

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

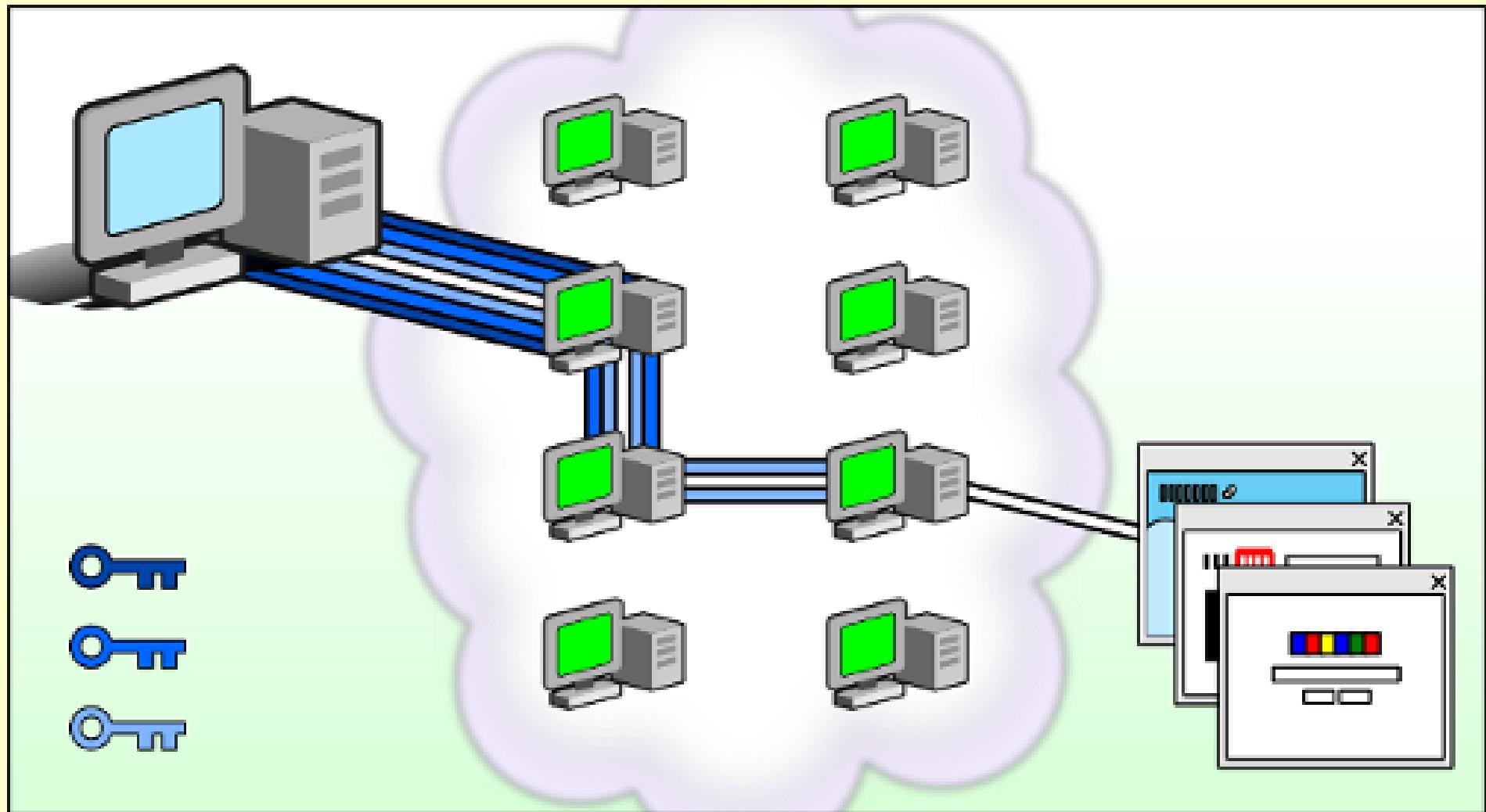
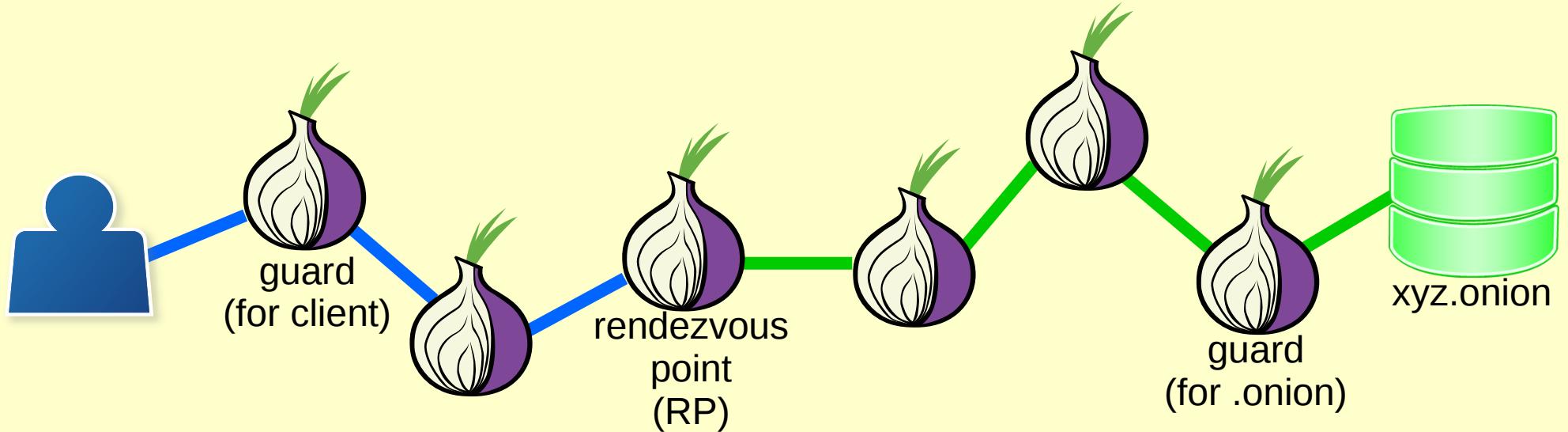


Image © The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License.



Onion Services – Intro



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



In the browser...

DuckDuckGo - Tor Browser

duck duck go onion a... × DuckDuckGo × +

🔍 Duck Duck Go, Inc. (US) | https://3g2upl4pq6kufc4m.onion | ⌂ 🔍 duck duck go onion → 🛡️ ⏓



DuckDuckGo

S

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





.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
 - ...

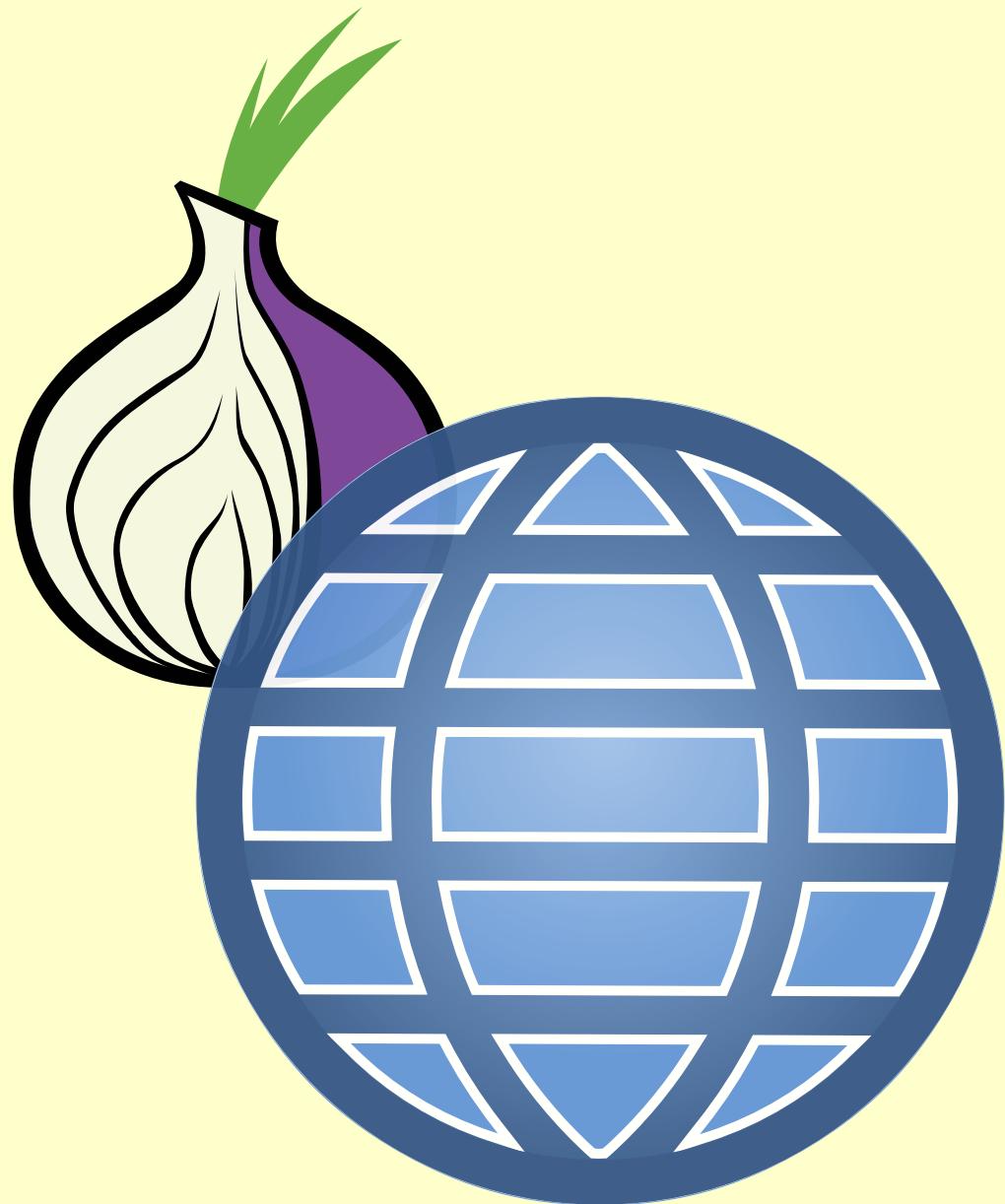


DEMO TIME

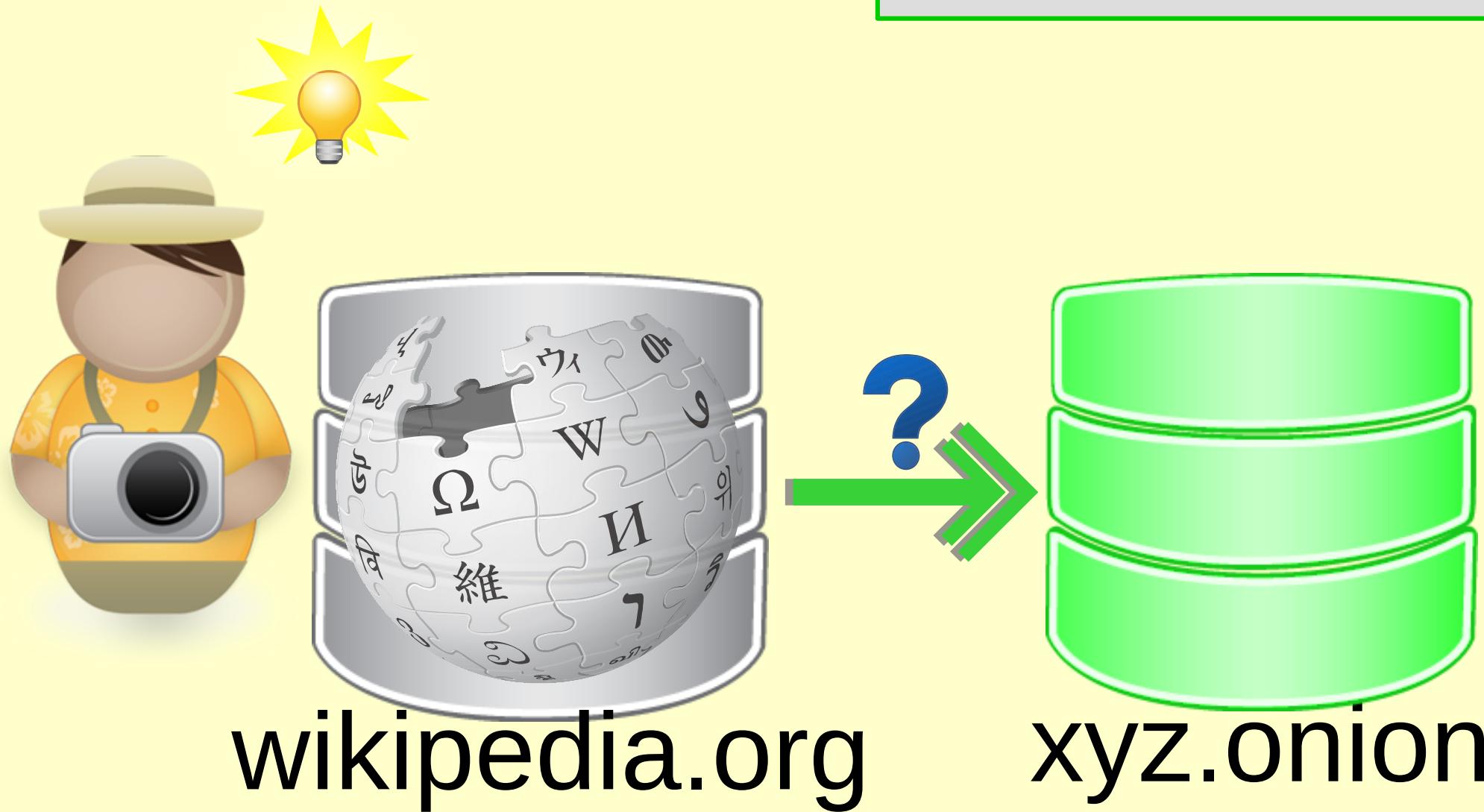
BANG



ground survey: public



Bootstrapping? Discoverability?





here be dragons

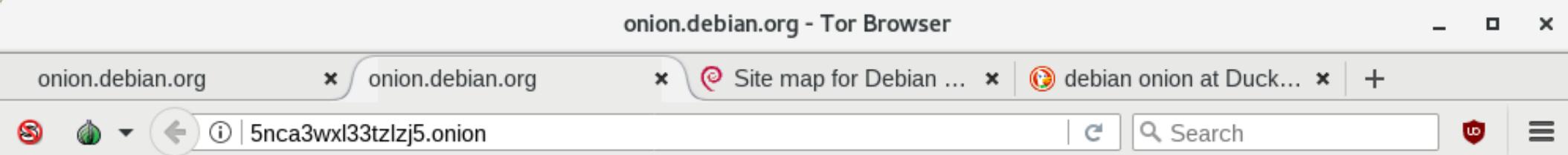
Bootstrapping? Discoverability?

