Sunrise DNS-over-TLS! Sunset DNSSEC?

Benno Overeinder and Willem Toorop
NLnet Labs

ICANN DNS Symposium 2018

NLNETLABS

Puzzlement over difference between DNSSEC and DNS-over-TLS

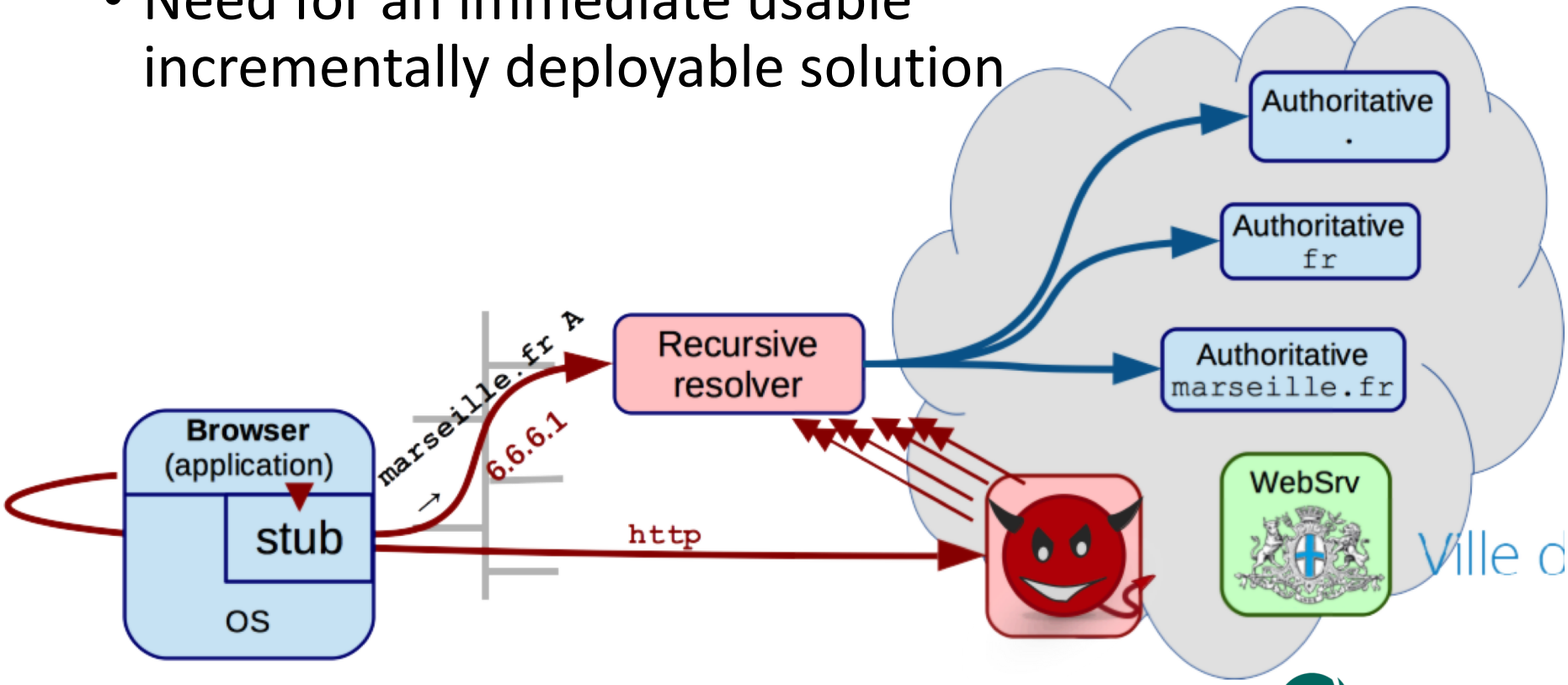
- DNSSEC Coordination dnssec-coord@elist.isoc.org:
  “People thought that using DNS-over-TLS meant they didn’t need to use DNSSEC. They have TLS, therefore are all good, right?”
- Twitter:
  “Will jump on DoH first, then see if dnssec is still needed.”
- draft-ietf-doh-dns-over-https:
  “In the absence of DNSSEC information, a DoH server can give a client invalid data in response to a DNS query. Section 4 disallows the use of DoH DNS responses that do not originate from configured servers. This prohibition does not guarantee protection against invalid data, but it does reduce the risk.”

