nwvk3svshonwqfjs.onion/
- **fr.debconf.org**: http://ythg247lqkx2gpgx.onion/
- **ftp.debian.org**: http://vwakviie2ienjx6t.onion/
- **ftp.ports.debian.org**: http://nbybwh4atabu6xq3.onion/

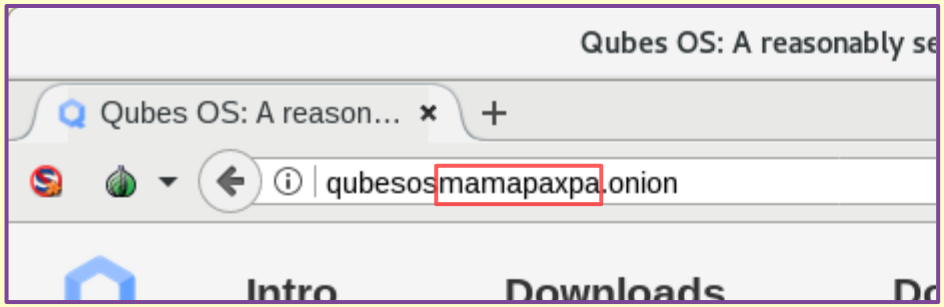
Bootstrapping? Discoverability?

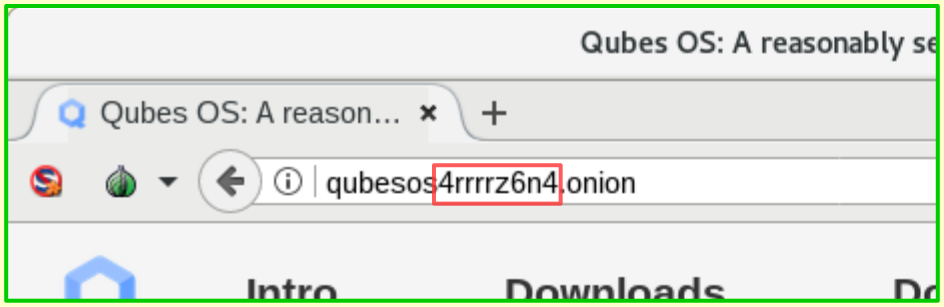


Bootstrapping? Discoverability?

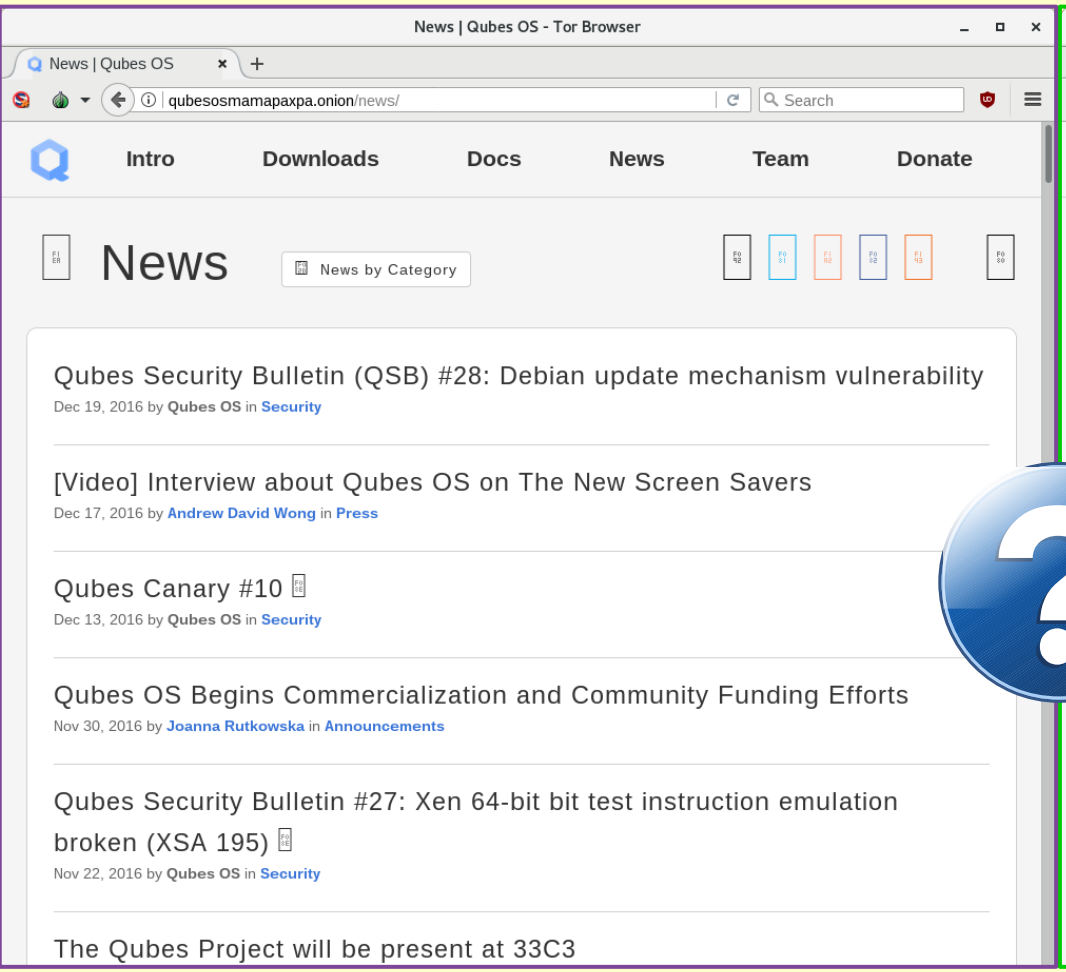


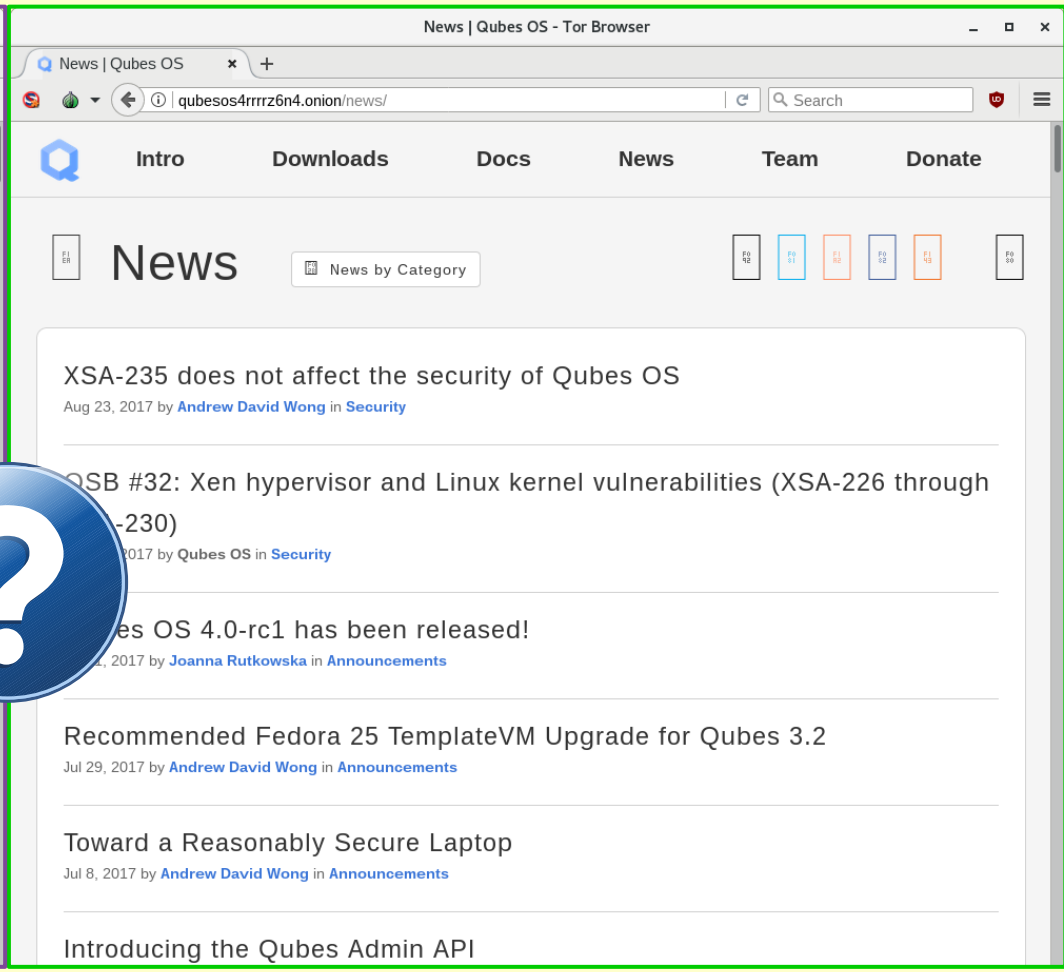






Bootstrapping? Discoverability?





Bootstrapping? Discoverability?

Bootstrapping may even be **unsafe**...

...when not done over Tor...

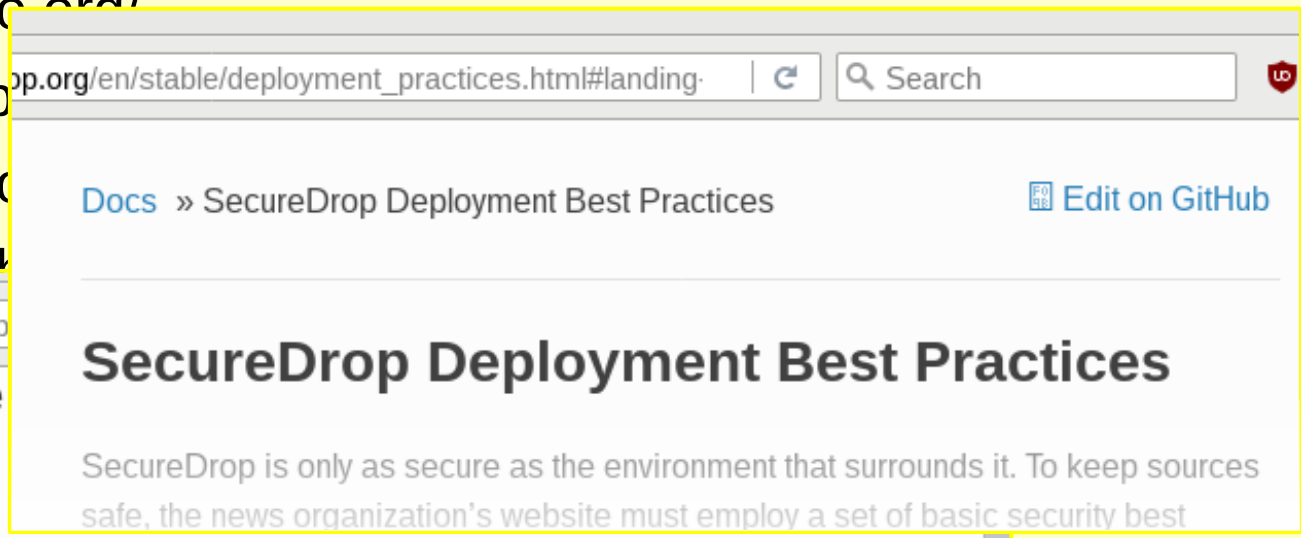
- SNI anyone? *(**S**erver **N**ame **I**ndication in TLS)*
  - https://securedrop.theguardian.com/
  - https://securedrop.pogo.org/
  - https://securedrop.propublica.org/
  - https://securedrop.radio24syv.dk/
  - https://securedrop.dagbladet.no/
  - https://sec.theglobeandmail.com/securedrop/
  - https://sourceanonyme.radio-canada.ca/
  - https://contact.buzzfeed.com/
  - https://newstips.sfchronicle.com/
  - https://newstips.usatoday.com/securedrop.html
  - https://www.nytimes.com/tips#securedrop

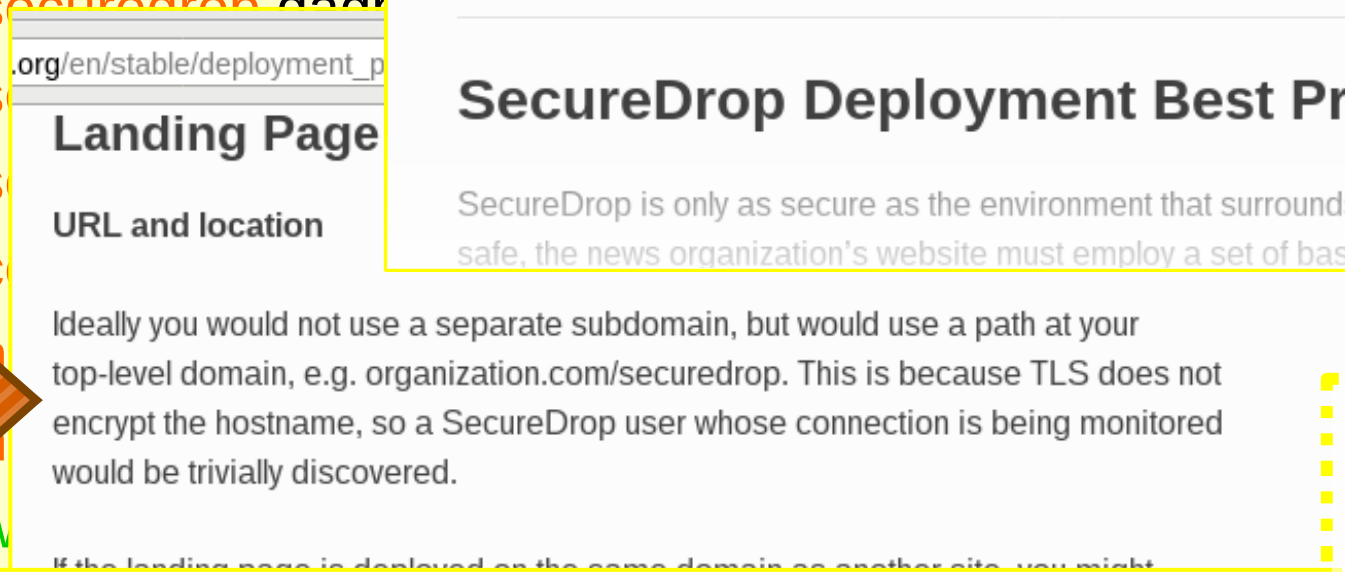
Bootstrapping? Discoverability?

Bootstrapping may even be **unsafe**...

...when not done over Tor...

- SNI anyone? *(**S**erver **N**ame **I**ndication in TLS)*
  - https://securedrop.theguardian.com/
  - https://securedrop.pogo.org/
  - https://securedrop.prop
  - https://securedrop.radio
  - https://s
  - https://s
  - https://s
  - https://c
  - https://w