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/): <http://b5tearqs4v4nvbup.onion/>
- [appstream.debian.org](http://5j7saze5byfqccf3.onion/): <http://5j7saze5byfqccf3.onion/>
- [apt.buildd.debian.org](http://ito4xpoj3re4wctm.onion/): <http://ito4xpoj3re4wctm.onion/>
- [backports.debian.org](http://6f6ejaiiixypfqaf.onion/): <http://6f6ejaiiixypfqaf.onion/>
- [bits.debian.org](http://4ypuij3wwrg5zoxm.onion/): <http://4ypuij3wwrg5zoxm.onion/>
- [blends.debian.org](http://bcwpy5wca456u7tz.onion/): <http://bcwpy5wca456u7tz.onion/>
- [bootstrap.debian.net](http://ihdhoeovbtgutfm.onion/): <http://ihdhoeovbtgutfm.onion/>
- [cdimage-search.debian.org](http://4zhlmuhqvjkvspwb.onion/): <http://4zhlmuhqvjkvspwb.onion/>
- [d-i.debian.org](http://f6syxyjdgzbeacry.onion/): <http://f6syxyjdgzbeacry.onion/>
- [debaday.debian.net](http://ammd7ytxcpeavif2.onion/): <http://ammd7ytxcpeavif2.onion/>
- [debconf0.debconf.org](http://ynr7muu3263jikep.onion/): <http://ynr7muu3263jikep.onion/>
- [debconf1.debconf.org](http://4do6yq4iwstidagh.onion/): <http://4do6yq4iwstidagh.onion/>
- [debconf16.debconf.org](http://6nhxqcogfcwqzgnm.onion/): <http://6nhxqcogfcwqzgnm.onion/>
- [debconf2.debconf.org](http://ugw3zjsayleoamaz.onion/): <http://ugw3zjsayleoamaz.onion/>
- [debconf3.debconf.org](http://zdfsyy3rubuhpq3.onion/): <http://zdfsyy3rubuhpq3.onion/>
- [debconf4.debconf.org](http://eeblrw5eh2is36az.onion/): <http://eeblrw5eh2is36az.onion/>
- [debconf5.debconf.org](http://3m2tlhjsoxws2akz.onion/): <http://3m2tlhjsoxws2akz.onion/>
- [debconf6.debconf.org](http://gmi5gld3uk5ozvrv.onion/): <http://gmi5gld3uk5ozvrv.onion/>
- [debconf7.debconf.org](http://465rf3c2oskkqc24.onion/): <http://465rf3c2oskkqc24.onion/>
- [debdtas.debian.net](http://vral2uljb3ndhhxr.onion/): <http://vral2uljb3ndhhxr.onion/>
- [debug.mirrors.debian.org](http://ktqxbqrhg5ai2c7f.onion/): <http://ktqxbqrhg5ai2c7f.onion/>
- [dpl.debian.org](http://i73wbfppplklpixbh.onion/): <http://i73wbfppplklpixbh.onion/>
- [dsa.debian.org](http://f7bphdxlqca3sevt.onion/): <http://f7bphdxlqca3sevt.onion/>
- [es.debconf.org](http://nwk3svshonwfqfs.onion/): <http://nwk3svshonwfqfs.onion/>
- [fr.debconf.org](http://ythg247lqkx2gpgx.onion/): <http://ythg247lqkx2gpgx.onion/>
- [ftp.debian.org](http://wwakviie2ienjx6t.onion/): <http://wwakviie2ienjx6t.onion/>
- [ftp.ports.debian.org](http://nbvhwh4atabu6xq3.onion/): <http://nbvhwh4atabu6xq3.onion/>

Bootstrapping? Discoverability?

Facebook - Log In or Sign Up - Tor Browser

Facebook - Log In or ... | facebook onion at Du... | facebookcorewwwi.o... | List of Tor hidden ser...

https://www.facebook.com

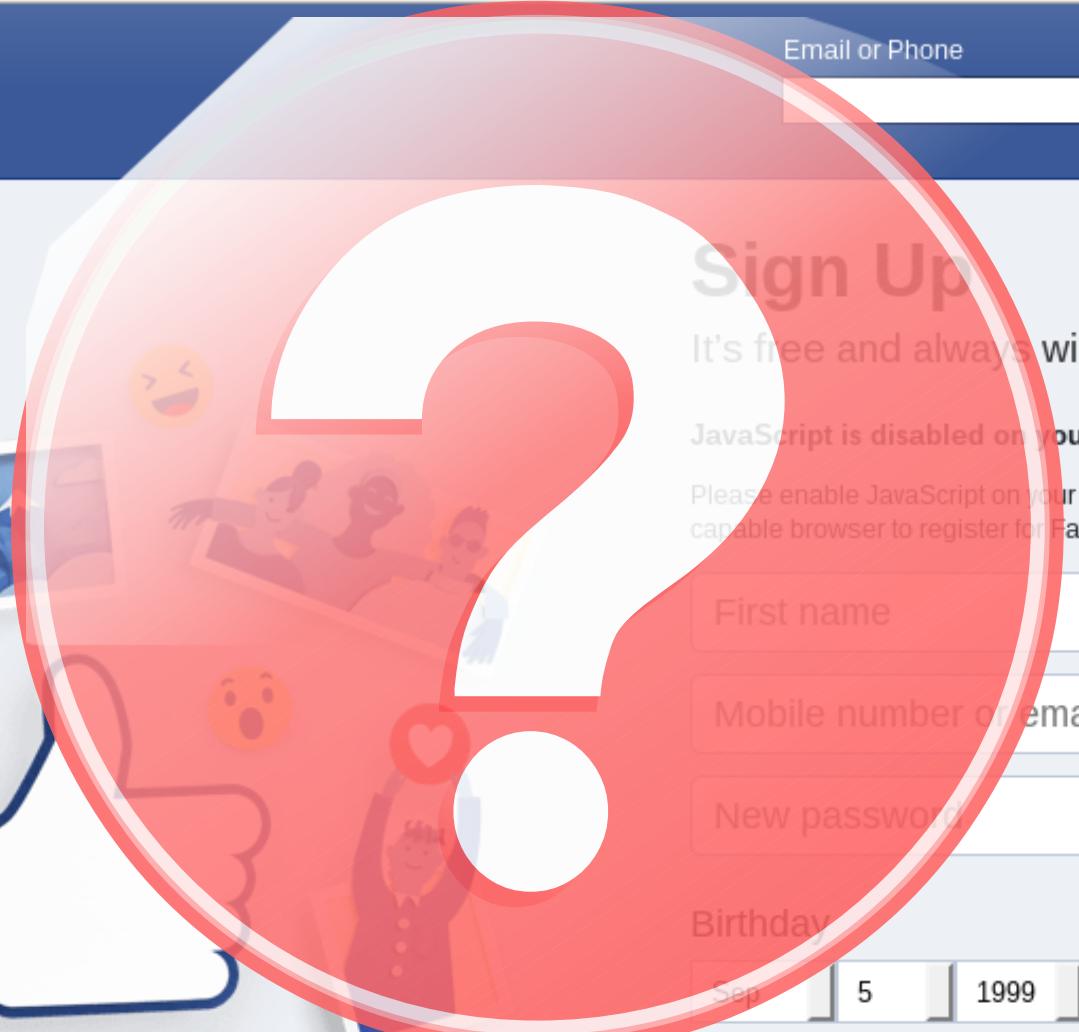
Search

Email or Phone
Password
Forgot account? Log In

Sign Up
It's free and always will be.
JavaScript is disabled on your browser.
Please enable JavaScript on your browser or upgrade to a JavaScript-capable browser to register for Facebook.

First name Last name
Mobile number or email
New password
Birthday
Sep 5 1999 Why do I need to provide my birthday?
 Female Male

Welcome to Facebook! We're glad you're here.



By clicking Create Account, you agree to our [Terms](#) and that you have read our [Data Policy](#), including our [Cookie Use](#). You may

Bootstrapping? Discoverability?

The image displays two side-by-side screenshots of the Qubes OS website, illustrating different URL formats and their discoverability.

Left Site (Purple Border):

- URL:** `qubesosmamapaxpa.onion`
- Content:** The page features a large blue button labeled "Download & Install Version 3.2". Below it are links for "What is Qubes OS?" and "Watch a Video Tour". A section titled "What the experts are saying" includes a quote from Ouhes: "If you're serious about security, Qubes..." and a quote from Hanny: "Hanny thought of the day: An attacker".

Right Site (Green Border):

- URL:** `qubesos4rrrz6n4.onion`
- Content:** The page features a large blue button labeled "Download & Install Version 3.2". Below it are links for "What is Qubes OS?" and "Watch a Video Tour". A section titled "What the experts are saying" includes a quote from Ouhes: "If you're serious about security, Qubes..." and a quote from Hanny: "Hanny thought of the day: An attacker".

In both cases, the URL in the browser's address bar is highlighted with a red box, emphasizing the difference between the two discoverable addresses.

Bootstrapping? Discoverability?

The image shows two identical screenshots of the Qubes OS website's news section, displayed side-by-side. A large, semi-transparent blue circle containing a white question mark is positioned in the center, overlapping both screens. The left screen has a purple border, and the right screen has a green border.

News | Qubes OS - Tor Browser

News | Qubes OS | qubesosmapapxa.onion/news/

Intro Downloads Docs News Team Donate

News

News by Category

F0 F1 F2 F3 F4 F5 F6

Qubes Security Bulletin (QSB) #28: Debian update mechanism vulnerability
Dec 19, 2016 by Qubes OS in [Security](#)

[Video] Interview about Qubes OS on The New Screen Savers
Dec 17, 2016 by [Andrew David Wong](#) in [Press](#)

Qubes Canary #10
Dec 13, 2016 by Qubes OS in [Security](#)

Qubes OS Begins Commercialization and Community Funding Efforts
Nov 30, 2016 by [Joanna Rutkowska](#) in [Announcements](#)

Qubes Security Bulletin #27: Xen 64-bit bit test instruction emulation broken (XSA 195)
Nov 22, 2016 by Qubes OS in [Security](#)

The Qubes Project will be present at 33C3

News

News by Category

F0 F1 F2 F3 F4 F5 F6

XSA-235 does not affect the security of Qubes OS
Aug 23, 2017 by [Andrew David Wong](#) in [Security](#)

QSB #32: Xen hypervisor and Linux kernel vulnerabilities (XSA-226 through XSA-230)
Aug 21, 2017 by Qubes OS in [Security](#)

Qubes OS 4.0-rc1 has been released!
Jul 21, 2017 by [Joanna Rutkowska](#) in [Announcements](#)

Recommended Fedora 25 TemplateVM Upgrade for Qubes 3.2
Jul 29, 2017 by [Andrew David Wong](#) in [Announcements](#)

Toward a Reasonably Secure Laptop
Jul 8, 2017 by [Andrew David Wong](#) in [Announcements](#)

Introducing the Qubes Admin API

News

News by Category

F0 F1 F2 F3 F4 F5 F6

Qubes Security Bulletin (QSB) #28: Debian update mechanism vulnerability
Dec 19, 2016 by Qubes OS in [Security](#)

News

News by Category

F0 F1 F2 F3 F4 F5 F6

XSA-235 does not affect the security of Qubes OS
Aug 23, 2017 by [Andrew David Wong](#) in [Security](#)

Bootstrapping? Discoverability?

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



...when not done over Tor...

- SNI anyone? (*Server Name Indication 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>



SECUREDROP

Bootstrapping? Discoverability?



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

...when not done over Tor...

- SNI anyone? (*Server Name Indication in TLS*)

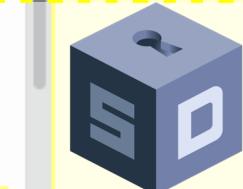
- <https://securedrop.theguardian.com/>
- <https://securedrop.pogo.org/>
- <https://securedrop.propublica.org/>
- <https://securedrop.radiotimes.com/>
- <https://securedrop.docksal.com/>
- <https://securedrop.secureDrop.org/>
- <https://securedrop.safelocality.com/>
- <https://censored.securedrop.org/>
- <https://www.securedrop.org/>

The screenshot shows a web browser window displaying the URL https://docs.securedrop.org/en/stable/deployment_practices.html#landing-page. The page title is "SecureDrop Deployment Best Practices". The main content discusses the security of the environment and the need for basic security best practices. A yellow callout box highlights the following text from the "Landing Page" section:

Ideally you would not use a separate subdomain, but would use a path at your top-level domain, e.g. organization.com/securedrop. This is because TLS does not encrypt the hostname, so a SecureDrop user whose connection is being monitored would be trivially discovered.