DNSSEC

History, motivation, solution, properties and limitations

DNSSEC – History & Motivation

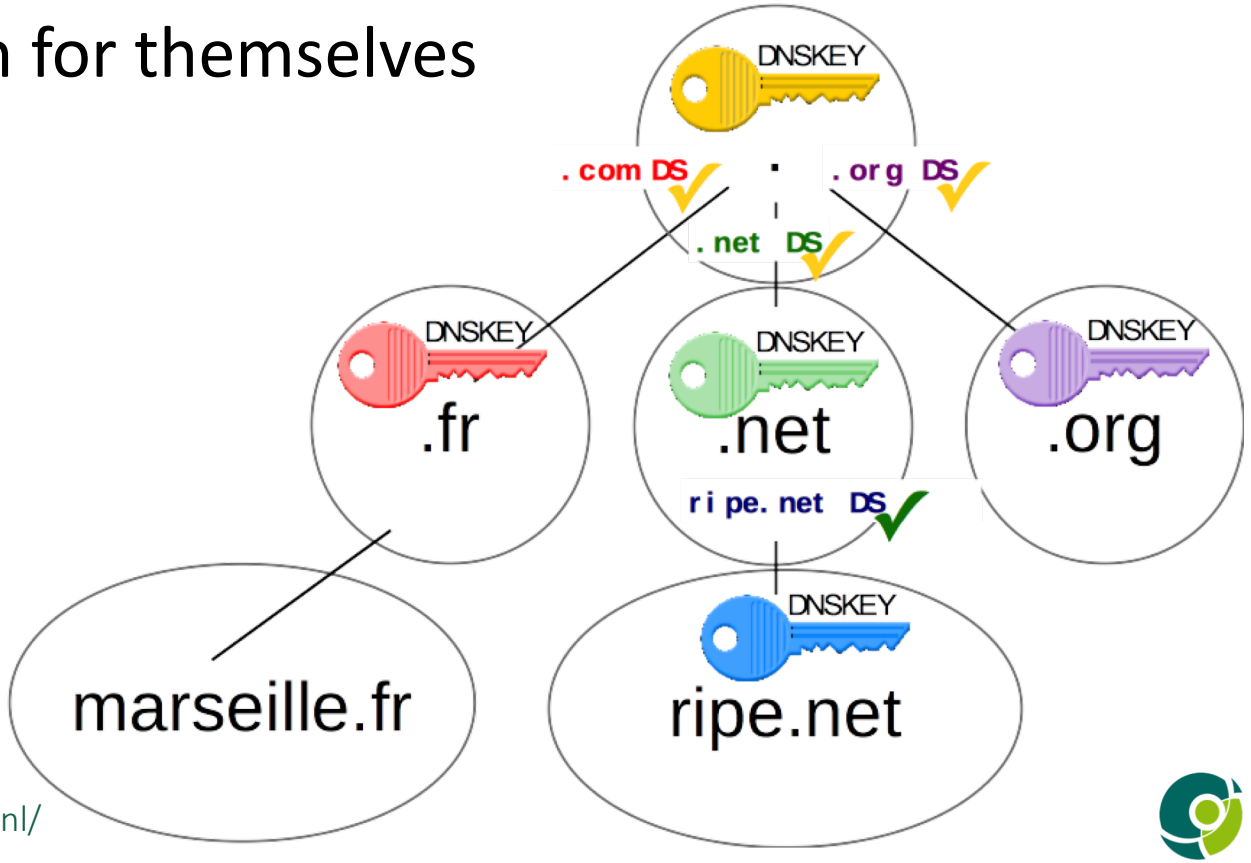
- UDP is easy to spoof
- Need for an immediate usable incrementally deployable solution



