# From DNS to DPKI

a.k.a. “Why secure decentralized namespaces are the future”

A presentation by Greg Slepak

at

NLUUG

**Greg Slepak**

@taoeffect

Espionage

okTurtles

- DNSChain / DPKI
- GroupIncome
- Group Currency

# Target Audience (You)

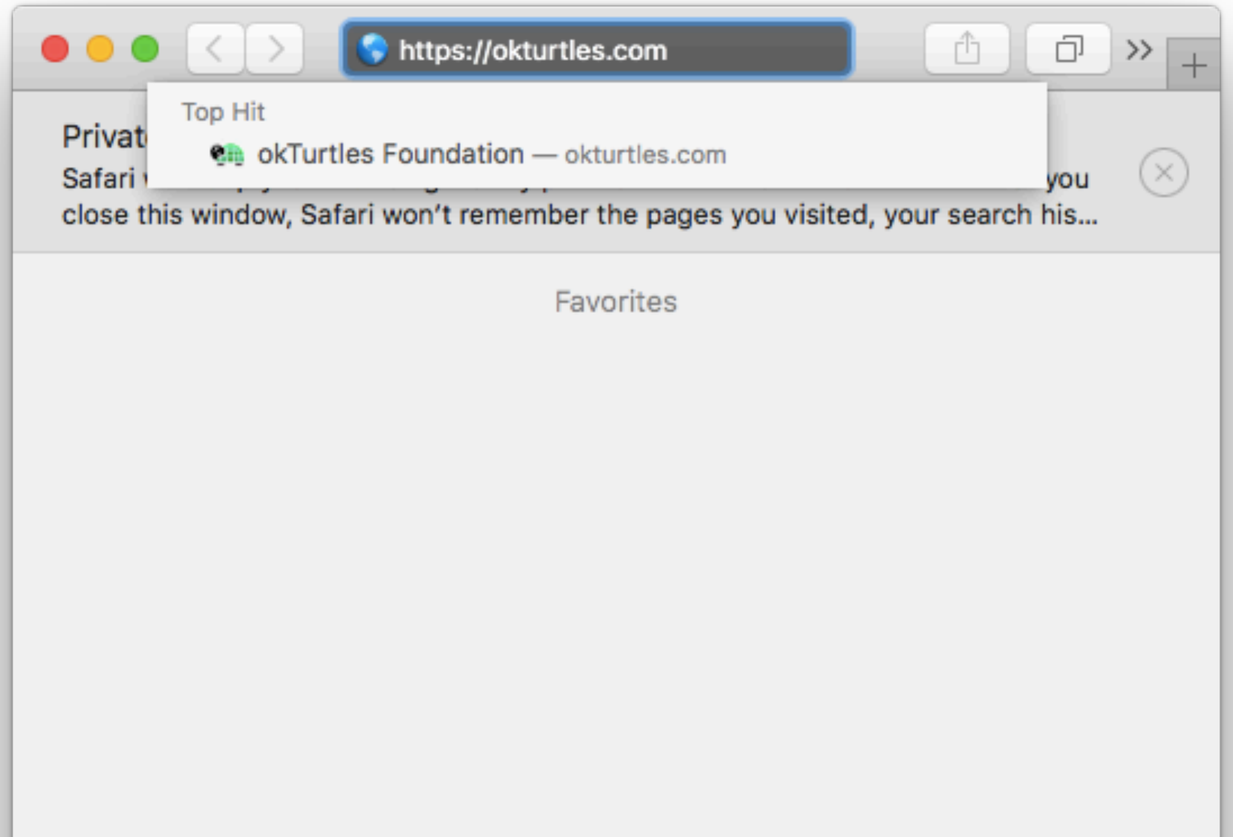
> Most of the crowd is in the systems and network administration corner, some in development […]