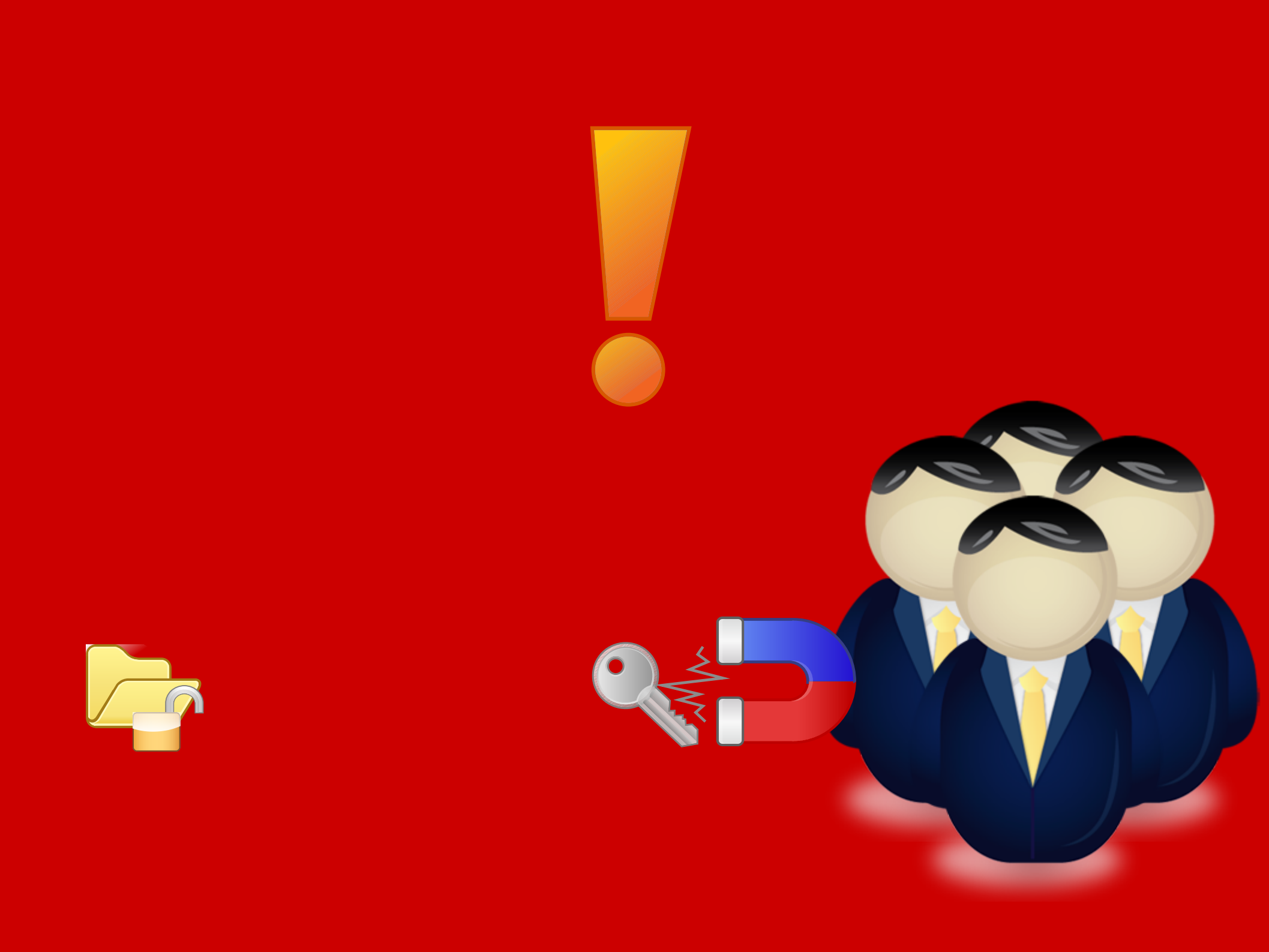




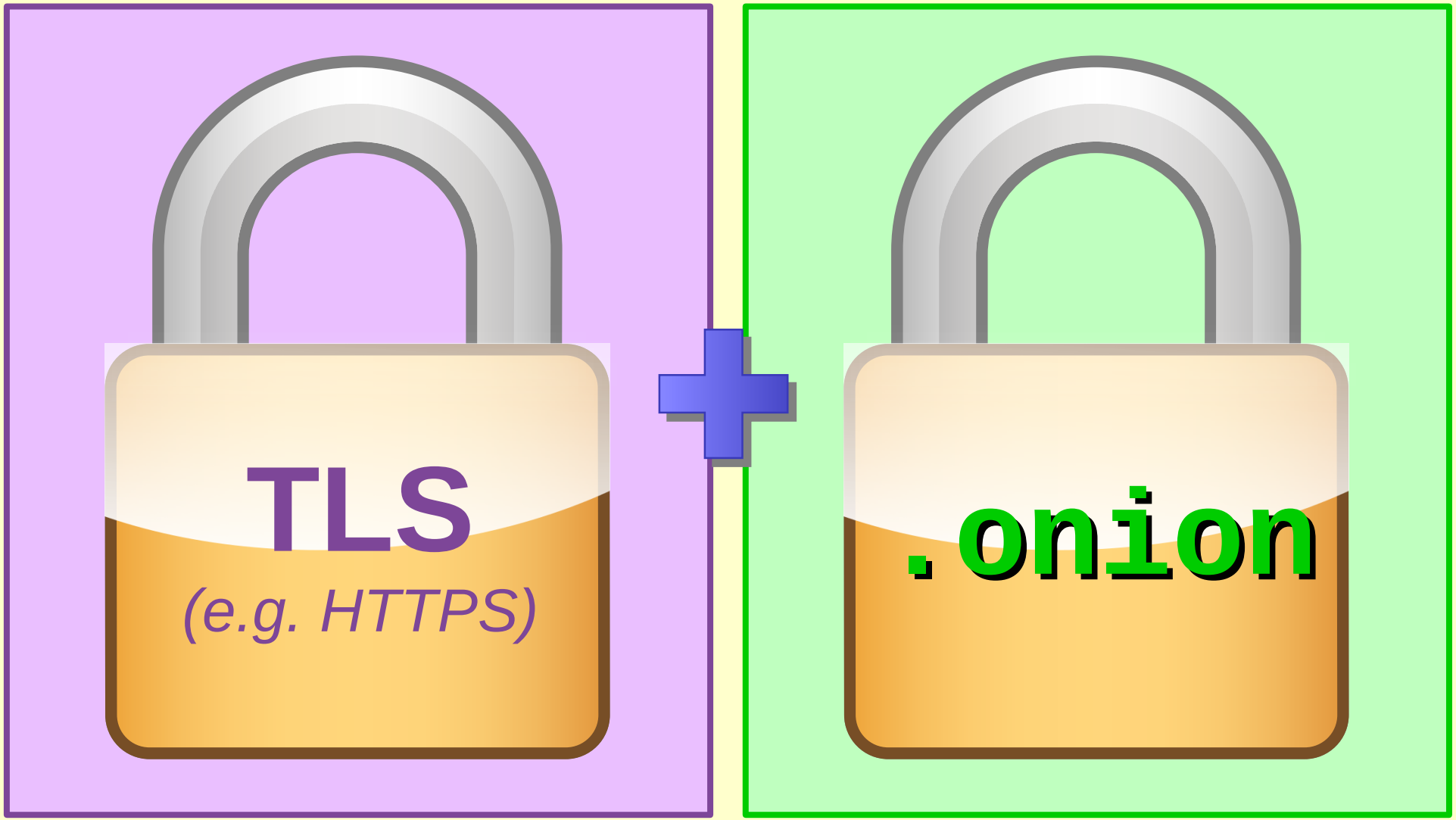
https://docs.securedrop.org/en/stable/deployment_practices.html#landing-page

SECUREDROP

Well, I think I found the right .onion …
… a year ago …
… or maybe it was last week …
I wrote it down / bookmarked it...



… but if we layer the security properties ...



HTTPS + .onion

TLS

- Transport-level *sec.*
- HSM use possible
- Revocable* cert
- **Authenticity** via CAs
  - address → **identity**
- Modern crypto
  - stronger primitives

.onion

- Network-level *sec.*
- No HSM support
- Irrevocable key/addr
- Limited **authenticity**
  - address → **key**
- Outdated* crypto
  - RSA1024, SHA1

* via OCSP, which leaks data if not using **OCSP stapling + Must-Staple**

* being addressed in next-gen. onions

HTTPS + .onion

A brief history...

~ June 2013 – DuckDuckGo – improper TLS onion (HTTPS presents domain mismatch)

- **Nov 2014 – 1st EV cert onion: Facebook**
- Dec 2014 – 2nd EV cert onion: Blockchain.info

~ Apr 2015 – 3rd EV cert onion: TheIntercept

- **Sep 2015 – .onion recognized as a special-use, top-level domain (officially allowing EV certs)**

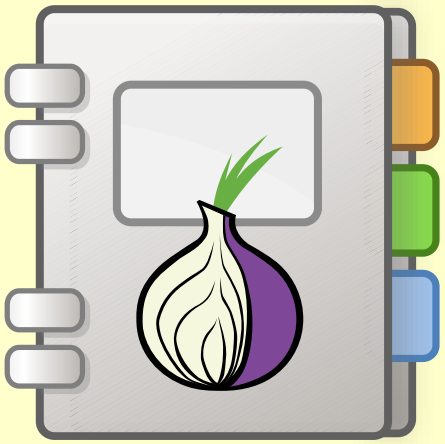
~ July 2016 – 7 organizations total deployed EV cert onion, per OnionScan report

- sometime after – DDG gets EV cert onion

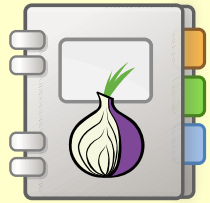
.onion usability, privacy

- .onion family “dropping”
- non-.onion resources (e.g. Google Analytics)
  - still use exits

.onion recipes



apt-transport-tor + .onion

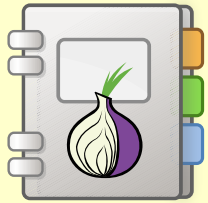


- repos over .onion exist for…
  - Debian
  - Tor Project
  - Whonix
  - Qubes
  - Tails
  - ...?

```
apt-get install apt-transport-tor

# edit /etc/apt/sources.list
#  and /etc/apt/sources.list.d/*.list
deb tor+http://abcdefghijklmnop.onion/path rel repos
```

- Privacy, but also security
  - refs: 2008 academic paper, apt CVE 2016-1252
- Not just for personal machines
  - ref: blog post about the server security gained from anonymity
- GPG is not enough
  - refs: Duo Tech Talk – Diogo Monico, The Update Framework (TUF)

GnuPG .onions

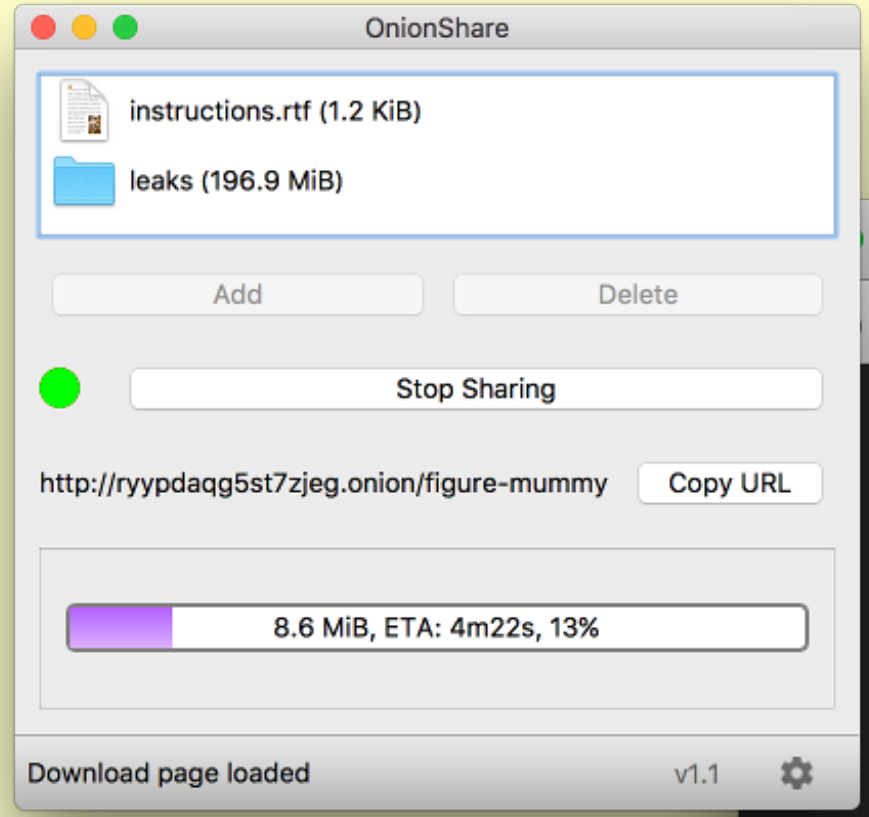


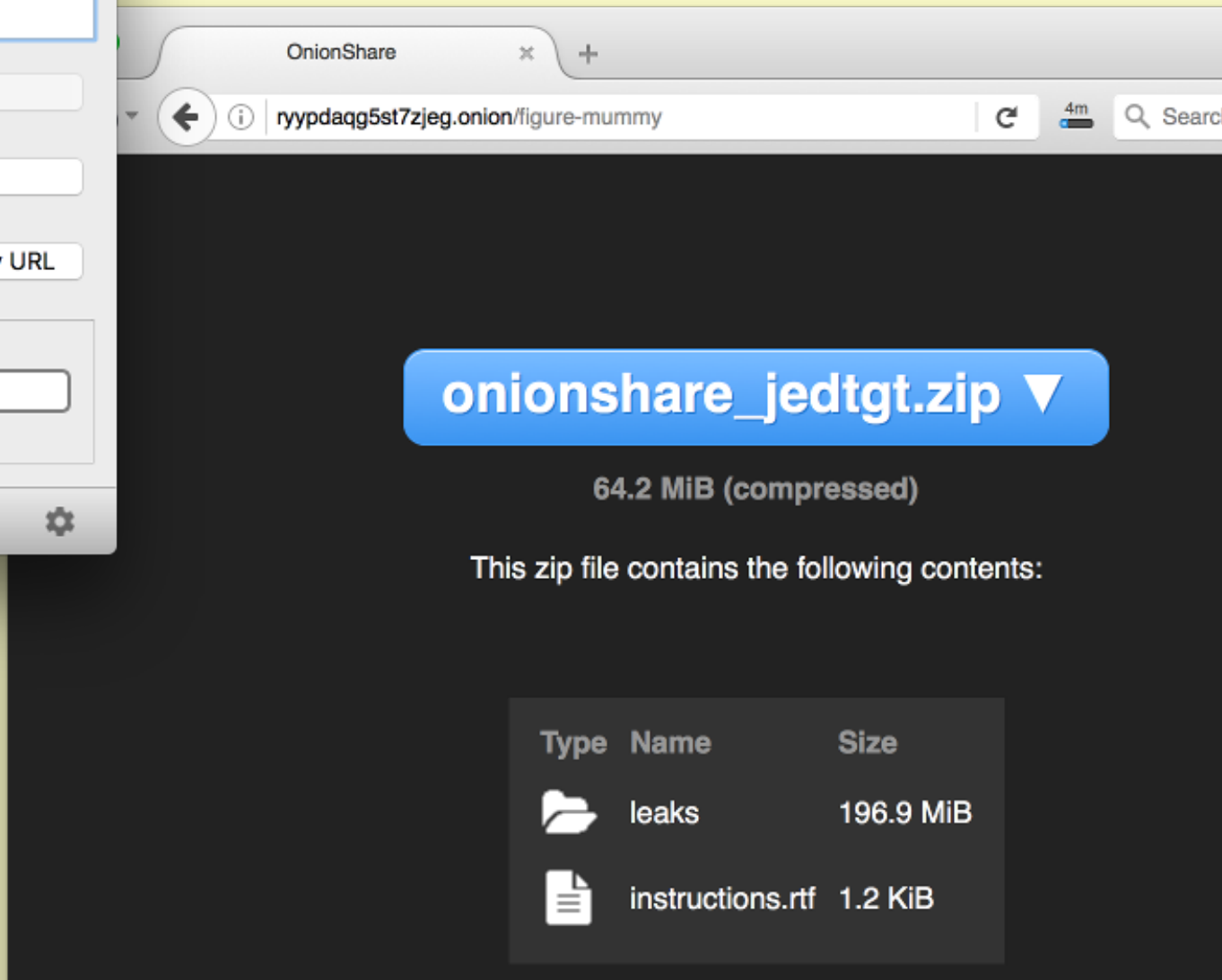
https://github.com/Whonix/anon-gpg-tweaks/blob/master/etc/skel/.gnupg/gpg.conf
- `hkp://qdigse2yzvuglcix.onion`

https://sks-keyservers.net/overview-of-pools.php#pool_tor
- `hkp://jirk5u4osbsr34t5.onion`

- gpg traffic typically “in the clear”
- gpg not designed for anonymity! Beware!
  - `torsocks -i gpg --refresh-keys`
    - parcimonie tool might help
  - gpg2… `dirmngr` started for not-tor

OnionShare


OnionShare
instructions.rtf (1.2 KiB)
leaks (196.9 MiB)
Add
Delete
Stop Sharing
http://ryypdaqg5st7zjeg.onion/figure-mummy
Copy URL
8.6 MiB, ETA: 4m22s, 13%
Download page loaded
v1.1

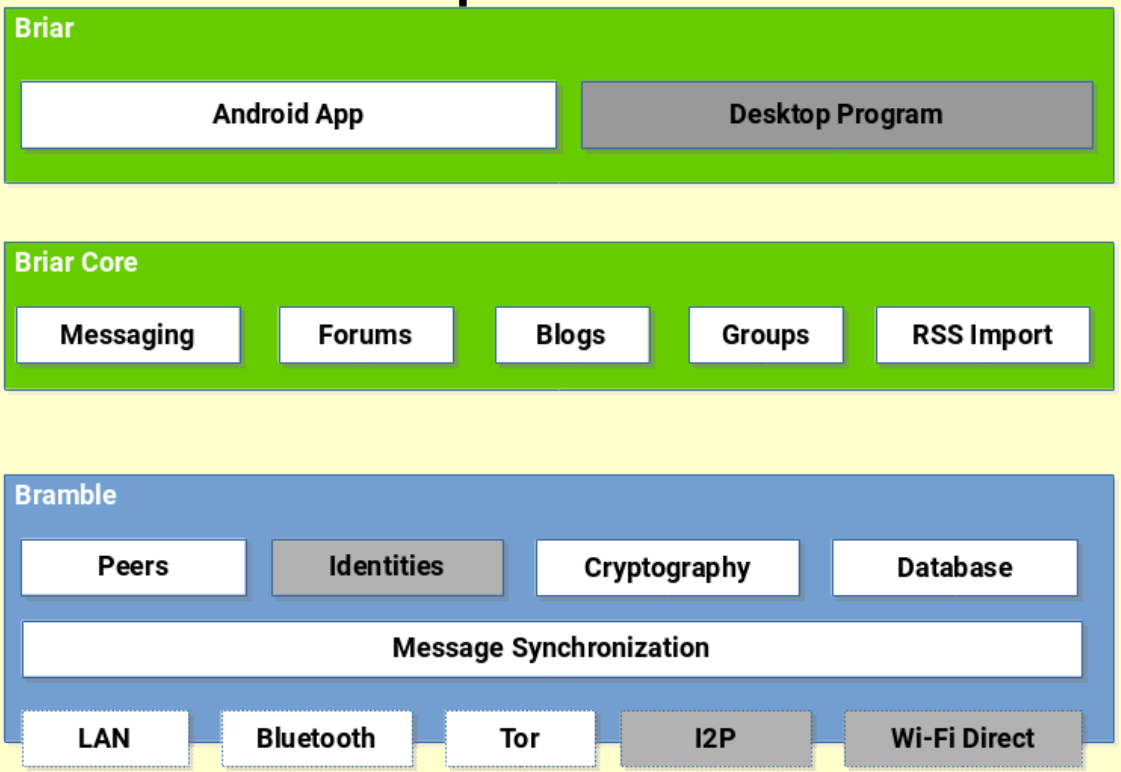

OnionShare
ryypdaqg5st7zjeg.onion/figure-mummy
onionshare_jedtgt.zip
64.2 MiB (compressed)
This zip file contains the following contents:
Type Name Size
leaks 196.9 MiB
instructions.rtf 1.2 KiB

