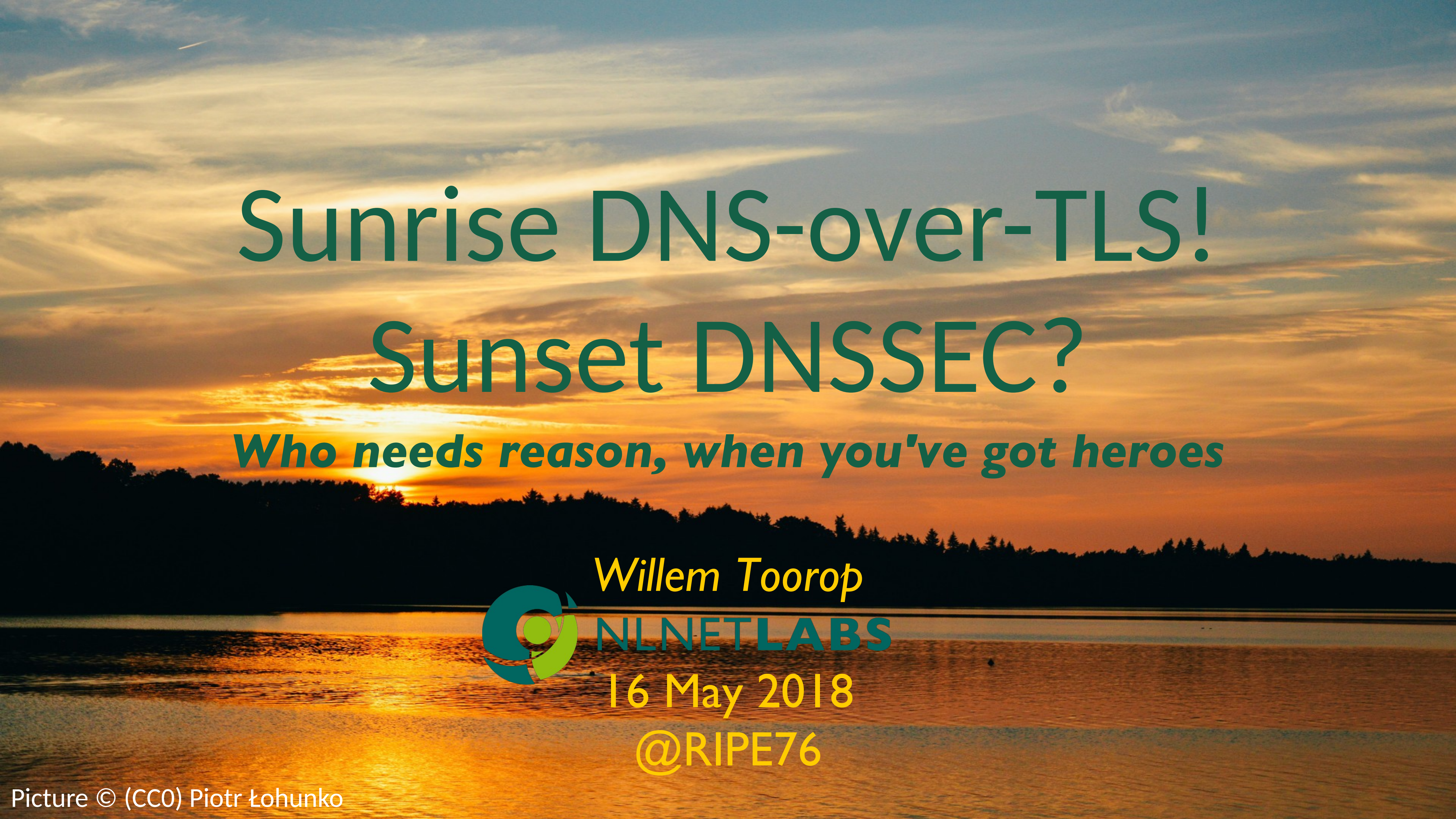


Sunrise DNS-over-TLS!
Sunset DNSSEC?

Who needs reason, when you've got heroes

Willem Toorop

NLNETLABS

16 May 2018

@RIPE76

Picture © (CC0) Piotr Łohunko

Motivation for this presentation

To: DNSSEC Coordination <dnssec-coord@elists.isoc.org>

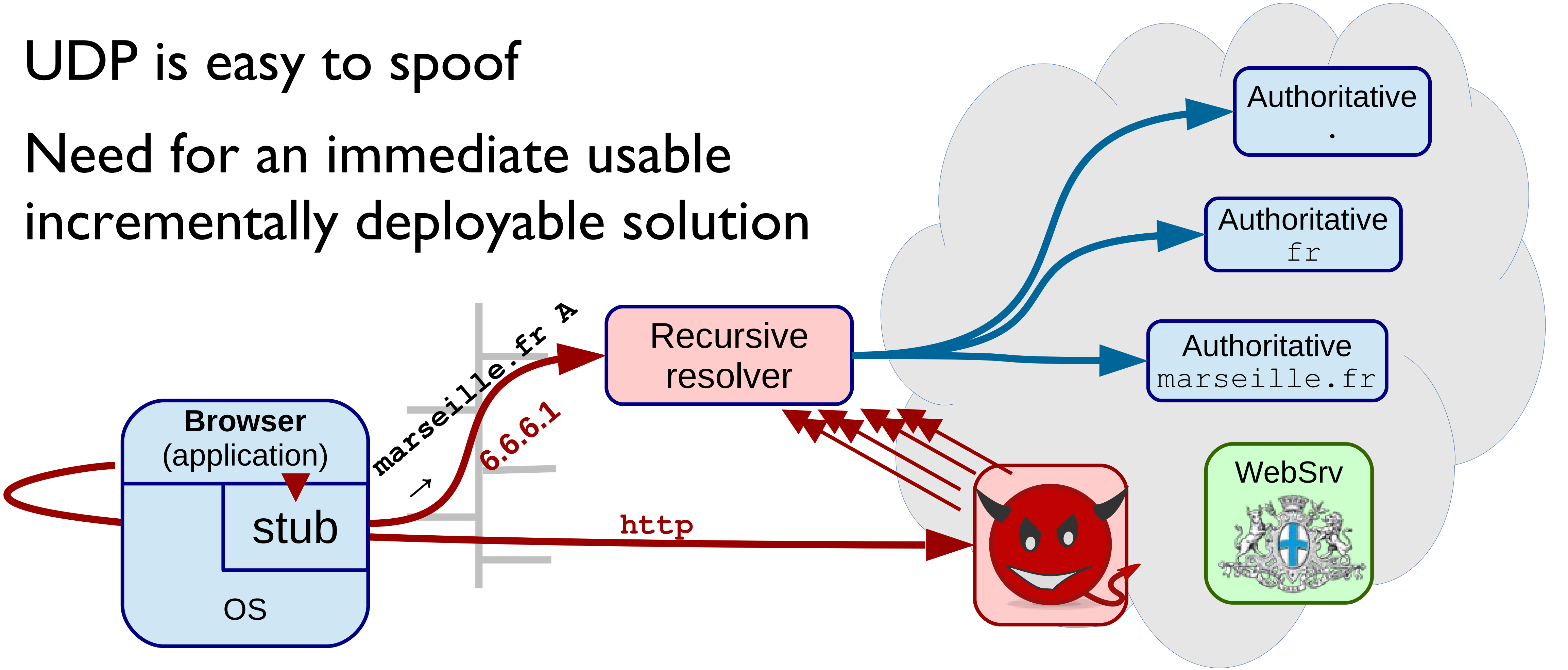
“ *People thought that using DNS-over-TLS meant they didn't need to use DNSSEC. They have TLS, therefore they are all good, right?* ”