NLNETLABS

DNSSEC – The Solution

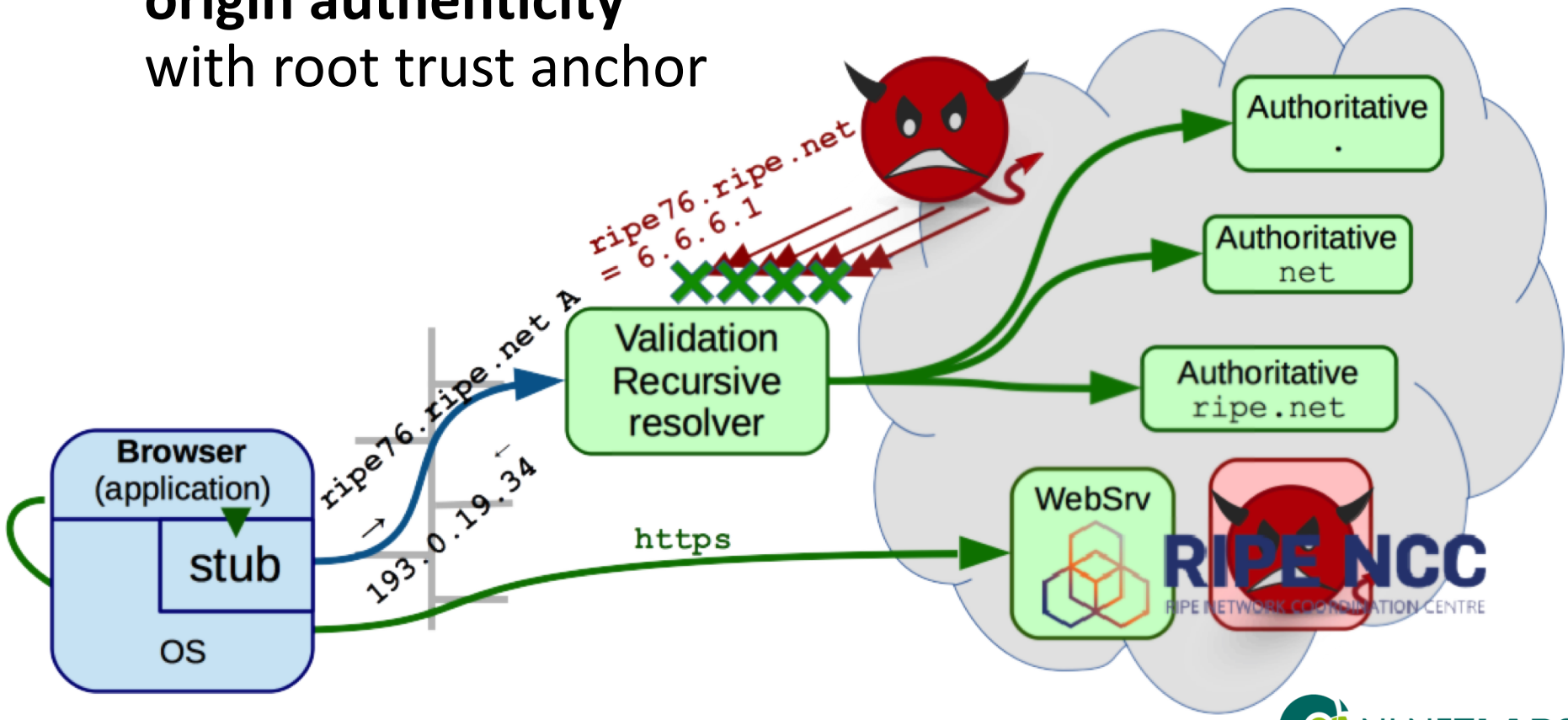
- Sign the zone content
- Child zones authorized *(by parent zone)* to sign for themselves



NLNETLABS

DNSSEC – The Solution (cont'd)