.onion messaging

- Ricochet

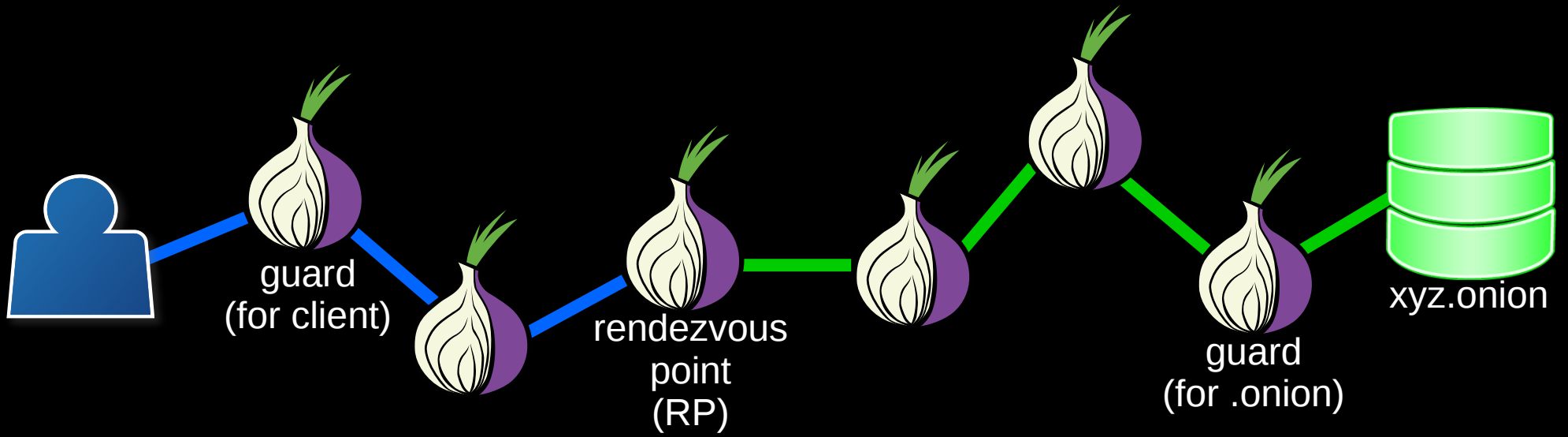
- unMessage – alpha
- Pond *(??)*

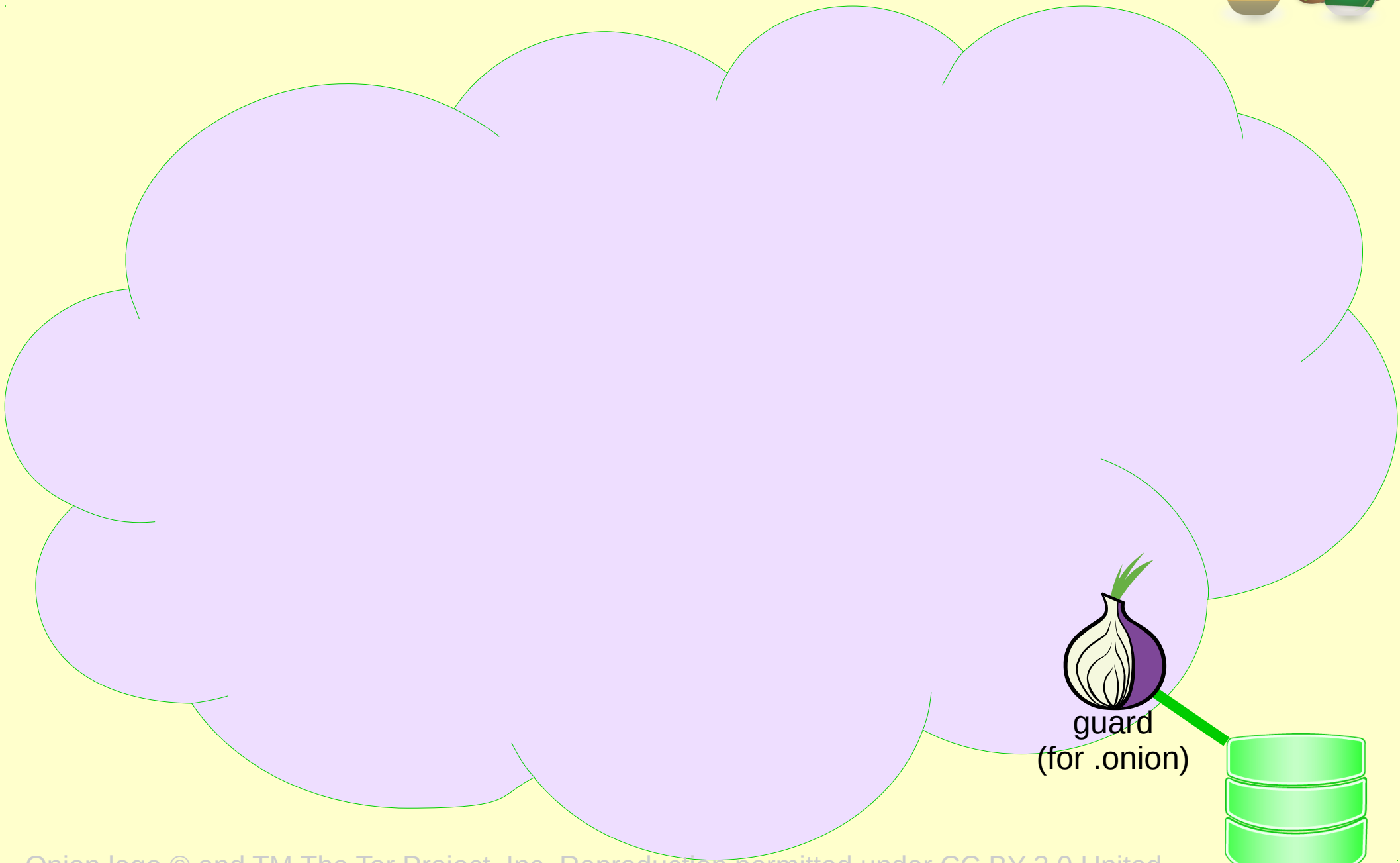
- Briar – public beta

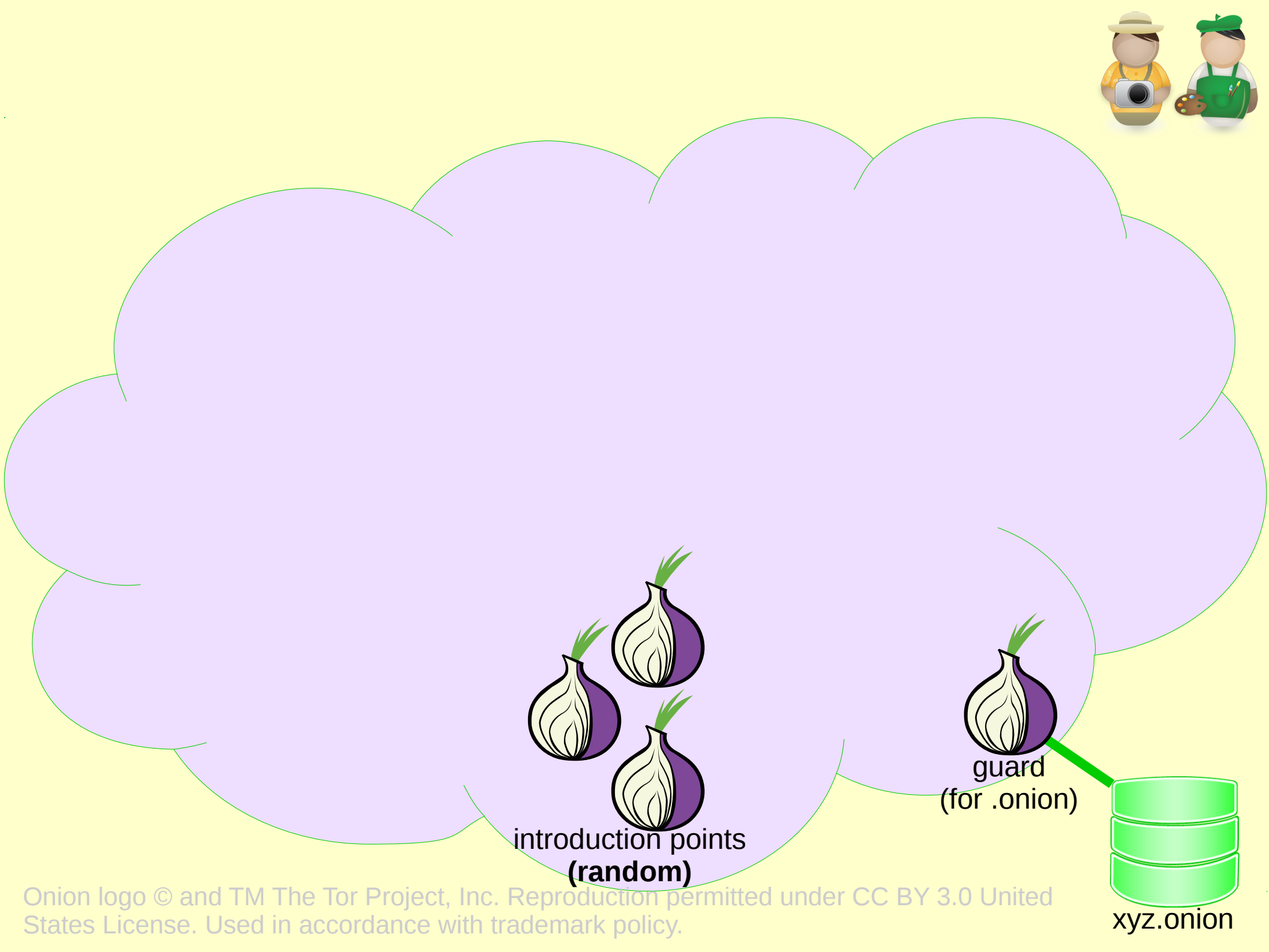


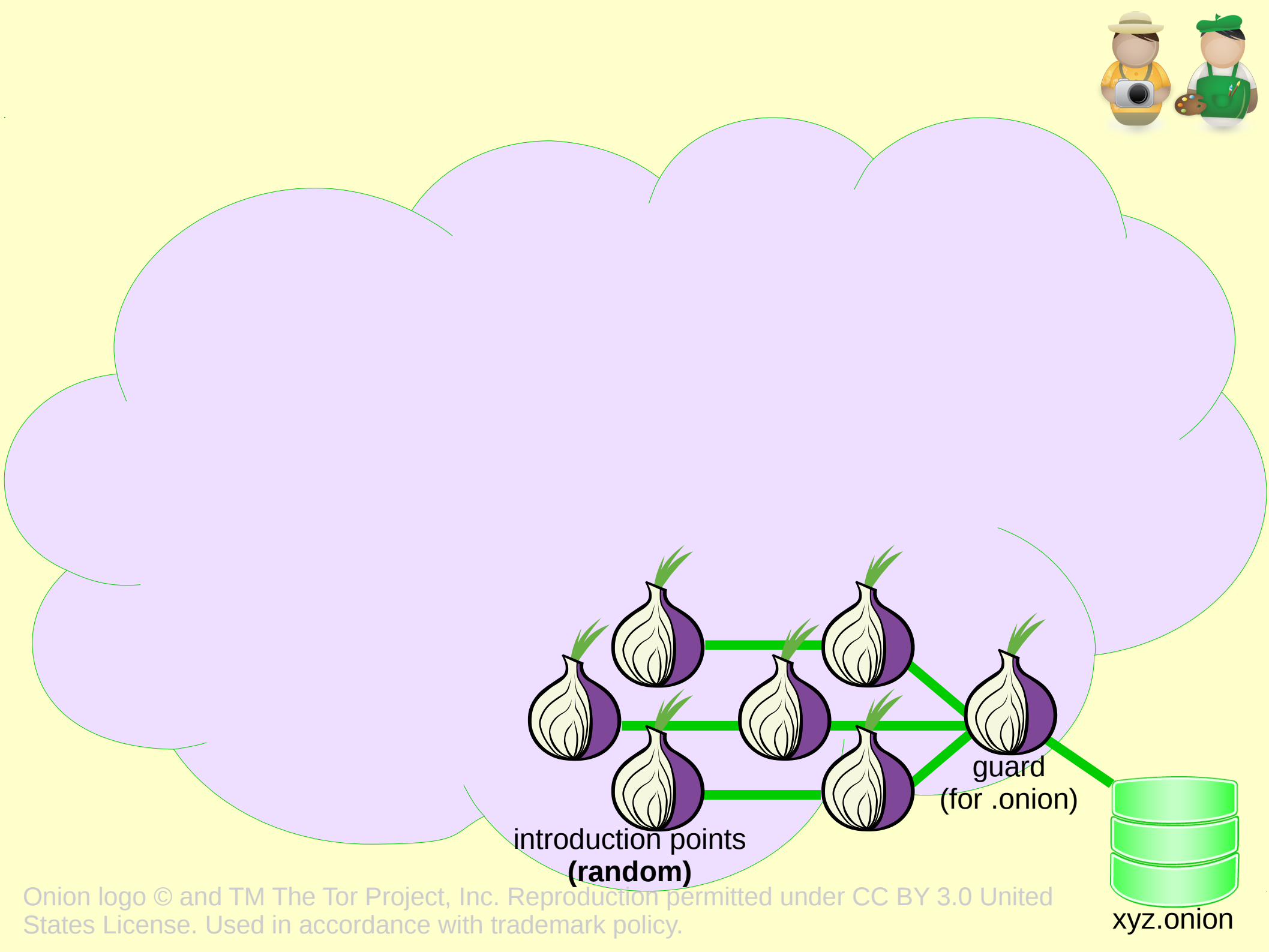
Rendezvous

Rendezvous


guard
(for client)
rendezvous