https://github.com/dohwg/draft-ietf-doh-dns-over-https

“ *In the absence of information about the authenticity of responses, such as DNSSEC, a DNS API server can give a client invalid data in responses. A client MUST NOT authorize arbitrary DNS API servers. Instead, a client MUST specifically authorize DNS API servers using mechanisms such as explicit configuration.* ”

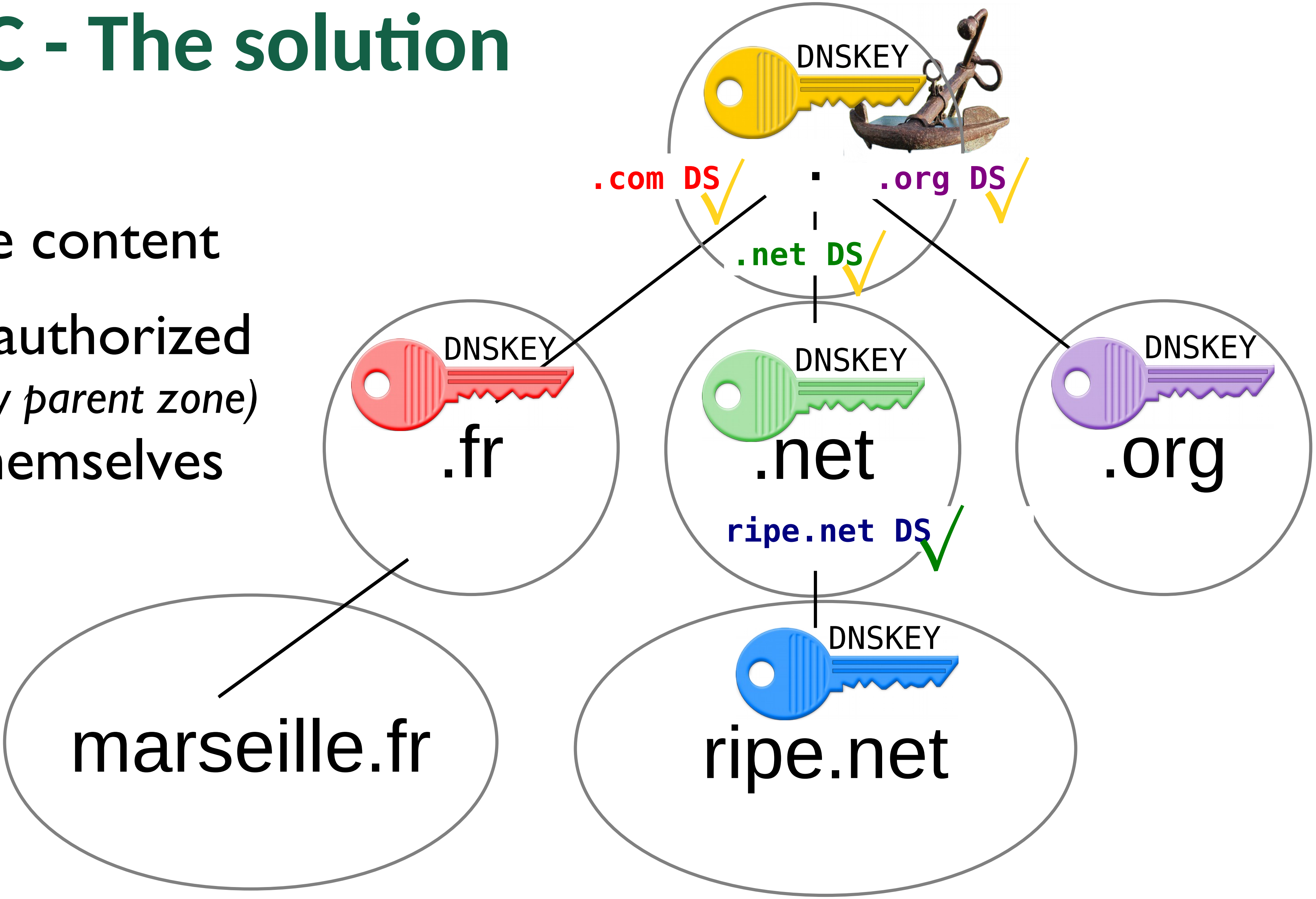
DNSSEC - History & Motivation

- UDP is easy to spoof
- Need for an immediate usable incrementally deployable solution