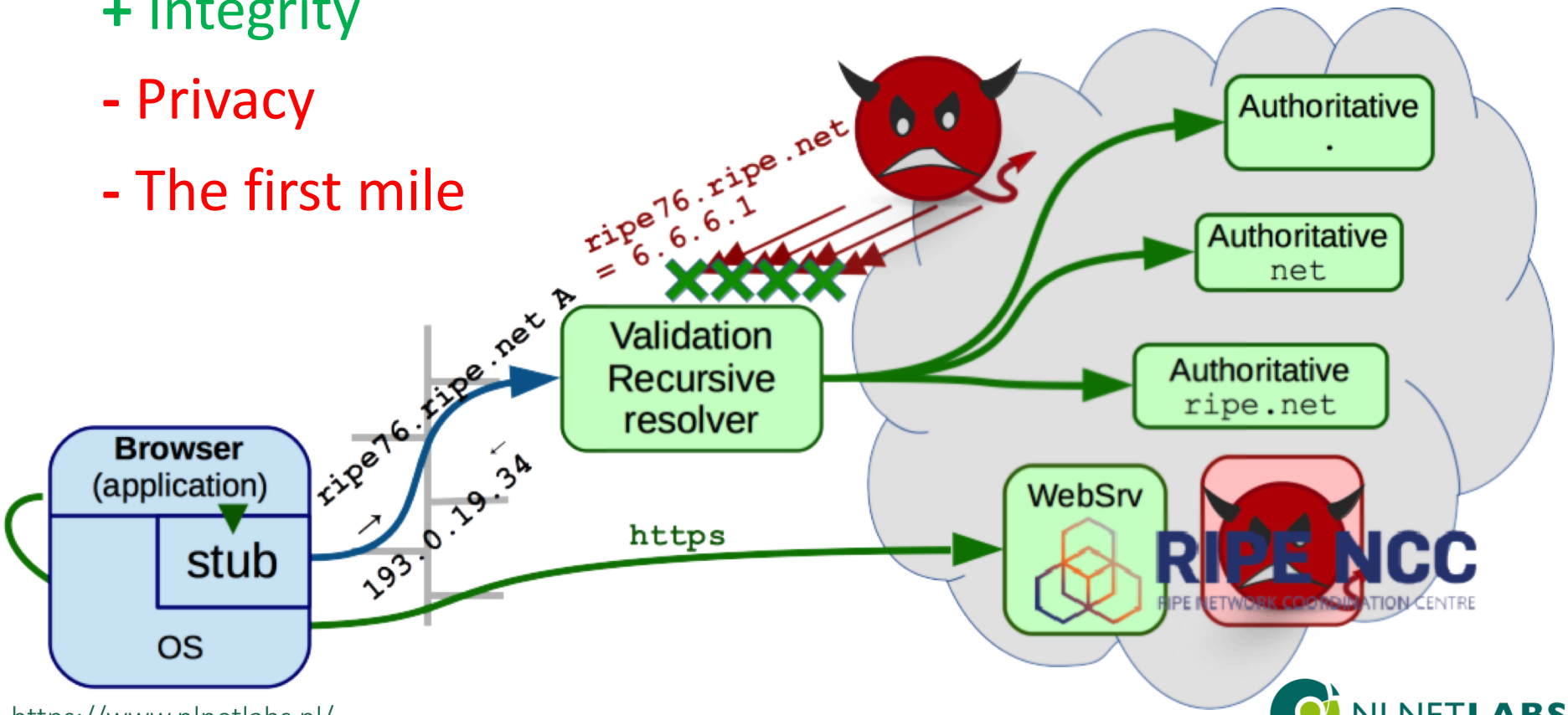
- Validating resolvers can verify **origin authenticity** with root trust anchor