point
(RP)
guard
(for .onion)
xyz.onion







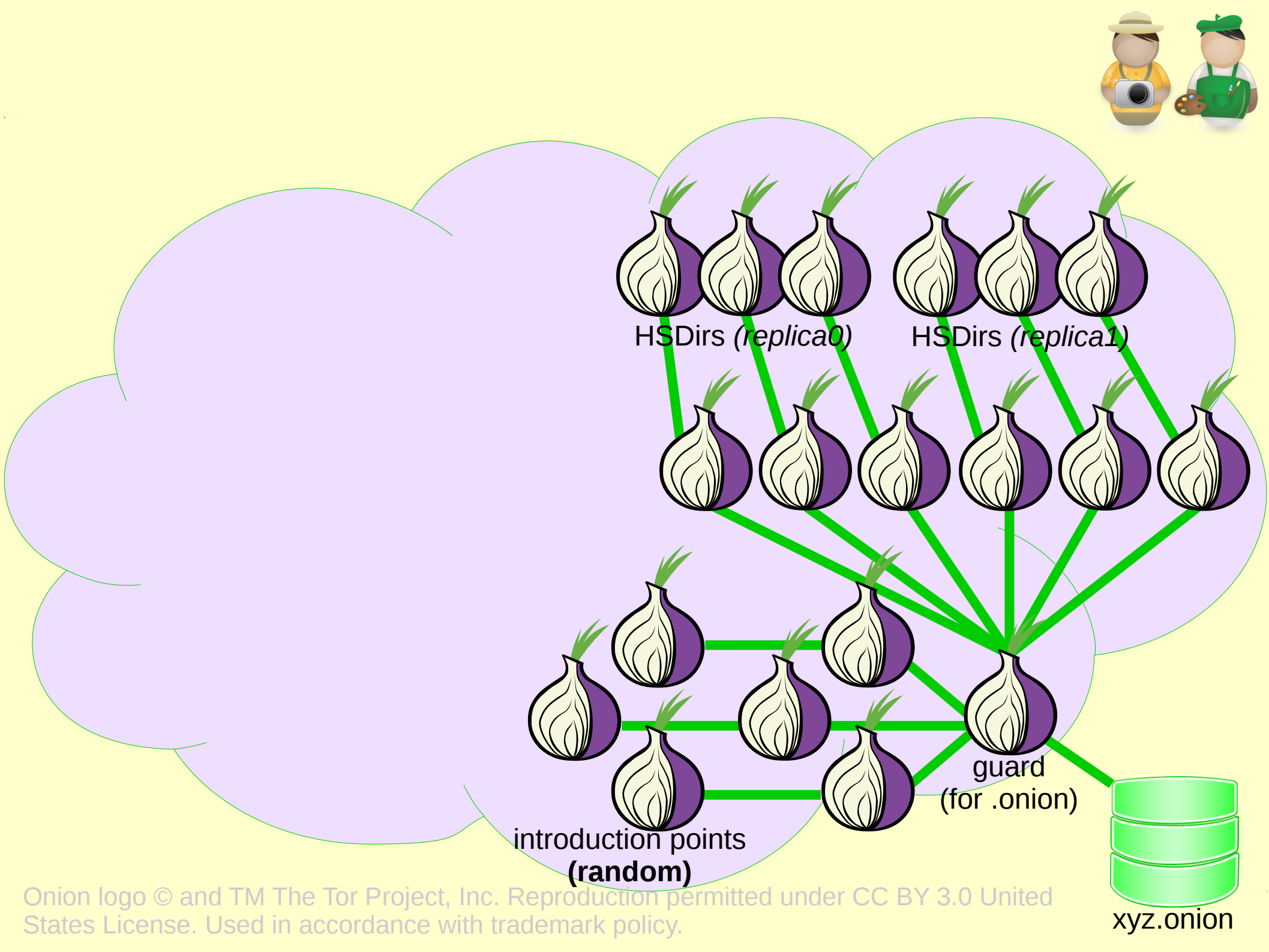
HSDirs *(replica0)*

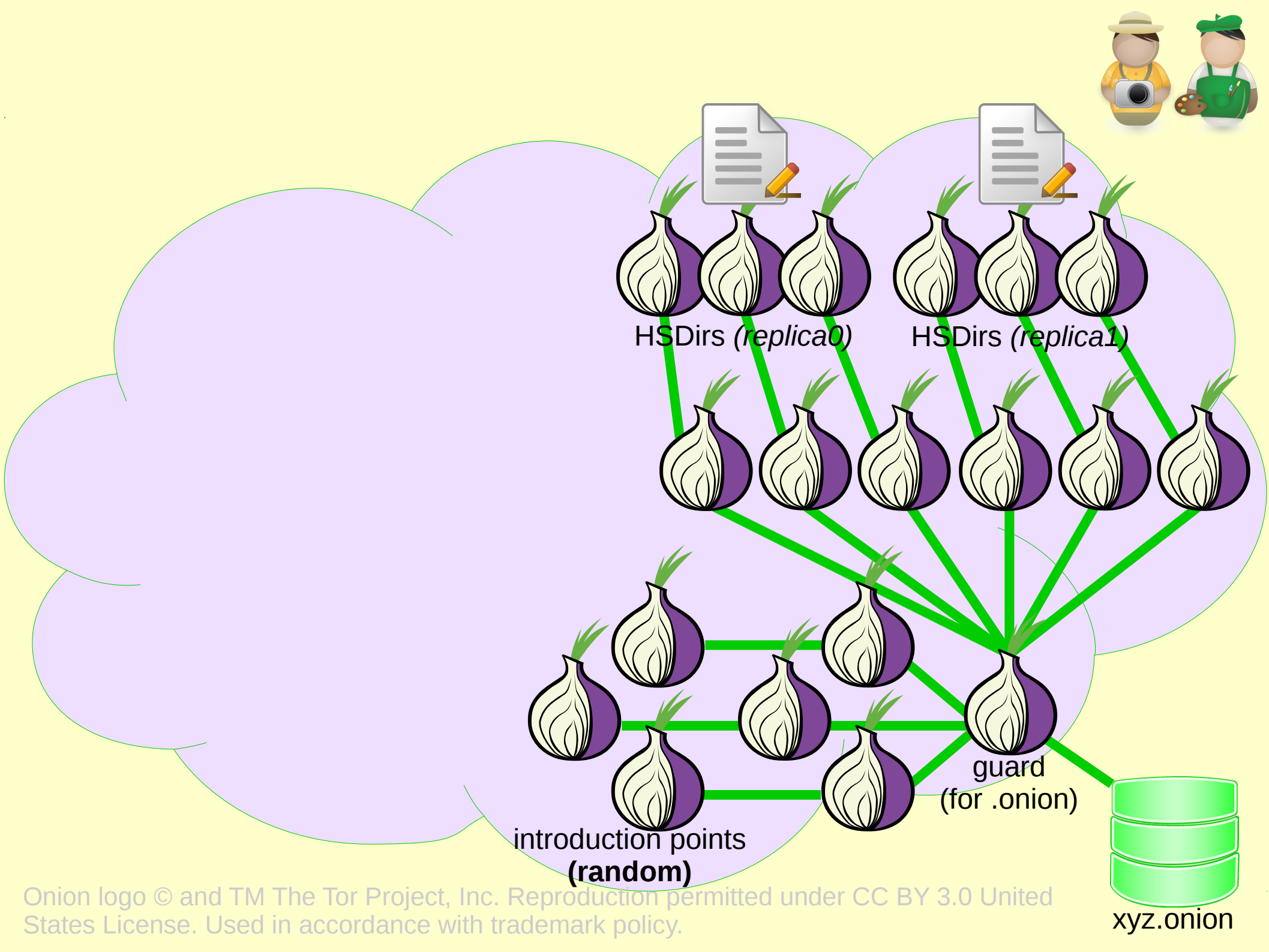
HSDirs *(replica1)*

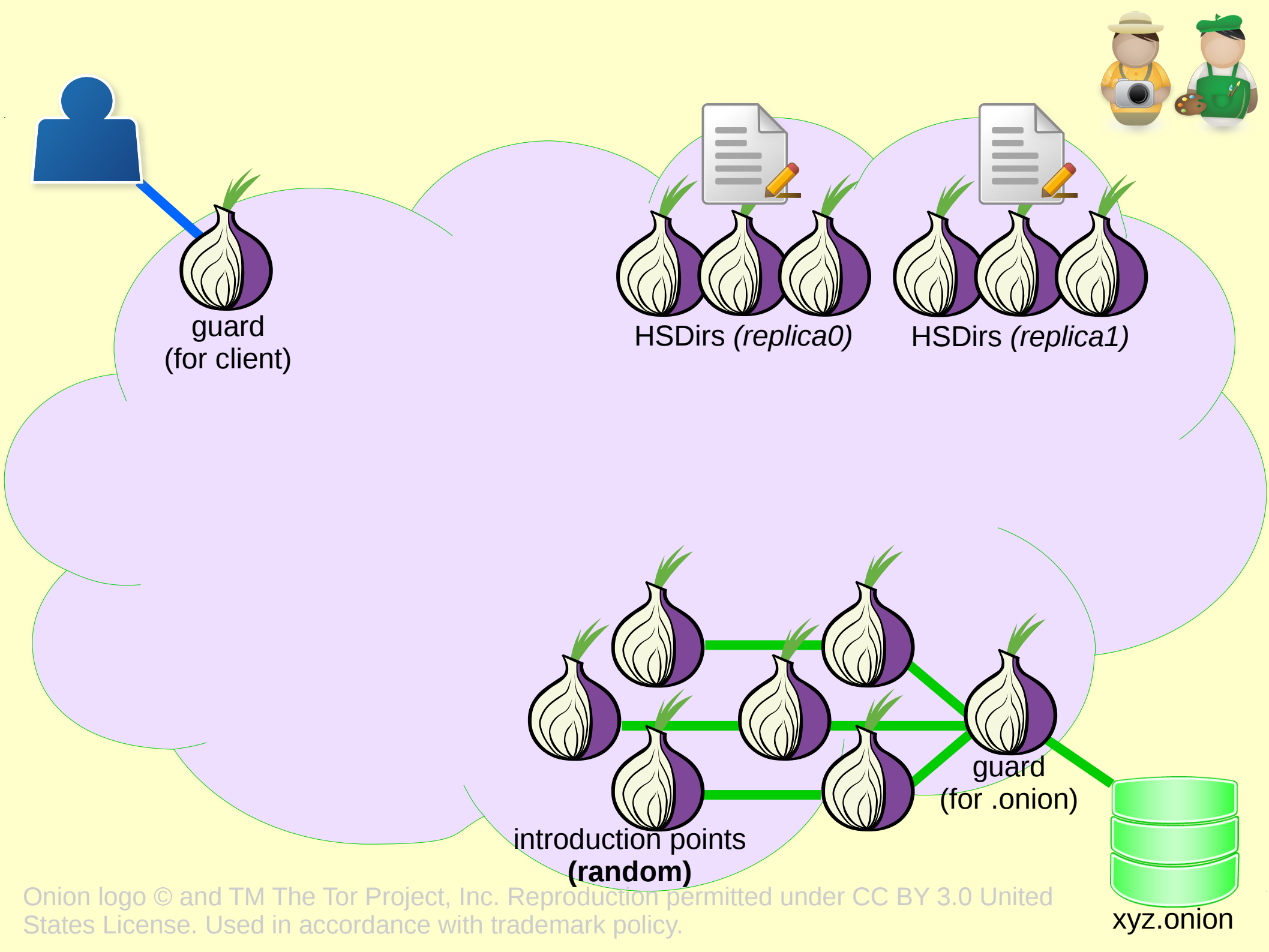
guard
(for .onion)

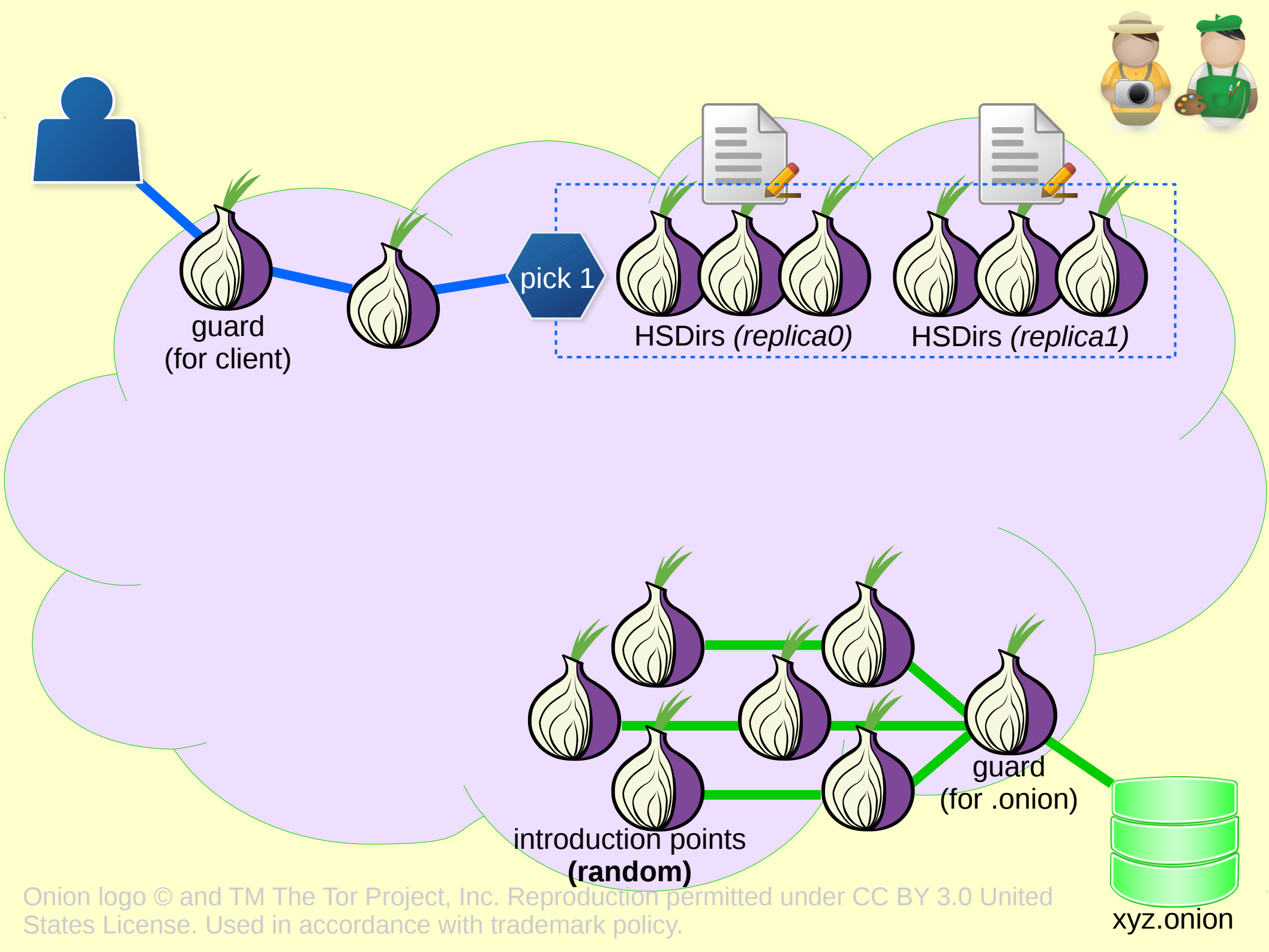
introduction points
(random)