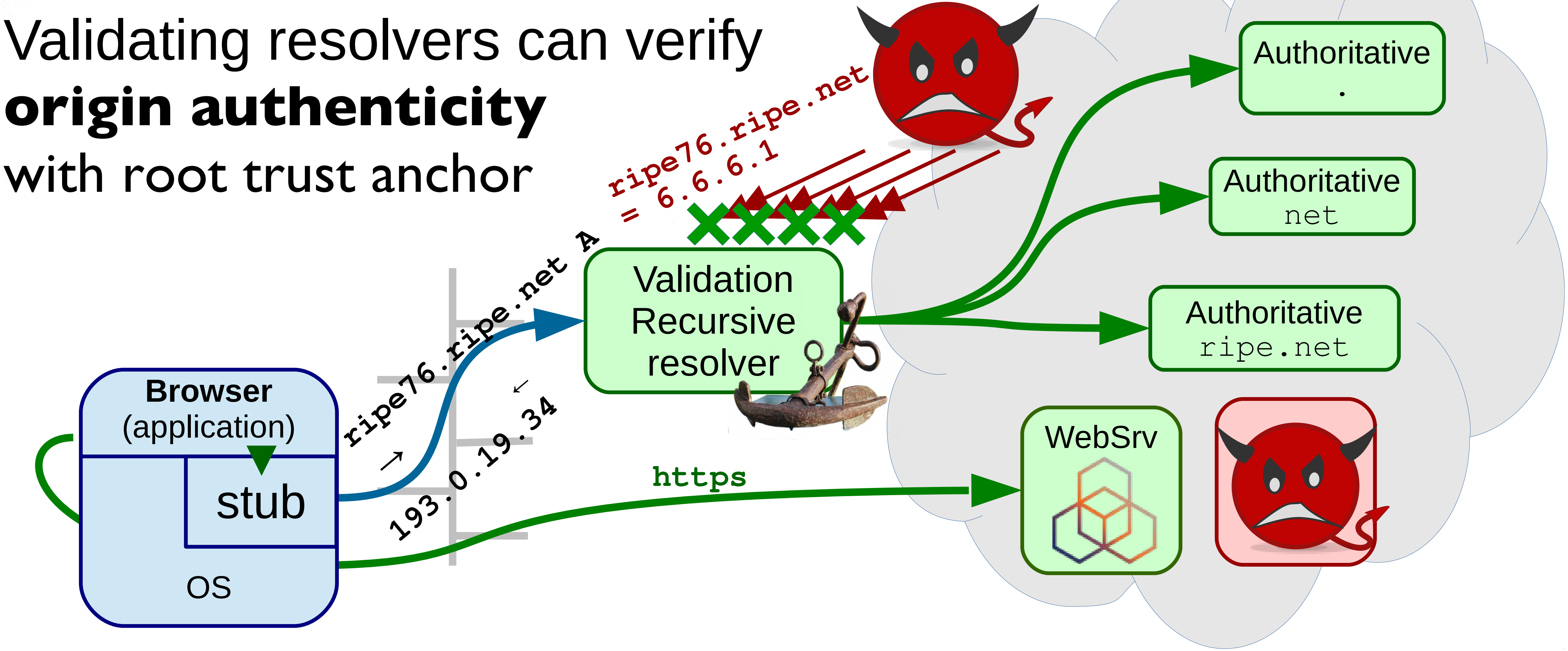
DNSSEC - The solution

- Sign the zone content
- Child zones authorized *(by parent zone)* to sign for themselves



DNSSEC - The solution

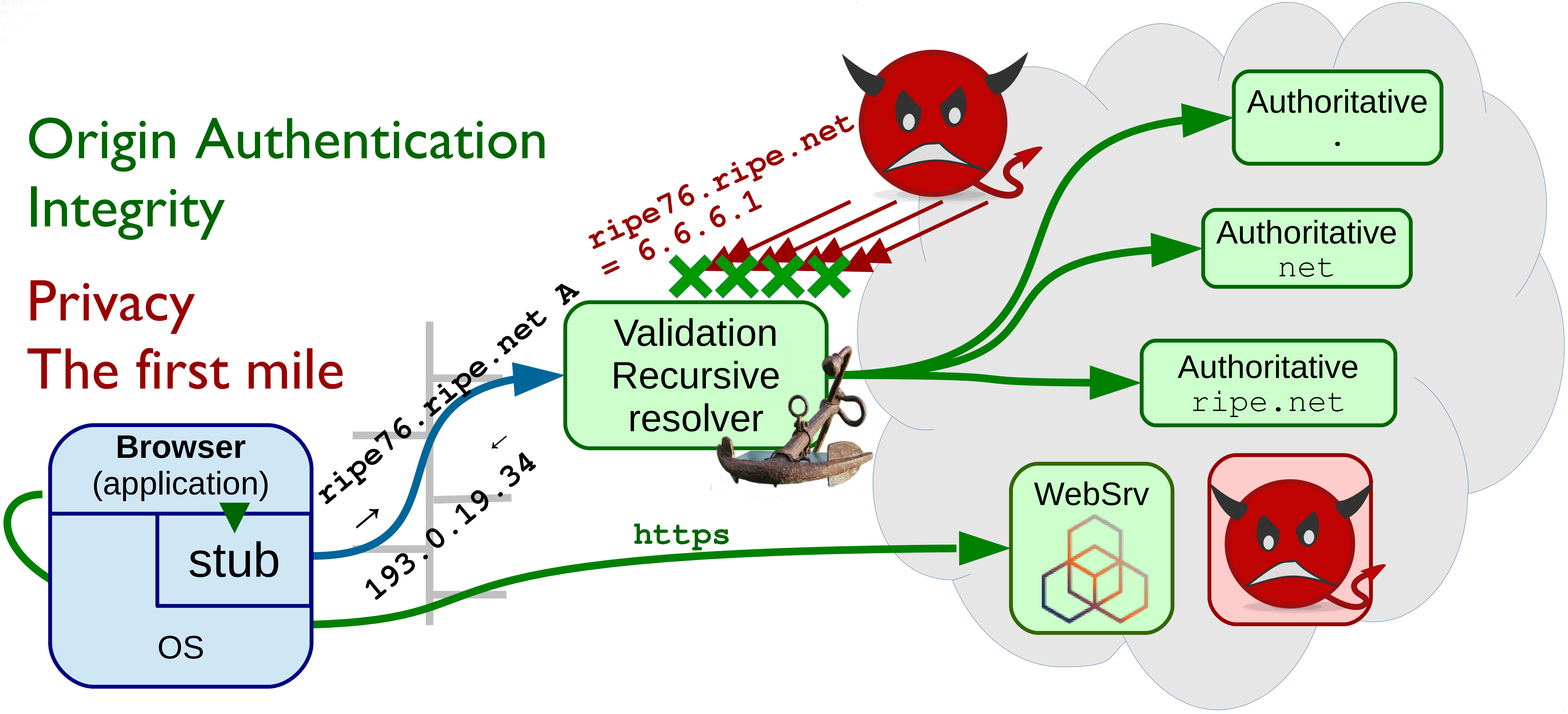
- Validating resolvers can verify **origin authenticity** with root trust anchor