NLNETLABS

DNSSEC – Properties & Limitations

+ Origin Authentication
+ Integrity
- Privacy
- The first mile

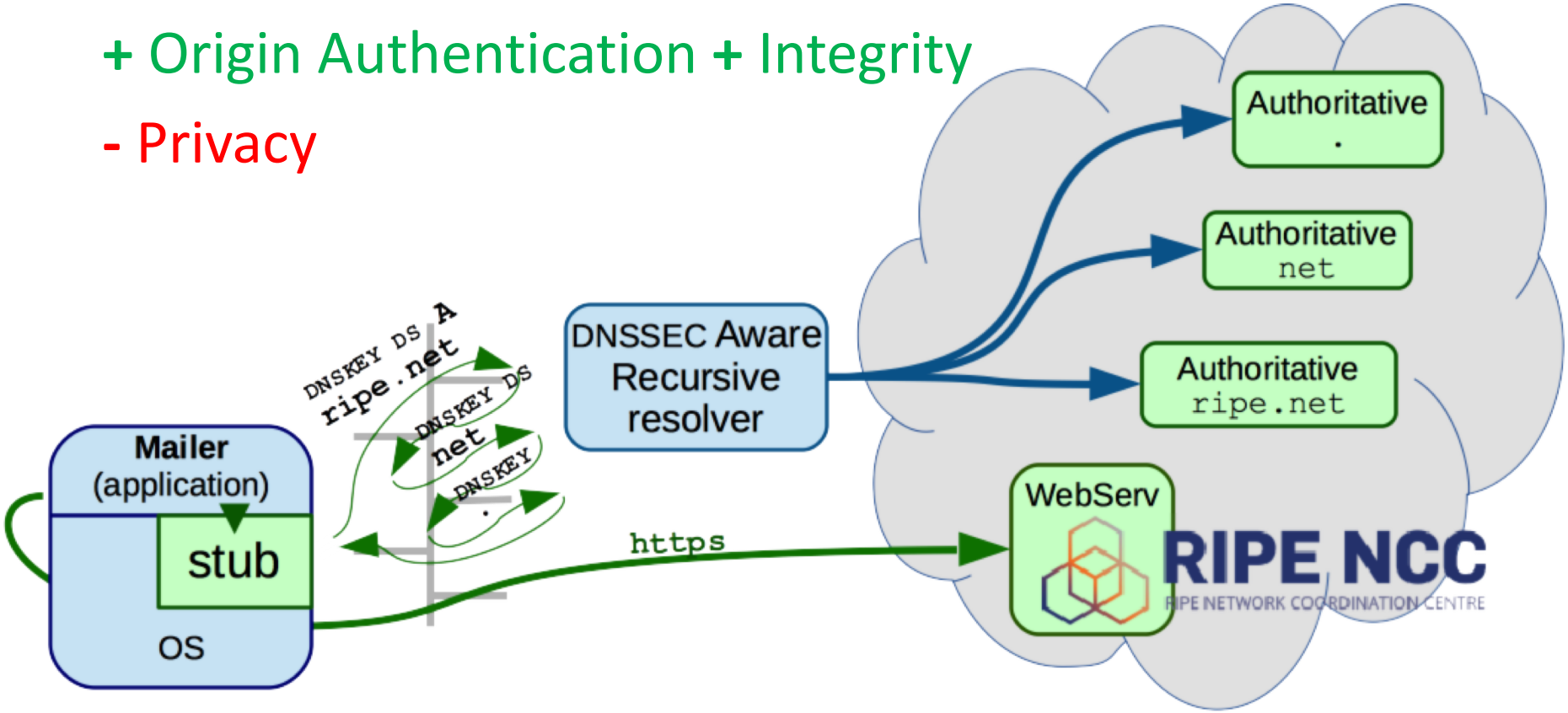


NLNETLABS

DNSSEC – Properties & Limitations (2)

+ Origin Authentication + Integrity

- Privacy



+ **Transitivity**

- Still first mile issues

https://www.nlnetlabs.nl/

NLNETLABS

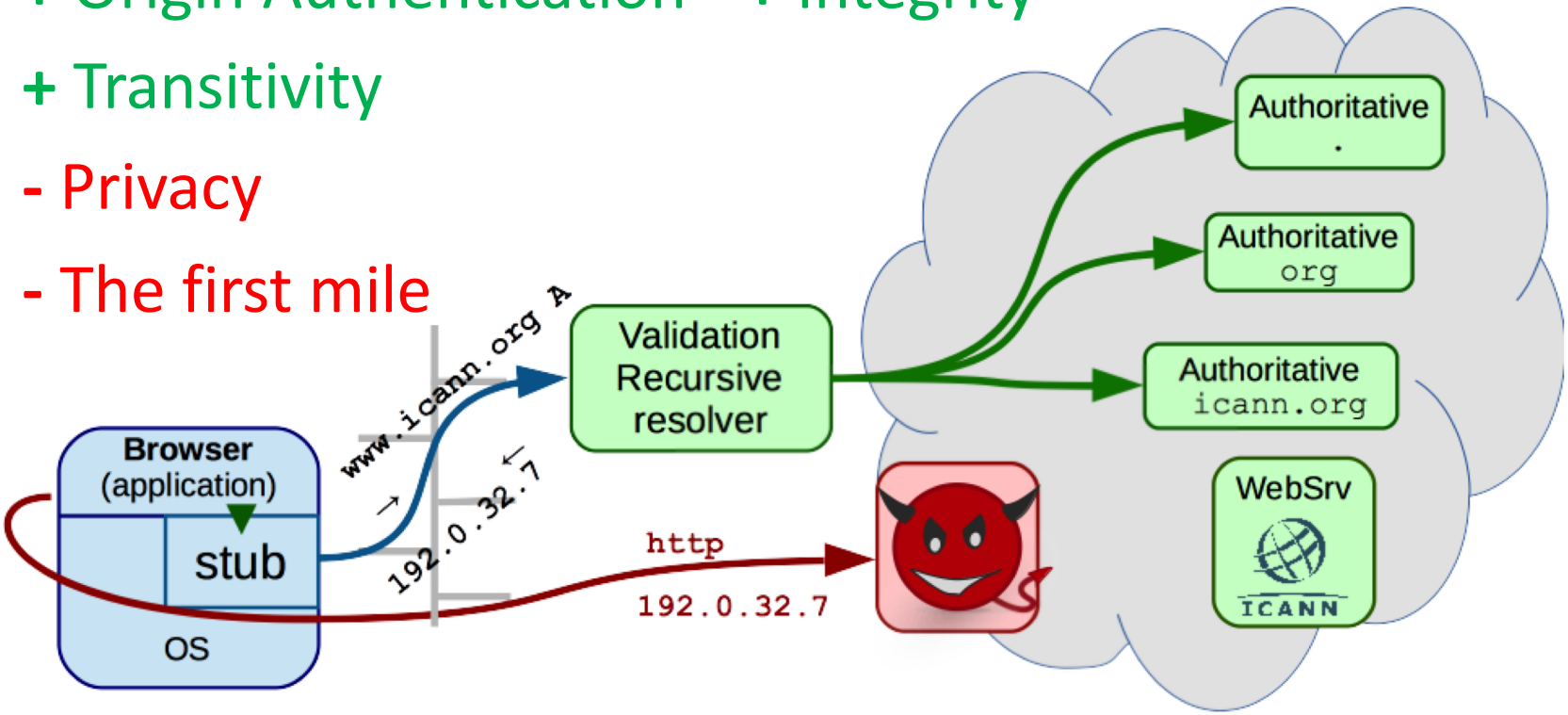
DNSSEC – Properties & Limitations (3)