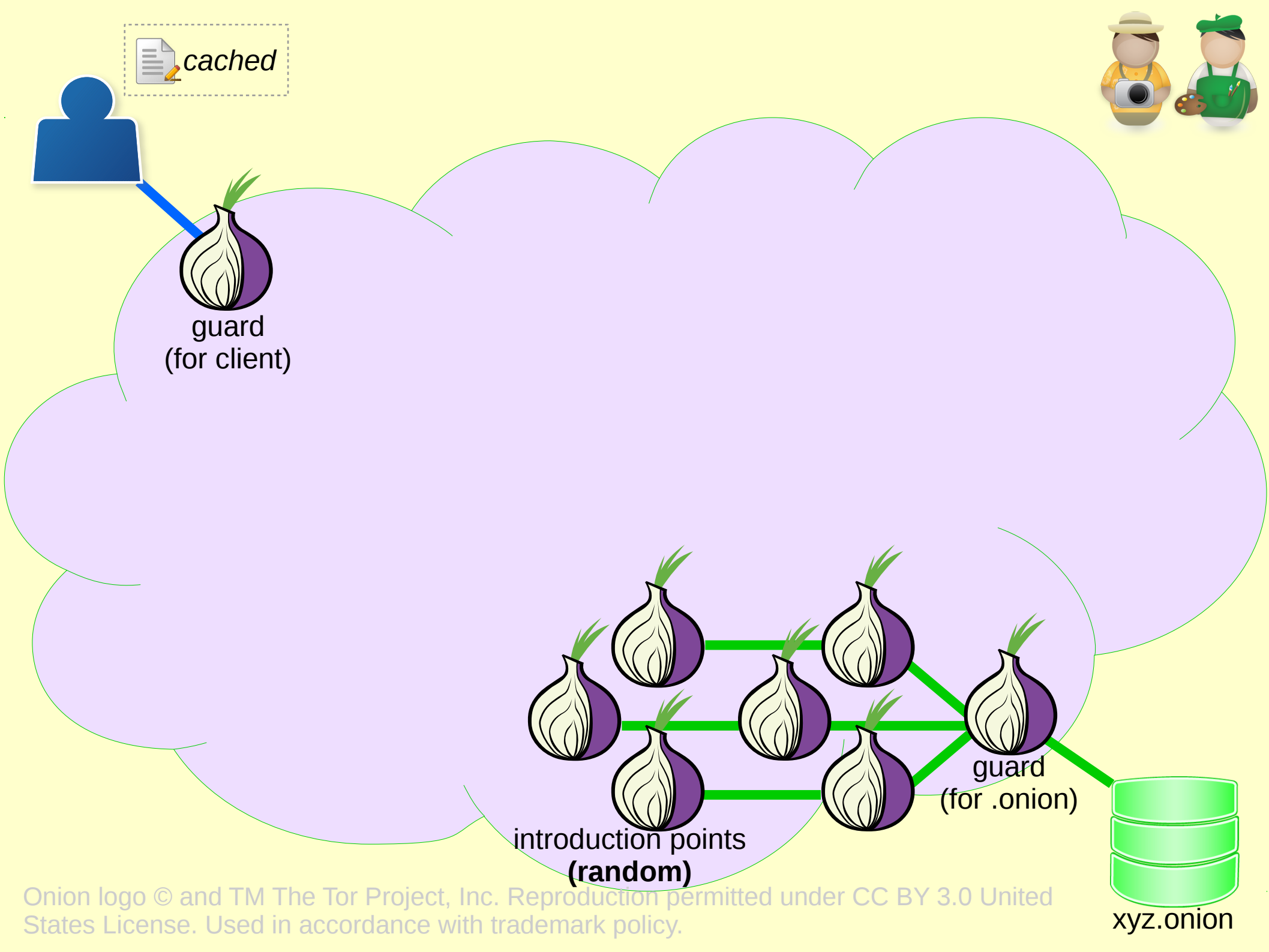
xyz.onion

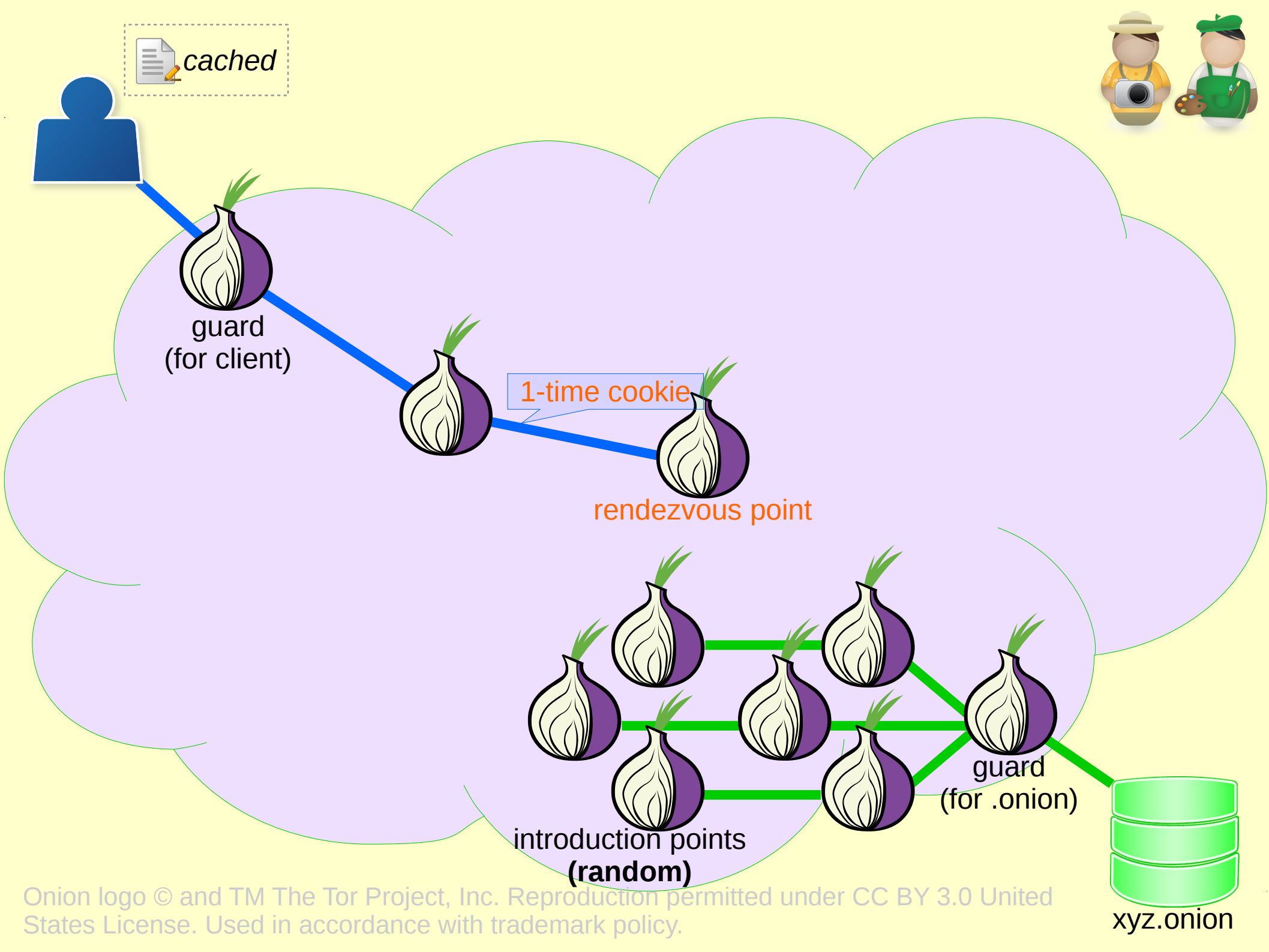


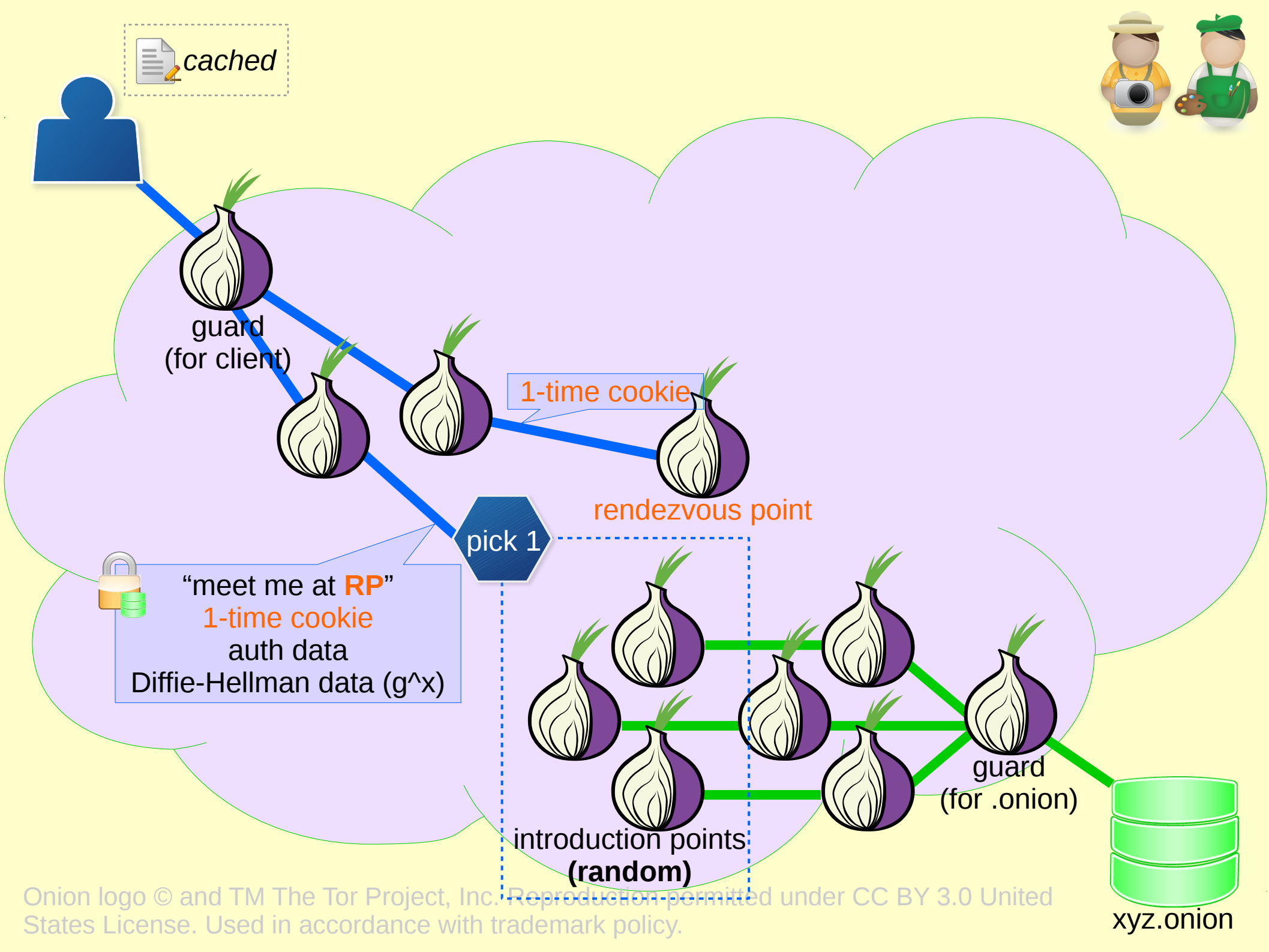


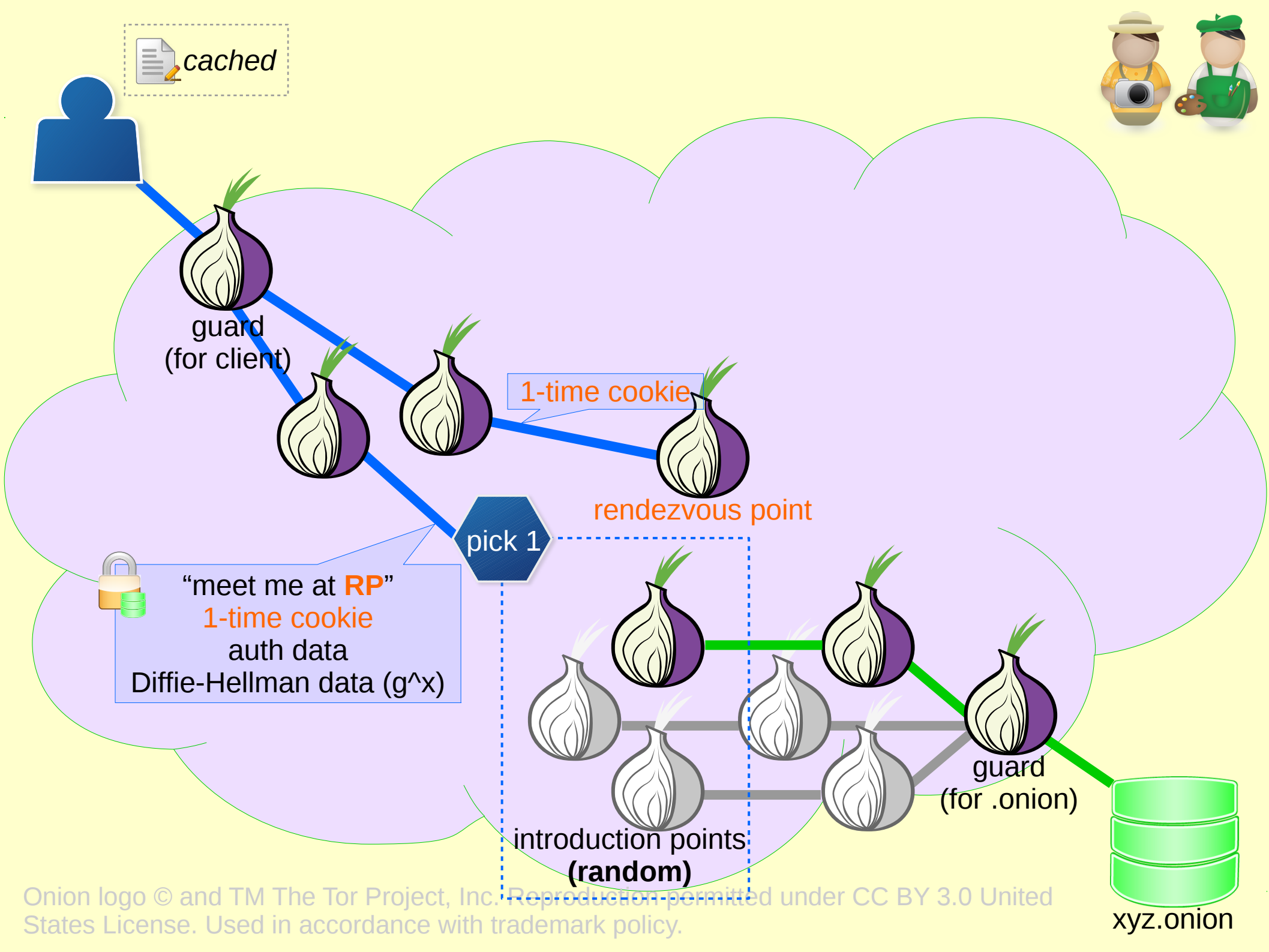


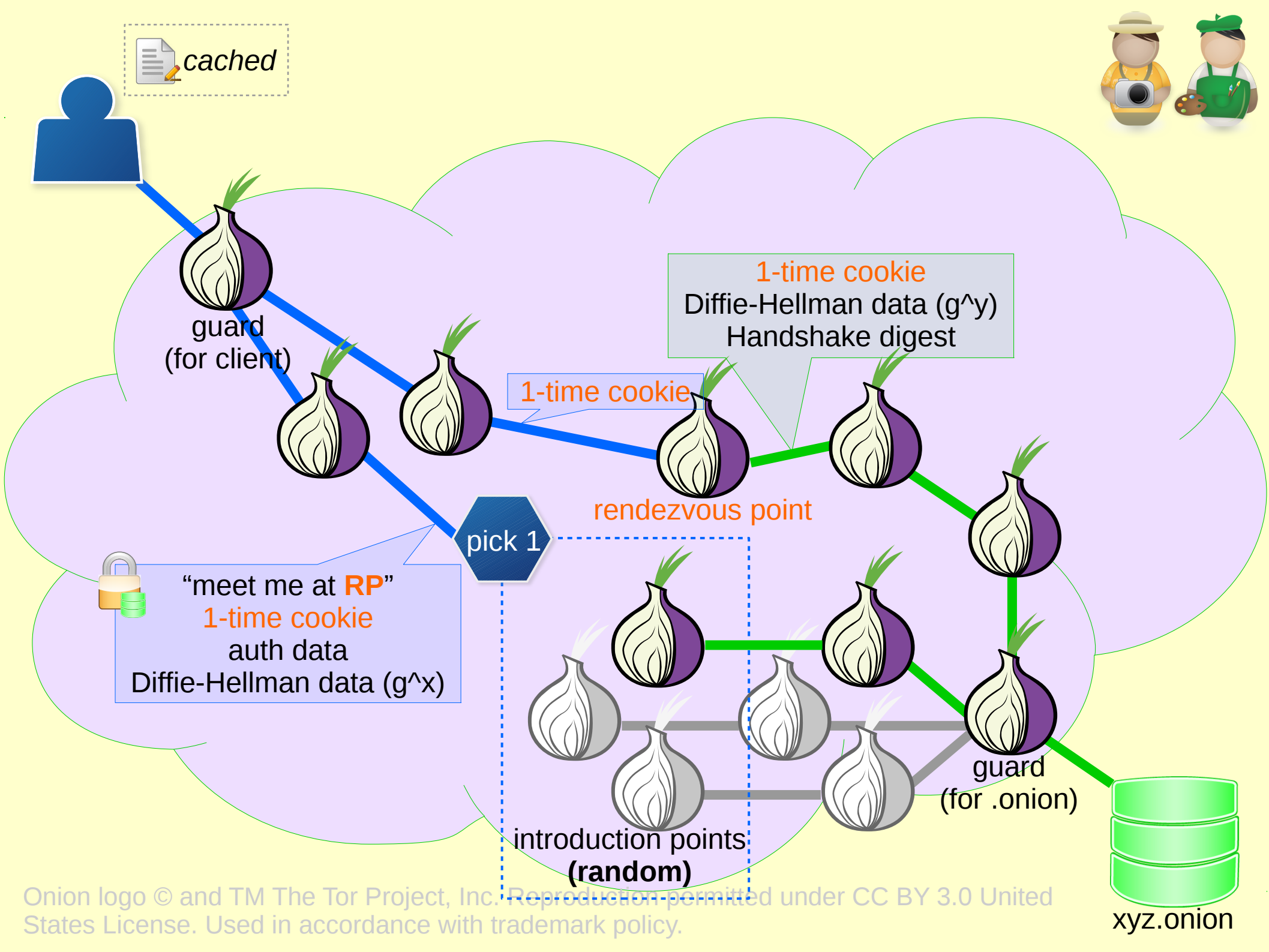


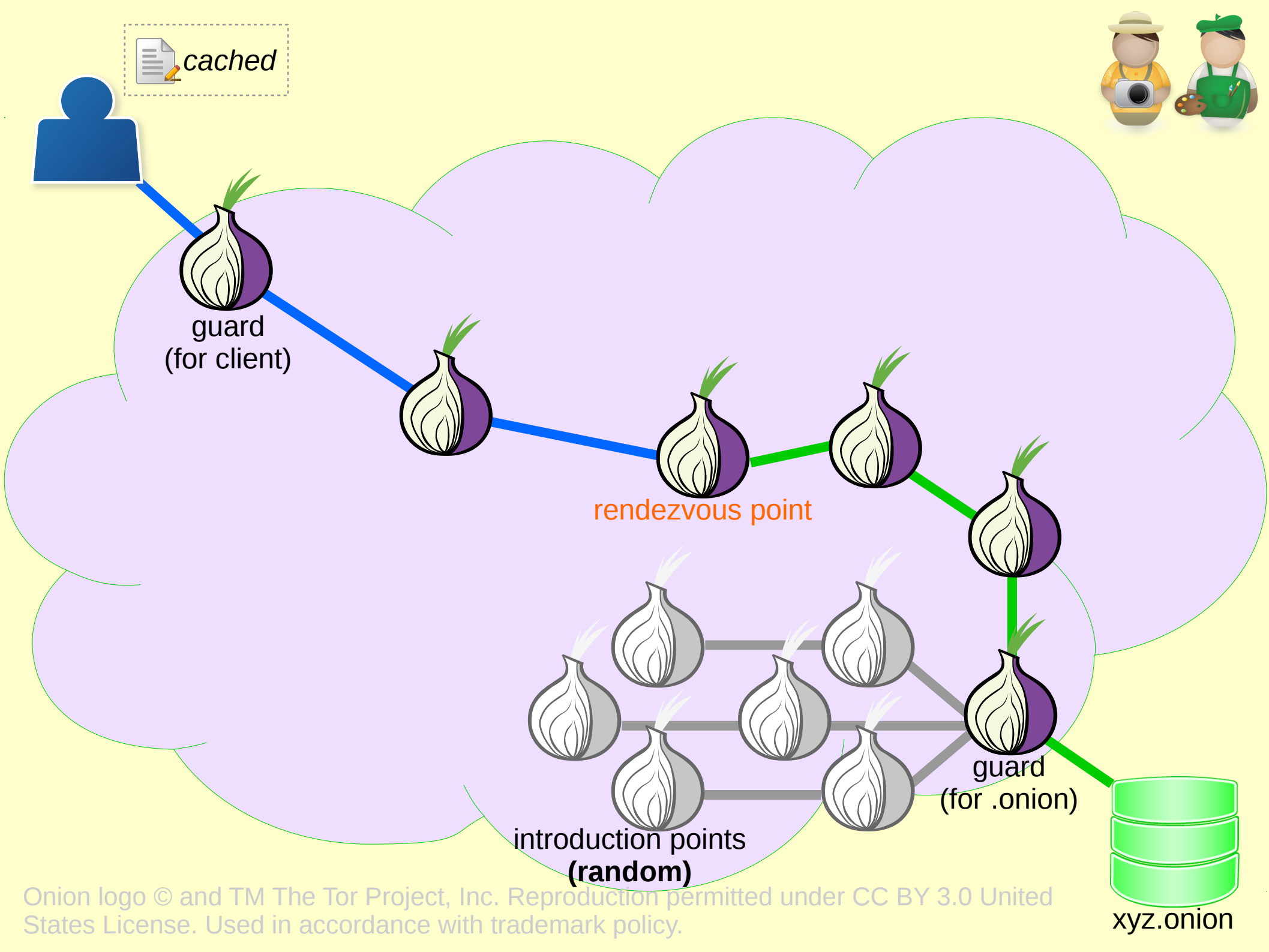












Descriptors, HSDirs, DHT

descriptor-id = H(permanent-id |
H(time-period | descriptor-cookie | replica))

replica = 0 or 1

permanent-id = H(public-key)[:10]
AKA ~base32-decode(onion address without ".onion")

time-period = (current-time + permanent-id-byte * 86400 / 256)
/ 86400
changes once per day, network-distributed offset

"current-time" :=
the current system time in seconds (since epoch)
"permanent-id-byte" :=
the first (unsigned) byte of the permanent identifier

Legend

H(…)	SHA1
|	concatenation
{grey}	**Invariant**
{purple}	**Variant, predictable**
{red}	**Secret**
{green}	**Random**