DNSSEC – Properties & Limitations

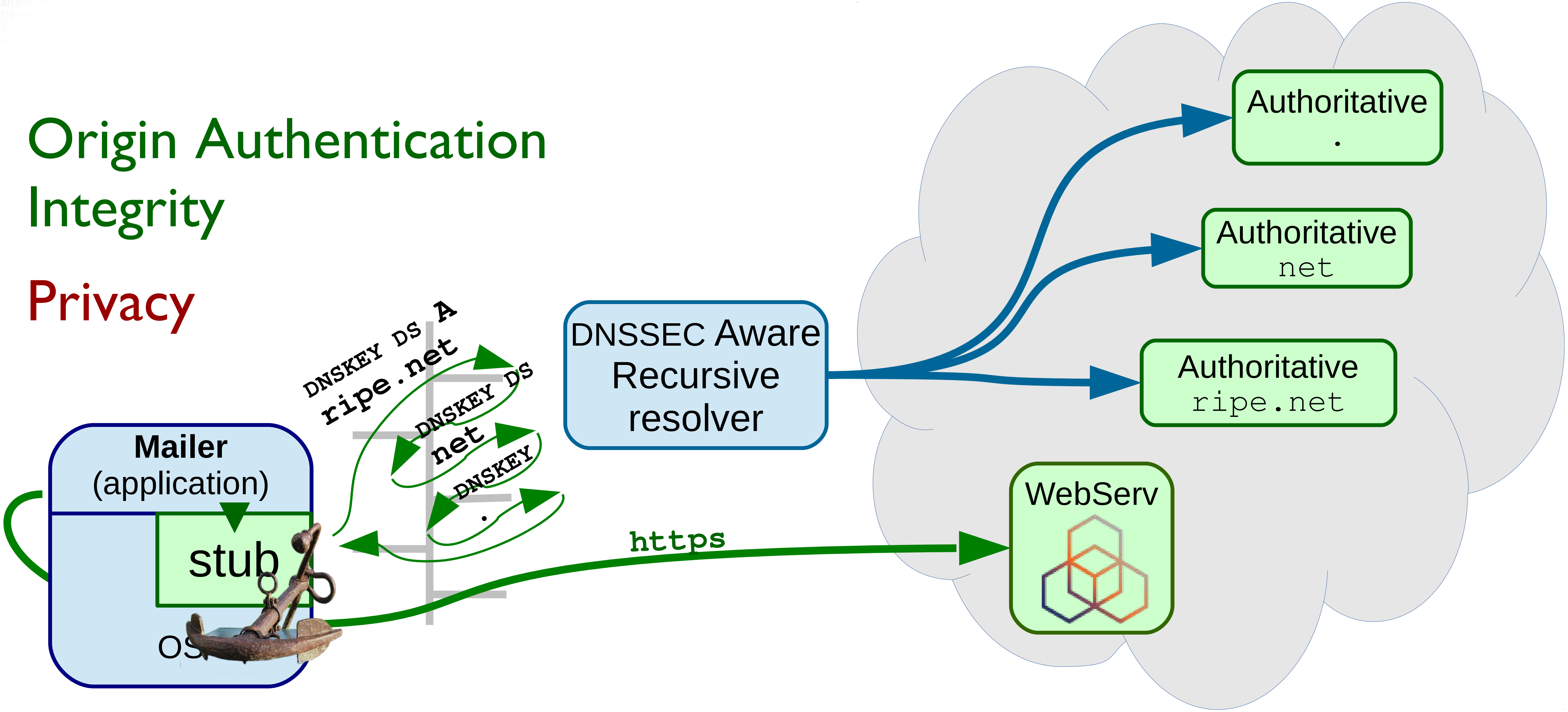
+ Origin Authentication
+ Integrity

- Privacy
- The first mile



DNSSEC – Properties & Limitations

- + Origin Authentication
- + Integrity
- - Privacy



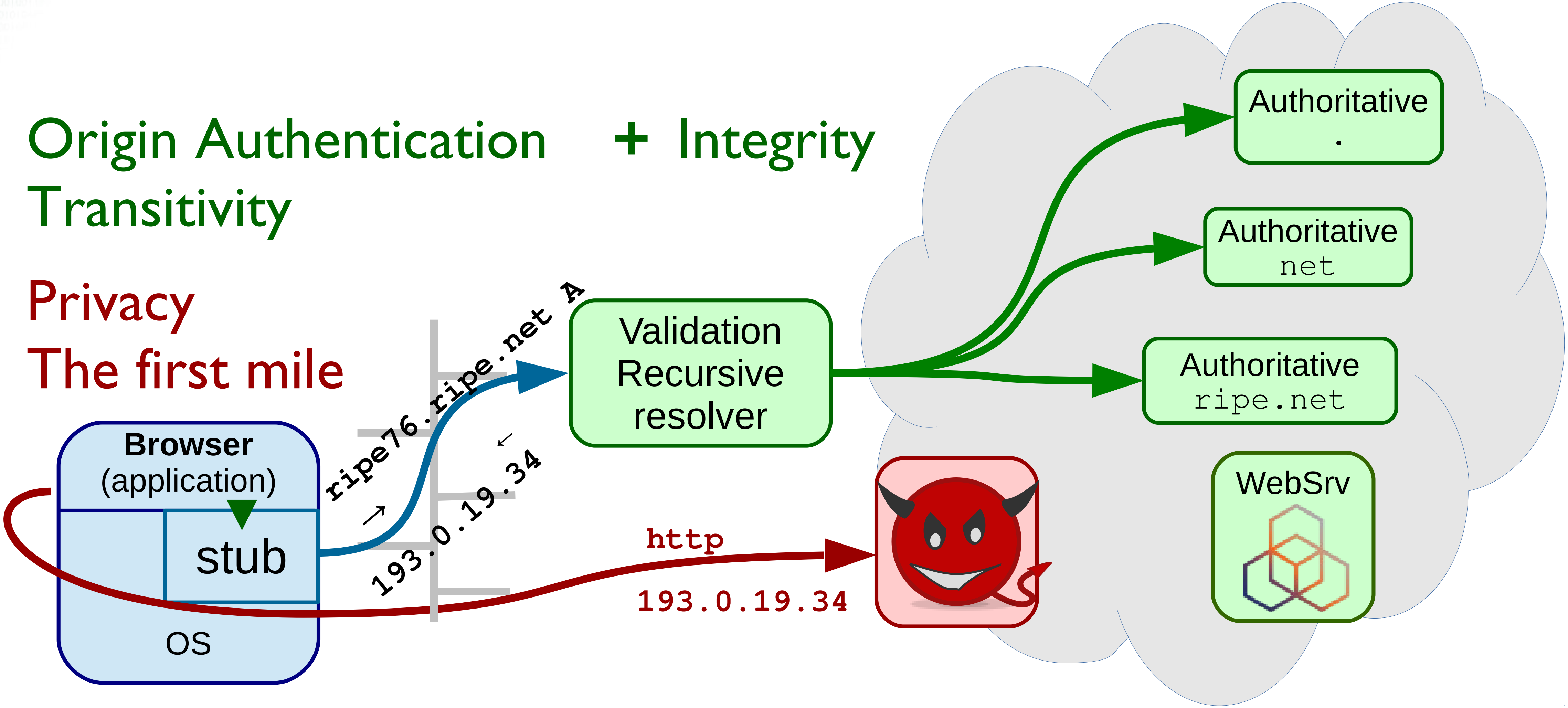