If the landing page is deployed on the same domain as another site, you might

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



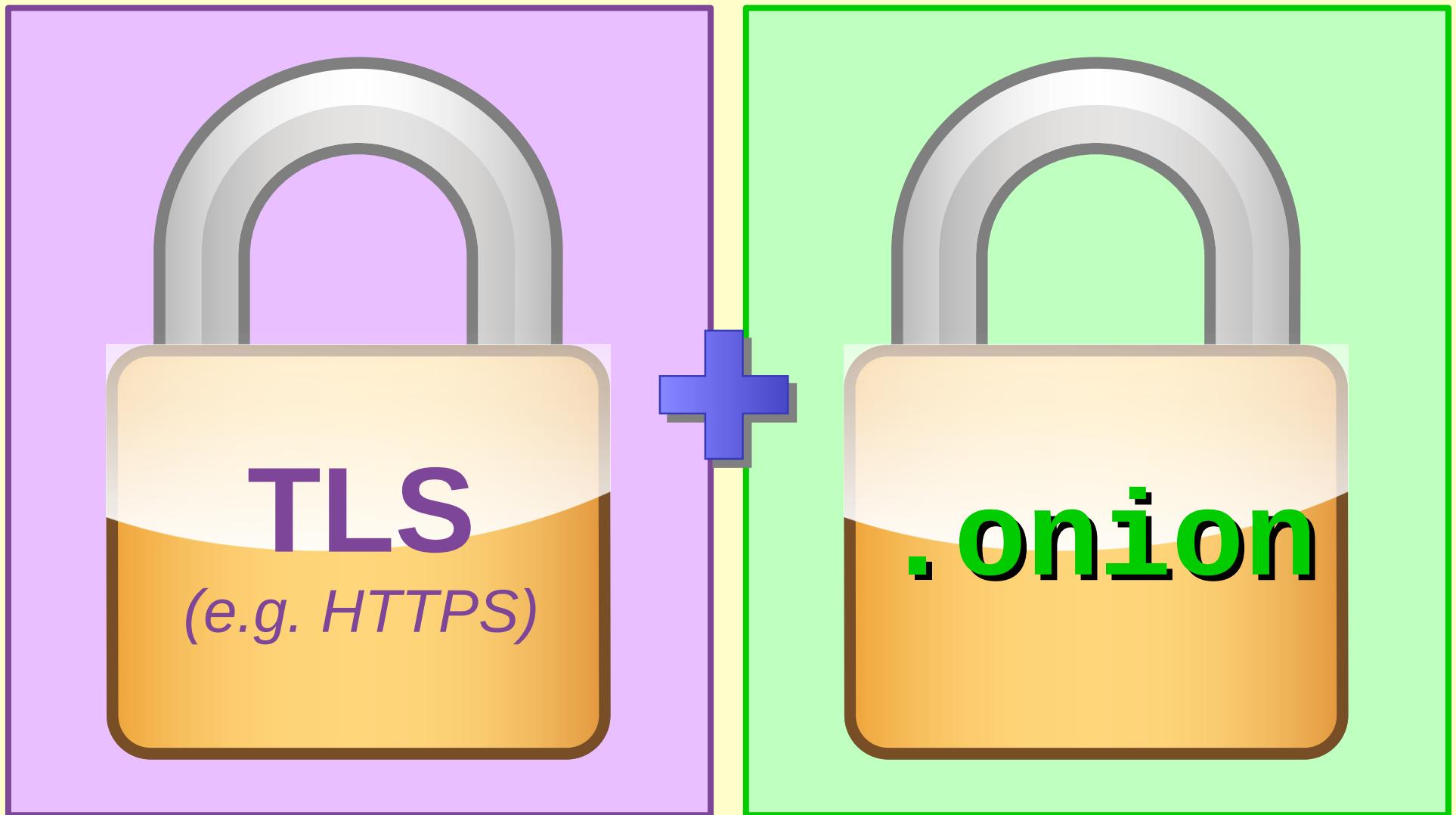
SECUREDROP

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 ...

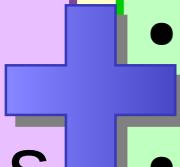


HTTPS + .onion



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

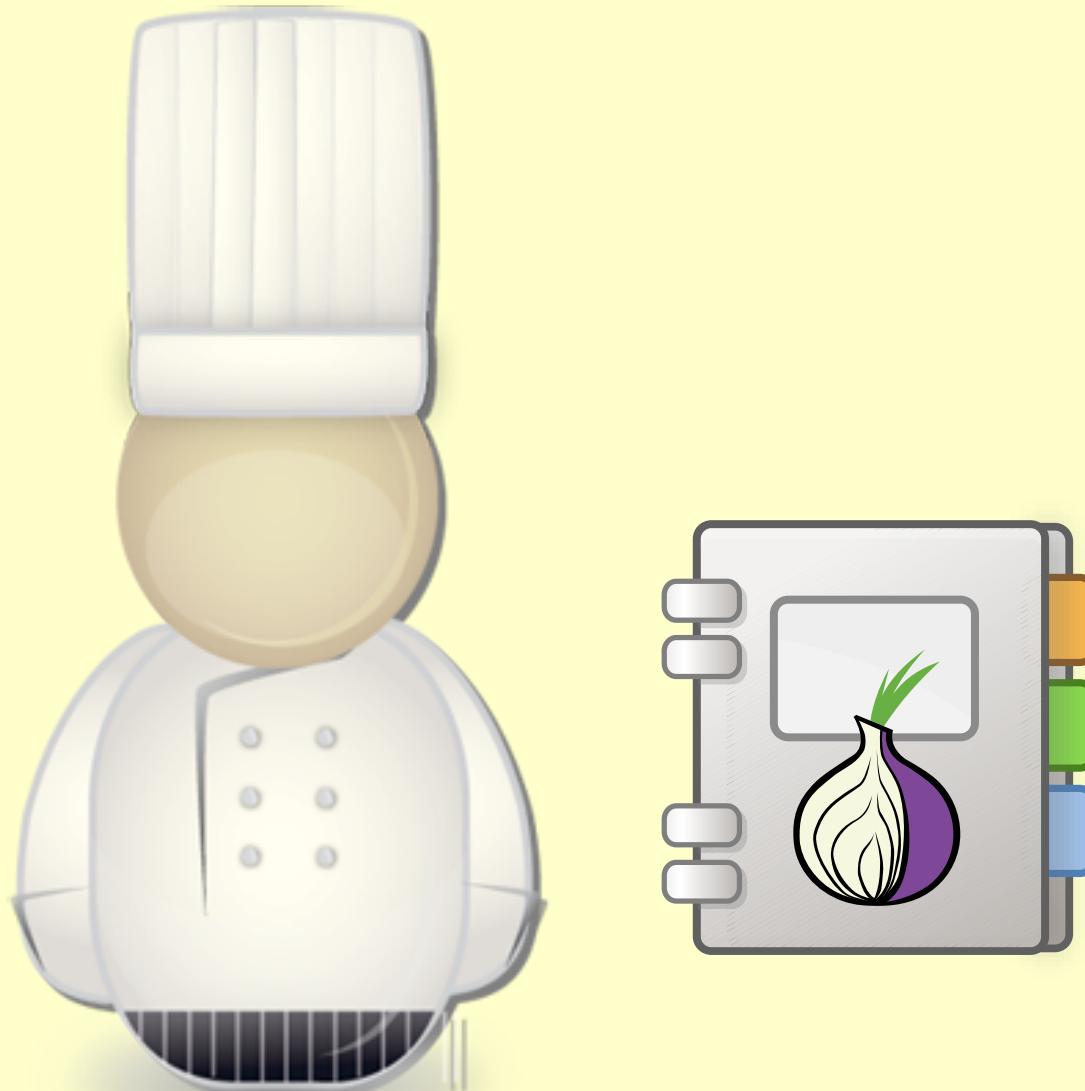


.onion usability, privacy

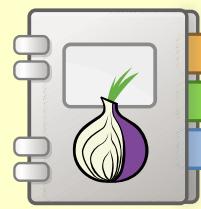
- .onion family “dropping”
- non-.onion resources (e.g. Google Analytics)
 - still use exits