— Ronny Lam, NLUUG

Brief overview of problem

user types website domain, hits <Enter>

# Step 1

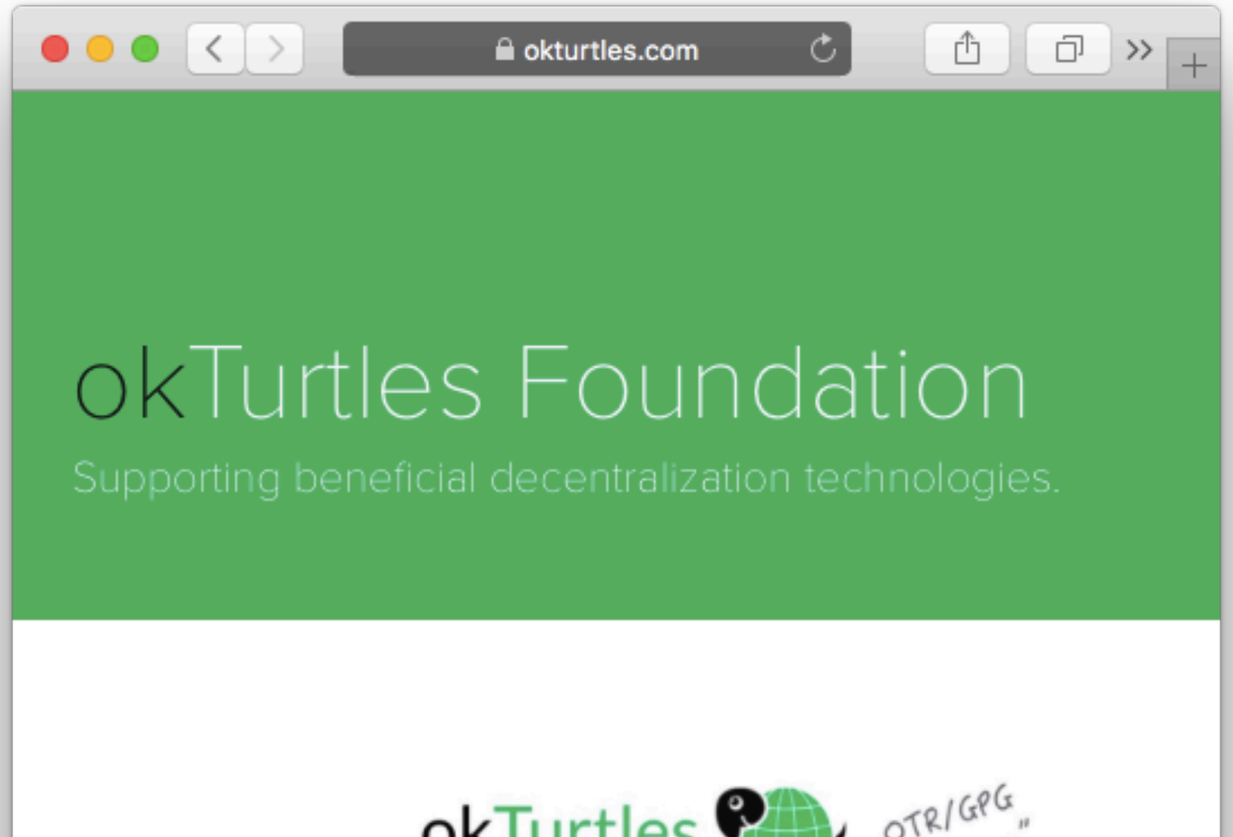


DNS → IP address

IP address → certificate

**certificate → SSL/TLS**

# Step 2

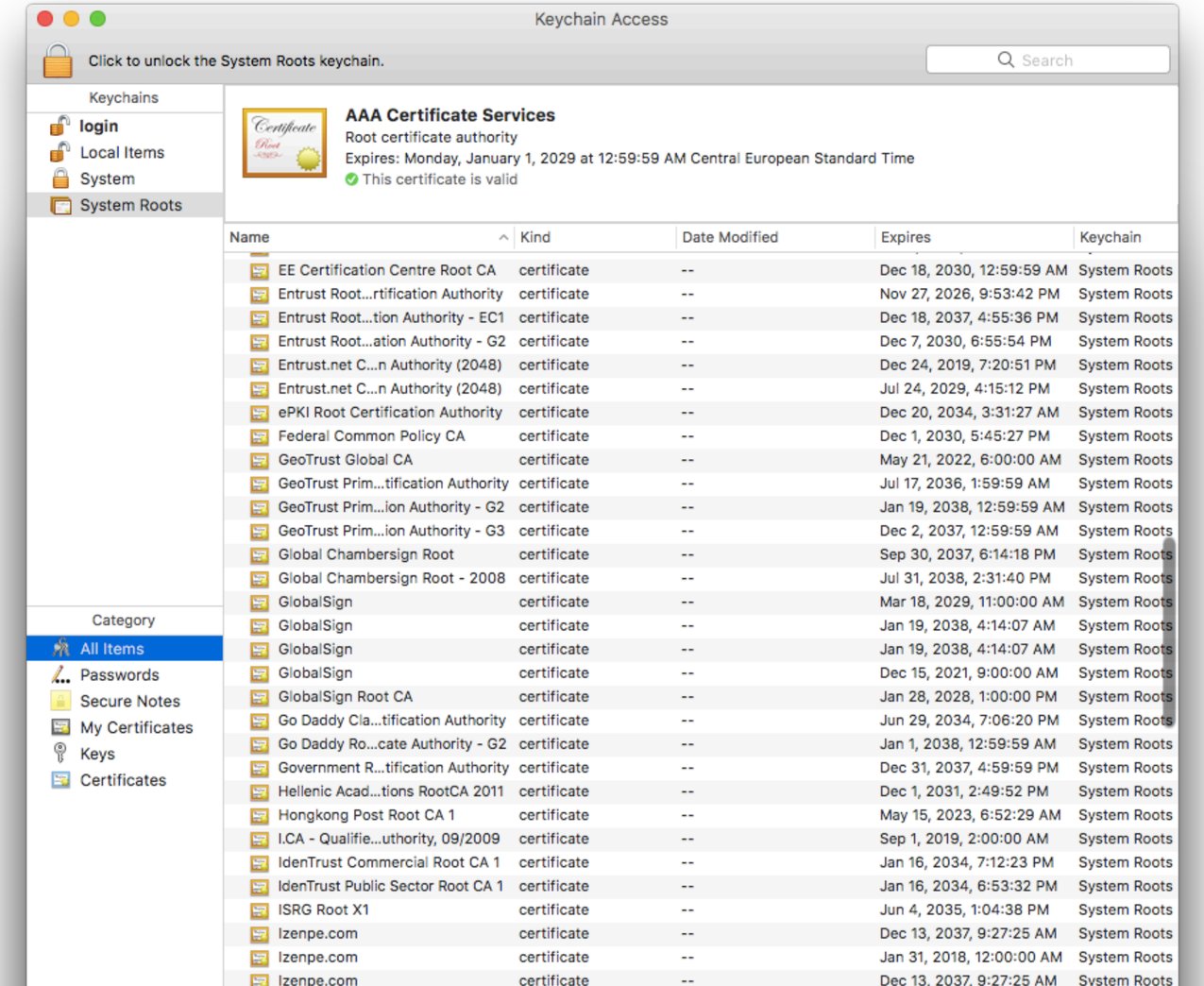


DNS → IP address

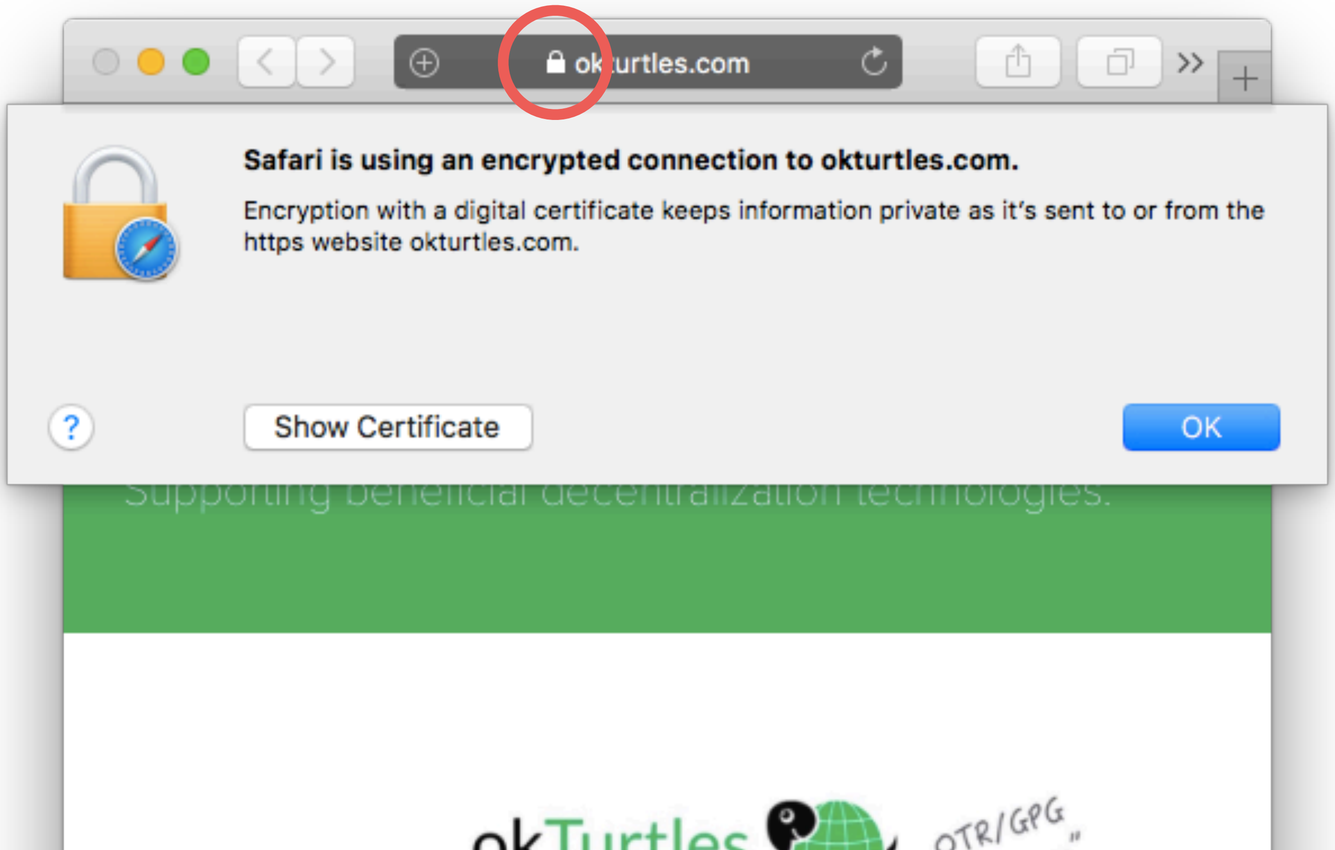
IP address → certificate

**certificate → SSL/TLS**

# Step 2

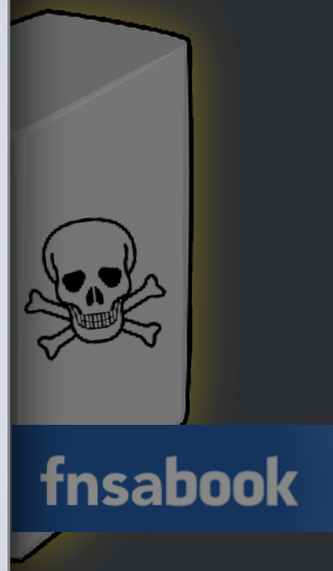


# Step 3


okturtles.com
Safari is using an encrypted connection to okturtles.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website okturtles.com.
Show Certificate
OK
Supporting beneficial decentralization technologies.
okTurtles
OTR/GPG

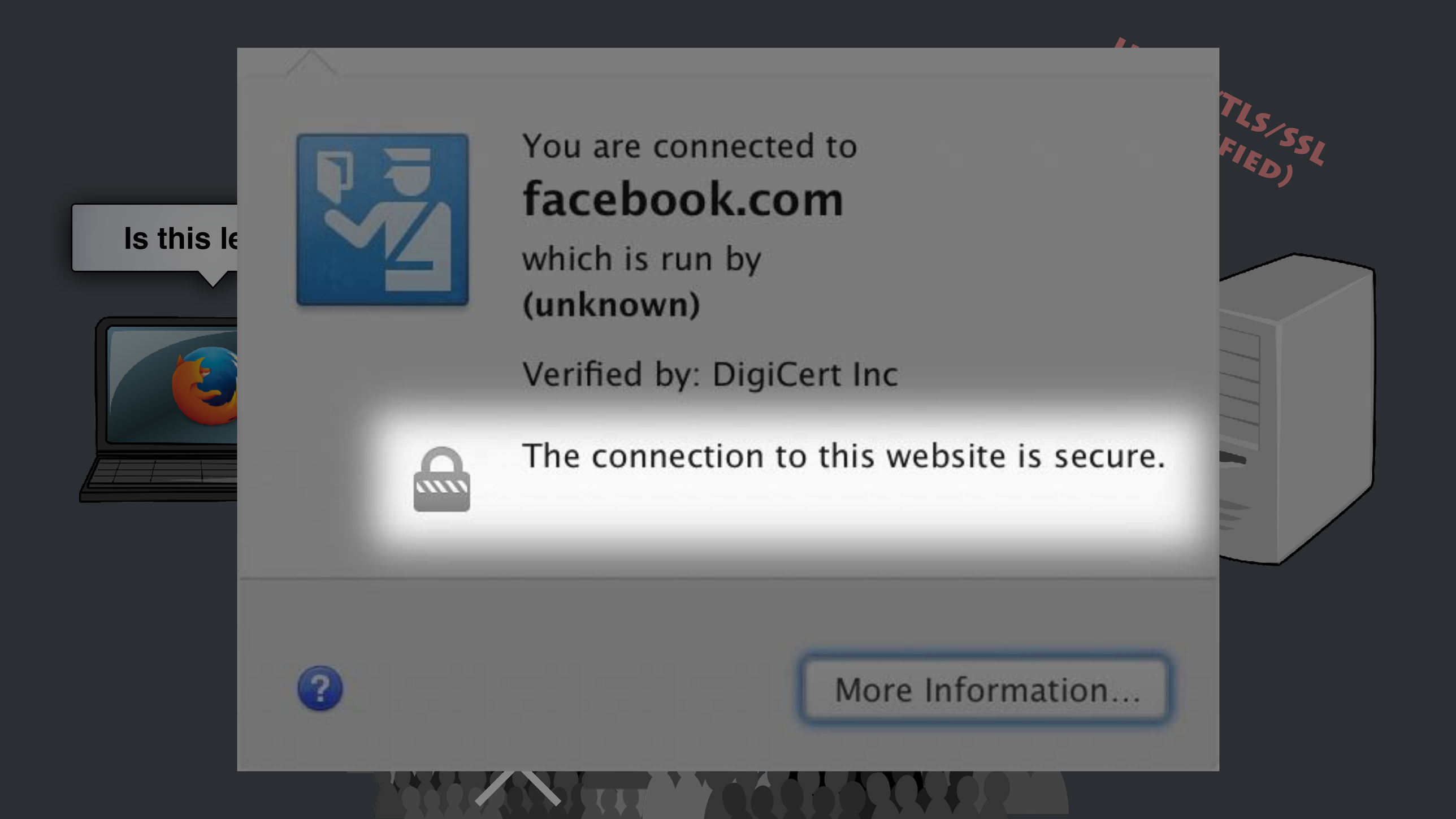
***“More than 1200 root and intermediate CAs can currently sign certificates for any domain and be trusted by popular browsers.”***

http://www.ietf.org/mail-archive/web/therightkey/current/msg00745.html



# Man-In-The-Middle

HTTPS/TLS/SSL
(SIMPLIFIED)


Is this le
TLS/SSL
FIED)
You are connected to
facebook.com
which is run by
(unknown)
Verified by: DigiCert Inc
The connection to this website is secure.
More Information...