+ **Transitivity**

- Still first mile issues

DNSSEC – Properties & Limitations

+ Origin Authentication
+ Integrity
+ Transitivity

- Privacy
- The first mile



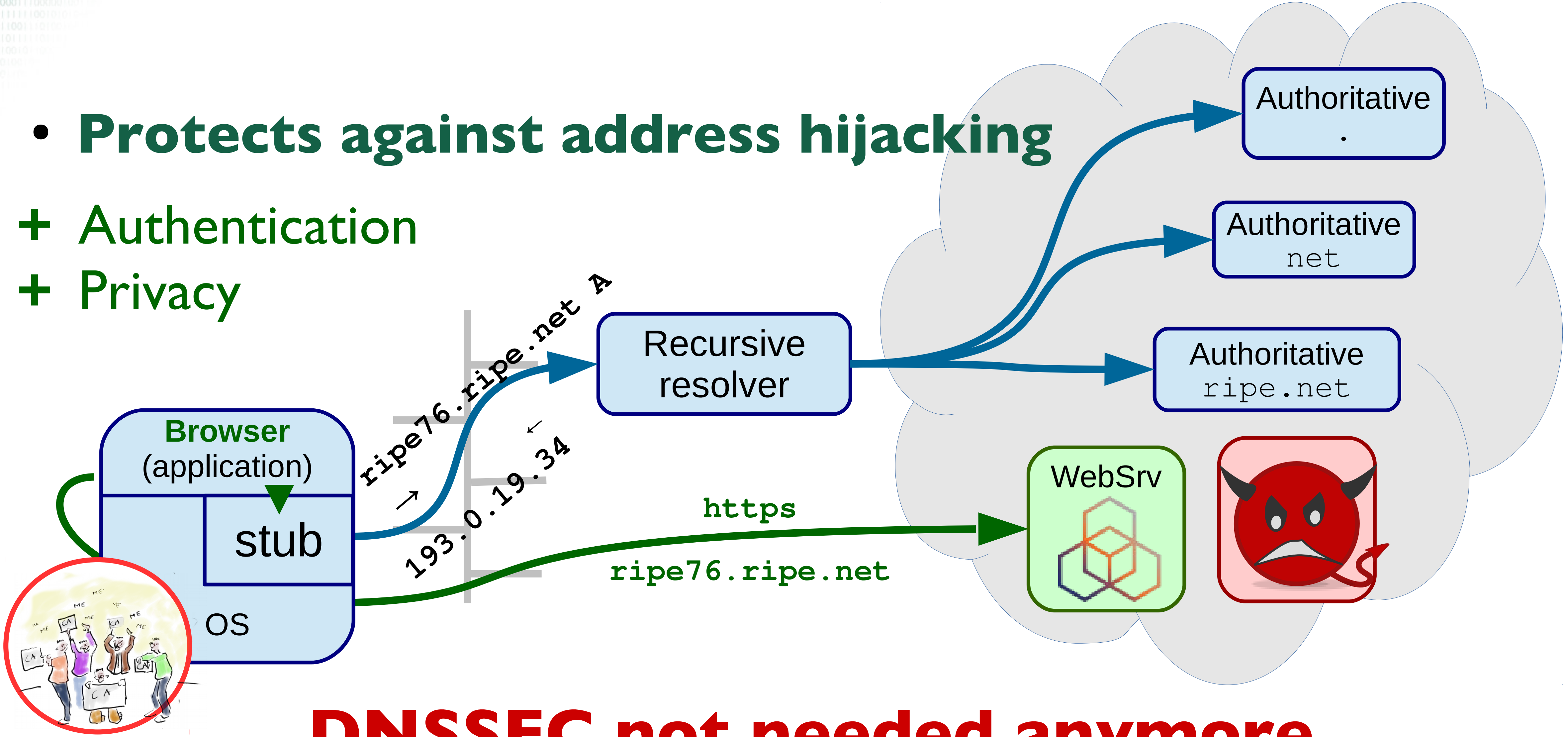
- Does not protect against address hijacking