.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://abcdefghijklmnopqrstuvwxyz.onion/path rel repos
```

- Privacy, but also security

- refs: 2008 academic paper, apt CVE 2016-1252

- Not just for personal machines

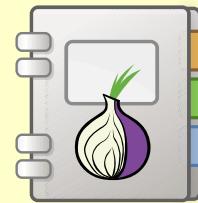
- ref: blog post about the server security gained from anonymity

- 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

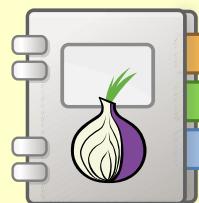
- hkp://jirk5u4osbsr34t5.onion

- 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

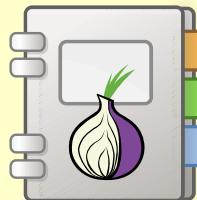
OnionShare ryypdaqg5st7zjeg.onion/figure-mummy

onionshare_jedtgt.zip ▾

64.2 MiB (compressed)

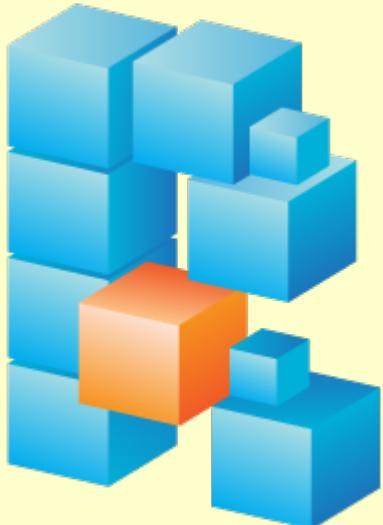
This zip file contains the following contents:

Type	Name	Size
Folder	leaks	196.9 MiB
File	instructions.rtf	1.2 KiB

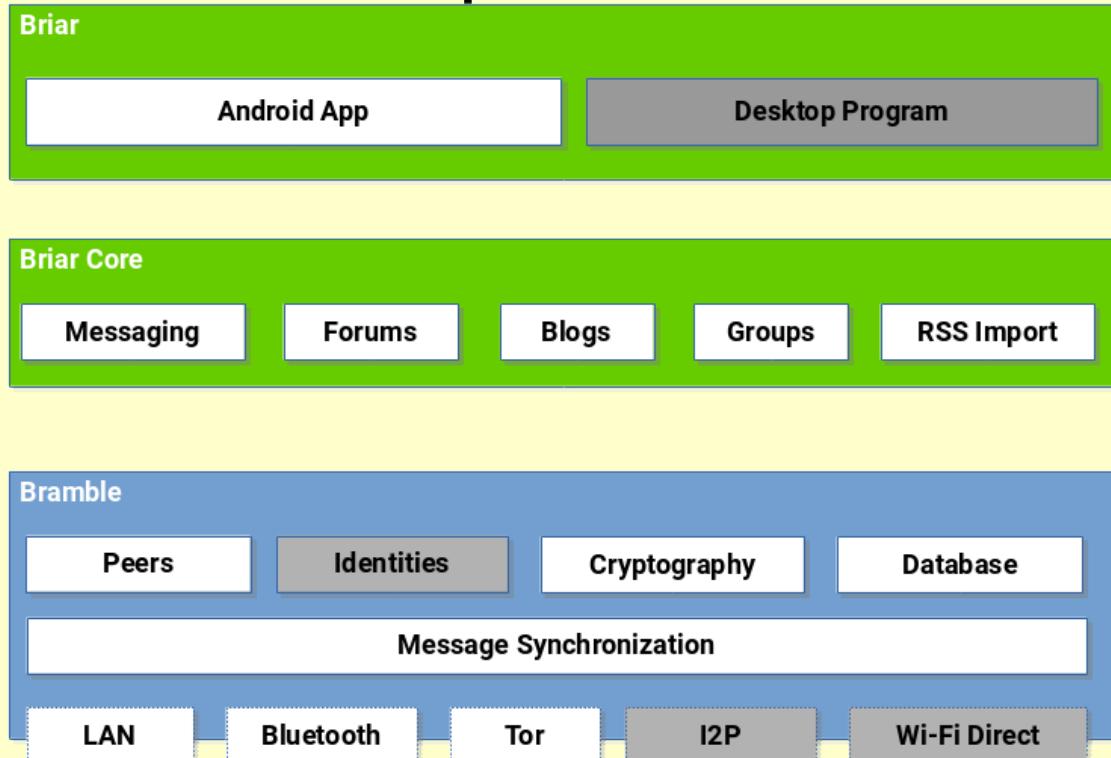


.onion messaging

- Ricochet



- Briar – public beta



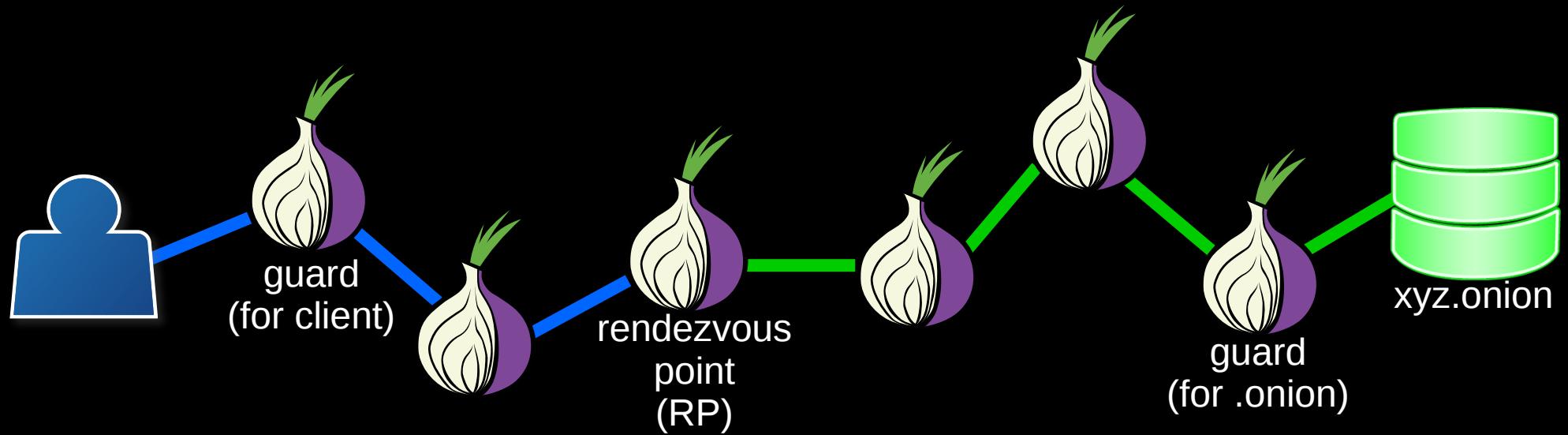
- unMessage – alpha
- Pond (??)

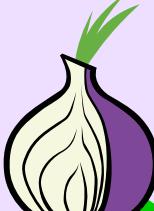


Rendezvous

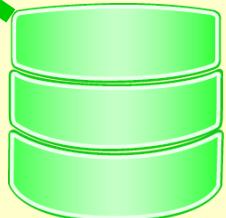


Rendezvous



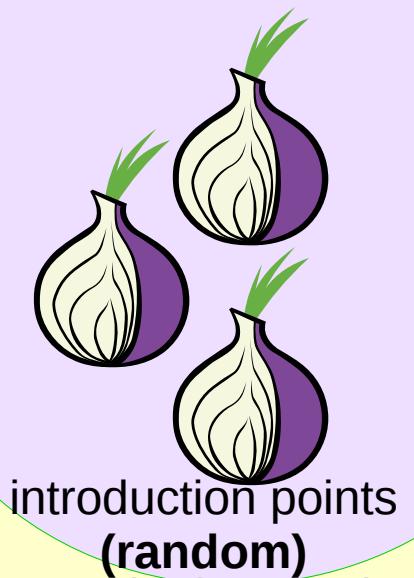


guard
(for .onion)

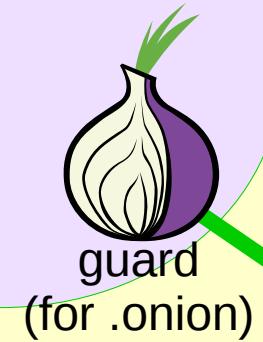


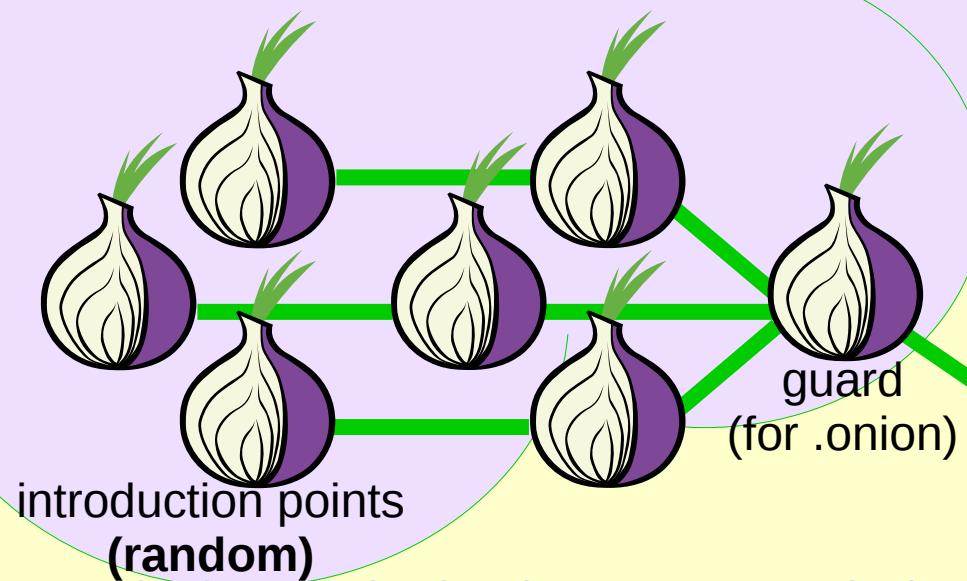
xyz.onion

Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.



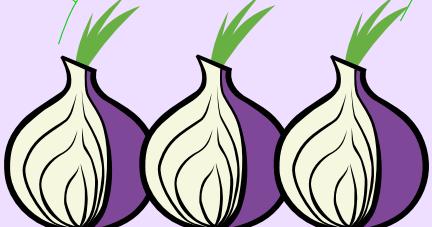
introduction points
(random)



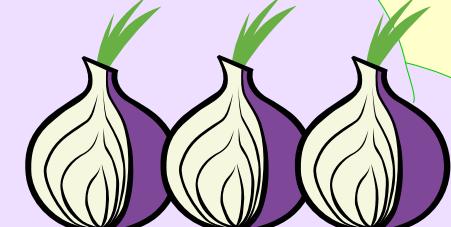


Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.

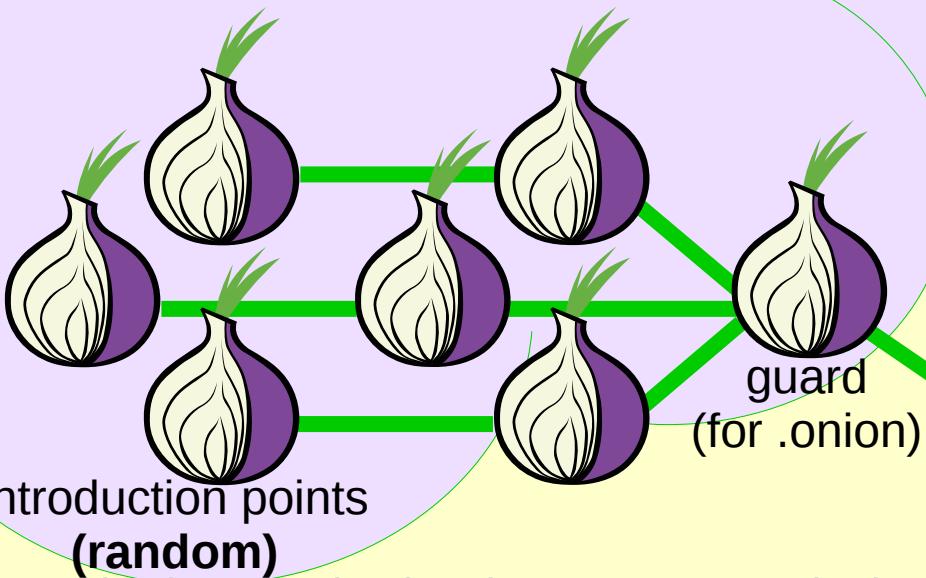
xyz.onion



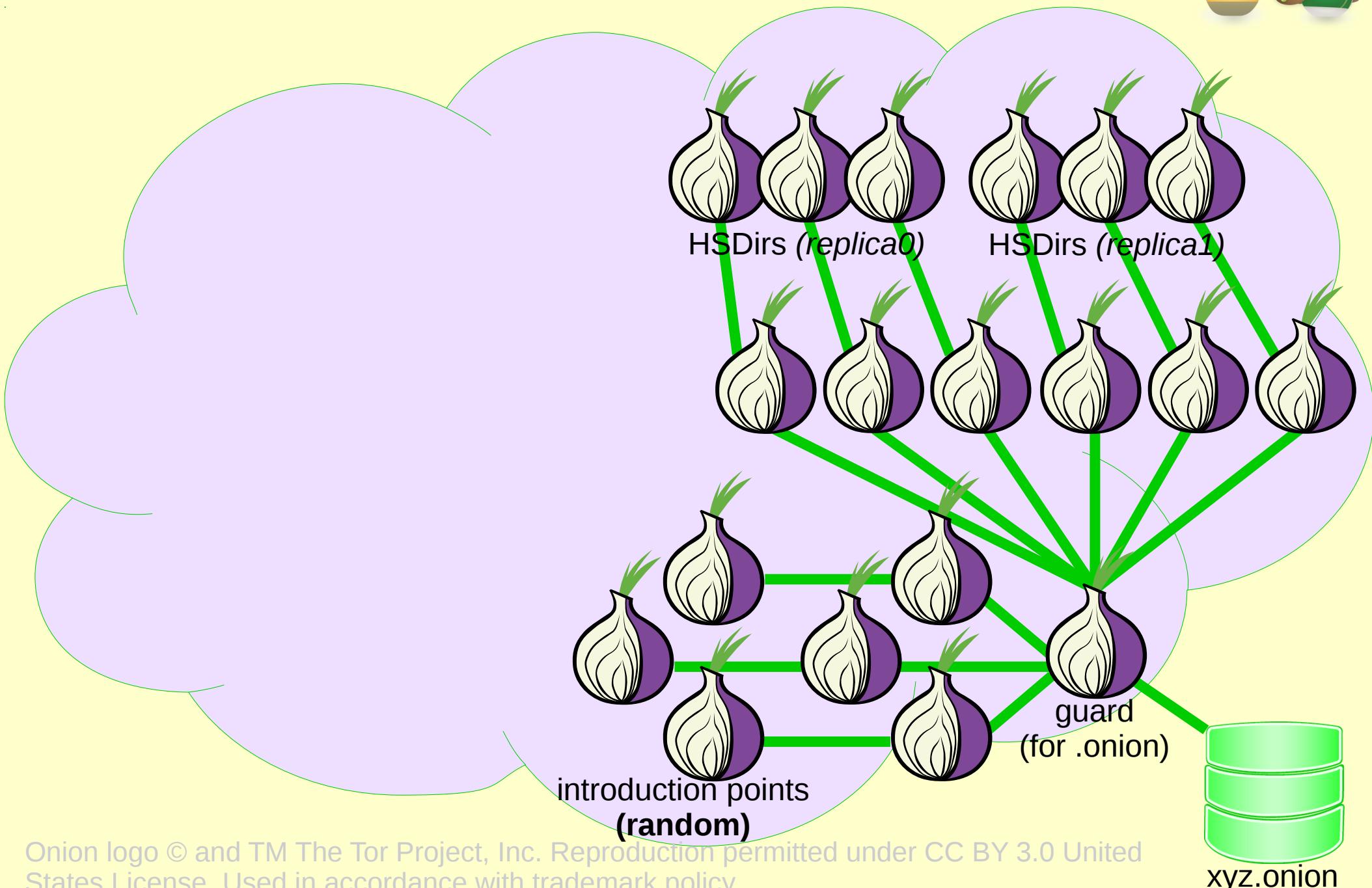
HSDirs (*replica0*)



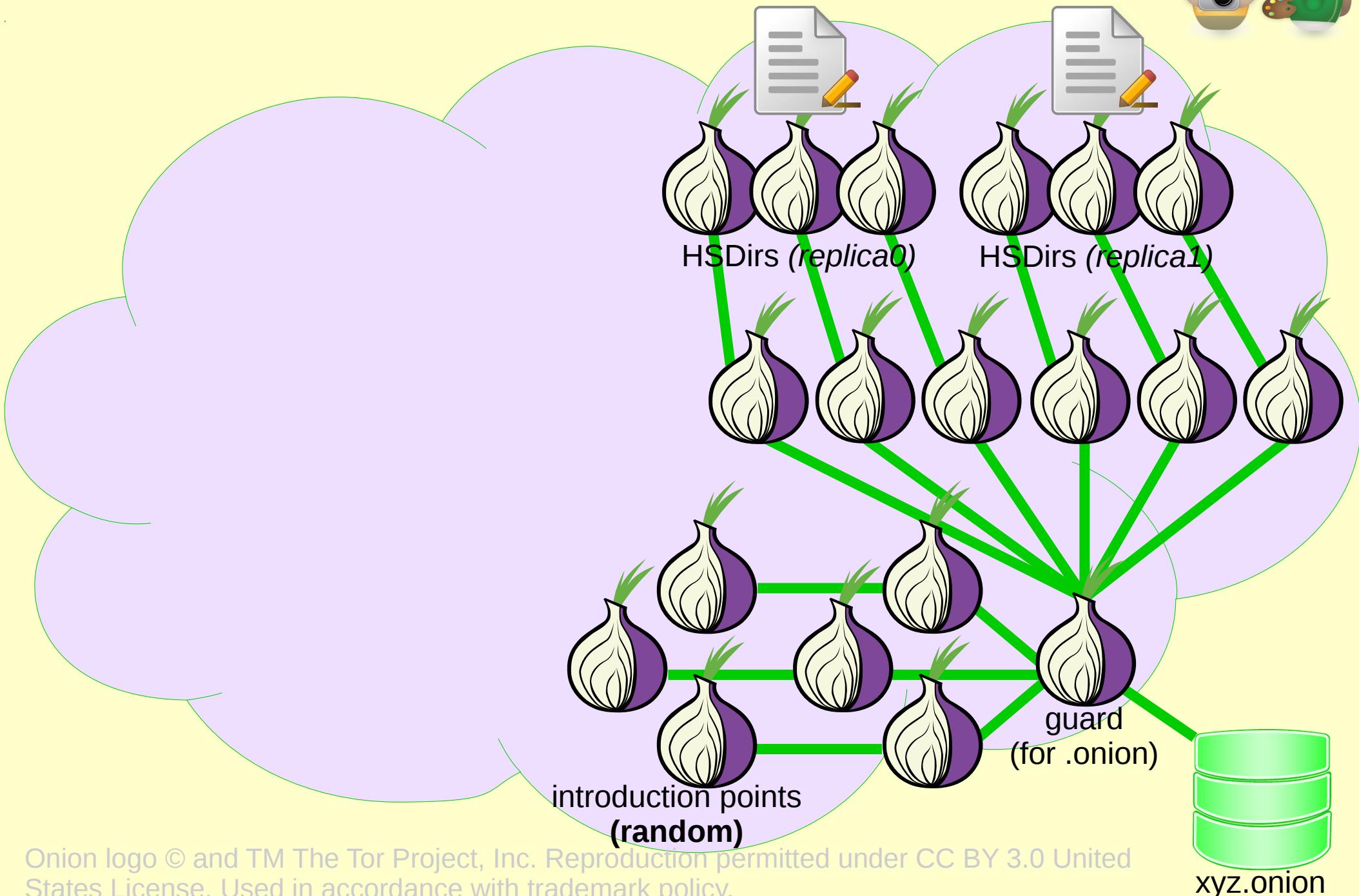
HSDirs (*replica1*)



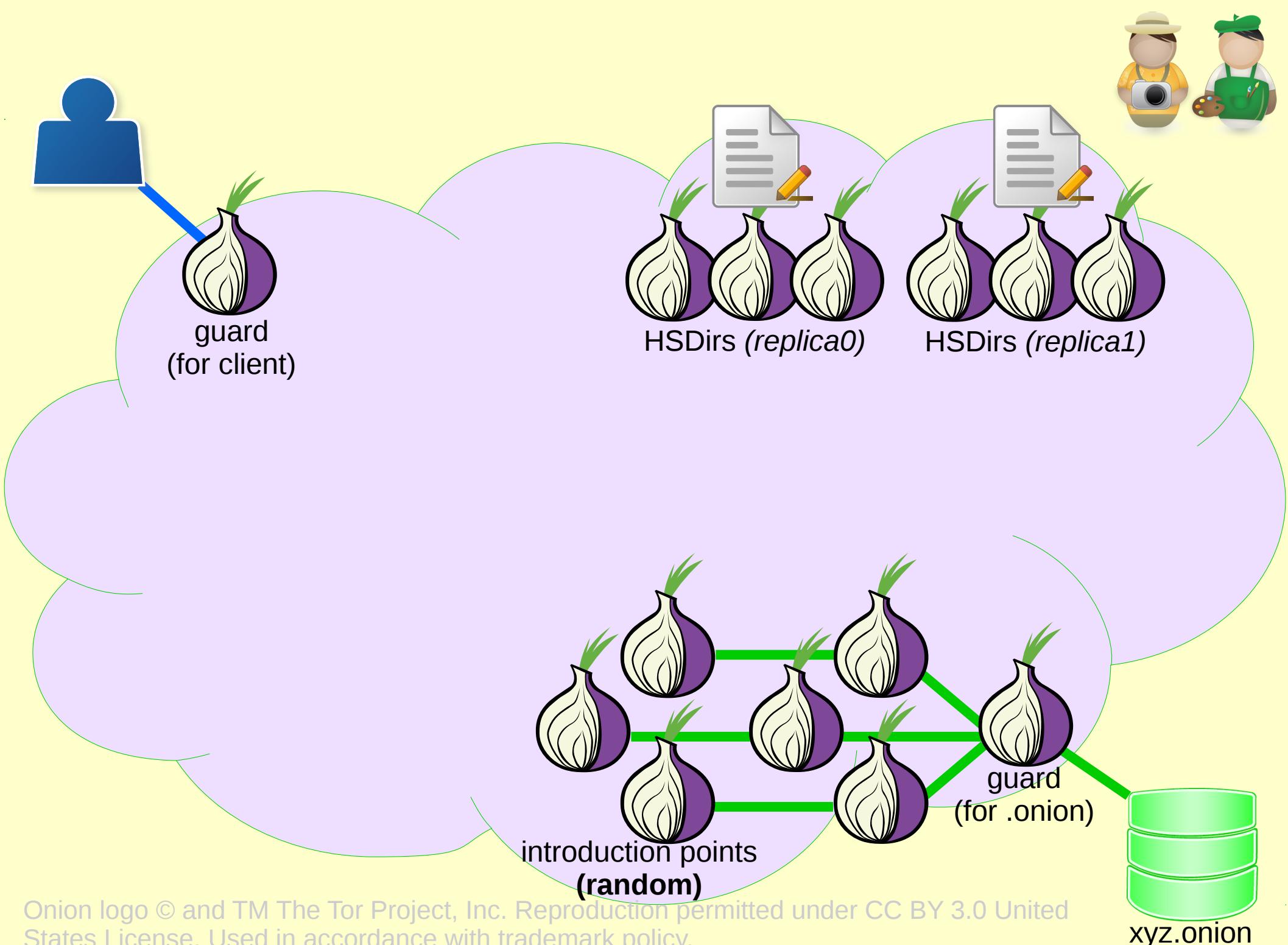
Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.

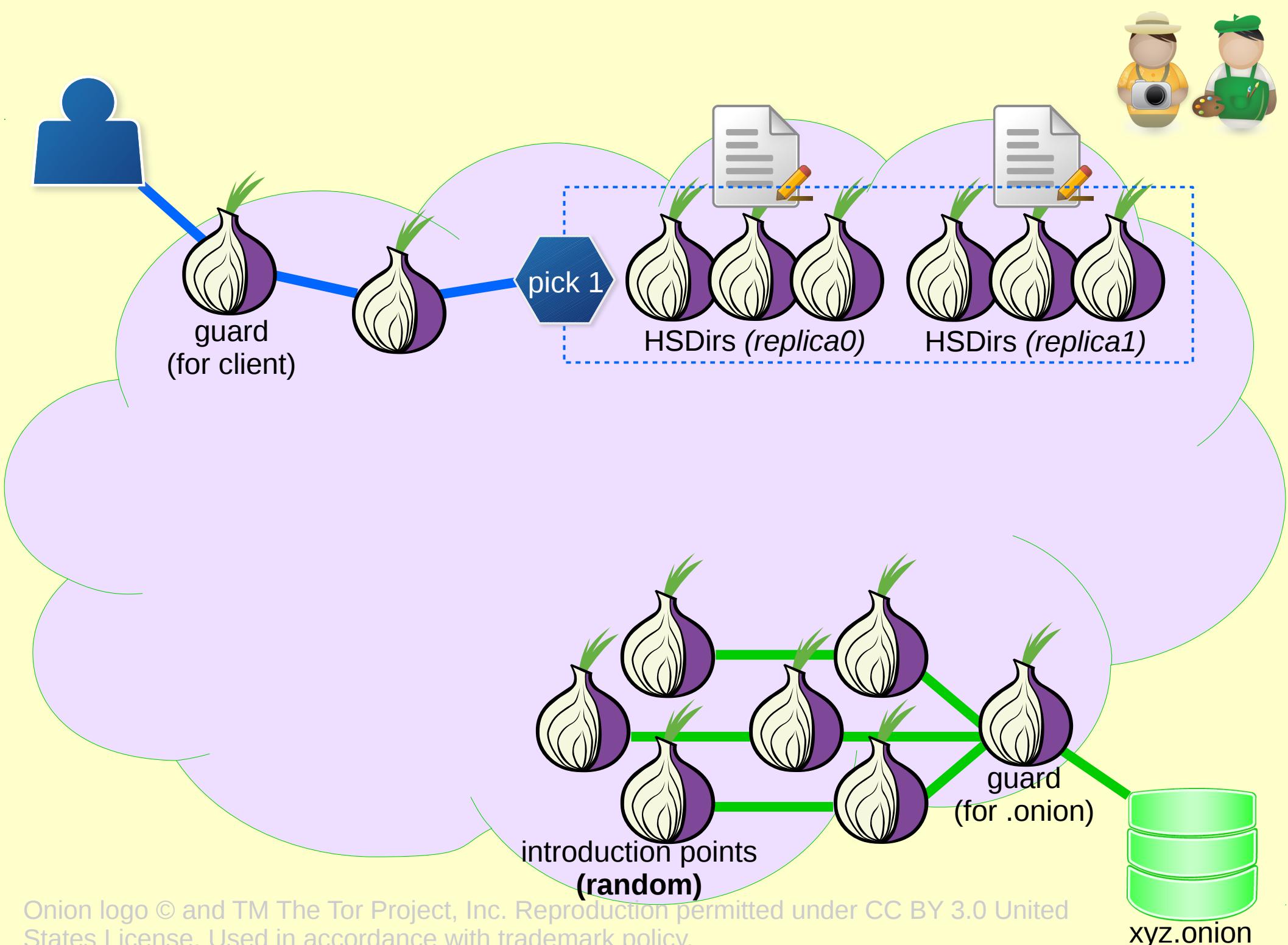


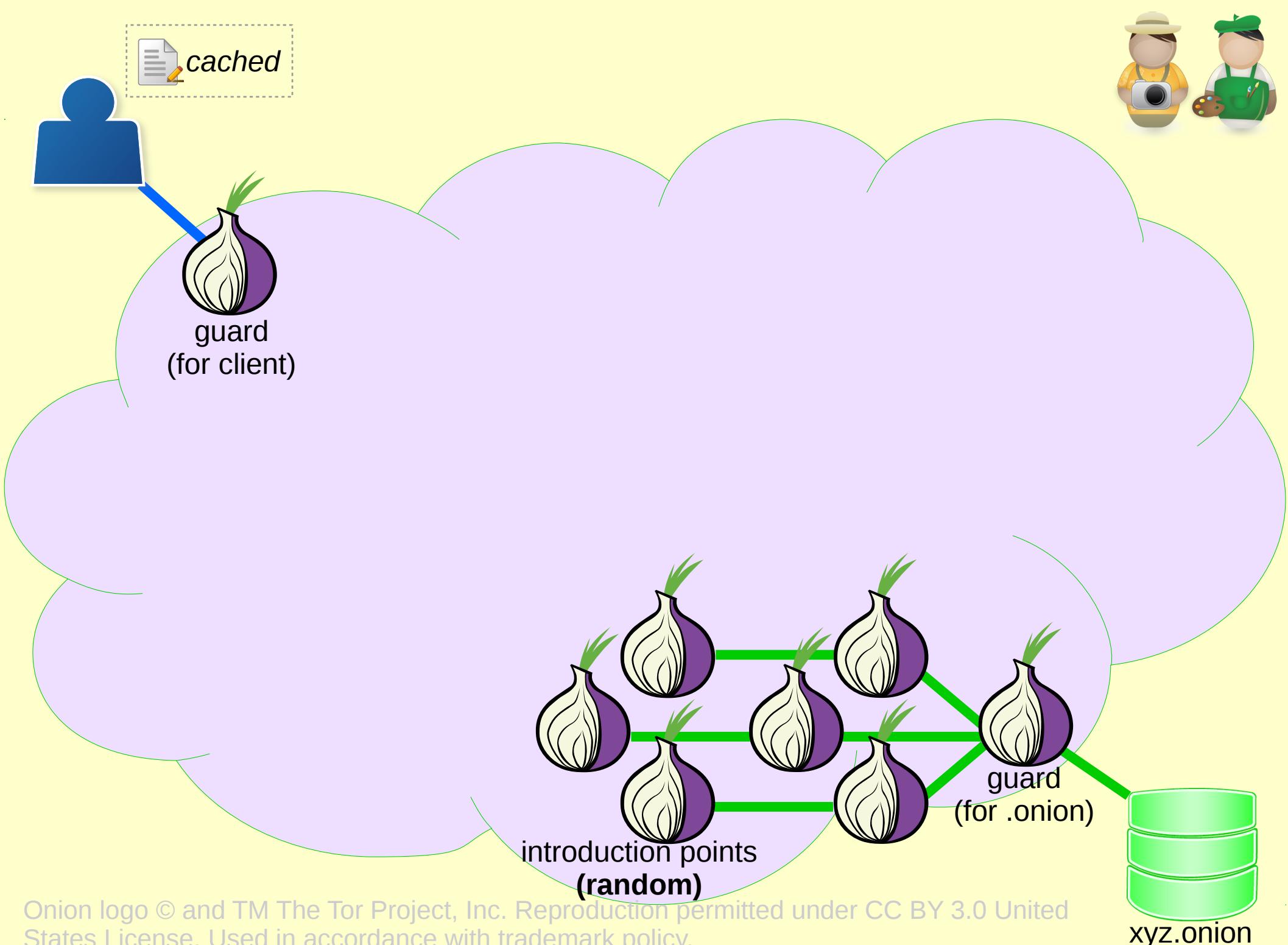
Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.



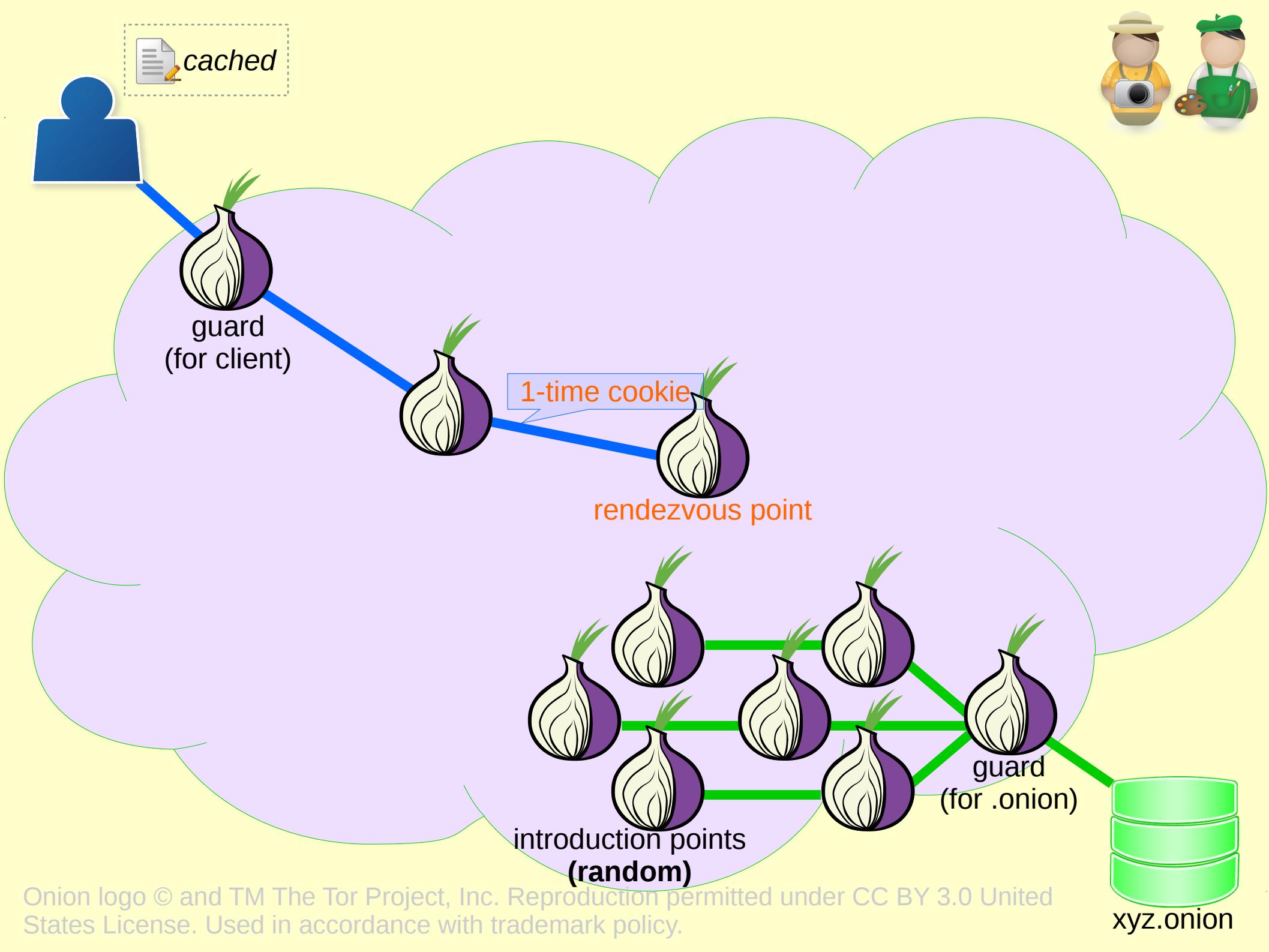
Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.



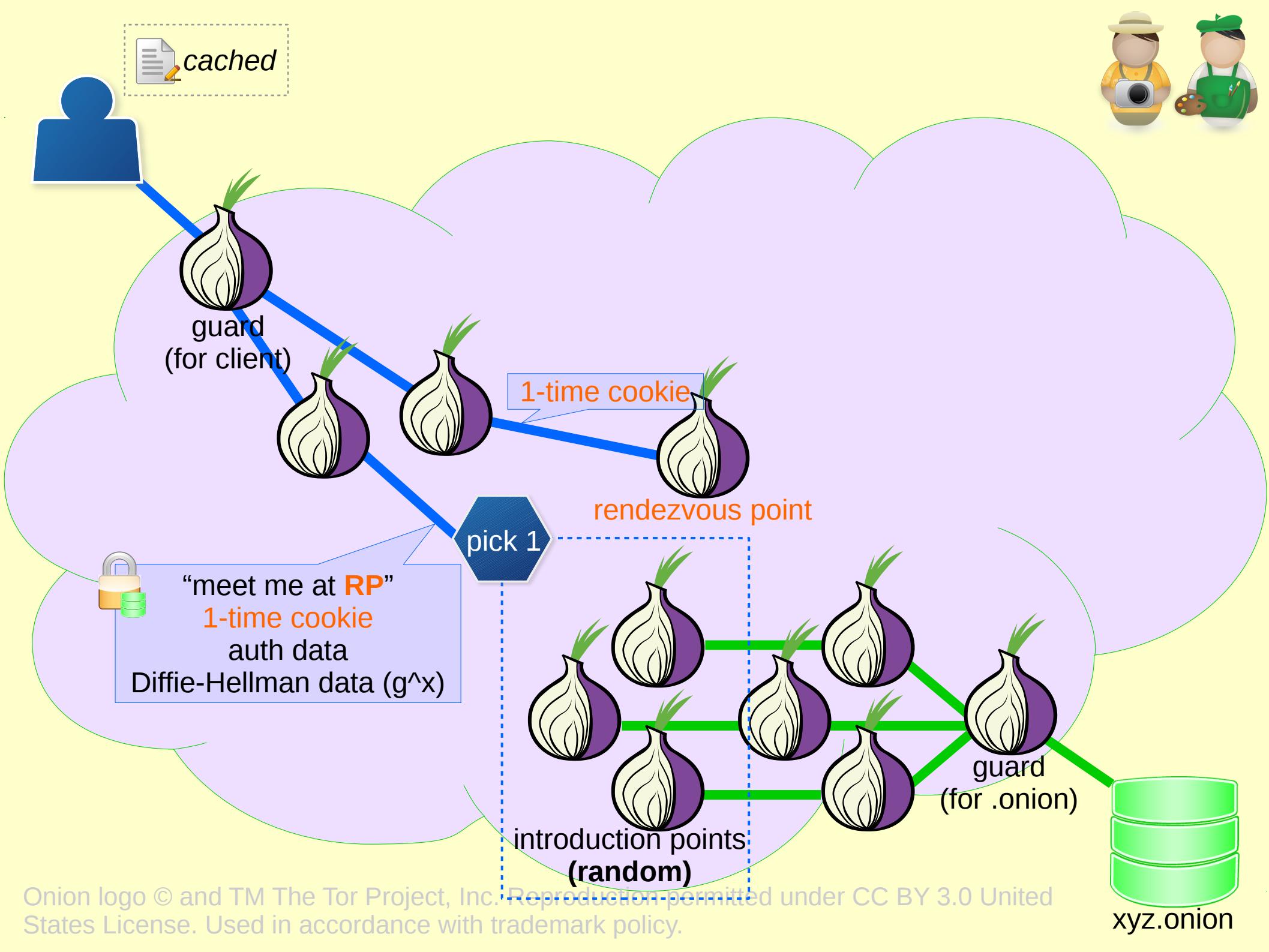


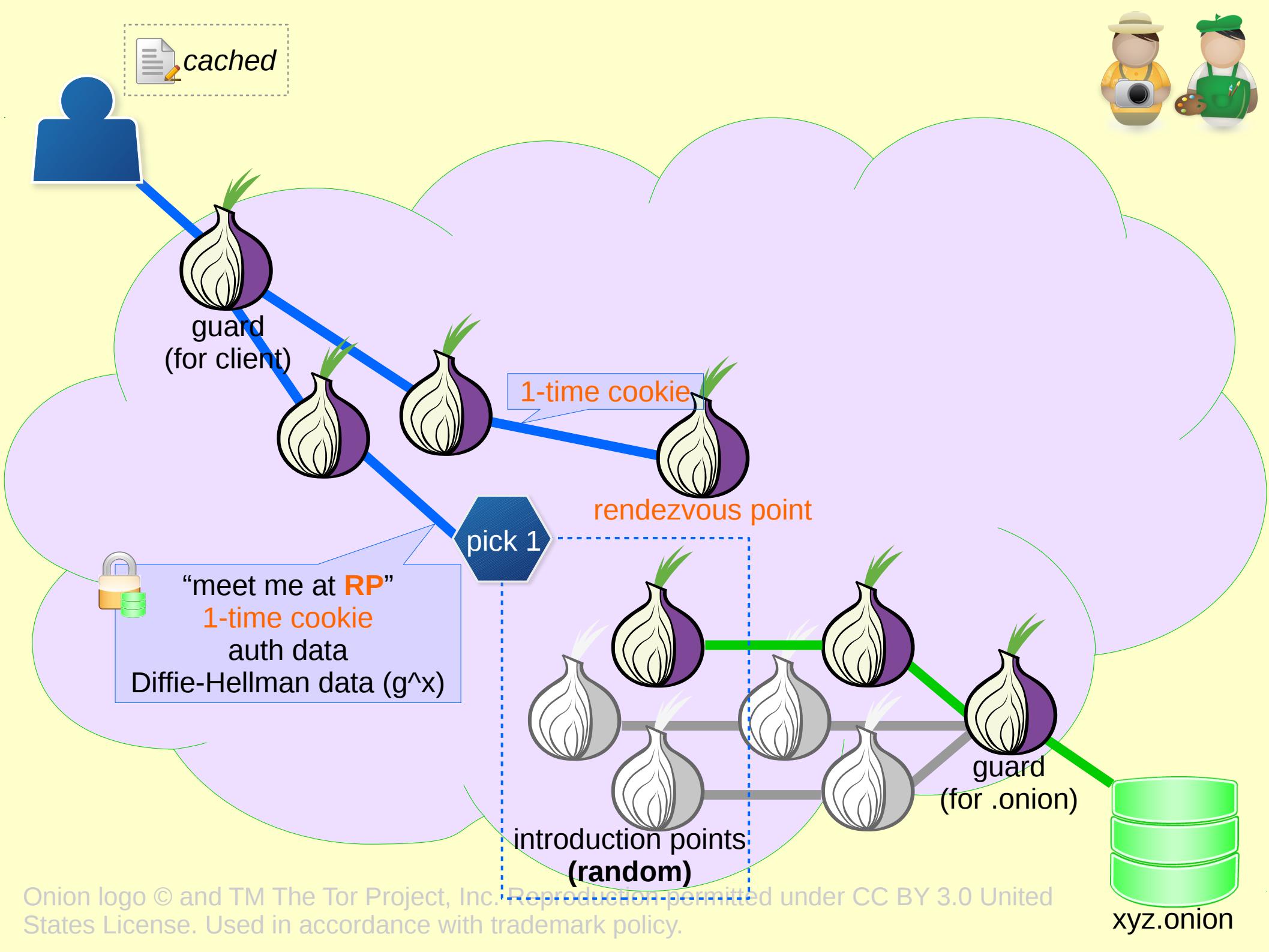


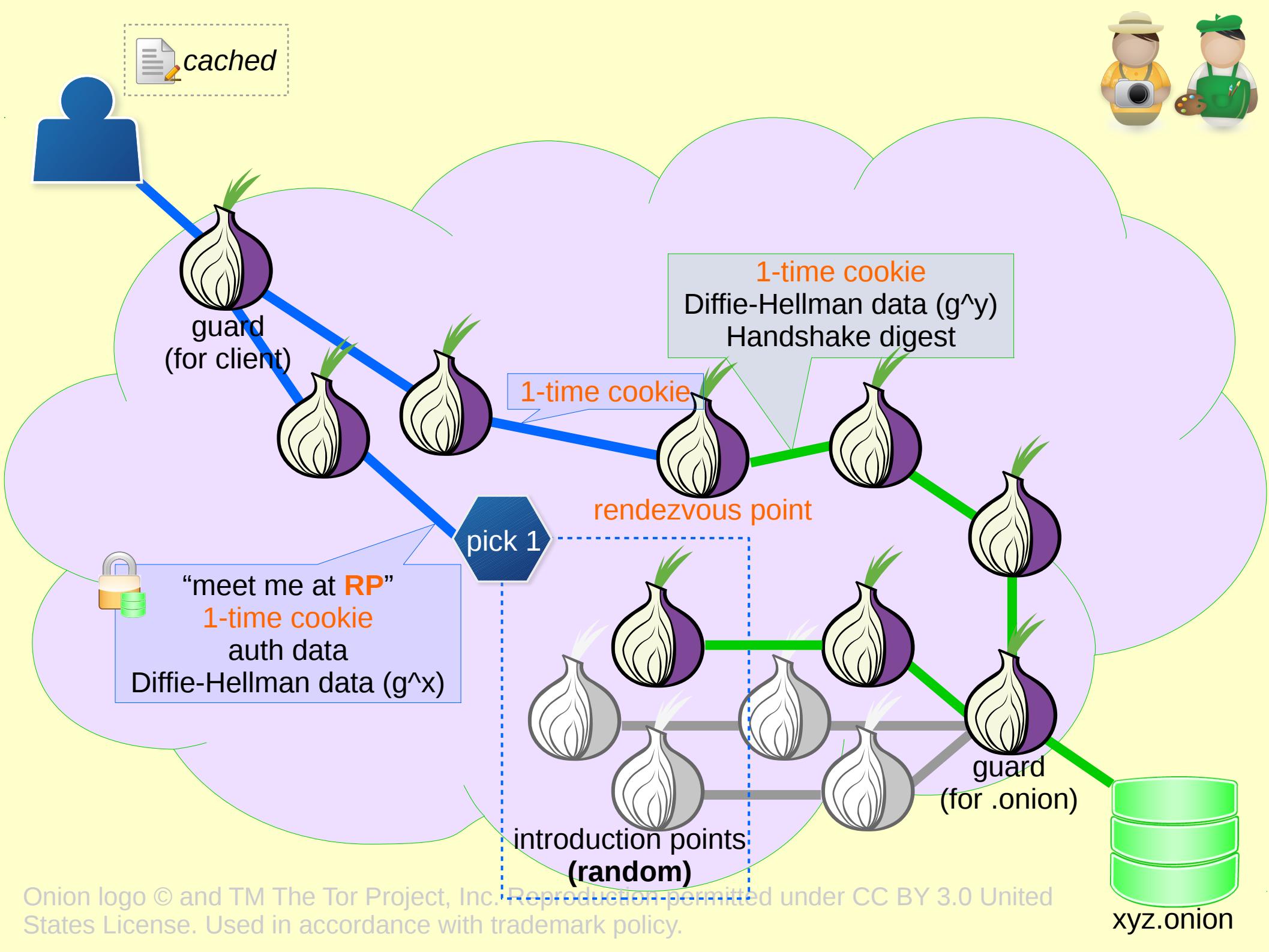
Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.

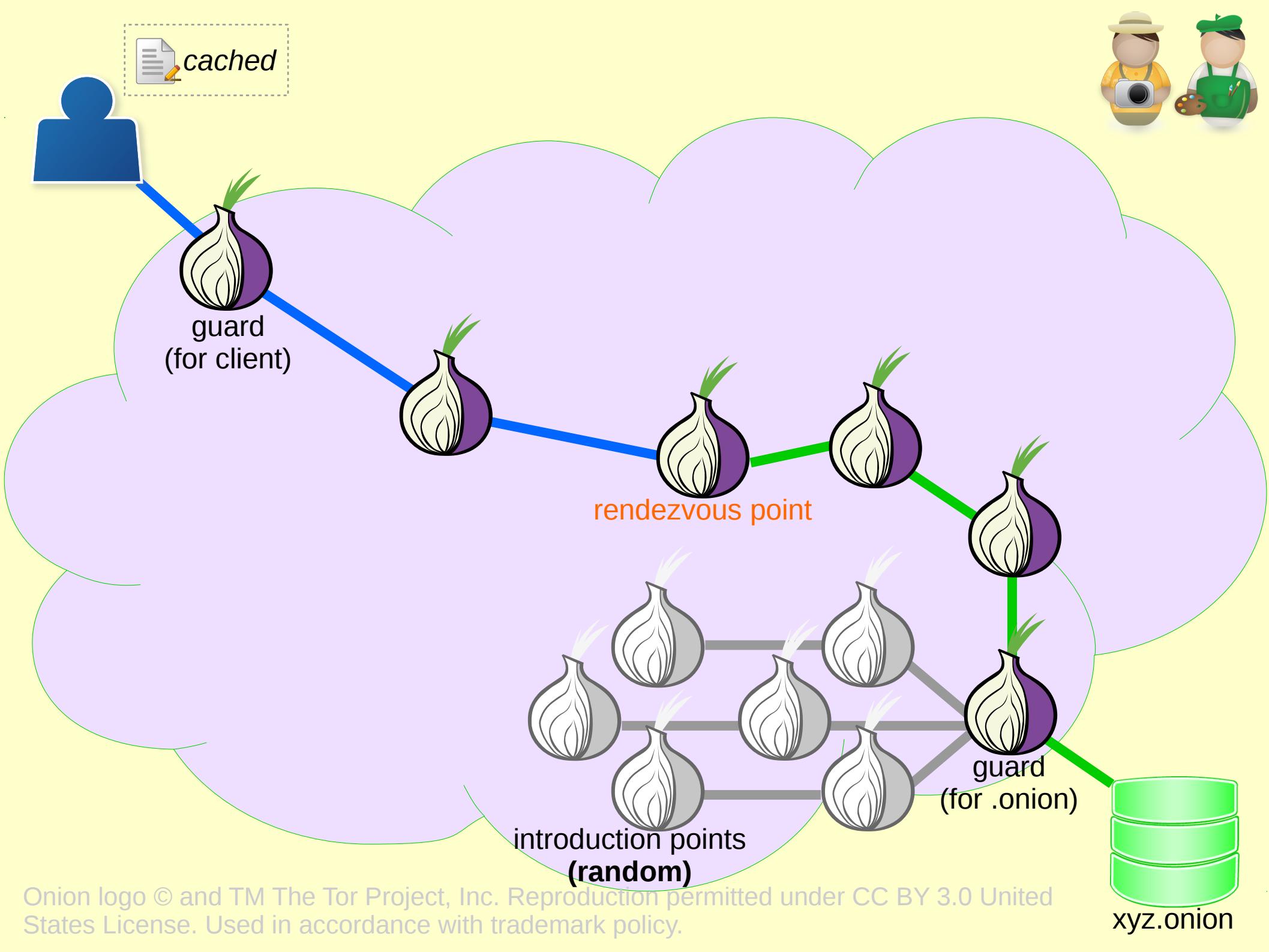


Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.









Onion logo © and TM The Tor Project, Inc. Reproduction permitted under CC BY 3.0 United States License. Used in accordance with trademark policy.



Descriptors, HSDirs, DHT



descriptor-id = $H(\text{permanent-id} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$

replica = 0 or 1

permanent-id = $H(\text{public-key})[:10]$

AKA *~base32-decode(onion address without ".onion")*

time-period = $(\text{current-time} + \text{permanent-id-byte} * 86400 / 256) / 86400$

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