Descriptors, HSDirs, DHT

descriptor-id = H(permanent-id |
H(time-period | descriptor-cookie | replica))

replica = 0 or 1

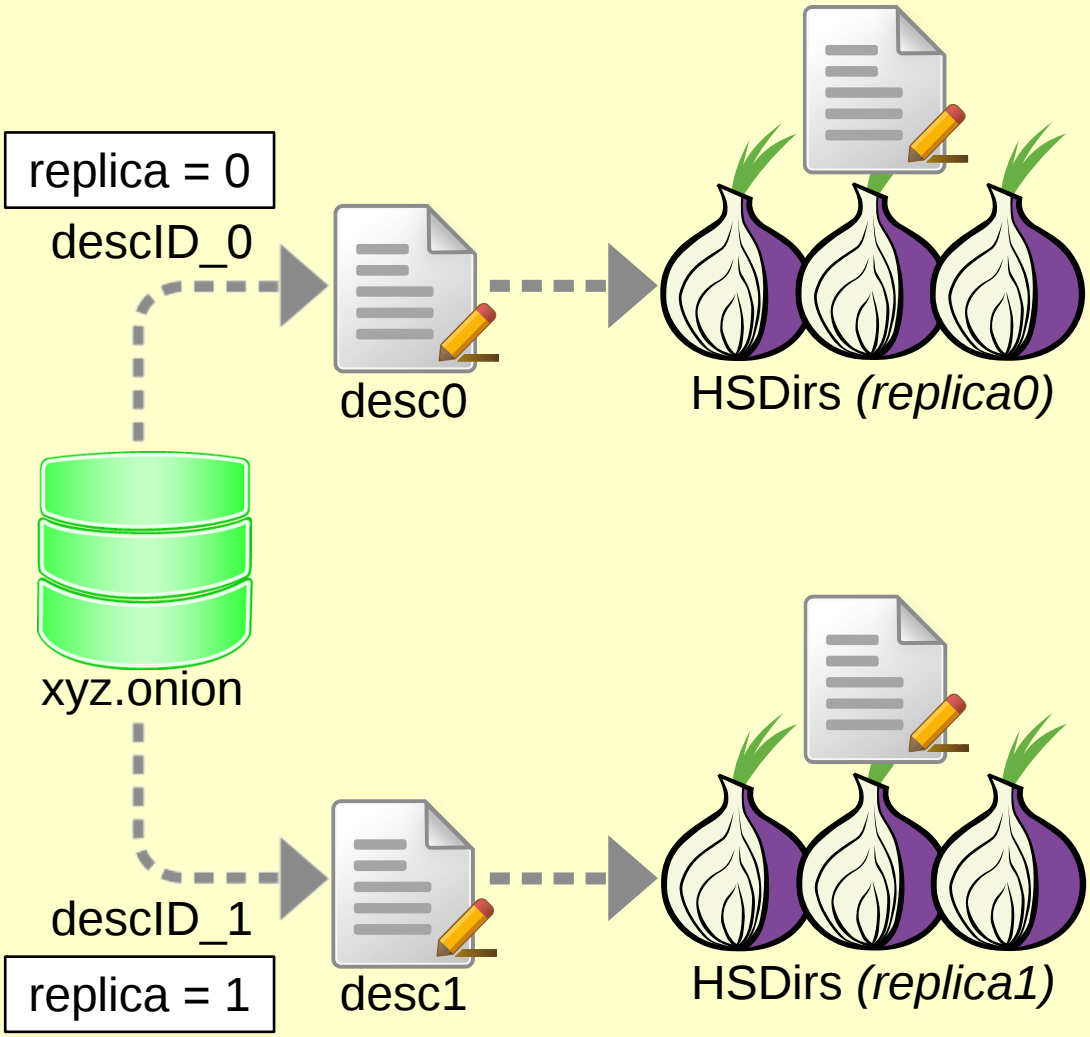
descID_0 = H(~"zti6p9h6spbtx5xr" |
H(17573 | "" | 0))

descID_0 = 3xqunszqnaolrrfmtzgaki7mxelgvkje

Descriptors, HSDirs, DHT

descriptor-id = H(permanent-id |
H(time-period | descriptor-cookie | replica))

replica = 0 or 1



Legend

H(…)	SHA1
|	concatenation
{grey}	**Invariant**
{purple}	**Variant, predictable**
{red}	**Secret**
{green}	**Random**

Descriptors, HSDirs, DHT

descriptor-id = H(permanent-id |
H(time-period | descriptor-cookie | replica))

replica = 0 or 1

descID_0 = 3xqunszqnaolrrfmtzgaki7mxelgvkje

Base16(descID_0) =
337871756E737A716E616F6C7272666D747A6761...

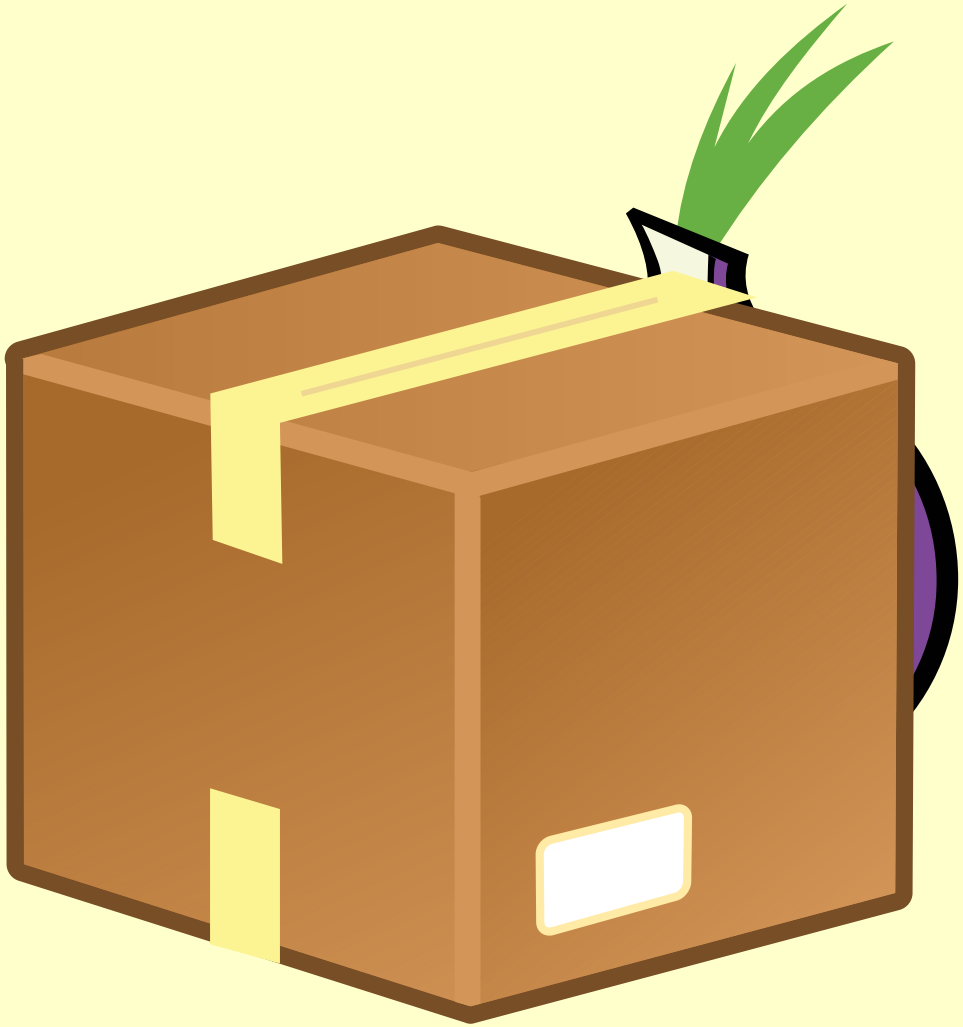
HSDirs:
33789F22470A22C8BEEF907CED29847781E15C5D
337B7E307550F48DCDADA7481FA8436B2FCDADA9
337DA8971BE4580EAC5D1D7AE4E508020CF04594

Descriptors, HSDirs, DHT

descriptor-id = H(permanent-id |
H(time-period | descriptor-cookie | replica))

replica = 0 or 1

Planting tip: stealth



DEMO TIME

https://cryptoanarchy.freed0m4all.net/wiki/Blackthrow

Blackthrow - Telecomix Crypto Munitions Bureau - Tor Browser

Telecomix ...

https://cryptoanarchy.freed0m4all.net/wiki/Blackthrow

Search

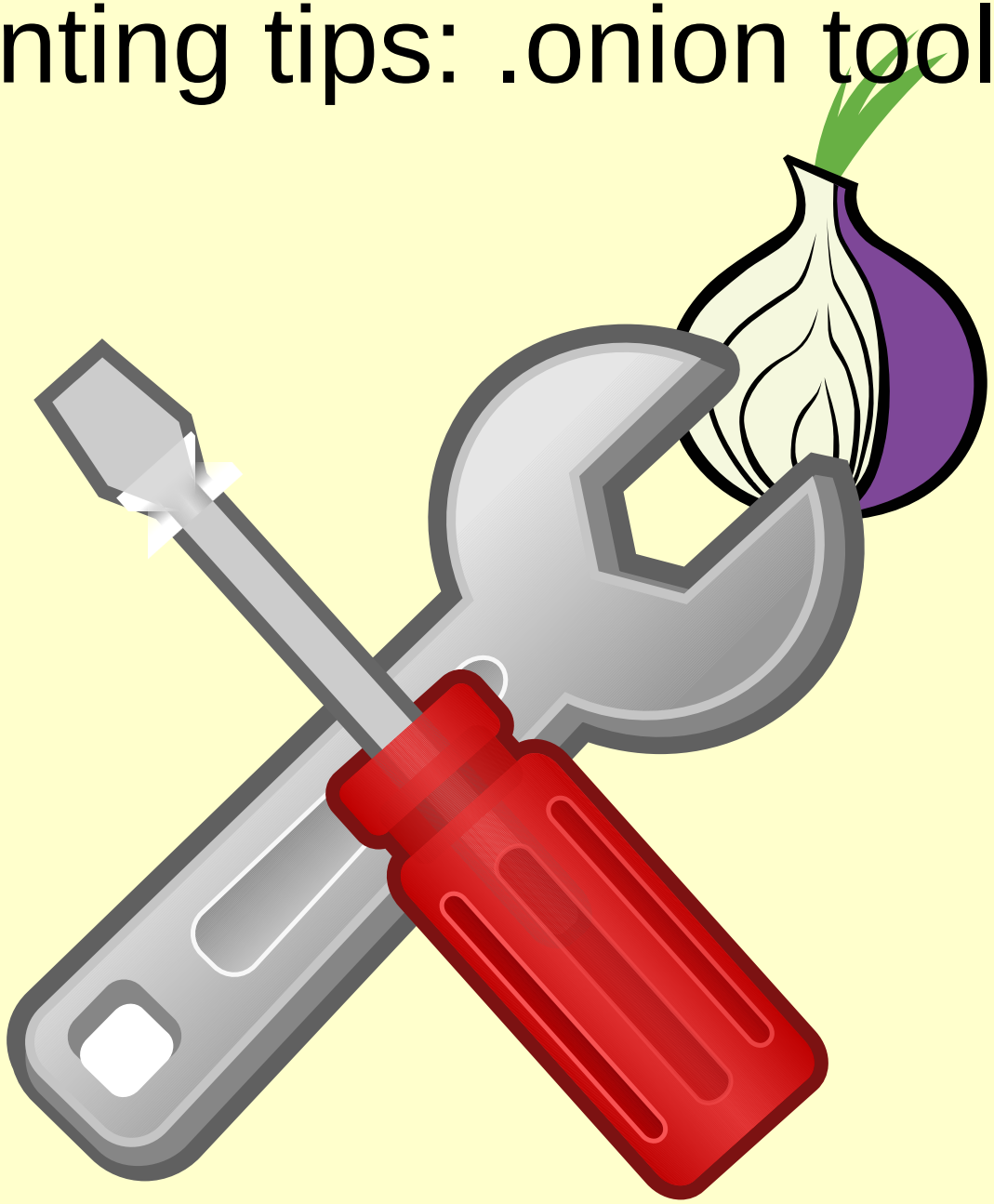
4.1 For anonymous remote control of the blackthrow, the secure shell (SSH) server needs to be made accessible as a hidden service. You need to edit two lines in the /etc/tor/torrc file. The file needs to contain the following two lines.

```
HiddenServiceDir /etc/tor/hidden/
HiddenServicePort 22 127.0.0.1:22
```

You will also need to create the /etc/tor/hidden/ directory. **(make sure it is owned by the account that TOR runs as. In debian, its *debian-tor*)**

Then restart TOR. Inside the file /etc/tor/hidden/hostname, there will now be a string that ends in ".onion". This is the anonymous destination of the blackthrows SSH server in the TOR network. It can be used to remotely control the machine anonymously.

Planting tips: .onion tools



Tools – especially for public...

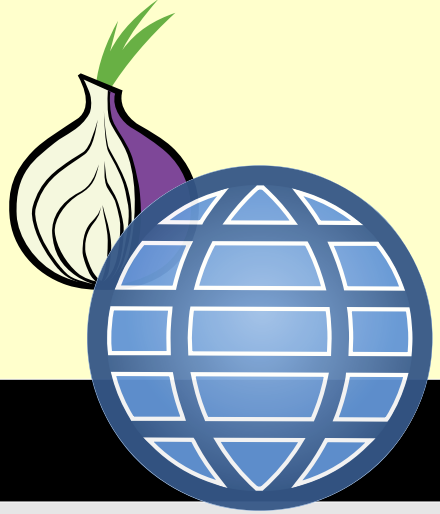
- OnionScan
- scallion (GPU,CPU) / shallot (CPU) / eschalot / etc.
  - vanity names
  - 8 characters easily doable
- OnionBalance
  - load balancing
  - identity-key separation
- Enterprise Onion Toolkit (EOTK) by Alec Muffett
- ALPaCA – fingerprinting defense
  - stage: research prototype

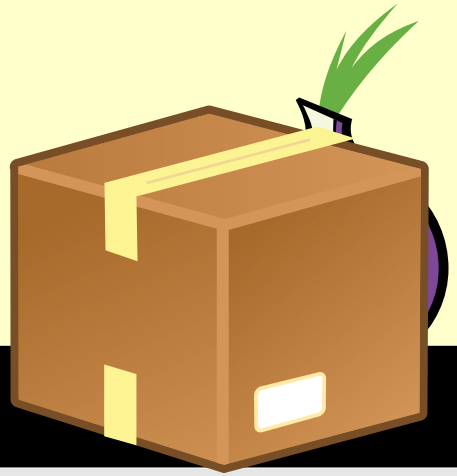
Tools – for private...

- OnionScan – security in depth
- OnionBalance – security in depth, maybe
- FreedomBox
  - make sure to set up stealth auth yourself
- home-assistant.io
- ALPaCA, potentially

Tools – more universal

- arm/nyx, as an example tor controller
- Whonix
  - VM separation for `tor` .onion and application
- corridor – tor-traffic whitelisting proxy
- Tails – live distro, much onions
- torsocks – use tor for non-tor-aware applications
  - Linux via LD_PRELOAD
  - mostly works
- parcimonie – all the gpg freshness





			Next Gen
Address is too short → authenticity?	**TLS (e.g. HTTPS)**	**Use additional crypto layer(s)**	✔
Outdated crypto	**TLS (e.g. HTTPS)**	**Use additional crypto layer(s)**	✔
HSDir camping	**Maintain clearnet service**	**client secret → cannot predict descriptor**	✔
HSDir sees public identity key	**“meh”**	**client secret → cannot connect**	✔
Guard discovery attack	**“meh”**	**client secret → cannot connect 9001 times**	✔
Website fingerprinting	ALPaCA (soon?)	Less of a concern, but ALPaCA potentially	?
HSDir deanonymization attack	?	Less of a concern, but ?	?
End-to-end correlation	?	Think about host location, networks	?

Refs: guides!

Alec Muffett's guide on a "Basic Production Onion Server"

https://github.com/alecmuffett/the-onion-diaries/blob/master/basic-production-onion-server.md

Riseup's Guide on best practices for Onion Services

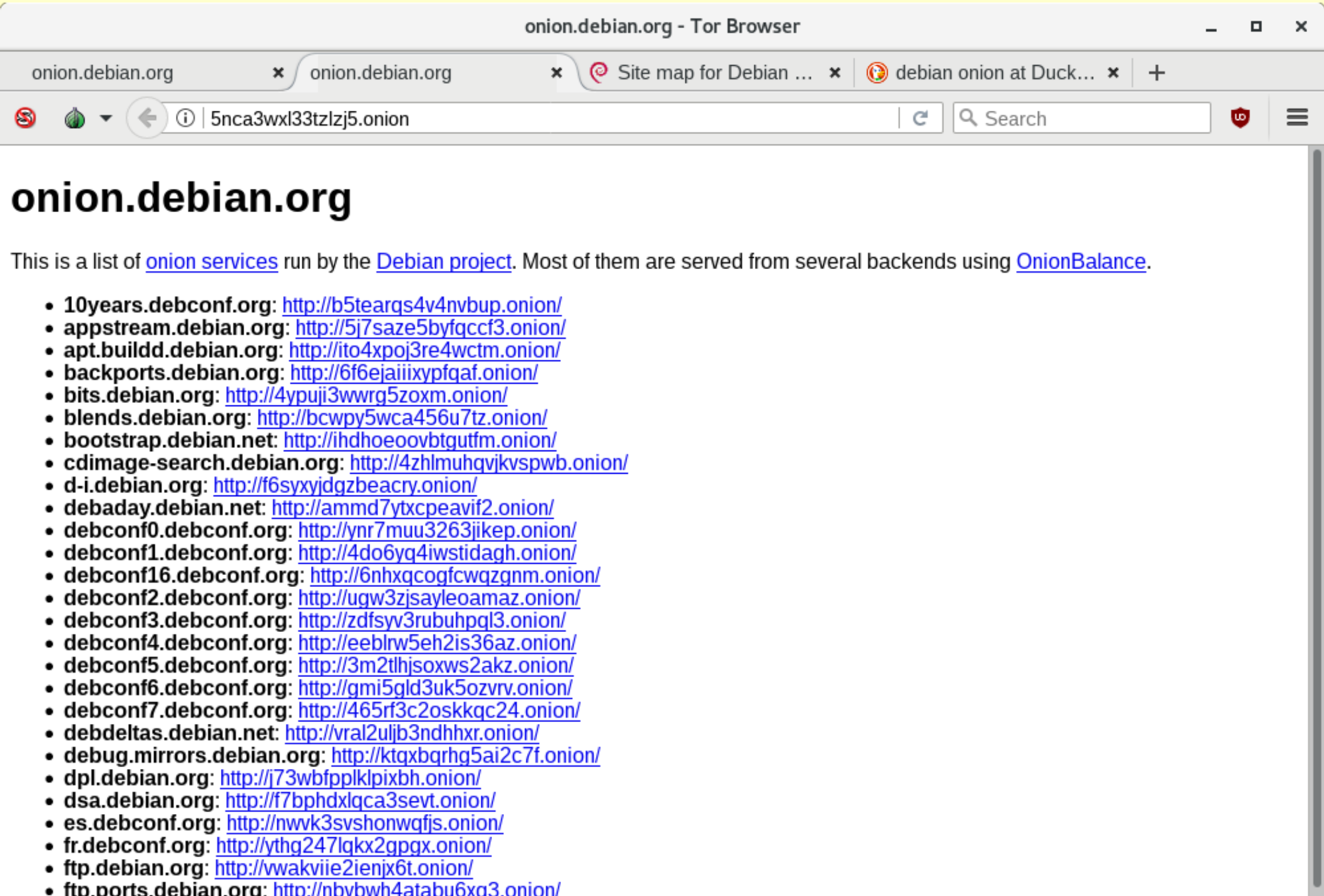
http://nzh3fv6jc6jskki3.onion/en/security/network-security/tor/onionservices-best-practices

https://riseup.net/en/security/network-security/tor/onionservices-best-practices

Questions?