TLS – Properties & Limitations

- **Protects against address hijacking**

+ Authentication

+ Privacy



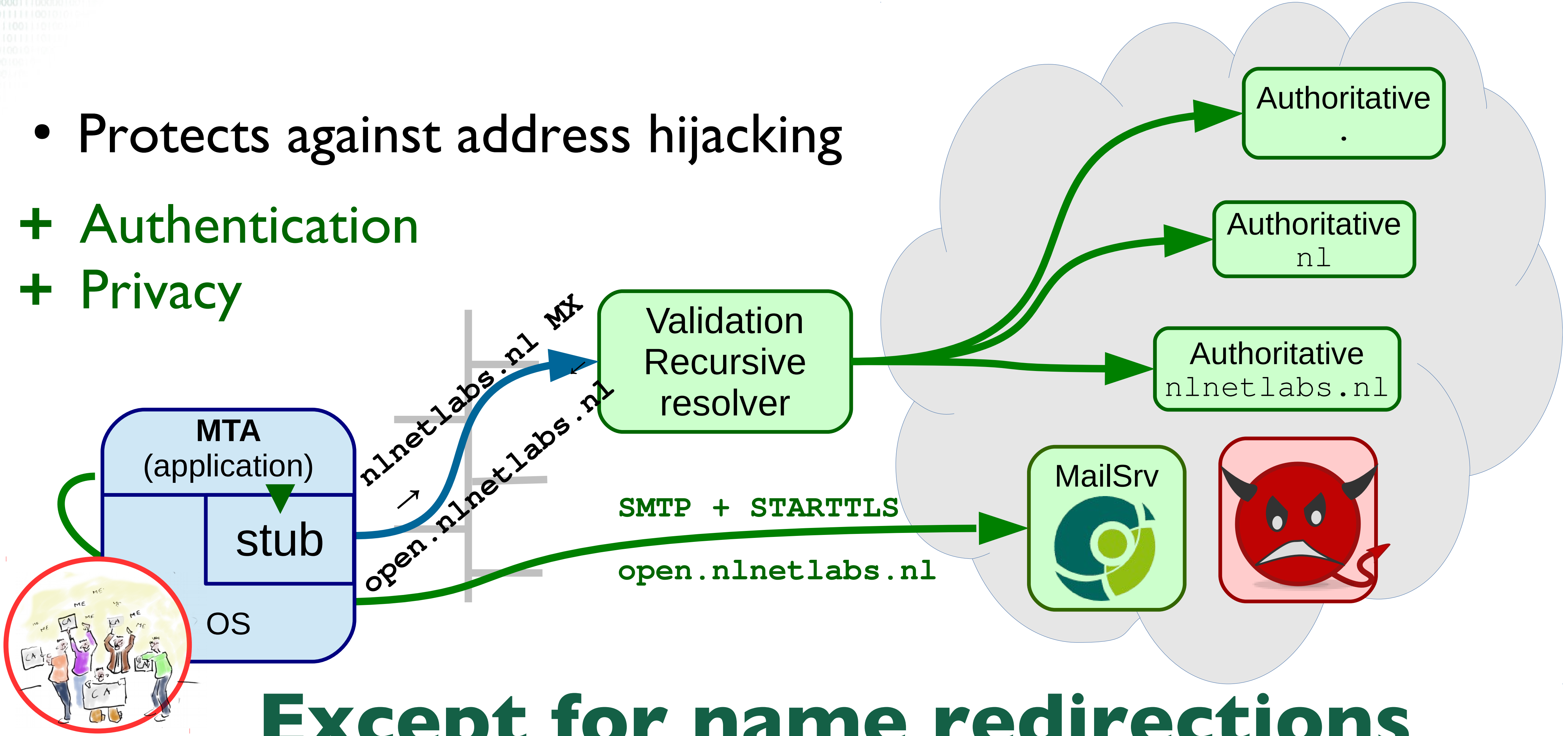
DNSSEC not needed anymore

TLS – Properties & Limitations

- Protects against address hijacking

+ Authentication

+ Privacy



Except for name redirections

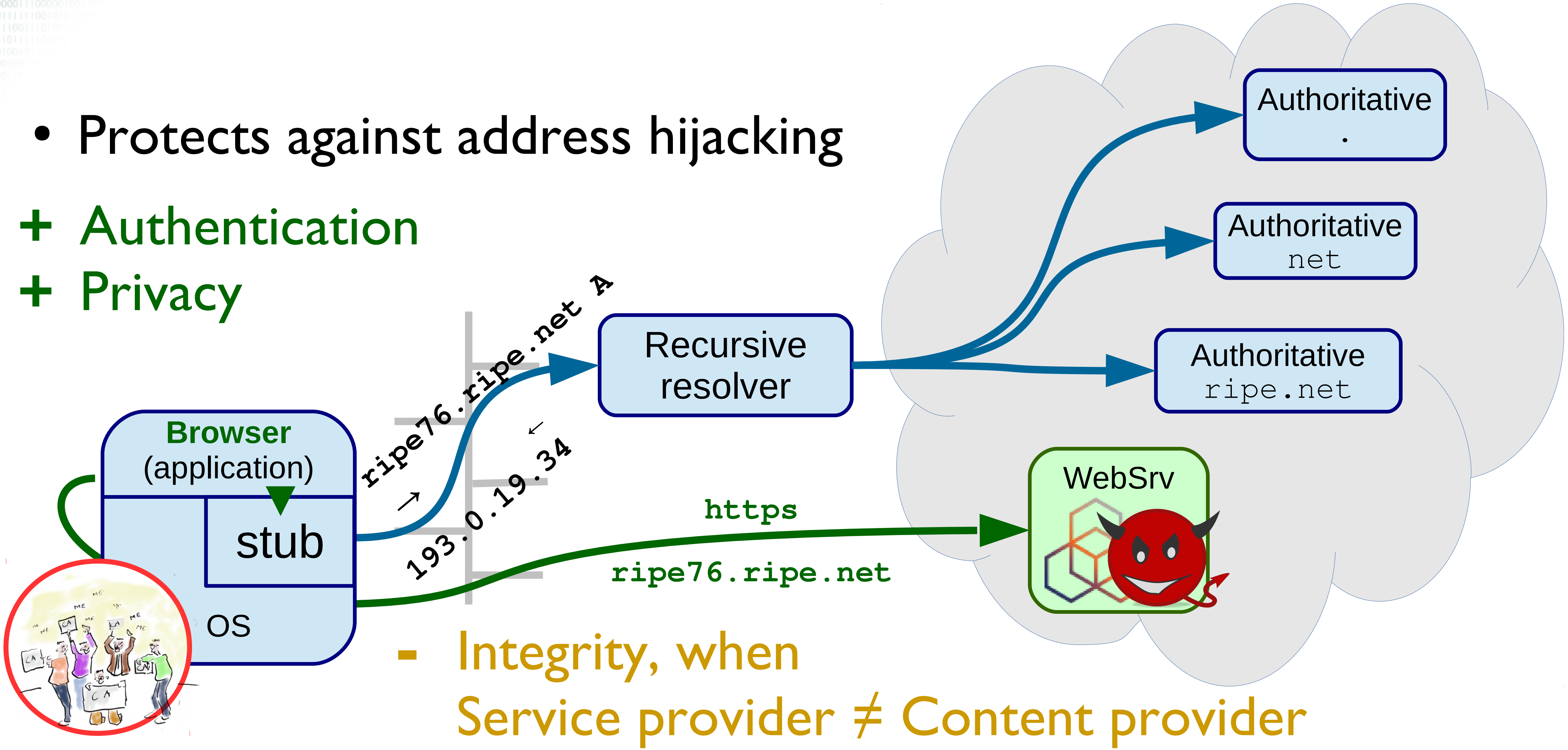
MX, CNAME, DNAME, SRV, NAPTR, LUA