$H(\dots)$	SHA1
	concatenation
{grey}	Invariant
{purple}	Variant, predictable
{red}	Secret
{green}	Random

Descriptors, HSDirs, DHT



descriptor-id = $H(\text{permanent-id} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}) \mid \dots)$

replica = 0 or 1

descID_0 = $H(\sim\text{"zti6p9h6spbt5xr"} \mid H(17573 \mid \text{""} \mid 0) \mid \dots)$

descID_0 = 3xqunszqnaolrrfmtzgaki7mxelgvkje

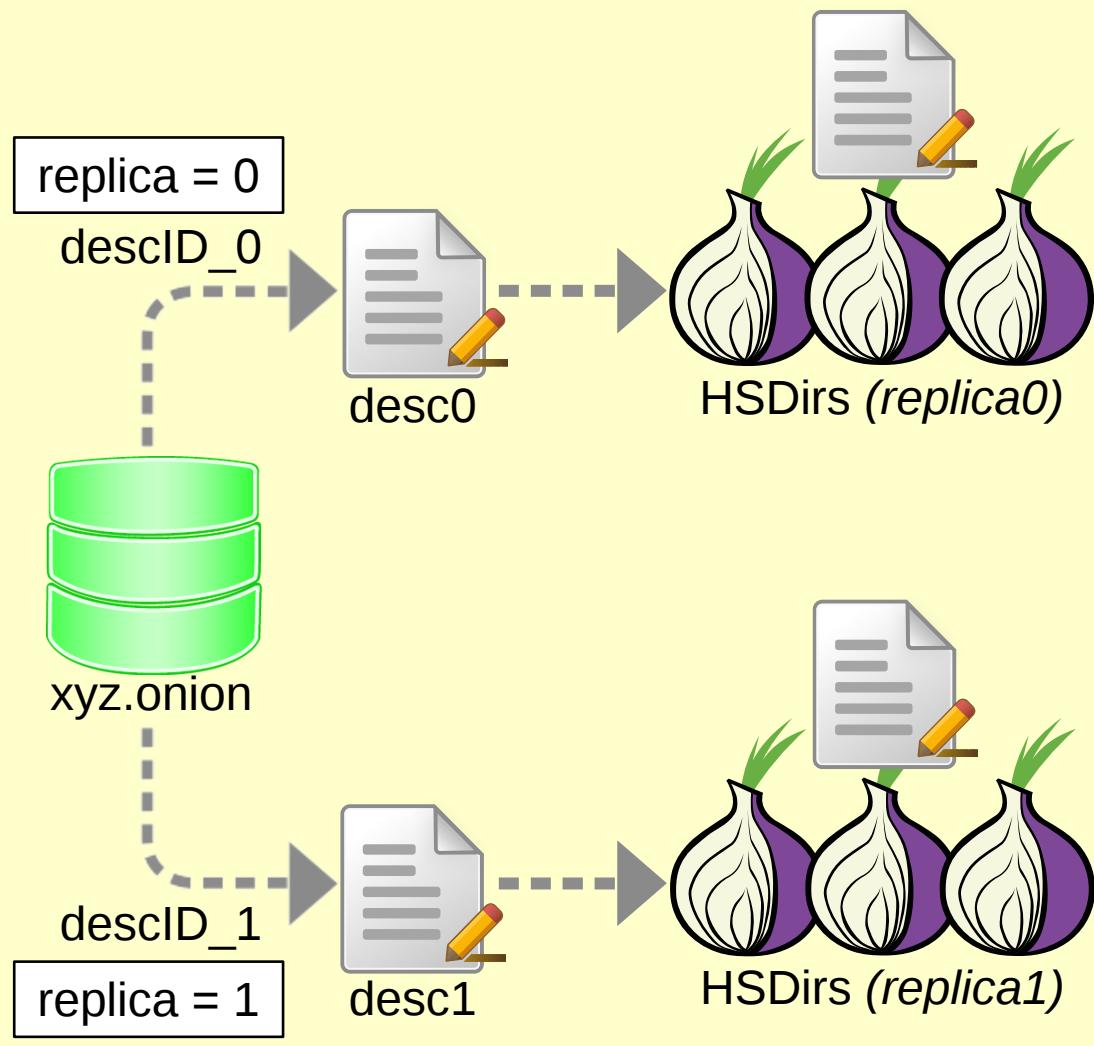


Descriptors, HSDirs, DHT



descriptor-id = $H(\text{permanent-id} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$

replica = 0 or 1



Legend

$H(\dots)$	SHA1
\mid	concatenation
{grey}	Invariant
{purple}	Variant, predictable
{red}	Secret
{green}	Random



Descriptors, HSDirs, DHT

descriptor-id = $H(\text{permanent-id} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$



replica = 0 or 1

descID_0 = 3xqunszqnaolrrfmtzgaki7mxelgvkje

Base16(descID_0) =

337871756E737A716E616F6C7272666D747A6761...



HSDirs:

33789F22470A22C8BEEF907CED29847781E15C5D

337B7E307550F48DCDADA7481FA8436B2FCDADA9

337DA8971BE4580EAC5D1D7AE4E508020CF04594

Descriptors, HSDirs, DHT

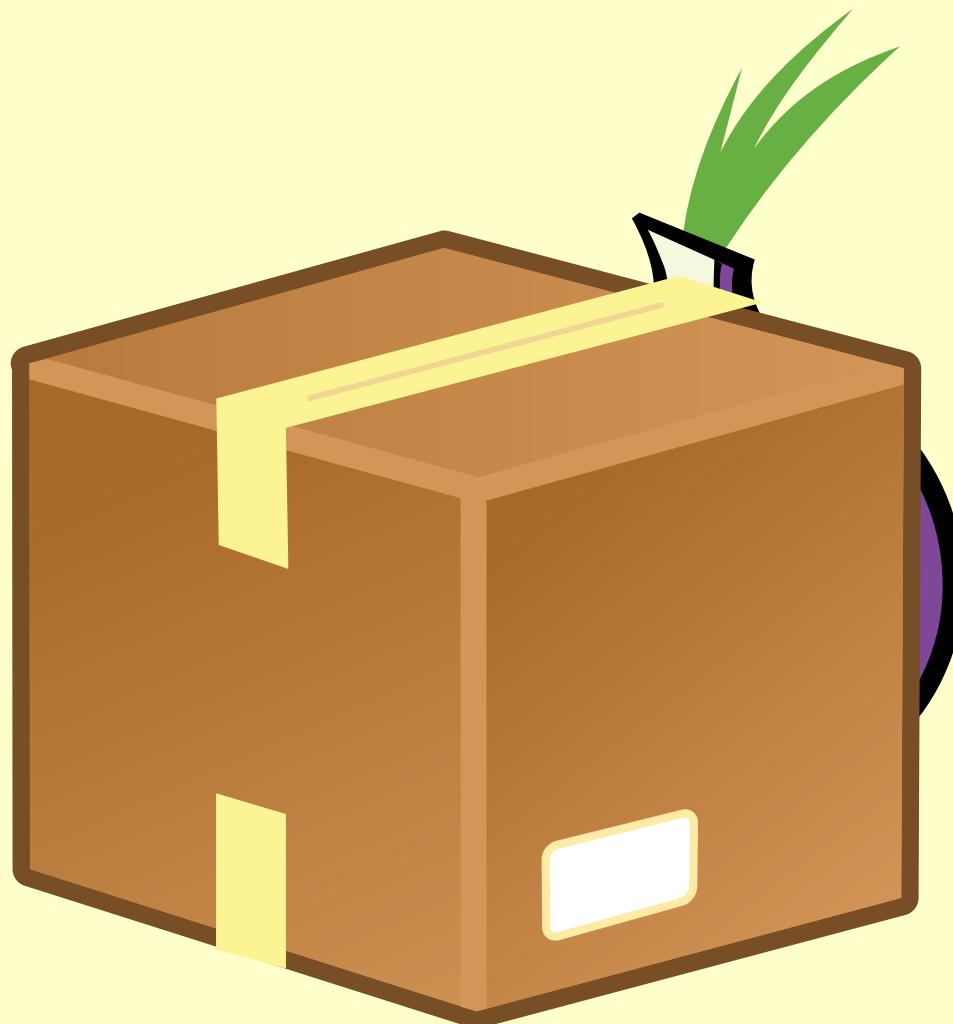


descriptor-id = $H(\text{permanent-id} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$

replica = 0 or 1



Planting tip: stealth



DEMO TIME

BANG





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

Blackthrow - Telecomix Crypto Munitions Bureau - Tor Browser

Telecomix ... x +



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.

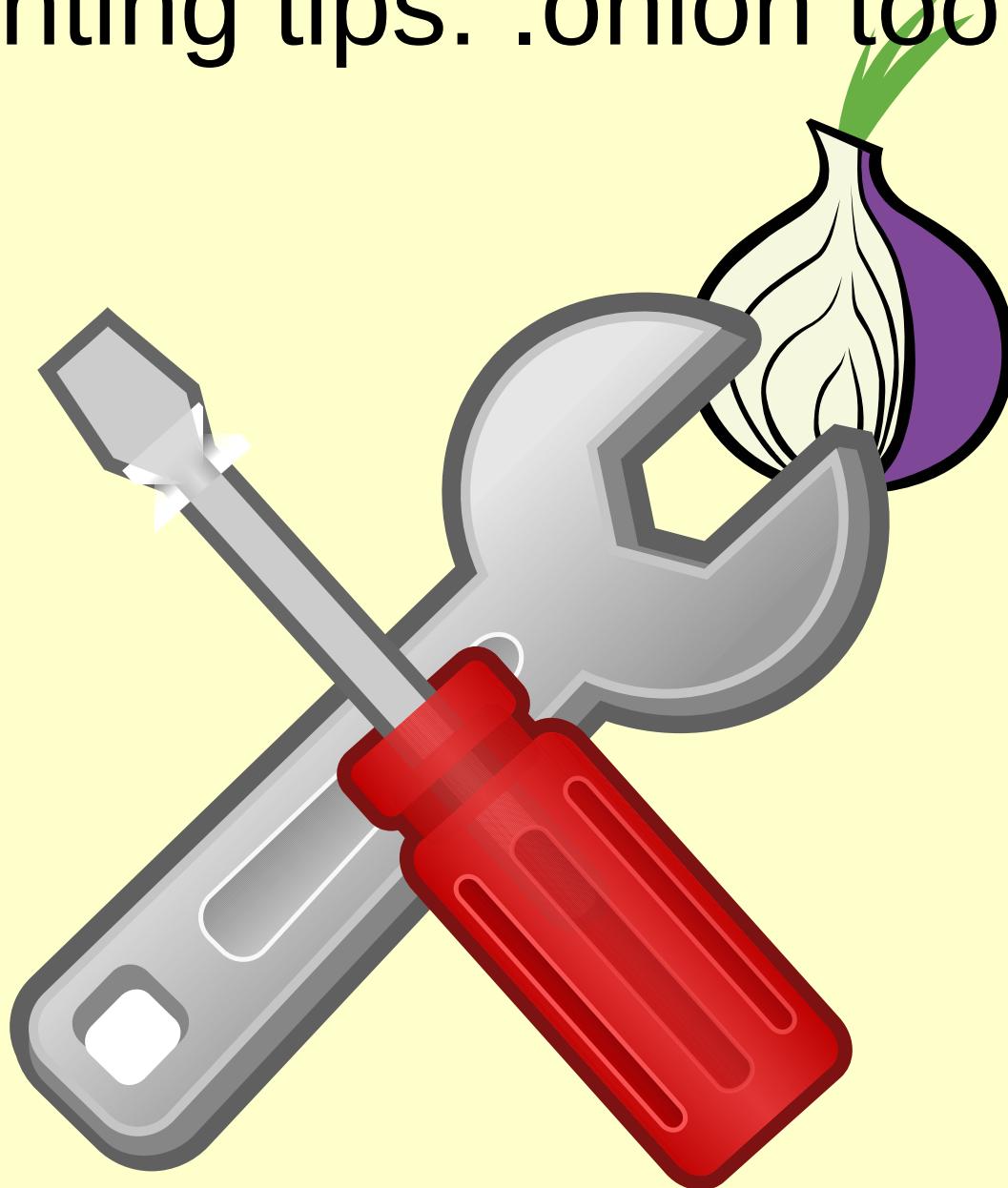
```
HiddenServiceDir /etc/tor/hidden/
HiddenServicePort 22 127.0.0.1:22
```

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

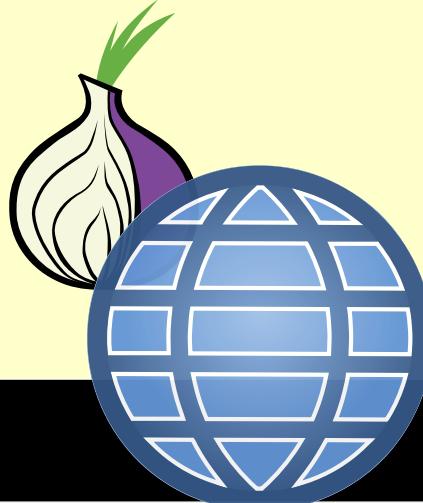




Tools – more universal

- **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

Attack Type	Current Solution	Proposed Solution	Next Gen Status
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?

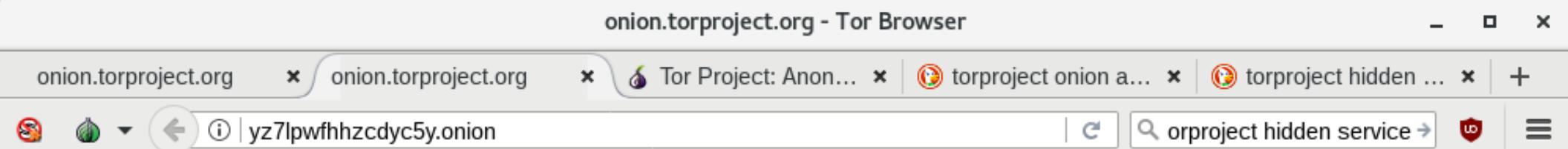
The screenshot shows a Tor Browser window with the title bar "onion.debian.org - Tor Browser". The address bar contains four tabs: "onion.debian.org", "onion.debian.org", "Site map for Debian ...", and "debian onion at Duck...". Below the address bar is a toolbar with icons for refresh, back, forward, and search. The main content area displays the "onion.debian.org" homepage, which lists various Debian services with their onion URLs.

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/): <http://b5tearqs4v4nvbup.onion/>
- [appstream.debian.org](http://5j7saze5byfqccf3.onion/): <http://5j7saze5byfqccf3.onion/>
- [apt.buildd.debian.org](http://ito4xpoj3re4wctm.onion/): <http://ito4xpoj3re4wctm.onion/>
- [backports.debian.org](http://6f6ejaiiixypfqaf.onion/): <http://6f6ejaiiixypfqaf.onion/>