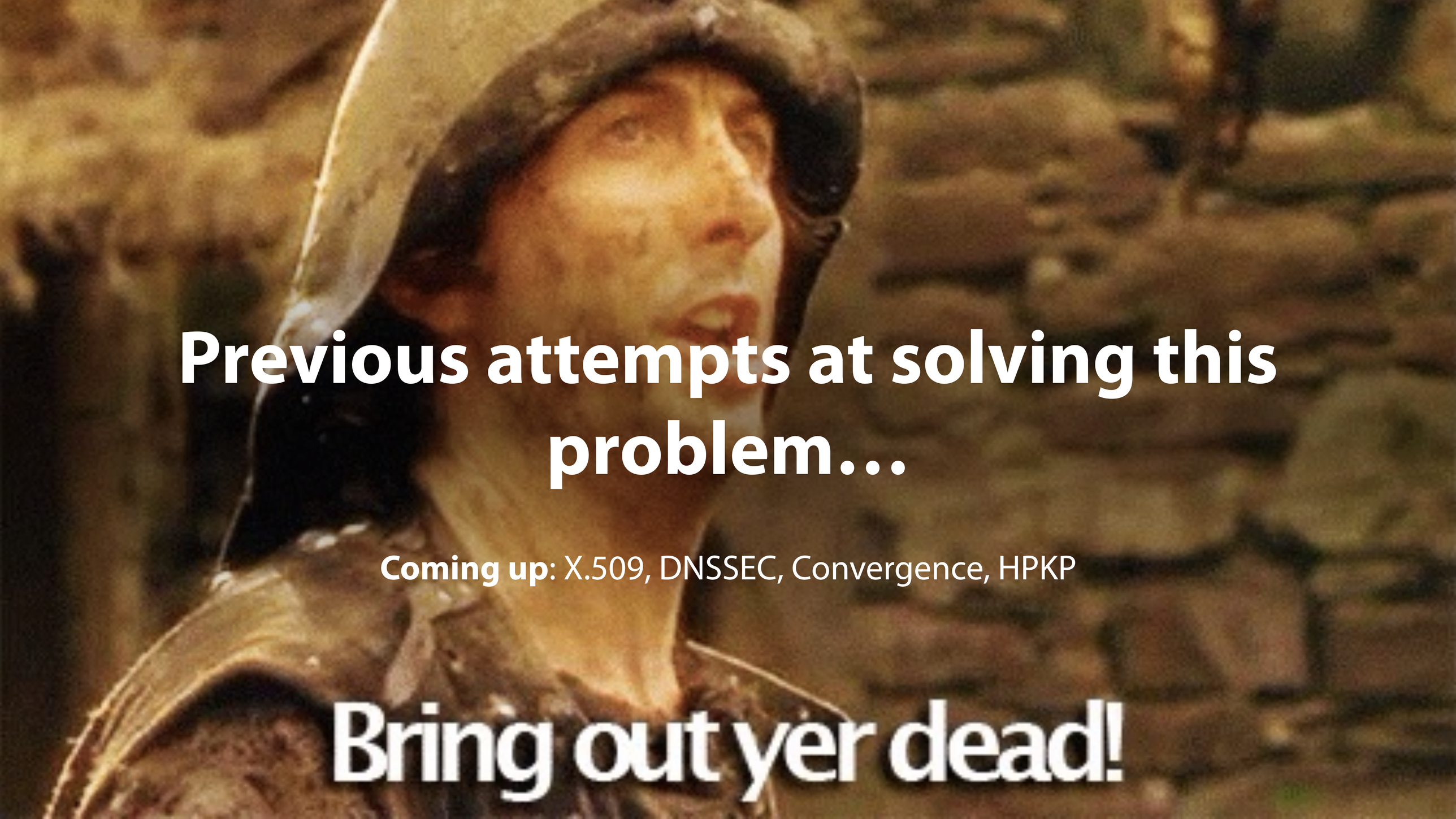
Let’s **clearly define** **The Problem™**

# The Problem™

1. ***Who*** **can define** ***your identity*** **to** **strangers** ***when you're not there?***

2. **Is there** ***a good reason*** **to** ***trust*** **those in (1)?**

3. **Is the mechanism** ***usable?***




# Previous attempts at solving this problem…

**Coming up**: X.509, DNSSEC, Convergence, HPKP

# X.509

(we just covered it)

# DNSSEC

# DNSSEC

is complicated

## IETF standards [ edit ]

- RFC 2535 Domain Name System Security Extensions
- RFC 3833 A Threat Analysis of the Domain Name System
- RFC 4033 DNS Security Introduction and Requirements (*DNSSEC-bis*)
- RFC 4034 Resource Records for the DNS Security Extensions (*DNSSEC-bis*)
- RFC 4035 Protocol Modifications for the DNS Security Extensions (*DNSSEC-bis*)
- RFC 4398 Storing Certificates in the Domain Name System (DNS)
- RFC 4470 Minimally Covering NSEC Records and DNSSEC On-line Signing
- RFC 4509 Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- RFC 5155 DNSSEC Hashed Authenticated Denial of Existence
- RFC 6781 DNSSEC Operational Practices, Version 2

## DNSSEC is Expensive To Deploy

DNSSEC is harder to deploy than TLS. TLS is hard to deploy (look how many guides sysadmins and devops teams write to relate their experience doing it). It's not hard to find out what a competent devops person makes. Do the math.

— Thomas & Erin Ptacek

"Against DNSSEC" — https://sockpuppet.org/blog/2015/01/15/against-dnssec/

# DNSSEC

is unnecessary

## DNSSEC is Unnecessary

All secure crypto on the Internet assumes that the DNS lookup from names to IP addresses are insecure. Securing those DNS lookups therefore enables no meaningful security. DNSSEC does make some attacks against insecure sites harder. But it doesn't make those attacks *infeasible*, so sites still need to adopt secure transports like TLS. With TLS properly configured, DNSSEC adds nothing.

— Thomas & Erin Ptacek

"Against DNSSEC" — https://sockpuppet.org/blog/2015/01/15/against-dnssec/

**“It’s essentially removing the authenticity element from SSL and using the one from DNSSEC instead.”**

— Moxie

“SSL And The Future Of Authenticity” — https://moxie.org/blog/ssl-and-the-future-of-authenticity/

# DNSSEC

is broken

next slide might take a second to load…

IANIX

Home About Privacy

# Major DNSSEC Outages and Validation Failures

Updated: May 14, 2017

This page lists only DNSSEC failures that have the potential to cause downtime for a significant number of domains, users, or both. It does not list smaller outages such as dominos.com ($1.425 Billion in yearly revenue), the Government of California, or other such "small" organizations. They are too frequent to mention. Technical and media/content organizations are held to a higher standard.

Principal sources of information: DNSViz, Verisign's DNSSEC Debugger, Zonemaster, dnscheck.iis.se, dnscheck.labs.nic.cz, and Unbound logs. Discussions on technical mailing lists are also used as sources.

**Note:** DNSViz has lost a portion of its archives multiple times, turning many citations on this page into 404s. And until recently, the dnssec-deployment.org mailing list archives were down for around 5 months, producing more 404s. **Constant DNSSEC outages desensitize people to downtime, making them think it's normal.**

## Root servers

- m.root-servers.net (March 2010) PMTU issues

https://ianix.com/pub/dnssec-outages.html

IANIX

Home About Privacy

## Major DNSSEC Outages and Validation Failures

Updated: May 14, 2017

This page lists only DNSSEC failures that have the potential to cause downtime for a significant number of domains, users, or both. It does not list smaller outages such as dominos.com ($1.425 Billion in yearly revenue), the Government of California, or other such "small" organizations. They are too frequent to mention. Technical and media/content organizations are held to a higher standard.

Principal sources of information: DNSViz, Verisign's DNSSEC Debugger, Zonemaster, dnscheck.iis.se, dnscheck.labs.nic.cz, and Unbound logs. Discussions on technical mailing lists are also used as sources.

**Note:** DNSViz has lost a portion of its archives multiple times, turning many citations on this page into 404s. And until recently, the dnssec-deployment.org mailing list archives were down for around 5 months, producing more 404s. **Constant DNSSEC outages desensitize people to downtime, making them think it's normal.**

### Root servers

- m.root-servers.net (March 2010) PMTU issues
- j.root-servers.net (May 2013)

### TLD DNSSEC outages

- .se — Sweden (October 2009)
- .arpa — Address and Routing Parameter Area (June 2010)
- .us — USA (September 2010)
- .be — Belgium (September 2010)
- .uk — United Kingdom (September 2010)
- .fr — France (September 2010)
- .be — Belgium (October 2010)
- .th — Thailand (November 2010)
- .be — Belgium (December 2010)
- .eu — Europe (December 2010)
- .gi — Gibraltar (January 2011)
- .fr — France (February 2011)
- .fr — France (March 2011)
- .kg — Kyrgyzstan (February 2011)
- .nz — New Zealand (December 2011) DNSSEC RFC non-compliance leads to failures with some BIND tools
- .cz — Czech Republic (February 2012) Affected DNSSEC software based on the Go RSA package
- .us — United States (February 2012) Affected DNSSEC software based on the Go RSA package
- .pl — Poland (June 2012) partial
- .gov — US Government (June 2012)
- .mm — Myanmar (July 2012)
- .dk — Denmark (August 2012) .gov — US Government (September 2012) Affected .gov servers near NYC
- .dk — Denmark (September 2012) partial outage limited to IPv6
- .nl — Netherlands (October 2012)
- .dk — Denmark (November 2012) partial
- .xn--mgbx4cd0ab — Malaysia (December 2012)
- .mil — US Military (December 2012)
- .mm — Myanmar (January 2013)
- .mm — Myanmar (March 2013)
- .com via b.gtld-servers.net (May 2013)
- .mil — US Military (May 2013)
- .biz — dot biz (June 2013)
- .mm — Myanmar (June 2013)
- .mm — Myanmar (July 2013)
- .gov — US Government (August 2013)
- .xn--l1acc — Mongolia (August 2013)
- .mm — Myanmar (August 2013)
- .xn--l1acc — Mongolia (September 2013)
- .xn--l1acc — Mongolia (October 2013)
- .xn--80asehdb — Cyrillic IDN (October 2013) bogus NSEC3s
- .xn--80aswg — Cyrillic IDN (October 2013) bogus NSEC3s
- .xn--80asehdb — Cyrillic IDN (November 2013)
- .xn--l1acc — Mongolia (November 2013)
- .xn--80aswg — Cyrillic IDN (November 2013)
- .xn--l1acc — Mongolia (December 2013)
- .kg — Kyrgyzstan (January 2014)
- .xn--l1acc — Mongolia (January 2014)
- .red — new gTLD (January 2014) Probably not operational
- .rich — new gTLD (January 2014) Probably not operational
- .xn--l1acc — Mongolia (February 2014)
- .pink — new gTLD (February 2014)
- .xn--l1acc — Mongolia (March 2014)
- .xn--l1acc — Mongolia (April 2014)
- .gop — Republican State Leadership Committee, Inc. (April 2014) Probably not operational
- .xn--6qq986b3xl — Tycoon Treasure Limited (April 2014)
- .xn--3bst00m — Eagle Horizon Limited (April 2014)
- .xn--l1acc — Mongolia (May 2014)
- .xn--l1acc — Mongolia (June 2014)
- .xn--l1acc — Mongolia (July 2014)
- .soy — new gTLD (July 2014)
- .foo — new gTLD (July 2014)
- .mm — Myanmar (July 2014)
- .xn--l1acc — Mongolia (August 2014)
- .ke — Kenya (August 2014) ke/SOA fails, affecting a small percentage of DNSSEC queries
- .link — new gTLD (August 2014)
- .mm — Myanmar (August 2014) partial
- .xn--l1acc — Mongolia (September 2014)
- .capetown — new gTLD (September 2014)
- .sx — Sint Maarten (September 2014) partial
- .firmdale — new gTLD (December 2014)
- .fashion — new gTLD (December 2014) partial
- .kg — Kyrgyzstan (January 2015)
- .lb — Lebanon (March 2015)
- .firmdale — new gTLD (March 2015)
- .ke — Kenya (March 2015)
- .xn--l1acc — Mongolia's IDN TLD (April 2015)
- .lat — Latino gTLD (May 2015) partial
- .xn--y9a3aq — Armenia (June 2015)
- .xn--y9a3aq — Armenia (July 2015)
- .mm — Myanmar (September 2015)
- .hr — Croatia (October 2015)
- .xn--y9a3aq — Armenia (November 2015)
- .zm — Zambia (December 2015)
- .mil — US Military (December 2015)
- .mm — Myanmar (December 2015)
- .bw — Botswana (December 2015 - January 2016)
- .bridgestone (January 2016)
- .epson (January 2016)
- .honda (January 2016)
- .hyundai (January 2016)
- .kia (January 2016)
- .komatsu (January 2016)
- .lixil (January 2016)
- .nec (January 2016)
- .ricoh (January 2016)
- .toyota (January 2016)
- .az — Azerbaijan (January 2016) partial
- .is — Iceland (January 2016)
- .mm — Myanmar (March 2016)
- .mm — Myanmar (April 2016)
- .mm — Myanmar (June 2016)
- .id — Indonesia (July 2016)
- .xn--pgbs0dh — Tunisia (July 2016)
- .xn--pgbs0dh — Tunisia (August 2016)
- .smart — new gTLD (October 2016)
- .win — new gTLD (November 2016)
- .bw — Botswana (November 2016)
- .ad — Andorra (December 2016)
- .ke — Kenya (December 2016)
- .mg — Madagascar (February 2017) Bogus NSEC records
- .org (February 2017) limited in scope
- .mg — Madagascar (February 2017)
- .xn--mgbx4cd0ab — Malaysia IDN (April 2017)
- .mg — Madagascar (April 2017)
- .co.id — Indonesia (April 2017)
- .org (April 2017) limited in scope
- .info (April 2017) limited in scope
- .mg — Madagascar (April 2017)
- .mg — Madagascar (April 2017)
- .hotels (May 2017)
- .mg — Madagascar (May 2017)