+ Origin Authentication + Integrity

+ Transitivity

- Privacy

- The first mile



- Does not protect against address hijacking

NLNETLABS

TLS

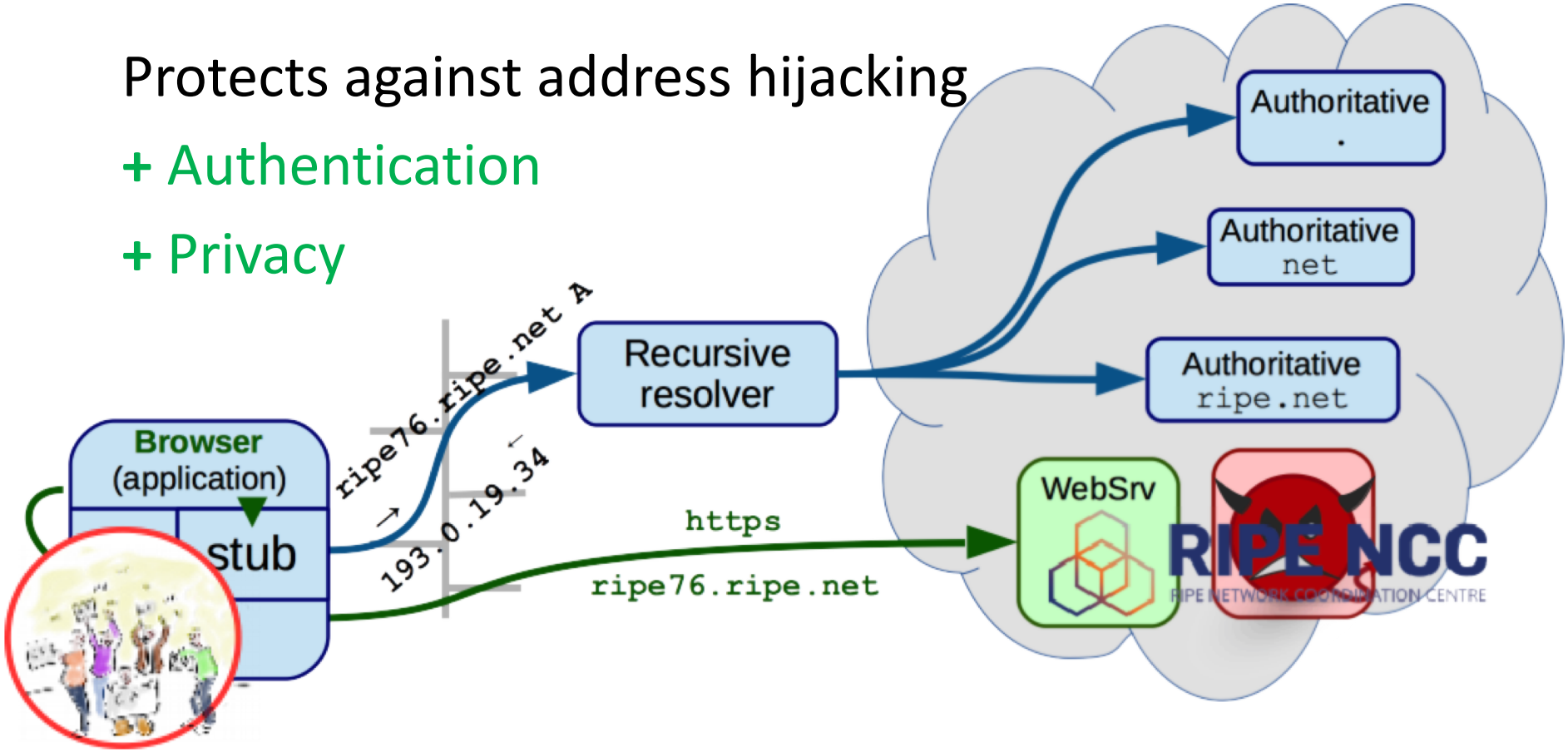
Properties and limitations