Appendix

Bootstrapping? Discoverability?

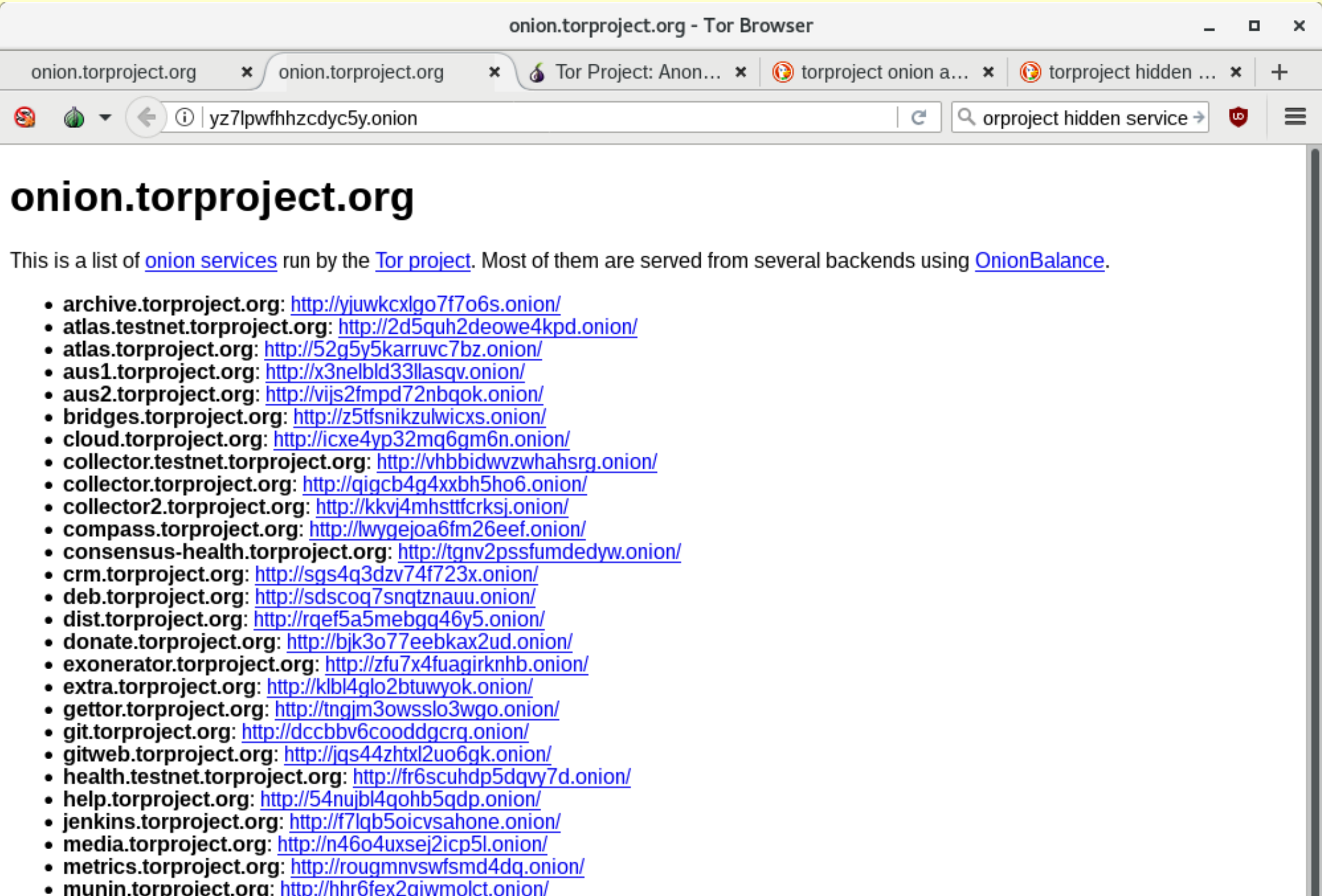


onion.debian.org

This is a list of onion services run by the Debian project. Most of them are served from several backends using OnionBalance.

- **10years.debconf.org**: http://b5tearqs4v4nvbup.onion/
- **appstream.debian.org**: http://5j7saze5byfqccf3.onion/
- **apt.buildd.debian.org**: http://ito4xpoj3re4wctm.onion/
- **backports.debian.org**: http://6f6ejaiiixypfqaf.onion/
- **bits.debian.org**: http://4ypuji3wwrg5zoxm.onion/
- **blends.debian.org**: http://bcwpy5wca456u7tz.onion/
- **bootstrap.debian.net**: http://ihdhoeoovbtgutfm.onion/
- **cdimage-search.debian.org**: http://4zhlmuhqvjkvspwb.onion/
- **d-i.debian.org**: http://f6syxyjdgzbeacry.onion/
- **debaday.debian.net**: http://ammd7ytxcpeavif2.onion/
- **debconf0.debconf.org**: http://ynr7muu3263jikep.onion/
- **debconf1.debconf.org**: http://4do6yq4iwstidagh.onion/
- **debconf16.debconf.org**: http://6nhxqcogfcwqzgnm.onion/
- **debconf2.debconf.org**: http://ugw3zjsayleoamaz.onion/
- **debconf3.debconf.org**: http://zdfsyv3rubuhpql3.onion/
- **debconf4.debconf.org**: http://eeblrw5eh2is36az.onion/
- **debconf5.debconf.org**: http://3m2tlhjsoxws2akz.onion/
- **debconf6.debconf.org**: http://gmi5gld3uk5ozvrv.onion/
- **debconf7.debconf.org**: http://465rf3c2oskkqc24.onion/
- **debdeltas.debian.net**: http://vral2uljb3ndhhxr.onion/
- **debug.mirrors.debian.org**: http://ktqxbqrhg5ai2c7f.onion/
- **dpl.debian.org**: http://j73wbfpplklpixbh.onion/
- **dsa.debian.org**: http://f7bphdxlqca3sevt.onion/
- **es.debconf.org**: http://nwvk3svshonwqfjs.onion/
- **fr.debconf.org**: http://ythg247lqkx2gpgx.onion/
- **ftp.debian.org**: http://vwakviie2ienjx6t.onion/
- **ftp.ports.debian.org**: http://nbybwh4atabu6xq3.onion/

Bootstrapping? Discoverability?

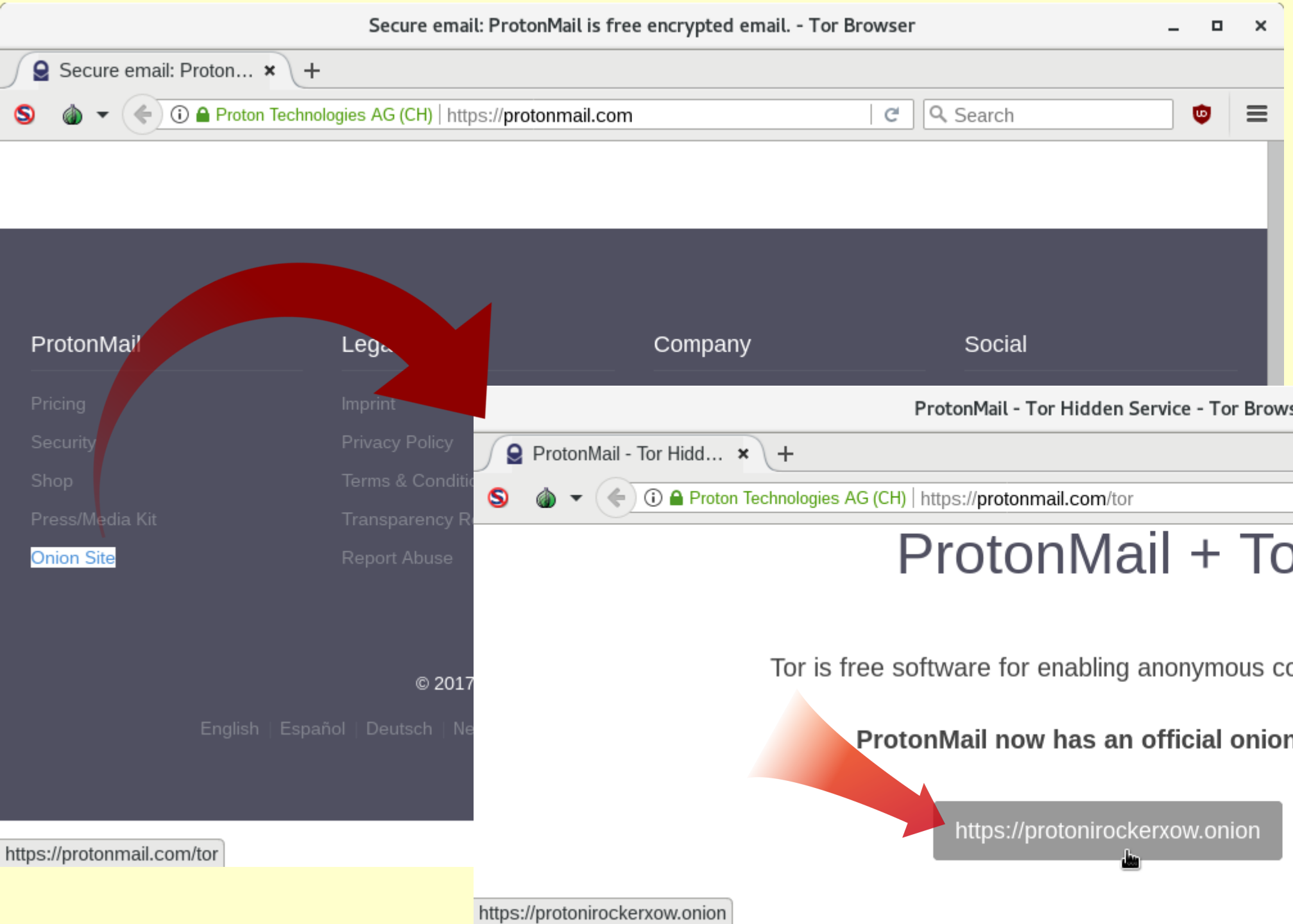


onion.torproject.org

This is a list of onion services run by the Tor project. Most of them are served from several backends using OnionBalance.

- **archive.torproject.org**: http://yjuwkcxlgo7f7o6s.onion/
- **atlas.testnet.torproject.org**: http://2d5quh2deowe4kpd.onion/
- **atlas.torproject.org**: http://52g5y5karruvc7bz.onion/
- **aus1.torproject.org**: http://x3nelbld33llasqv.onion/
- **aus2.torproject.org**: http://vijs2fmpd72nbqok.onion/
- **bridges.torproject.org**: http://z5tfsnikzulwicxs.onion/
- **cloud.torproject.org**: http://icxe4yp32mq6gm6n.onion/
- **collector.testnet.torproject.org**: http://vhbbidwvzwhahsrg.onion/
- **collector.torproject.org**: http://qigcb4g4xxbh5ho6.onion/
- **collector2.torproject.org**: http://kkvj4mhsttfcrksj.onion/
- **compass.torproject.org**: http://lwygejoa6fm26eef.onion/
- **consensus-health.torproject.org**: http://tgnv2pssfumdedyw.onion/
- **crm.torproject.org**: http://sgs4q3dzv74f723x.onion/
- **deb.torproject.org**: http://sdscoq7snqtznauu.onion/
- **dist.torproject.org**: http://rqef5a5mebgq46y5.onion/
- **donate.torproject.org**: http://bjk3o77eebkax2ud.onion/
- **exonerator.torproject.org**: http://zfu7x4fuagirknhb.onion/
- **extra.torproject.org**: http://klbl4glo2btuwyok.onion/
- **gettor.torproject.org**: http://tngjm3owsslo3wgo.onion/
- **git.torproject.org**: http://dccbbv6cooddgcrq.onion/
- **gitweb.torproject.org**: http://jqs44zhtxl2uo6gk.onion/
- **health.testnet.torproject.org**: http://fr6scuhdp5dqvy7d.onion/
- **help.torproject.org**: http://54nujbl4qohb5qdp.onion/
- **jenkins.torproject.org**: http://f7lqb5oicvsahone.onion/
- **media.torproject.org**: http://n46o4uxsej2icp5l.onion/
- **metrics.torproject.org**: http://rougmnvswfsmd4dq.onion/
- **munin.torproject.org**: http://hhr6fex2qiwmolct.onion/

Bootstrapping? Discoverability?

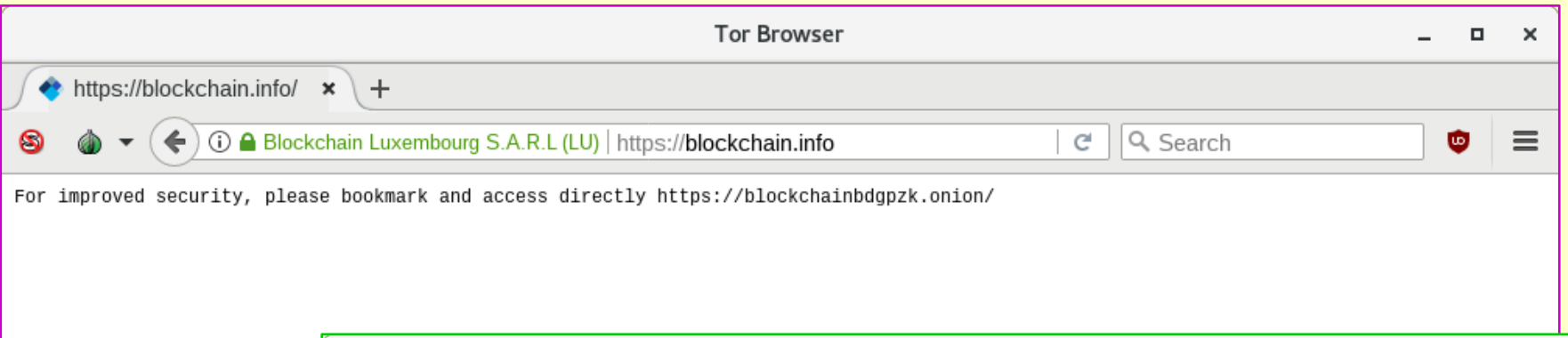


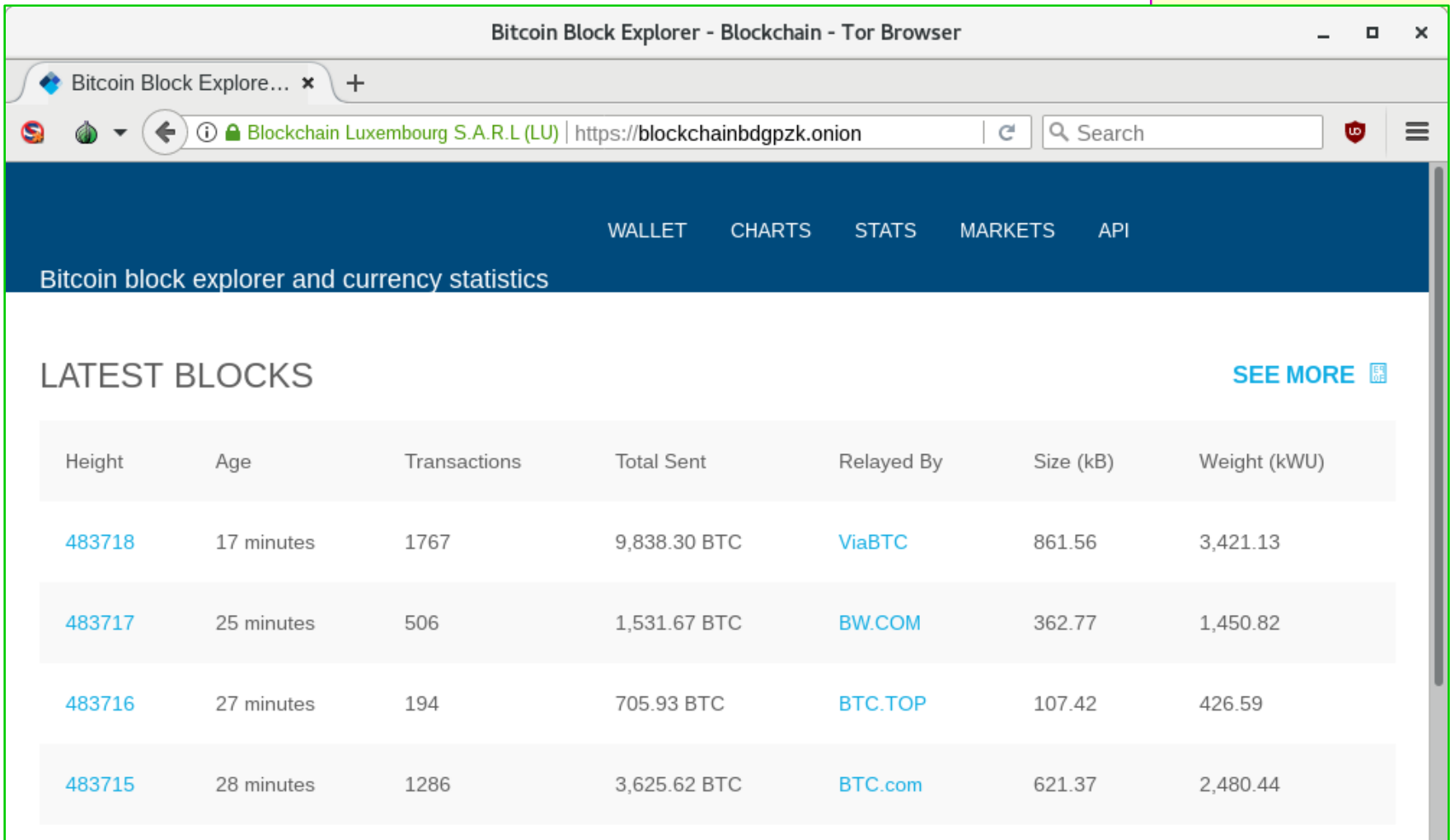
Bootstrapping? Discoverability?