### Major sites

- gov.dlv.isc.org (March 2009)
- edu.dlv.isc.org (April 2009)
- dlv.isc.org (April 2009)
- RIPE (December 2009) Affected Fedora Linux
- RIPE (June 2010) partial
- mozilla.org (September 2010)
- AFNIC.fr (November 2010)
- medicare.gov & cms.gov (December 2010)
- e164.arpa (February 2011)
- AFNIC.fr (March 2011)
- RIPE (April 2011)
- ip6.arpa (May 2011)
- co.th (June 2011)
- NIST (July 2011)
- Verisign (July 2011)
- FBI (November 2011)
- 54.in-addr.arpa (December 2011)
- secure.registry.be (December 2011)
- CAcert (December 2011)
- NASA (January 2012)
- Internet Software Consortium (February 2012)
- e.0.1.0.0.2.ip6.arpa (APNIC) (May 2012)
- Verisign (June 2012)
- Google Public DNS (November 2012) partial
- CDC: Centers for Disease Control and Prevention (December 2012)
- National Weather Service (December 2012)
- APNIC (December 2012)
- US Department of the Treasury (January 2013)
- 54.in-addr.arpa — ARIN (April 2013)
- mozilla.org (May 2013)
- ic.fbi.gov (July 2013) DNSSEC outage lasted until September
- IRS (August 2013)
- 174.in-addr.arpa: ARIN (November 2013)
- Dyn (December 2013) status page deleted
- USDA (December 2013)
- NBC News (January 2014)
- National Science Foundation (March 2014)
- af.mil (April 2014)
- 172.in-addr.arpa (May 2014)
- af.mil (June 2014) partial
- af.mil (June 2014)
- IETF (June 2014)
- NASA (July 2014)
- NASA (August 2014)
- getdnsapi.net (August 2014)
- Dyn (August 2014) status page deleted
- knot-dns.cz (August 2014) partial
- libreswan.org (September 2014) related to a nohats.ca DNSSEC outage
- root-dnssec.org (November 2014) DNS provided by ICANN!
- FBI (December 2014)
- opendnssec.org (January 2015)
- libreswan.org (February 2015) related to another nohats.ca DNSSEC outage
- HBO Now (March 2015)
- cloudflare-dnssec-auth.com (March 2015)
- af.mil (April 2015) xfinity.com (May 2015)
- af.mil (May 2015)
- internetsociety.org, isoc.org (June 2015)
- af.mil (June 2015)
- nasa.gov (August 2015)
- NICMX (August 2015)
- nasa.gov (August 2015)
- state.gov (September 2015)
- state.gov, usembassy.gov (September 2015)
- nasa.gov (October 2015) partial
- xfinity.com (October 2015)
- af.mil (December 2015) partial
- libreswan.org (March 2016) partial outage; related to another nohats.ca DNSSEC outage
- 65.in-addr.arpa (March 2016)
- lacnic.net (March 2016)
- APNIC (March 2016)
  - 1.in-addr.arpa
  - 14.in-addr.arpa
  - 27.in-addr.arpa
  - 36.in-addr.arpa
  - 39.in-addr.arpa
  - 42.in-addr.arpa
  - 43.in-addr.arpa
  - 49.in-addr.arpa
  - 58.in-addr.arpa
  - 59.in-addr.arpa
  - 60.in-addr.arpa
  - 61.in-addr.arpa
  - 101.in-addr.arpa
  - 103.in-addr.arpa
  - 106.in-addr.arpa
  - 110.in-addr.arpa
  - 111.in-addr.arpa
  - 112.in-addr.arpa
  - 113.in-addr.arpa
  - 114.in-addr.arpa
  - 115.in-addr.arpa
  - 116.in-addr.arpa
  - 117.in-addr.arpa
  - 118.in-addr.arpa
  - 119.in-addr.arpa
  - 120.in-addr.arpa
  - 121.in-addr.arpa
  - 122.in-addr.arpa
  - 123.in-addr.arpa
  - 124.in-addr.arpa
  - 125.in-addr.arpa
  - 150.in-addr.arpa
  - 153.in-addr.arpa
  - 163.in-addr.arpa
  - 171.in-addr.arpa
  - 175.in-addr.arpa
  - 180.in-addr.arpa
  - 182.in-addr.arpa
  - 183.in-addr.arpa
  - 202.in-addr.arpa
  - 203.in-addr.arpa
  - 210.in-addr.arpa
  - 211.in-addr.arpa
  - 218.in-addr.arpa
  - 219.in-addr.arpa
  - 220.in-addr.arpa
  - 221.in-addr.arpa
  - 223.in-addr.arpa
- libsodium.org & dnscrypt.org (April 2016)
- libsodium.org (May 2016)
- dnscrypt.org (June 2016)
- yadifa.eu (June 2016)
- opendnssec.org (July 2016)
- www.nsf.gov/A (July 2016)
- afnic.fr (July 2016)
- secure64.com (July 2016)
- af.mil (August 2016)
- www.nist.gov and time.nist.gov (August 2016)
- nist.gov (September 2016)
- pch.net (September 2016)
- opendnssec.org (October 2016)
- dnssek.info (October 2016)
- dnssec-tools.org (October 2016)
- berkeley.edu (December 2016) partial
- time.nist.gov (December 2016) partial
- dnssek.info (December 2016)
- opendnssec.org (December 2016)
- cia.gov (January 2017)
- tinydnssec.org (January 2017) partial
- service-now.com (January 2017)
- Georgia State University (January 2017)
- abuse.ch (February 2017)
- internetsociety.org (February 2017)
- danyork.com (February 2017)
- Godaddy (domaincontrol.com) DNS (March 2017) affected DANE users
- libreswan.org (April 2017)related to more nohats.ca DNSSEC trouble
- nic.in (April 2017)
- iastate.edu (May 2017)

### Long DNSSEC outages

The median duration of a DNSSEC outage is 8 days. The following may or may not concern large organizations, but when duration is taken into account, a major outage is implied. Bidding starts at 1 DNSSEC-year.

**Terminology note:** The coveted 1000-day DNSSEC outage is known as a *kiloday*.

- **397 days**: xn--l1acc (Mongolia's IDN TLD) — beginning to end.
- **457 days**: moprosecutors.gov — oldest saved to final outage to end(ish).
  - Plus **85 days** to maintain eye contact,
  - followed by **139 days** to assert its dominance,
  - and **11 more days** to cool down,
  - then **19 days** posing provocatively in the mirror,
  - and finally **433 days** to leave the Internet behind.
- **495 days**: mojavedata.gov — beginning to last to unsigned.
- **652 days**: gatrees.gov — beginning to ongoing.
- **676 days**: nepa.gov — beginning to ongoing.
- **976 days**: learnatf.gov — oldest archived to ongoing.
- **976 days**: eureka-mt.gov — oldest archived to ongoing.
- **1016 days**: dmg.gov — beginning to ongoing.
  - Also: **213 days** beginning to end.
- **1341 days**: validatorsearch.verisignlabs.com — beginning to ongoing.
- **1605 days**: educom.edu — oldest archived to ongoing.

### Software

- BIND: CVE-2001-0497: insecure permissions for a HMAC-MD5 shared

https://ianix.com/pub/dnssec-outages.html

# DNSSEC

is less secure than X.509

slower. But if the basic structure is the same, the next obvious question is whether there might be any improvement in how the DNSSEC trust relationships work compared to the current CA system.

It turns out that in the case of DNSSEC, there are three classes of people that we have to simultaneously trust:

*(Registrars, TLDs, and ICANN)*

— Moxie

"SSL And The Future Of Authenticity" — https://moxie.org/blog/ssl-and-the-future-of-authenticity/

DNSSEC is the world's most ambitious key escrow scheme: **a backdoor that hands over control of Internet cryptography to world governments**. Thankfully, it's also a total market failure. We should hope it stays that way.

— Thomas & Erin Ptacek

https://sockpuppet.org/blog/2016/10/27/14-dns-nerds-dont-control-the-internet/

# Convergence / Perspectives

is a real improvement, however…

| | NSC | IR | GA | TA | NTTP | IS | US |
|---|---|---|---|---|---|---|---|
| **Certificate Transparency** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes**(4) |
| DANE (but see note (7)) | No | Yes | Yes | Yes | No | Yes | No (5) |
| CAA (1) | No | Yes | No | No | No | Yes | No (5) |
| Pinning | Yes | No | Yes (2) | Yes (2) | Yes | Yes (3) | No (6) |
| Convergence | No | No | No | Yes | No | No | Yes |
| TACK | Yes | No | Yes (2) | Yes (2) | No | Yes (3) | No (6) |

NSC (No side-channels): our experiments show that side-channel requests to third parties during the SSL handshake (e.g. OCSP checks) fail at least 1% of the time, often a great deal more, depending on what protocol they use. This level of failure makes it impossible to hard fail with protocols that use side channels.

IR (Instant recovery from loss of key): if the server loses its private key, can it immediately roll out a new certificate?

GA (Detects Global Attack): if the server is replaced by an evil server that everyone sees, does the protocol protect clients?

TA (Detects targeted attack): if the server is replaced by an evil server (or MitM) for one person or a small number of people, can the protocol protect those people?

NTTP (No trusted third parties): does the protocol avoid the need for the client to trust a third party?