TLS – Properties & Limitations

Protects against address hijacking

+ Authentication

+ Privacy



DNSSEC not needed anymore

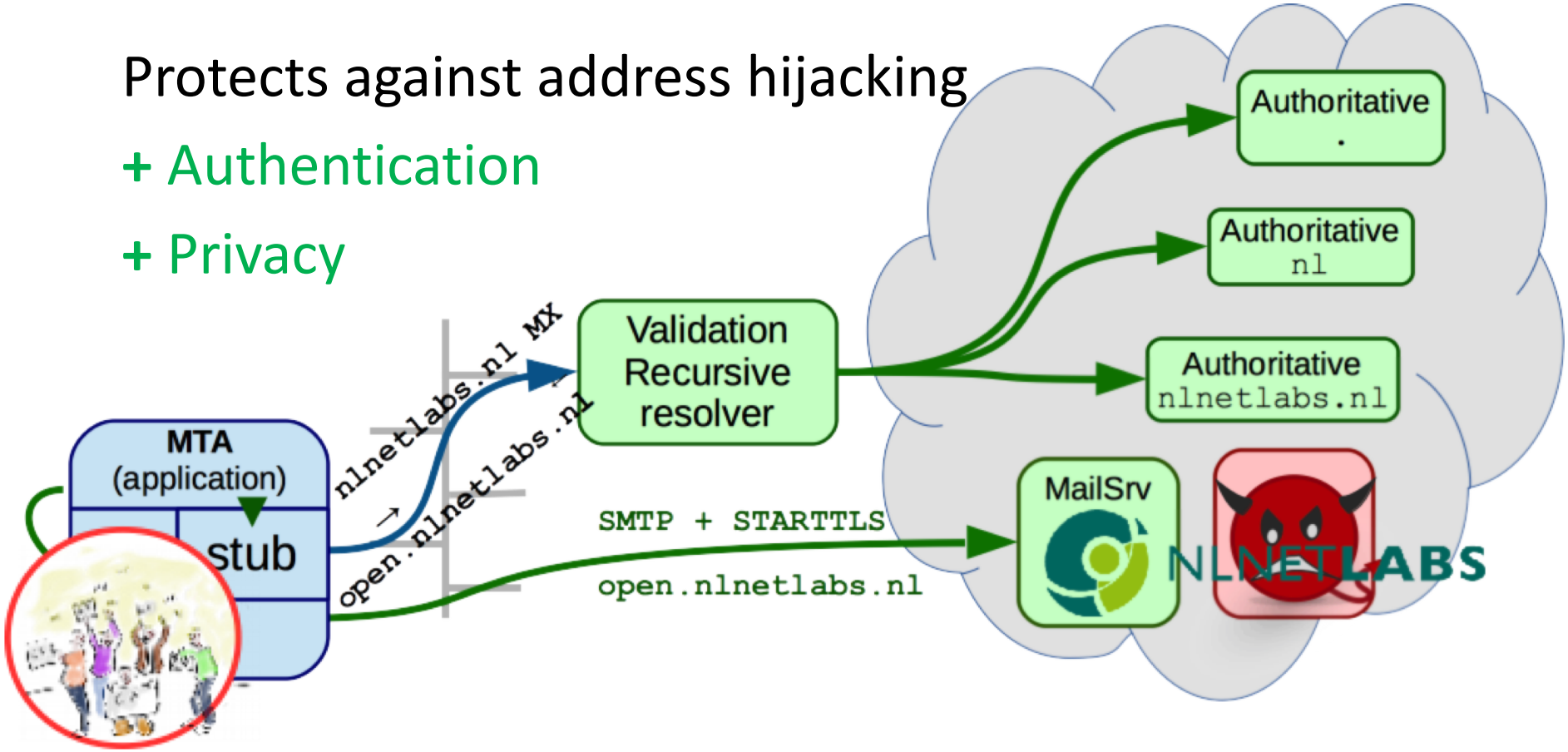
NLNETLABS

TLS – Properties & Limitations (2)