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512


riseup.net:          nzh3fv6jc6jskki3.onion (port 80)
help.riseup.net:     nzh3fv6jc6jskki3.onion (port 80)
black.riseup.net:    cwoiopiifrlzcuos.onion (port 80)
imap.riseup.net:     zsolxunfmbfuq7wf.onion (port 993)
lists.riseup.net:    xpgylzydxykgdqyg.onion (port 80)
mail.riseup.net:     zsolxunfmbfuq7wf.onion (ports 80, 465, 587)
mx1.riseup.net:      wy6zk3pmcwiyhiao.onion (port 25)
pad.riseup.net:      5jp7xtmox6jyoqd5.onion (port 80)
pop.riseup.net:      zsolxunfmbfuq7wf.onion (port 995)
share.riseup.net:    6zc6sejeho3fwrd4.onion (port 80)
smtp.riseup.net:     zsolxunfmbfuq7wf.onion (ports 465, 587)
account.riseup.net:  j6uhdvbhz74oefxf.onion (port 80)
we.riseup.net:       7lvd7fa5yfbdqaii.onion (port 443)
xmpp.riseup.net:     4cjw6cwpeaeppfqz.onion (ports 5222, 5269)
0xacab.org           vivmyccb3jdb7yij.onion (port 80)
-----BEGIN PGP SIGNATURE-----

iQKTBAEBCgB9FiEETgeRJo98Z+q+iPGwMEPitxOado4FAli0RZhfFIAAAAAALgAo
aXNzdWVyLWZwckBub3RhdGlvbnMub3BlbnBncC5maWZ0aGhvcnNlbWFuLm5ldDRF
MDc5MTI2OEY3QzY3RUFCRTg4RjFCMDMwNDNFMkI3MTM5QTc2OEUACgkQMEPitxOa
do5u7BAAuBPYcnuU4HAQtddb+p8y0V+Fw76fPszPjIE19ACTtfN39U+NyhSj/5LI
i7n2++O6lXhNfwnh1A5OPIHxv8ZbA9pMeXZFYA3gHC1IVRNokRq22uxvCrfastS6
BNmGICsTuHqIcbiZJgkkaQImywpOryT0aoWHgGU1QgprK27sWIz6tfUt5KXH5vvx
EAyx8itiREJtNQwVMFk3epVCAnl1rAfay/6Gk/jz7rLji3mFjVzGf3wEXff3OuTS
jVg5NqAO99k8RjHvaNqVCVkMOdPjoByvVrvJ68XHtbk+ICKDQtwTMiktgKBdAaVr
2tf/vWeOyB/egvjpM89+uLHsxIujvUjGAUxUt/W0cu1mCC3VpdAeR7Wj+1NomNlw
Iw0U07LVT8fqBL42CaZowtkiVAuGZ9+Aeam+ys53CksQ2/phLCZ18JNgzpBZKBnr
x62vnfskmezW0SRjTlMbwlVejtg2HTlx6aVUd2wS8BTNyl+c7W6MMybYIxV/iNA4
S/y5sJbcJNn5iRqIg33i95+1hhTvUqZYnvXFsXCdsgTvy4CrUt5n5vSkU9vPqBA8
bIojBuofKErdf/vTT112c3hz0xE5LDerGuftCO4UmeOx1Cf3d2JiRRmWD0Xg5sdx
4BL4mJThuyabxTNdLX8lS0kRvXtgY/1owiQ90VAS0ykg4FqXe8U=
=2Mol
-----END PGP SIGNATURE-----
```

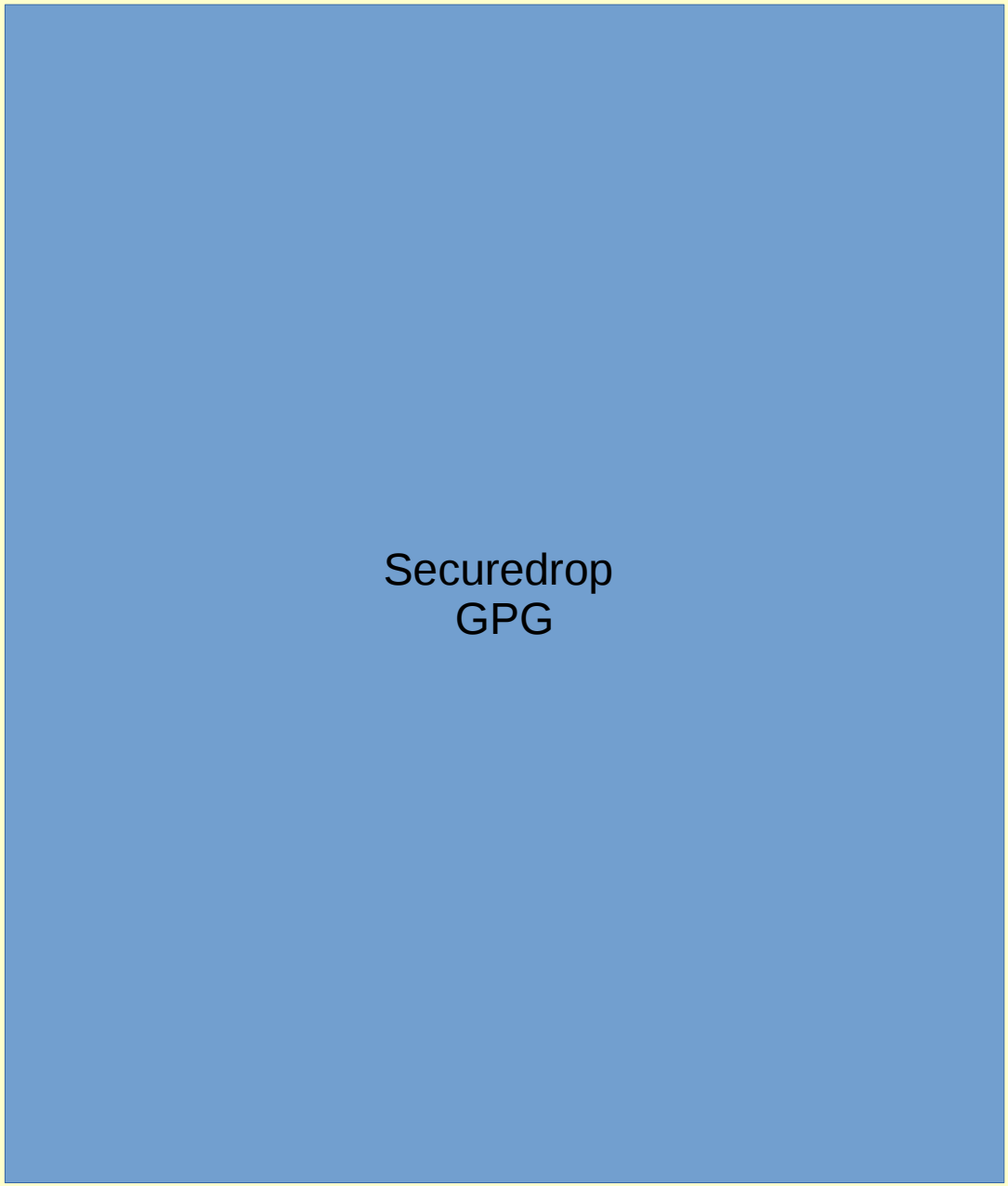
http://nzh3fv6jc6jskki3.onion/security/network-security/tor/hs-addresses-signed.txt
https://riseup.net/security/network-security/tor/hs-addresses-signed.txt

Bootstrapping? Discoverability?





Bootstrapping? Discoverability?



Bootstrapping? Discoverability?

Riseup, about to type in url

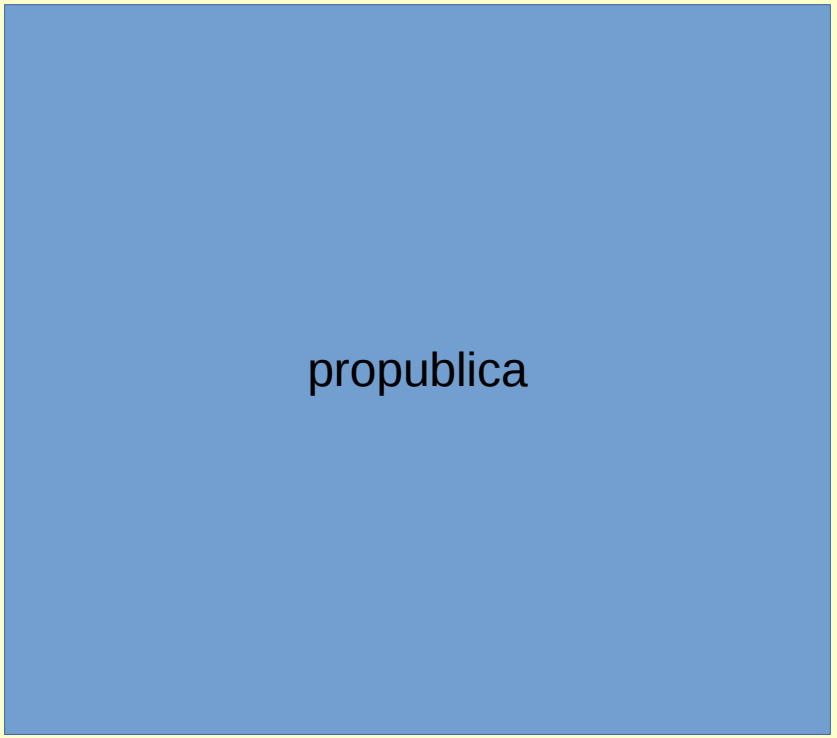
.onion redirect

Bootstrapping? Discoverability?

whonix

qubes

Bootstrapping? Discoverability?

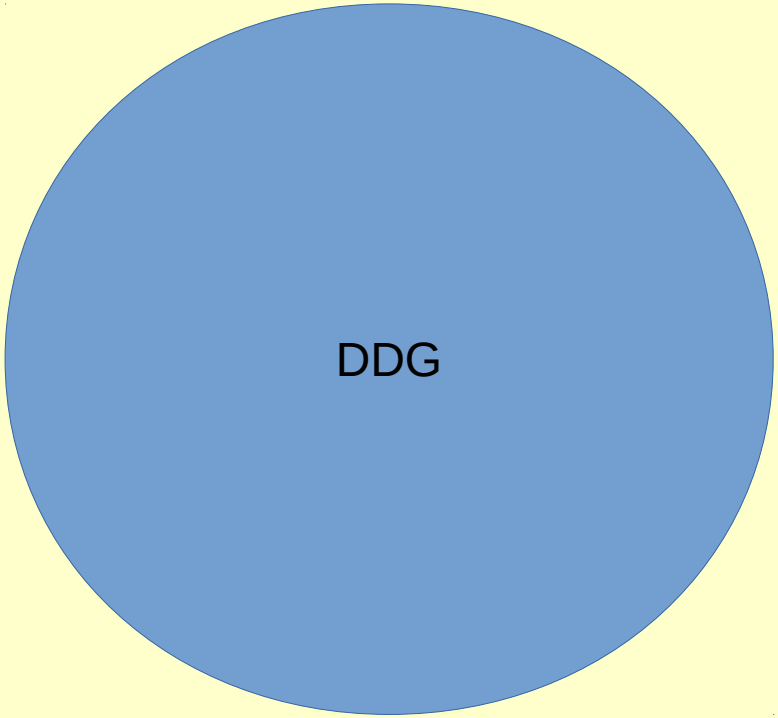


Bootstrapping? Discoverability?

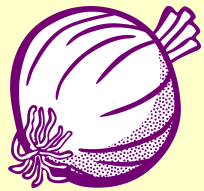
Autistici/Inventati

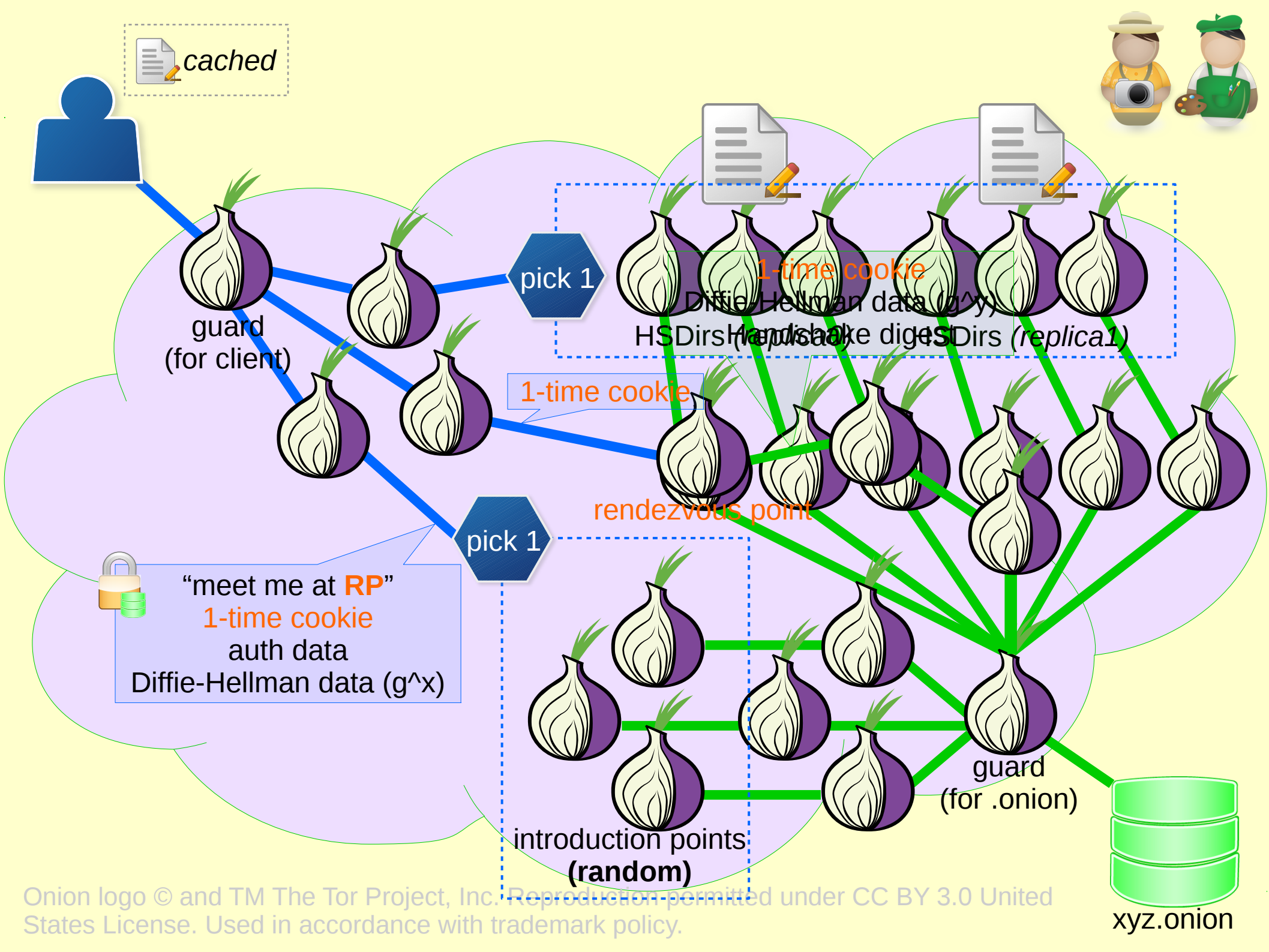
Bootstrapping? Discoverability?

Tails logo

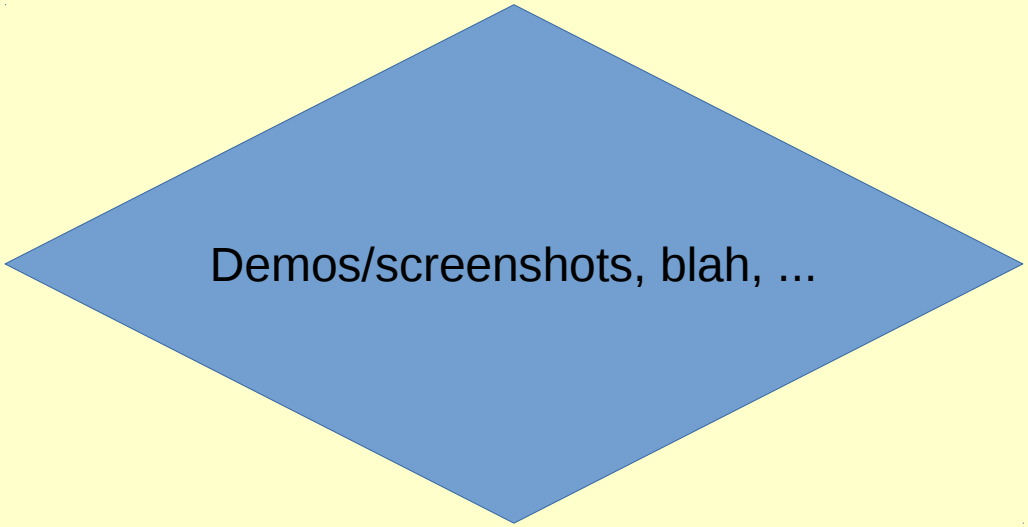


Bootstrapping? Discoverability?





HTTPS + .onion



HTTPS + .onion

Metrics...