IS (Instant startup): can a new server use a new certificate immediately and be trusted by clients?

US (Unmodified Servers): can it be used without server changes?

*“Rather than employing a traditionally hard-coded list of immutable CAs, Convergence allows you to configure a dynamic set of Notaries which use network perspective to validate your communication.”*

**Misleading.**

99.9% of users won’t know what notaries are or how to select them.
In practice, there will be a hard-coded list of CAs.
The improvement comes from the existence of **consensus**.

*Conv* *work*

## Consensus:

**When a group of independent entities agree[1] on a decision (e.g. if a key is valid) by some voting threshold[2]**

[1] The voting mechanism can be very different, but this idea is the same

[2] Typically **greater than 50%**. See:
https://groupincome.org/2016/06/what-makes-a-good-voting-system/
https://groupincome.org/2016/09/deprecating-mays-theorem/

99.9% of users won't know what notaries are or how to select them.
In practice, there will be a hard-coded list of CAs.
The improvement comes from the existence of **consensus**.

# Convergence / Perspectives

is ineffective against server-side MITM

(nothing securing connection from notaries to server)

# Pinning (HPKP/TACK)

is difficult to use

# Pinning (HPKP/TACK)

is ineffective against MITM on first visit

# Pinning (HPKP/TACK)

is broken for users with broken clocks

What are their answers
to The Problem™?

# Answers to The Problem™

| | Who can define your identity? | Reason to trust? | Usable? |
|---|---|---|---|
| **X.509** | Governments, CAs | None | Yes |
| **DNSSEC** | Governments, registrars, TLDs, ICANN | None | No |
| **Convergence** | nation-state, colluding notaries | Potential to choose consensus group | Yes |
| **HPKP** | the CA you picked (if you picked one) | TOFU-based, CA chosen by **you** | No |

(and hackers)

# New attempts! 😄🙌

**Coming up**: Certificate Transparency, Key Transparency, CONIKS, DPKI and SCP

# DPKI? What about DNSChain?

DNSChain
paper + website

•

Nov 2013

# DPKI? What about DNSChain?

| DNSChain paper + website | HackerNews front page | 0.0.1 Released | EFF CUP demo + video | Onename's first blog post |
|---|---|---|---|---|
| Nov 2013 | Xmas day 2013 | Feb 2014 | May 2014 | June 2014 |

# DPKI? What about DNSChain?

| UP video | Onename's first blog post | Ongoing collaboration with Namecoin & Onename | Engadget & others cover DNSChain | Onename announces funding |
|---|---|---|---|---|
| 014 | June 2014 | June - … ongoing | Sept 2014 | Nov 2014 |

# DPKI? What about DNSChain?

| Onename announces funding | okTurtles Blockchain ID specification | Onename releases Blockstore | Blockstore migrates Namecoin to Bitcoin | DPKI paper at at Rebooting Web-of-Trust | Onename → Blockstack + RWoT #2 |
|---|---|---|---|---|---|
| Nov 2014 | Jan 2015 | Feb 2015 | Sept 2015 | Feb 2015 | May 2016 |

# DPKI? What about DNSChain?

**Onename**
**➜**
**Blockstack**
**+**
**RWoT #2**

May 2016

**One of**
**DPKI co-authors**
**announces uPort**

Aug 2016

**"Slepak's Triangle"**
**(DCS Triangle)**
**draft at RWoT #3**

Oct 2016

With even Microsoft exploring blockchain identity, the need for a blockchain-agnostic protocol, like **DPKI**, continues to grow

# Back to those new attempts!

# Long story short…

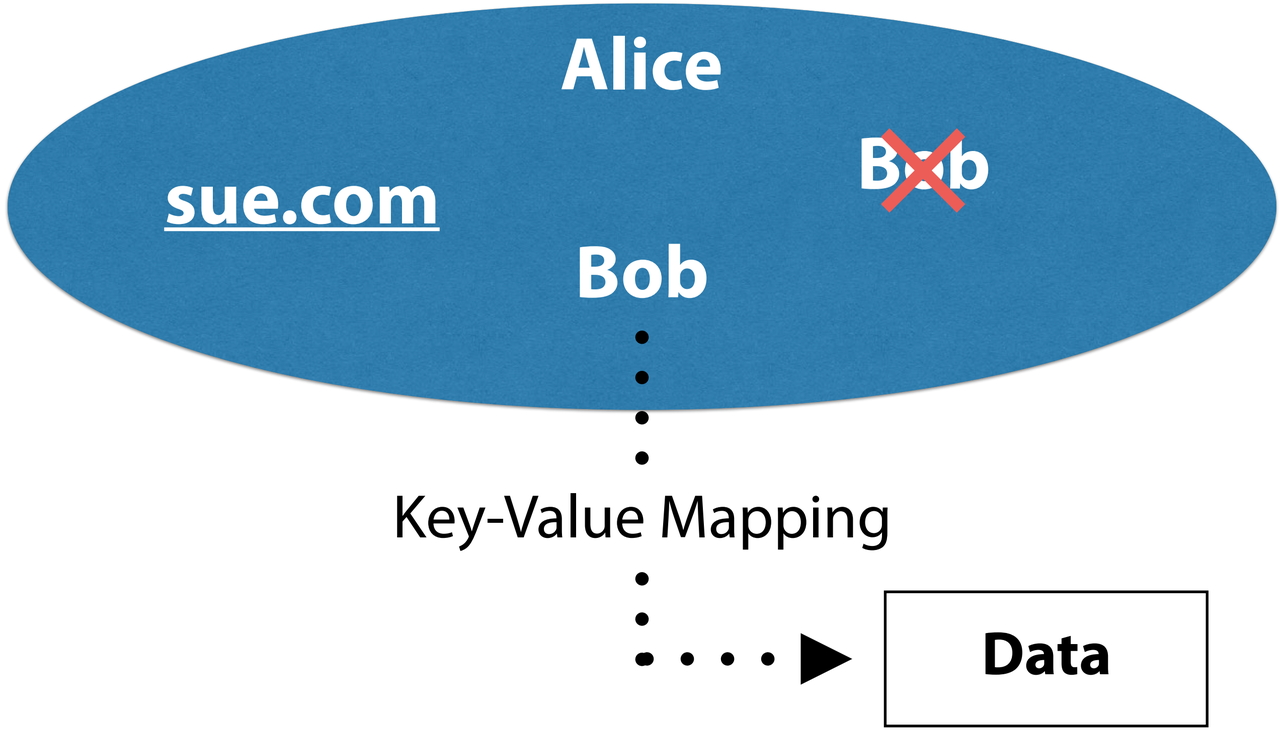
| | Google's CT | Google's KT | CONIKS | DPKI |
|---|---|---|---|---|
| MITM-detection | 🤔 | 🤔 | ✅ | ✅ |
| MITM-prevention | ❌ | ❌ | ✅(*) | ✅ |
| Internet scalable | ✅ | ✅ | ✅ | 🤔 |
| Economically backed security | ❌ | ❌ | ❌ | ✅ |
| Censorship resistant | 🤔 | ❌ | ❌ | ✅ |
| DoS resistant | ✅ | 🤔 | 🤔 | ✅ |

*(*) MITM-prevention in CONIKS depends on novel zero-knowledge proof cryptography that few have verified. Assuming it Works As Advertised, and assuming gossip is successful, and assuming a single entity does not control the server and all messenger implementations using it, it should be capable of preventing MITM attacks.*

https://blog.okturtles.com/2017/02/coniks-vs-key-transparency-vs-certificate-transparency-vs-blockchains/

# Quick Lesson: Namespaces

# What is a namespace?



**Today**

DNS – – – – – X.509

(This is why DNSSEC is unnecessary)

Notice: neither DNS nor X.509 enforce unique key-value mapping.

- **`dig apple.com`** can return arbitrary results
- CAs can issue arbitrary certificates for the same domain

**There is no consensus on what the mapping should be!**

DNS –

## Who should decide what the mapping should be?

Psst… **You!**

(The person who registered it!)

force

n

(This is why DNSSEC is unnecessary)

**There is no consensus on what the mapping should be!**

Centralized Namespaces

vs

Decentralized Namespaces

## Centralized Namespaces

Global

vs

## Decentralized Namespaces

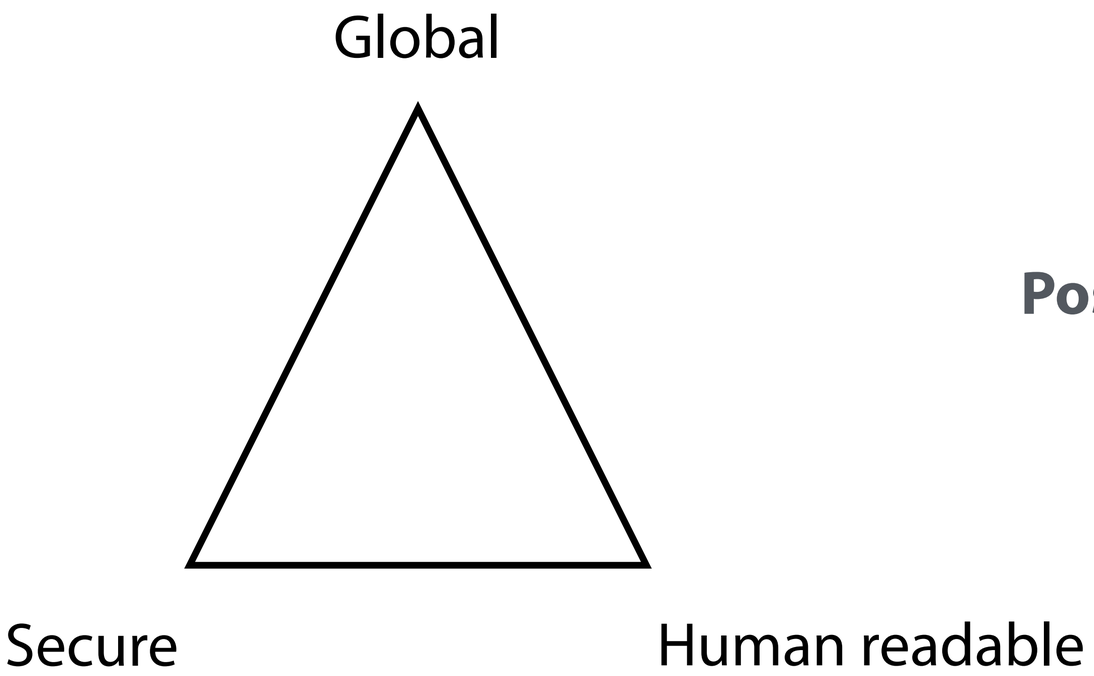
Global

- Who controls mappings? **Not you.**
- **Incapable** of providing ownership of an identifier
- **Incapable** of censorship-resistance

- Real ownership and censorship-resistance
- Who controls mappings? **You.***
- The Internet requires it

* As long as they remain decentralized. See **consensus capture**.