- [bits.debian.org](http://4ypuij3wwrg5zoxm.onion/): <http://4ypuij3wwrg5zoxm.onion/>
- [blends.debian.org](http://bcwpy5wca456u7tz.onion/): <http://bcwpy5wca456u7tz.onion/>
- [bootstrap.debian.net](http://ihdhoeovbtgutfm.onion/): <http://ihdhoeovbtgutfm.onion/>
- [cdimage-search.debian.org](http://4zhlmuhqvjkvspwb.onion/): <http://4zhlmuhqvjkvspwb.onion/>
- [d-i.debian.org](http://f6syxyjdgzbeacry.onion/): <http://f6syxyjdgzbeacry.onion/>
- [debaday.debian.net](http://ammd7ytxcpeavif2.onion/): <http://ammd7ytxcpeavif2.onion/>
- [debconf0.debconf.org](http://ynr7muu3263jikep.onion/): <http://ynr7muu3263jikep.onion/>
- [debconf1.debconf.org](http://4do6yq4iwstidagh.onion/): <http://4do6yq4iwstidagh.onion/>
- [debconf16.debconf.org](http://6nhxqcogfcwqzgnm.onion/): <http://6nhxqcogfcwqzgnm.onion/>
- [debconf2.debconf.org](http://ugw3zjsayleoamaz.onion/): <http://ugw3zjsayleoamaz.onion/>
- [debconf3.debconf.org](http://zdfsyy3rubuhpq3.onion/): <http://zdfsyy3rubuhpq3.onion/>
- [debconf4.debconf.org](http://eeblrw5eh2is36az.onion/): <http://eeblrw5eh2is36az.onion/>
- [debconf5.debconf.org](http://3m2tlhjsoxws2akz.onion/): <http://3m2tlhjsoxws2akz.onion/>
- [debconf6.debconf.org](http://gmi5gld3uk5ozvrv.onion/): <http://gmi5gld3uk5ozvrv.onion/>
- [debconf7.debconf.org](http://465rf3c2oskkqc24.onion/): <http://465rf3c2oskkqc24.onion/>
- [debdtas.debian.net](http://vral2uljb3ndhhxr.onion/): <http://vral2uljb3ndhhxr.onion/>
- [debug.mirrors.debian.org](http://ktqxbqrhg5ai2c7f.onion/): <http://ktqxbqrhg5ai2c7f.onion/>
- [dpl.debian.org](http://i73wbfppplklpixbh.onion/): <http://i73wbfppplklpixbh.onion/>
- [dsa.debian.org](http://f7bphdxlqca3sevt.onion/): <http://f7bphdxlqca3sevt.onion/>
- [es.debconf.org](http://nwk3svshonwfqfs.onion/): <http://nwk3svshonwfqfs.onion/>
- [fr.debconf.org](http://ythg247lqkx2gpgx.onion/): <http://ythg247lqkx2gpgx.onion/>
- [ftp.debian.org](http://wwakviie2ienjx6t.onion/): <http://wwakviie2ienjx6t.onion/>
- [ftp.ports.debian.org](http://nbvhwh4atabu6xq3.onion/): <http://nbvhwh4atabu6xq3.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/): <http://yjuwkcxlgo7f7o6s.onion/>
- [atlas.testnet.torproject.org](http://2d5quh2deowe4kpd.onion/): <http://2d5quh2deowe4kpd.onion/>
- [atlas.torproject.org](http://52g5y5karruvc7bz.onion/): <http://52g5y5karruvc7bz.onion/>
- [aus1.torproject.org](http://x3nelbld33llasqv.onion/): <http://x3nelbld33llasqv.onion/>
- [aus2.torproject.org](http://vijs2fmpd72nbqok.onion/): <http://vijs2fmpd72nbqok.onion/>
- [bridges.torproject.org](http://z5tfsnikzulwicxs.onion/): <http://z5tfsnikzulwicxs.onion/>
- [cloud.torproject.org](http://icxe4yp32mq6gm6n.onion/): <http://icxe4yp32mq6gm6n.onion/>
- [collector.testnet.torproject.org](http://vhbbidwzwhahsrg.onion/): <http://vhbbidwzwhahsrg.onion/>
- [collector.torproject.org](http://qigcb4g4xxbh5ho6.onion/): <http://qigcb4g4xxbh5ho6.onion/>