TLS – Properties & Limitations

- Protects against address hijacking

+ Authentication

+ Privacy



- Integrity, when Service provider ≠ Content provider

TLS – Properties & Limitations

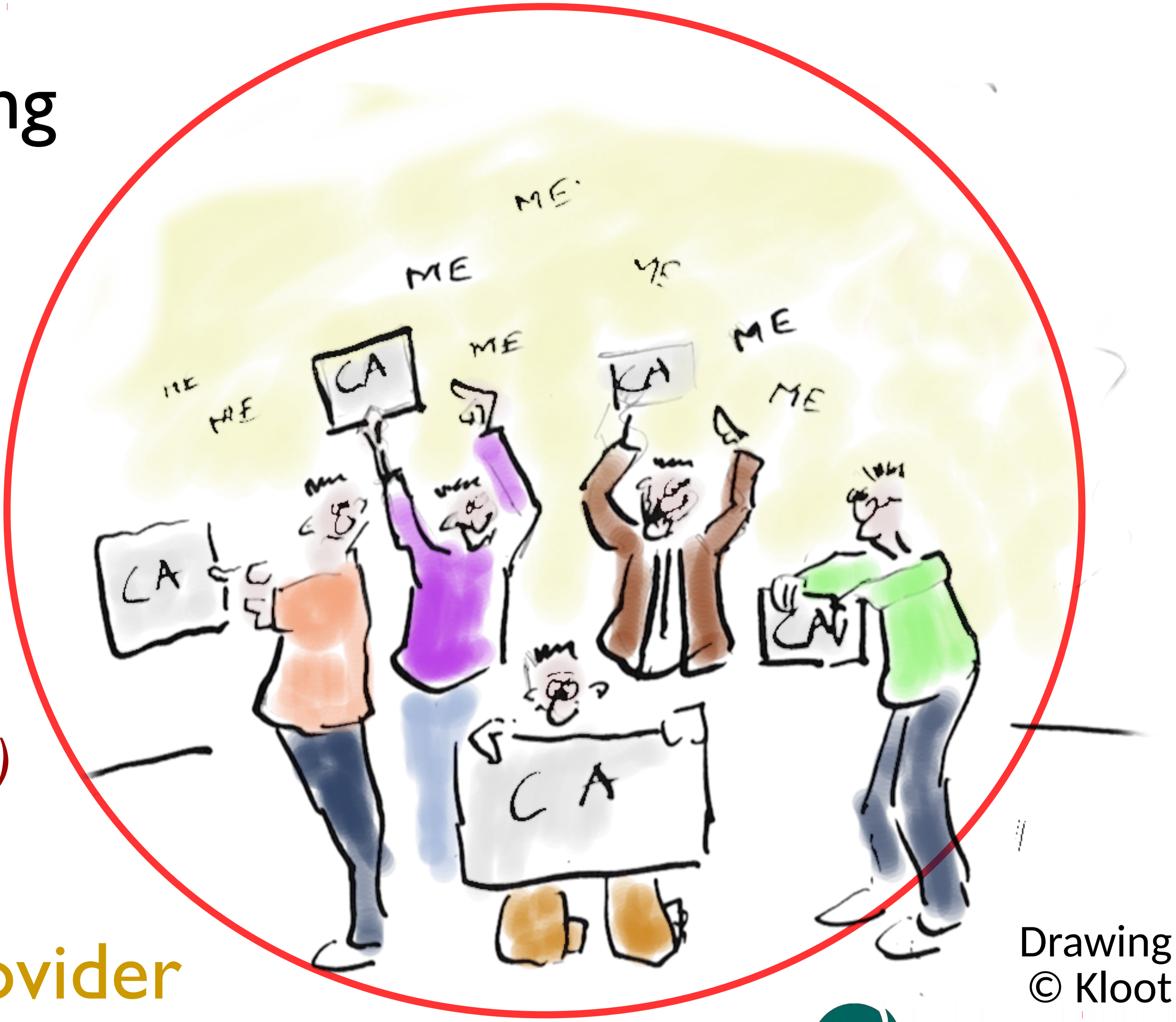
- Protects against address hijacking

+ Authentication

+ Privacy

- 1500+ Certificate authorities
(in 2010, see https://www.eff.org/observatory)