# Zooko's Triangle




**Possible to "square"?**

# Decentralized Public Key Infrastructure (DPKI)

# DPKI

is different

*has to be* different

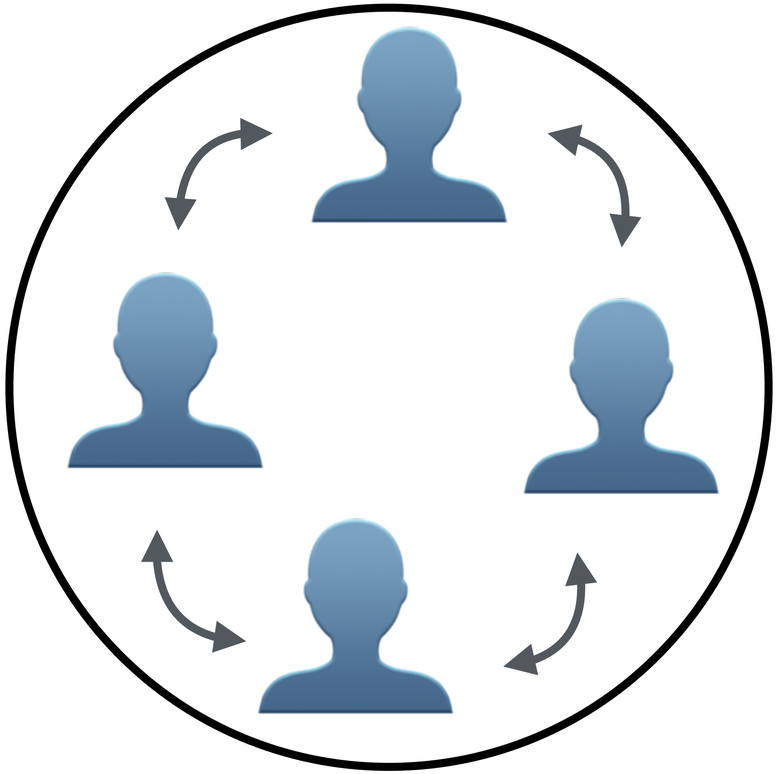
# DPKI

because it recognizes consensus capture

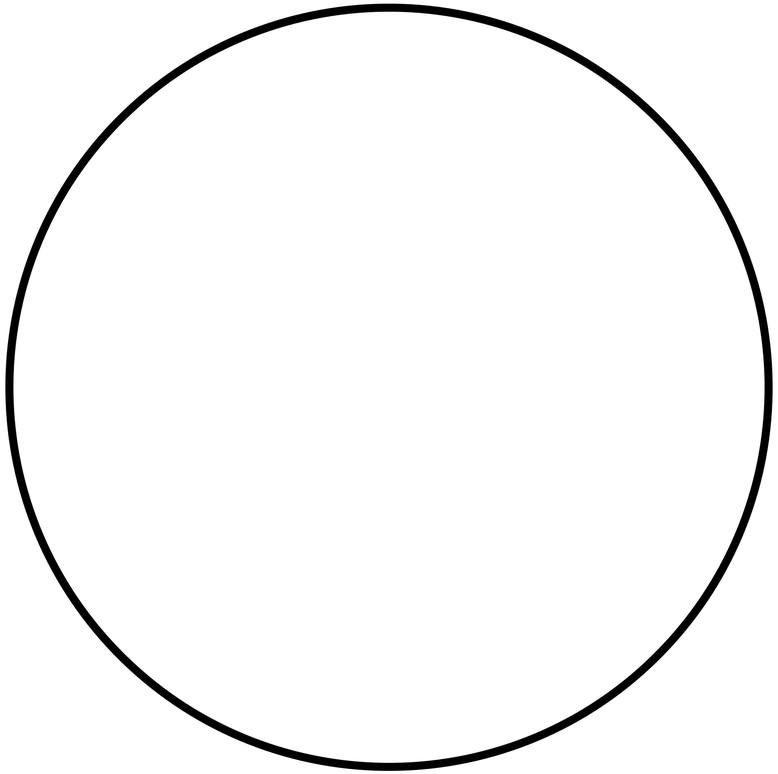
# Consensus Capture

# Consensus Capture

**Our consensus group:**



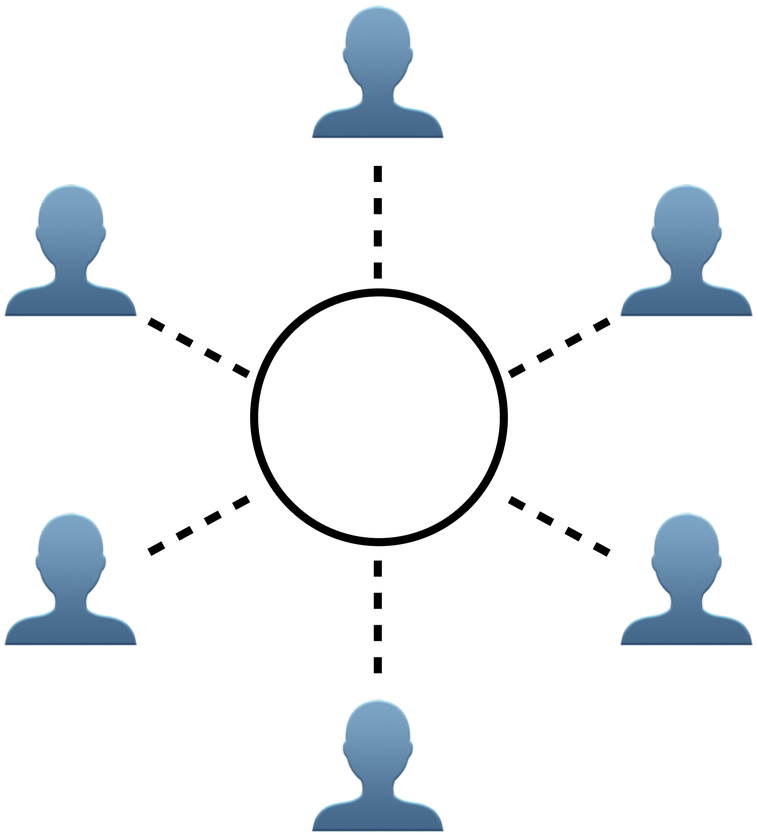
# Consensus Capture



Consensus participants:

**100%**

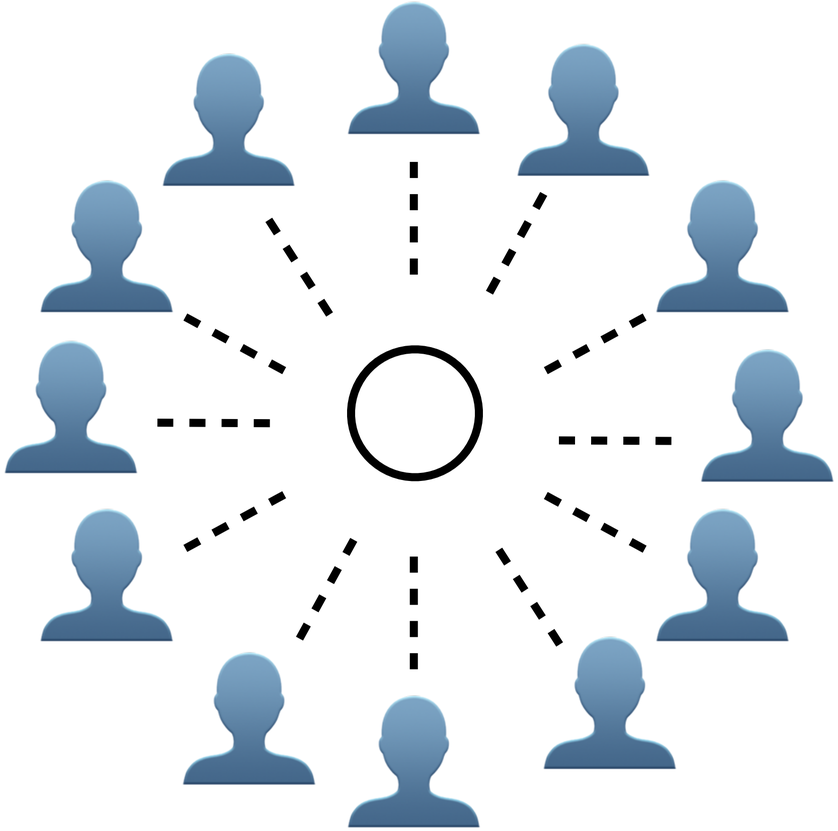
# Consensus Capture



Consensus participants:

**40%**

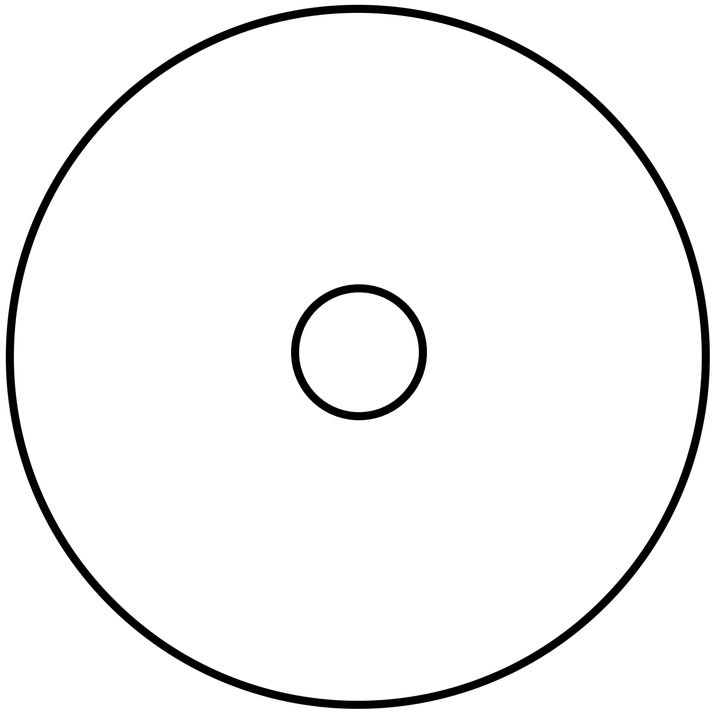
# Consensus Capture



Consensus participants:

**25%**

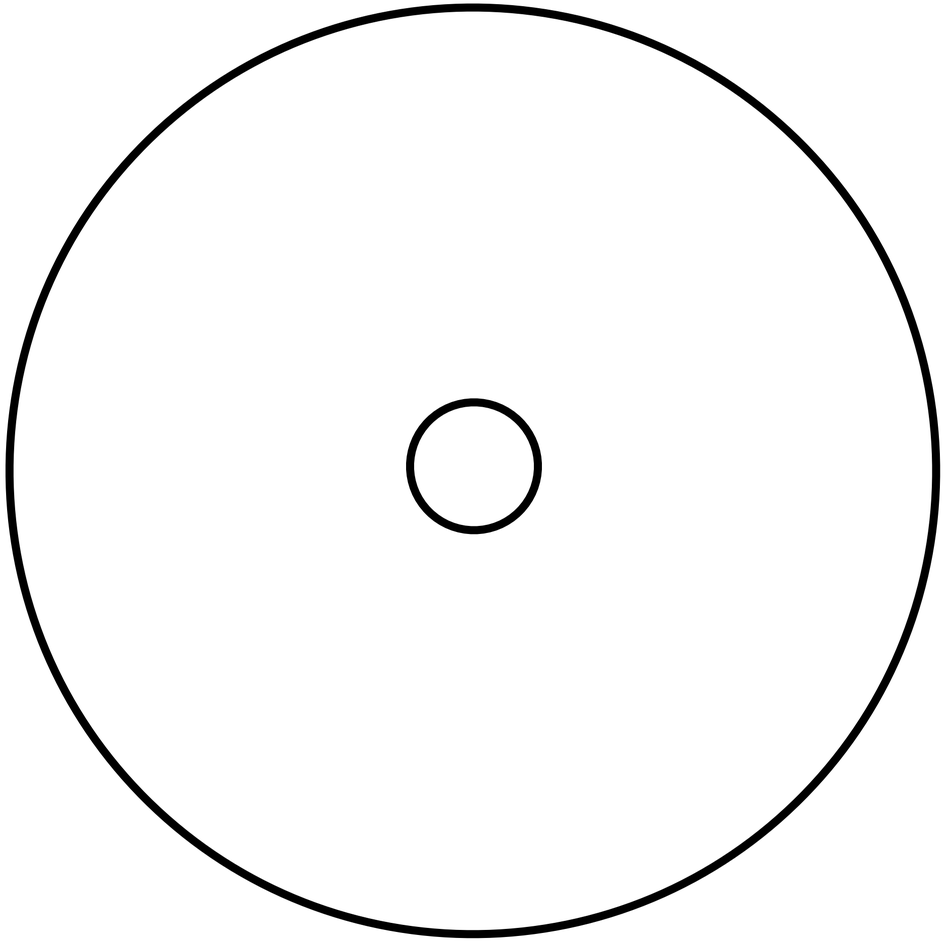
# Consensus Capture



Consensus participants:

**25%**

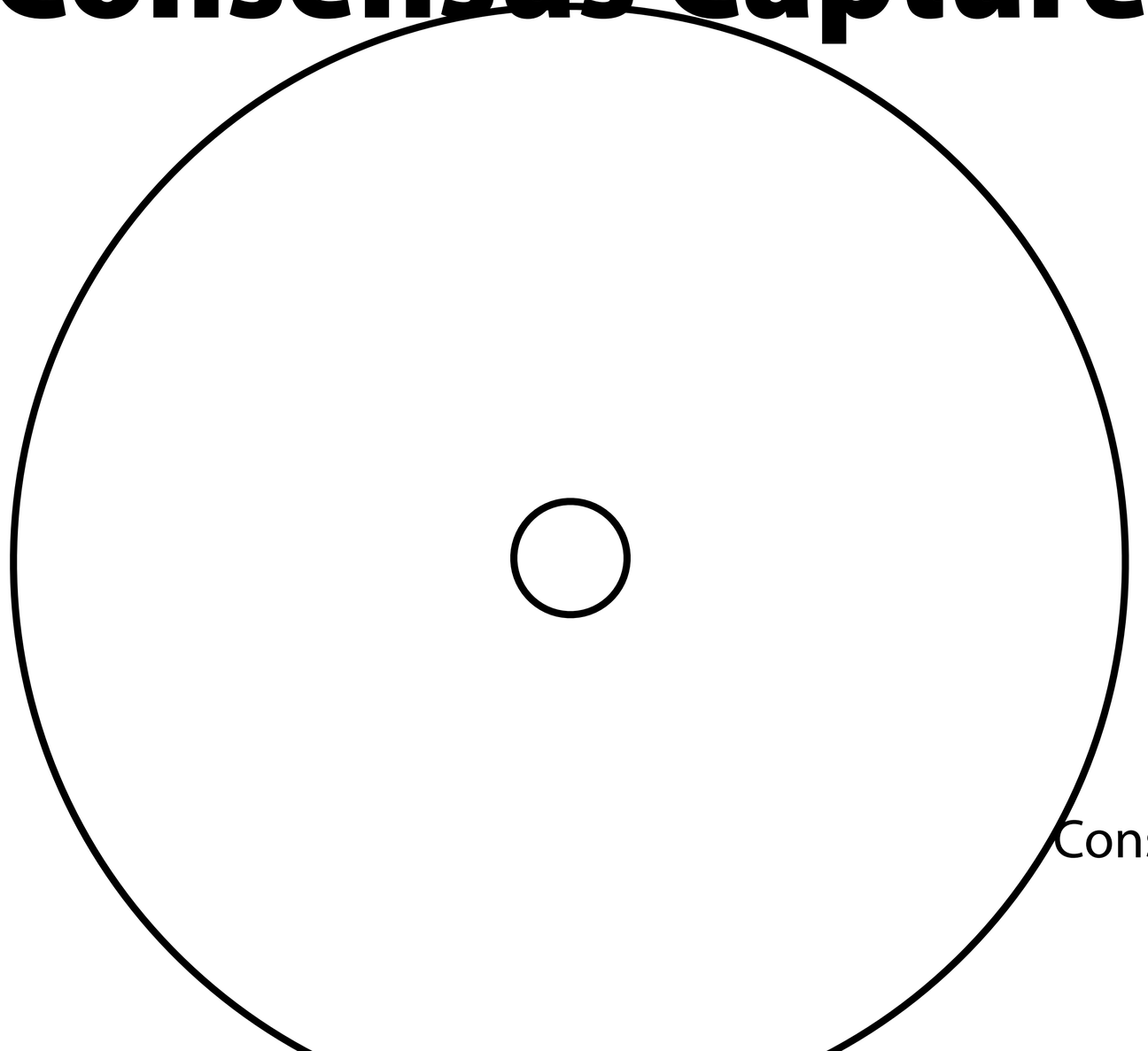
# Consensus Capture



Consensus participants:

**5%**

# Consensus Capture

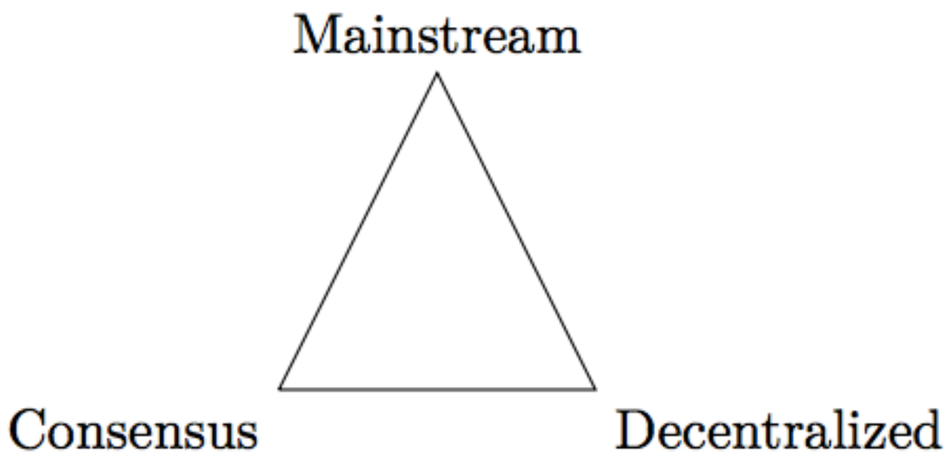


Consensus participants:

**1%**

# DCS Triangle

We observe that any single system may possess, at most, two of three properties:




- **Consensus** means the system has participants who regularly come to agreement about changes to the system's shared state (shared resource). The interval at which the system comes to agreement is its *period*, $\pi$.
- **Mainstream** (or **Scalable**) means the system is, *by itself*, capable of competing with the transactional demands placed on a leading centralized competitor.[1]
- **Decentralized** means the system meets two related notions of *decentralization*:

**Decentralized** means the system meets two related notions of *decentralization*:

1. *The system has no single point of failure.* This first notion of decentralization, $D_1$, is measured by counting the number of "doors" to knock on to compromise the *intended behavior* of the system,[2] where each "door" can be an individual or a technical component of the system. By this notion, a system is decentralized when:

$$D_1 \Rightarrow \texttt{doors\_to\_compromise}(\mathit{system}) \geq 2$$

2. *The system's behavior is not dictated by a small group.* Whereas $D_1$ focuses on the ability to compromise the intended behavior of a system, $D_2$ focuses on *who defines and controls the intended behavior in the first place.* Redefining a protocol is a type of system compromise if it is done against the interests of the users of the system, therefore $D_2$ is a superset of $D_1$ that says not only must there not be a central point of failure, but there must also not be a central point of control that can change the system without the consent of its users.

$$D_2 \Rightarrow \texttt{redefinition\_threshold}(\mathit{system}) > 75\%$$

**Decentralized** means the system meets two related notions of *decentralization*:

1. *The system has no single point of failure.* This first notion of decentralization, $D_1$, is measured by counting the number of "doors" to knock on to compromise the *intended behavior* of the system,[2] where each "door" can be an individual or a technical component of the system. By this notion, a system is decentralized when:

$$D_1 \Rightarrow \texttt{doors\_to\_compromise}(system) \geq 2$$

2. *The system's behavior is not dictated by a small group.* Whereas $D_1$ focuses on the ability to compromise the intended behavior of a system, $D_2$ focuses on *who defines and controls the intended behavior in the first place.* Redefining a protocol is a type of system compromise if it is done against the interests of the users of the system, therefore $D_2$ is a superset of $D_1$ that says not only must there not be a central point of failure, but there must also not be a central point of control that can change the system without the consent of its users.

$$D_2 \Rightarrow \texttt{redefinition\_threshold}(system) > 75\%$$

Note: questionable threshold

https://okturtles.com/dcs

# DPKI

it does not specify consensus
it is a protocol for consensus protocols

# DPKI in 2 Parts

# Part 1: DPKI namespaces

| TLD | Consensus network/protocol |
| --- | --- |
| `.eth` | |
| `.bit` | |

# Part 1: DPKI namespaces

TLD

Consensus network/protocol

**Trust assumptions at each step.**

`.eth`

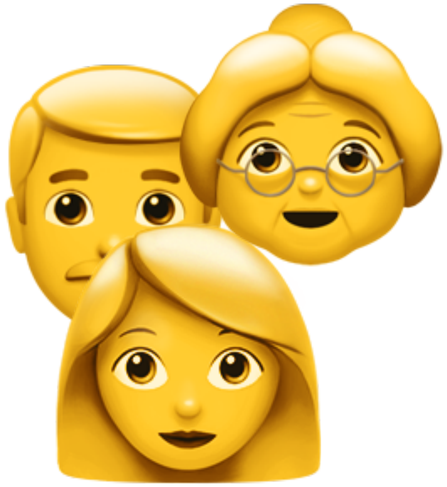
For most users, this is the most dangerous step. Thin client needed, but most blockchains don't yet have one. This is where DNSChain used to fit in, and still can, but if it doesn't use a thin client then it's not much different than Convergence