- [collector2.torproject.org](http://kkvj4mhsttfcrksj.onion/): <http://kkvj4mhsttfcrksj.onion/>
- [compass.torproject.org](http://lwygejoa6fm26eef.onion/): <http://lwygejoa6fm26eef.onion/>
- [consensus-health.torproject.org](http://tgnv2pssfumdedyw.onion/): <http://tgnv2pssfumdedyw.onion/>
- [crm.torproject.org](http://sgs4q3dzv74f723x.onion/): <http://sgs4q3dzv74f723x.onion/>
- [deb.torproject.org](http://sdscq7snqtznauu.onion/): <http://sdscq7snqtznauu.onion/>
- [dist.torproject.org](http://rqef5a5mebgq46y5.onion/): <http://rqef5a5mebgq46y5.onion/>
- [donate.torproject.org](http://bjk3o77eebkax2ud.onion/): <http://bjk3o77eebkax2ud.onion/>
- [exonerator.torproject.org](http://zfu7x4fuagirknhb.onion/): <http://zfu7x4fuagirknhb.onion/>
- [extra.torproject.org](http://klb4glo2btuwyok.onion/): <http://klb4glo2btuwyok.onion/>
- [gettor.torproject.org](http://tngjm3owsslo3wgo.onion/): <http://tngjm3owsslo3wgo.onion/>
- [git.torproject.org](http://dccbbv6cooddgcrq.onion/): <http://dccbbv6cooddgcrq.onion/>
- [gitweb.torproject.org](http://jqs44zhtlx2uo6gk.onion/): <http://jqs44zhtlx2uo6gk.onion/>
- [health.testnet.torproject.org](http://fr6scuhdp5dqvy7d.onion/): <http://fr6scuhdp5dqvy7d.onion/>
- [help.torproject.org](http://54nujbl4qohb5qd.p.onion/): <http://54nujbl4qohb5qd.p.onion/>
- [jenkins.torproject.org](http://f7lqb5oicvsahone.onion/): <http://f7lqb5oicvsahone.onion/>
- [media.torproject.org](http://n46o4uxsej2icp5l.onion/): <http://n46o4uxsej2icp5l.onion/>
- [metrics.torproject.org](http://rougmnvswfsm4dq.onion/): <http://rougmnvswfsm4dq.onion/>
- [munin.torproject.org](http://hhr6fex2qjwmolct.onion/): <http://hhr6fex2qjwmolct.onion/>

Bootstrapping? Discoverability?

The screenshot shows a Tor Browser window with two tabs open:

- Tab 1:** [Secure email: ProtonMail is free encrypted email. - Tor Browser](https://protonmail.com). This tab displays the main ProtonMail website. A large red arrow points from the "Legal" link in the sidebar to the "Imprint" link in the main content area. The sidebar also lists other links: Pricing, Security, Shop, Press/Media Kit, and Onion Site.
- Tab 2:** [ProtonMail - Tor Hidden Service - Tor Browser](https://protonmail.com/tor). This tab displays the ProtonMail onion site. The page title is "ProtonMail + Tor". It includes a statement about Tor being free software for anonymous communication and a prominent orange arrow pointing to the URL <https://protonirockerxow.onion>.

At the bottom of the image, there are two URLs:

- <https://protonmail.com/tor>
- <https://protonirockerxow.onion>

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:    71vd7fa5yfbdqaii.onion (port 443)
xmpp.riseup.net:  4cjw6cwpeaeppfqz.onion (ports 5222, 5269)
0xacab.org:        vivmyccb3jdb7yij.onion (port 80)
```