- Integrity, when
Service provider ≠ Content provider



Drawing
© Kloot

DNS over TLS – History & Motivation

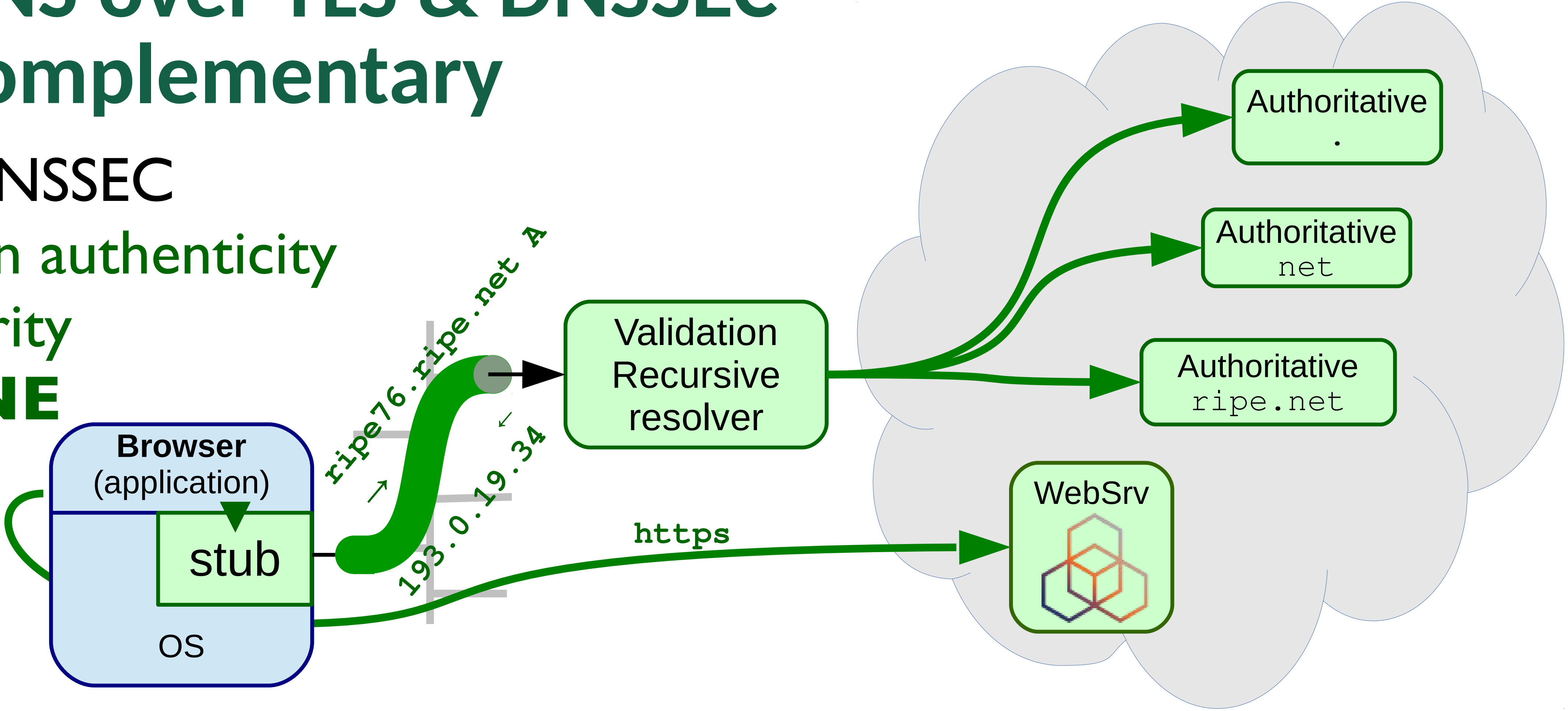
Encryption everywhere

Picture © (CC BY 3.0) Laura Poitras

DNS over TLS & DNSSEC – Complementary

From DNSSEC

- + Origin authenticity
- + Integrity
- + **DANE**

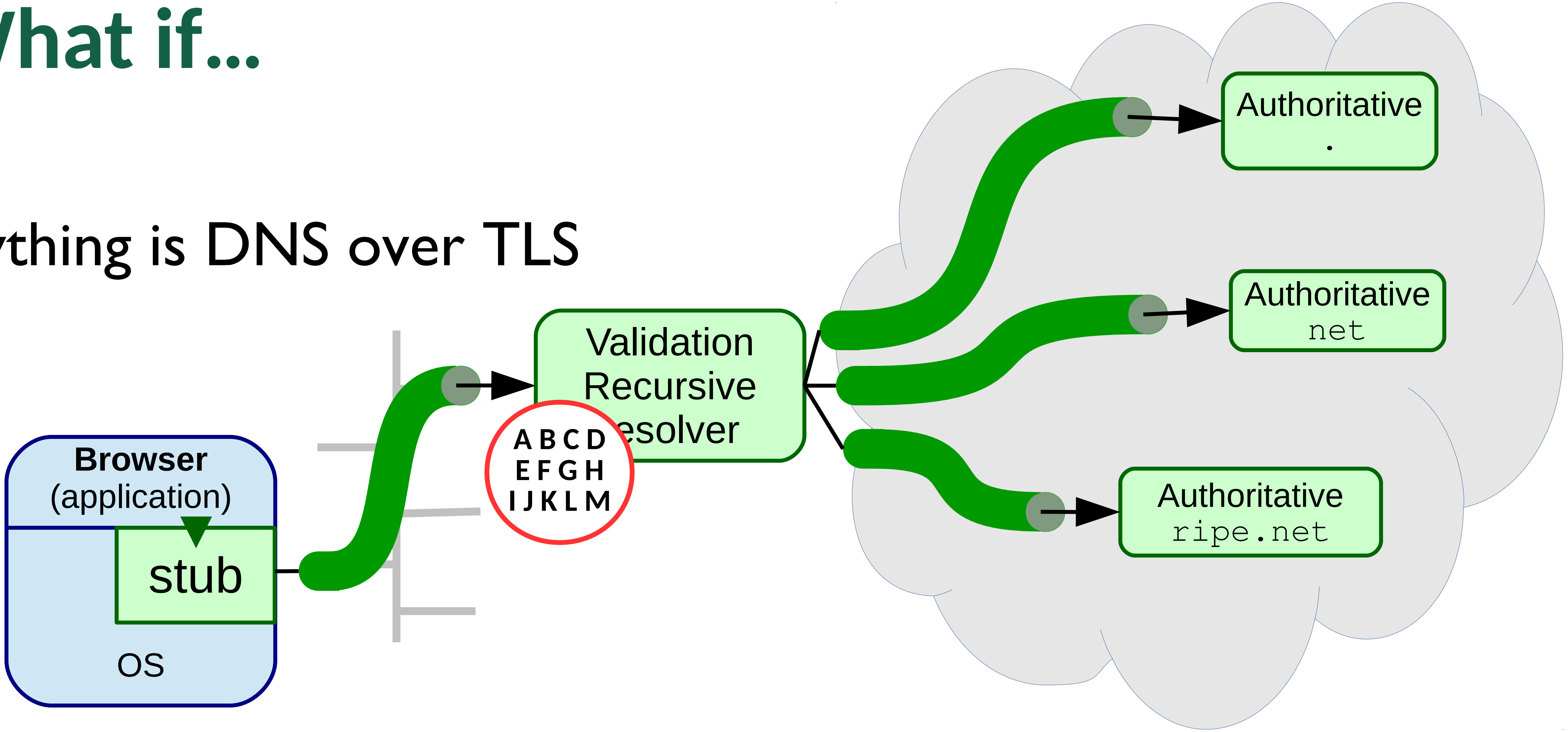


From DNS over TLS

- + Privacy *(except from the resolver operator)*
- + **First mile** *(by authenticating a trusted resolver)*

What if...

- Everything is DNS over TLS



- Start with CA store with CAs of the 13 root operators
- Learn CA of child zone operator when following delegations

Who needs reason, when you’ve got heroes

Listen to reason?

- Trust zones to vouch for their own data

- Stub either DNSSEC validates itself, or
- trusts resolver operator that vouches (via DANE) for itself

Rely on our heroes!

- Trust DNS operators chosen to serve the zone

- Trust CAs to authenticate stub → resolver path

What say you?