This assumes consensus capture has not occurred. If it has, attacker is usually limited to censorship of identifier -> key binding, but a poorly designed protocol can allow more

# Part 2: Identifier lifecycle

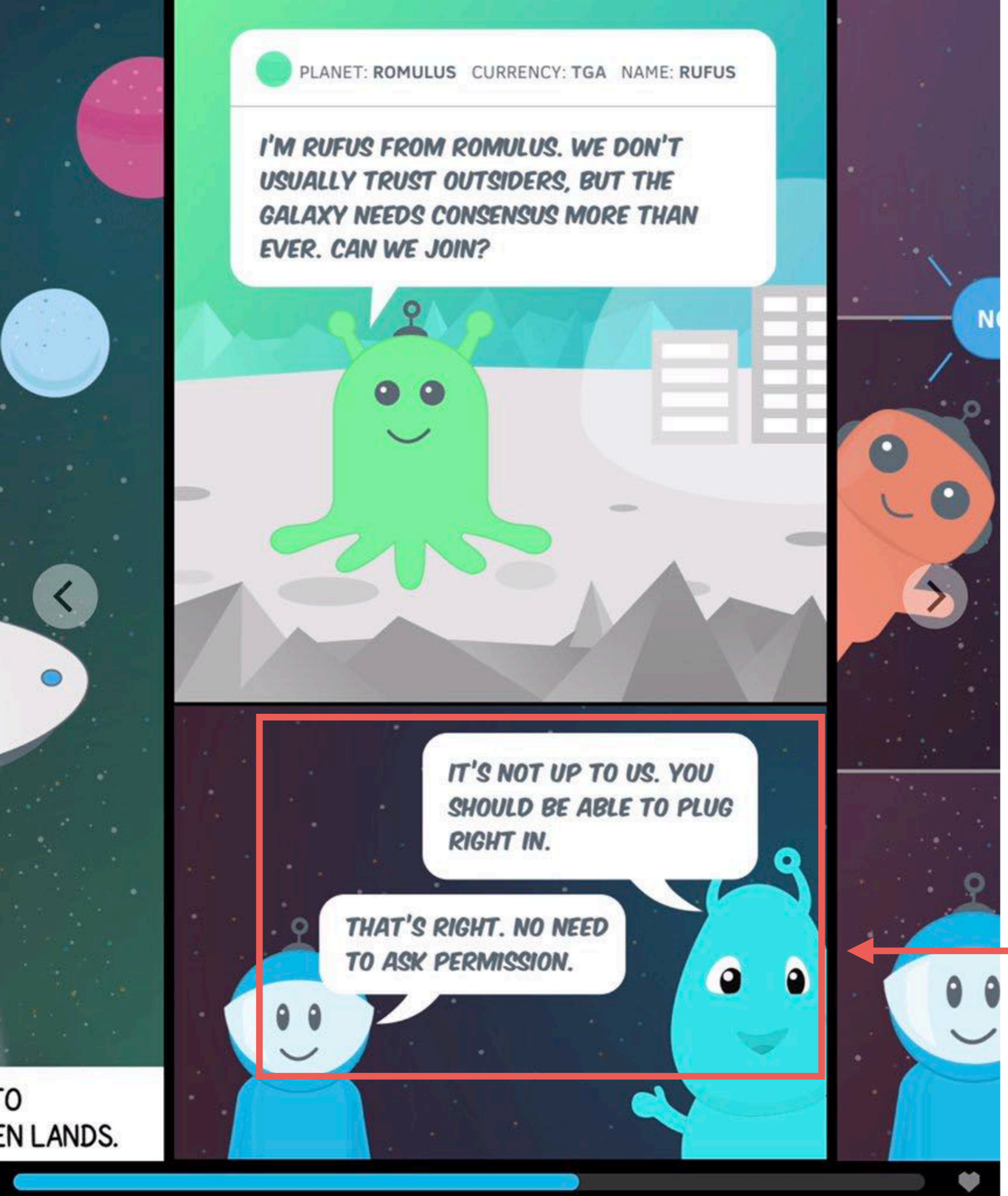
Loss/recovery

Additional devices



More info: Rebooting Web-of-Trust

# Stellar Consensus Protocol (SCP)




**Greg Slepak**
@taoeffect

.@JedMcCaleb @iang_fc @bascule Stellar's marketing is grossly misleading on this point. "No need to ask permission [to *listen*!]"

https://twitter.com/taoeffect/status/832284907342688256

# Danger!

# Don’t break the Internet!

Mail Archive

Sign in

Date Thread

# [Ilc] Genuine concern: is the the purpose of this group to create an Internet-cartel?

Tao Effect <contact@taoeffect.com> | Thu, 16 February 2017 06:30 UTC | Show header

Hi list,

Judging by the name of this group I will not be surprised if this email is simply ignored, but I'm obligated by conscience to voice my concern, if only so that future historians can search these archives and see that yes, someone did contact this group and ask them if they were aware of the consequences, i.e. the high likelihood of turning the Internet back into 20th century cable news.

It is not clear to me, from the name of this working group, whether it understands the meaning of "consensus".

My OS X dictionary says:

mong judges

Email to IETF "Internet-level Consensus" group

https://mailarchive.ietf.org/arch/msg/ilc/BmFgooRm5GikT6mwhx9yOZgL1G8

rchive

Thread

cern: is the the purpose of this group to create an Internet-cartel?

aoeffect.com> | Thu, 16 February 2017 06:30 UTC | Show header

me of this group I will not be surprised if this email is simply igno
conscience to voice my concern, if only so that future historians car
d see that yes, someone did contact this group and ask them if they w
es, i.e. the high likelihood of turning the Internet back into 20th c

Email to IETF "Internet-level Consensus" group

https://mailarchive.ietf.org/arch/msg/ilc/BmFgooRm5GikT6mwhx9yOZgL1G8

This is why DPKI explicitly allows arbitrary consensus protocols.

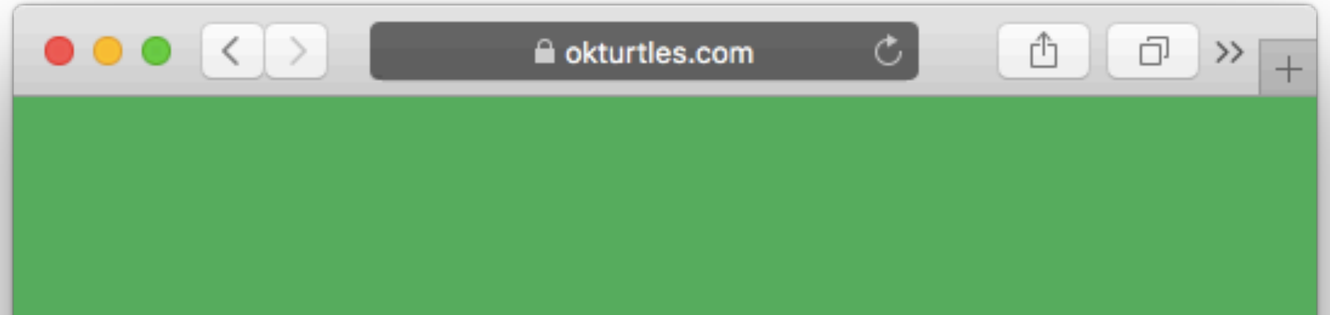
(As long as they fit the mathematical notion of decentralization.)

# Answers to The Problem™

| | Who can define your identity? | Reason to trust? | Usable? |
|---|---|---|---|
| **CT** | Governments, CAs | Almost none | Yes |
| **KT** | Key Server, app developer | Server: None<br>App dev: maybe you'll find a good one | Yes |
| **CONIKS** | If correctly implemented, server can only censor, not define | TOFU-based, though gossip questionable | Yes |
| **SCP** | Probably a cartel | Maybe it will be a good cartel | (?) Probably |
| **DPKI** | Your chosen delegates, and depends on chosen namespace consensus | Many.<br>**See next slide.** | Yes |

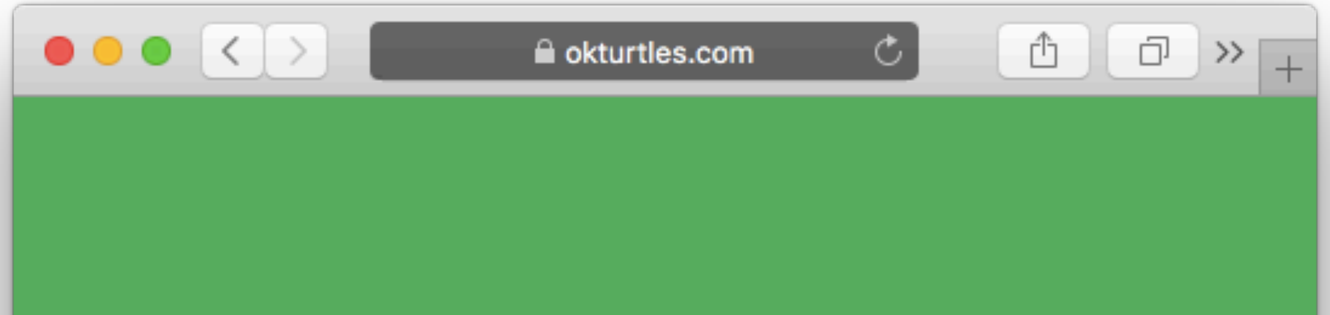
(and hackers)

DPKI gives you reason to have faith in the lock icon



# DPKI gives you reason to have faith in the lock icon

- Only decentralized namespaces allowed
- Identity controlled by **you**
- Spec **requires** decentralization at every point to minimize trust, including lookup
- Spec **requires** private keys never be generated or stored on a server
- Your choice of consensus system



# Potentially DPKI-friendly protocols and implementations

# Potentially DPKI-friendly

- **EIP 137** — Ethereum Domain Name Service[1]
- **Blockstack**
- **uPort**
- …More? Feel free to suggest!

[1] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-137.md

# How to contribute

- Read the DPKI paper

  And the DPKI issues in:
  github.com/WebOfTrustInfo/rebooting-the-web-of-trust

- Attend Rebooting Web-of-Trust → weboftrust.info
- No need to ask for permission to contribute, feel free to pick up where we left off
- Be friendly, ask questions!