-----BEGIN PGP SIGNATURE-----

```
iQKTBAEBCgB9FiEETgeRJo98Z+q+iPGwMEPitxOado4FAli0RZhffIAAAAAALgAo
aXNzdWVyLWZwckBub3RhG1vbnMub3BlbnBncC5maWZ0aGhvcnNlbWFuLm51dDRF
MDc5MTI20EY3QzY3RUFCRTg4RjFCMDMwNDNFmkI3MTM5QtC20EUACgkQMEPitx0a
do5u7BAAbPYcnuU4HAQtddb+p8y0V+Fw76fPszPjIE19ACTtfN39U+NyhSj/5LI
i7n2++06lXhnFwnh1A50PIHxv8ZbA9pMeXZYA3gHC1IVRNokRq22uxvCrfastS6
BNmGICsTuHqIcbizJgkkaQImywpoRyT0aoWhGU1QgprK27sWIz6tfut5KXH5vvx
EAyx8itiREJtNQwVMFk3epVCAnl1rAfay/6Gk/jz7rLji3mFjVzGf3wEXff30uTS
jVg5NqA099k8RjHvaNqVCVkm0dPjoByvVrvJ68Xhtbk+ICKDQtwTMiktgKBdAaVr
2tf/vWe0yB/egvjpM89+uLhsxIujvUjGAUxUt/W0cu1mCC3VpdAeR7Wj+1NomNlw
Iw0U07LVT8fqBL42CaZowtkiVAuGZ9+Aeam+ys53CksQ2/phLCZ18JNgzpBZKBnr
x62vnfskmezW0SRjT1MbwlVejtg2HTlx6aVUd2ws8BTNy1+c7W6MMybYIxV/iNA4
S/y5sJbcJNn5iRqIg33i95+1hhTvUqZYnvXFxCdsgTvy4CrUt5n5vSKU9vPqBA8
bIojBuofKErdf/vTT112c3hz0xE5LDerGuftC04Ume0x1Cf3d2JiRRmWD0Xg5sdx
4BL4mJThuyabxTNdLX81S0kRvXtgY/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?

Tor Browser

https://blockchain.info/ +

Blockchain Luxembourg S.A.R.L (LU) | https://blockchain.info | Search

For improved security, please bookmark and access directly https://blockchainbdgpzk.onion/

Bitcoin Block Explorer - Blockchain - Tor Browser

Bitcoin Block Explore... +

Blockchain Luxembourg S.A.R.L (LU) | https://blockchainbdgpzk.onion | Search

WALLET CHARTS STATS MARKETS API

Bitcoin block explorer and currency statistics

LATEST BLOCKS SEE MORE

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
483718	17 minutes	1767	9,838.30 BTC	ViaBTC	861.56	3,421.13
483717	25 minutes	506	1,531.67 BTC	BW.COM	362.77	1,450.82
483716	27 minutes	194	705.93 BTC	BTC.TOP	107.42	426.59
483715	28 minutes	1286	3,625.62 BTC	BTC.com	621.37	2,480.44



Bootstrapping? Discoverability?

Securedrop
GPG



Bootstrapping? Discoverability?

Riseup, about to type in url

.onion redirect



Bootstrapping? Discoverability?

whonix

qubes



Bootstrapping? Discoverability?

propublica

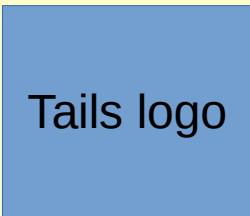


Bootstrapping? Discoverability?

Autistici/Inventati

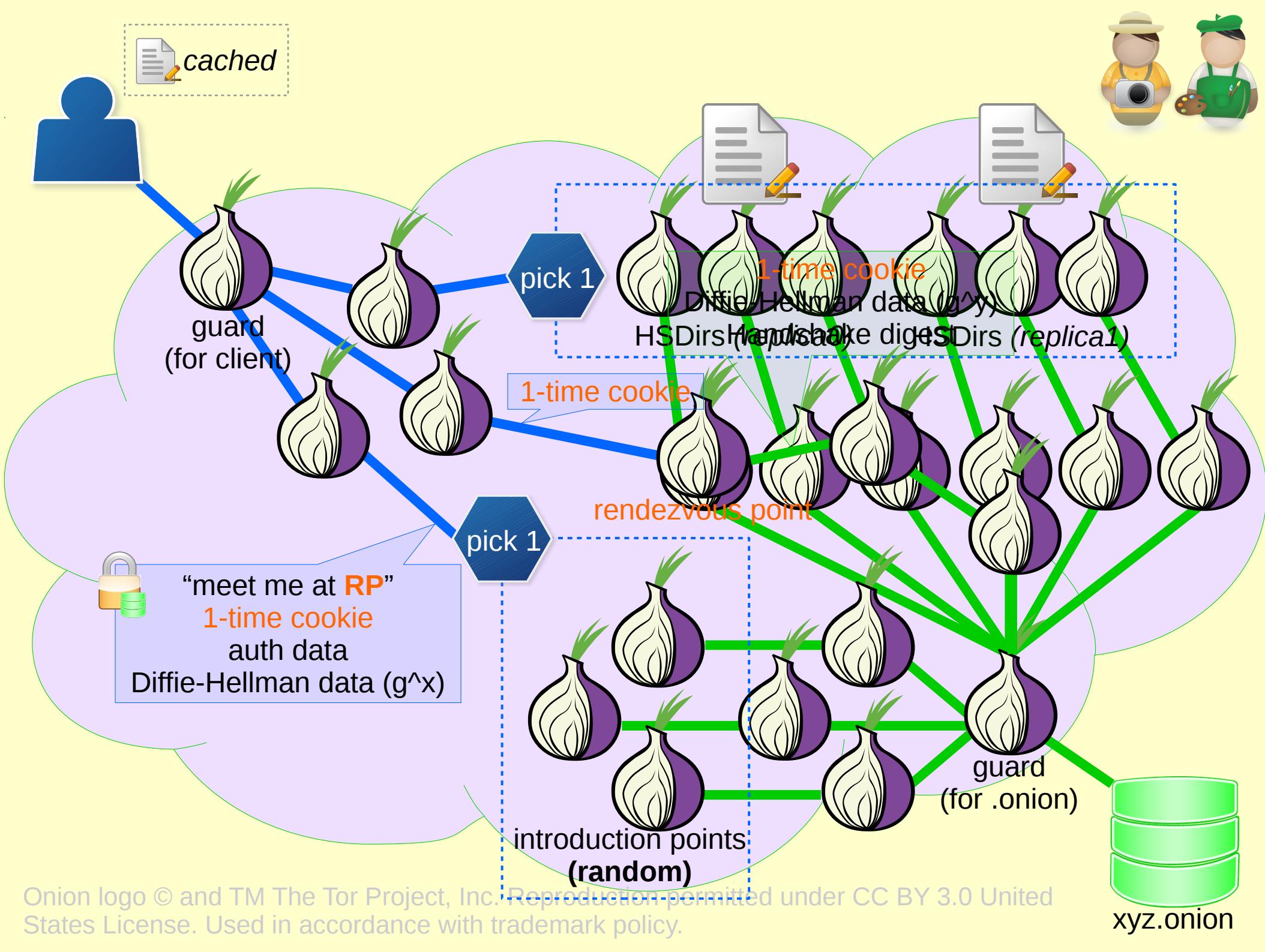


Bootstrapping? Discoverability?



Bootstrapping? Discoverability?





HTTPS + .onion

Demos/screenshots, blah, ...



HTTPS + .onion



Metrics...