Protects against address hijacking

+ Authentication

+ Privacy



Except for name redirections

- MX, CNAME, DNAME, SRV, NAPTR, …

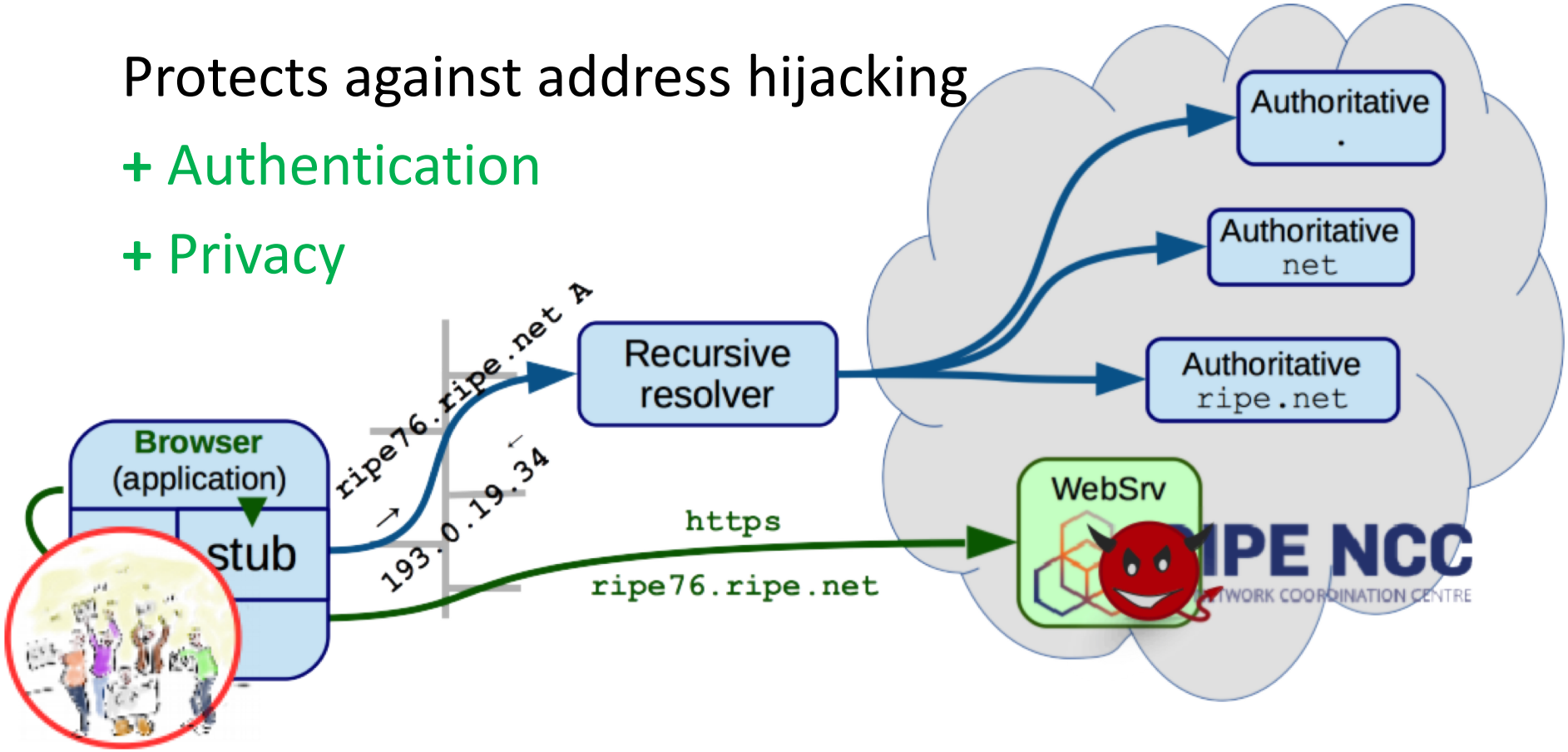
NLNETLABS

TLS – Properties & Limitations (3)

Protects against address hijacking

+ Authentication

+ Privacy



- Integrity when service provider ≠ content provider

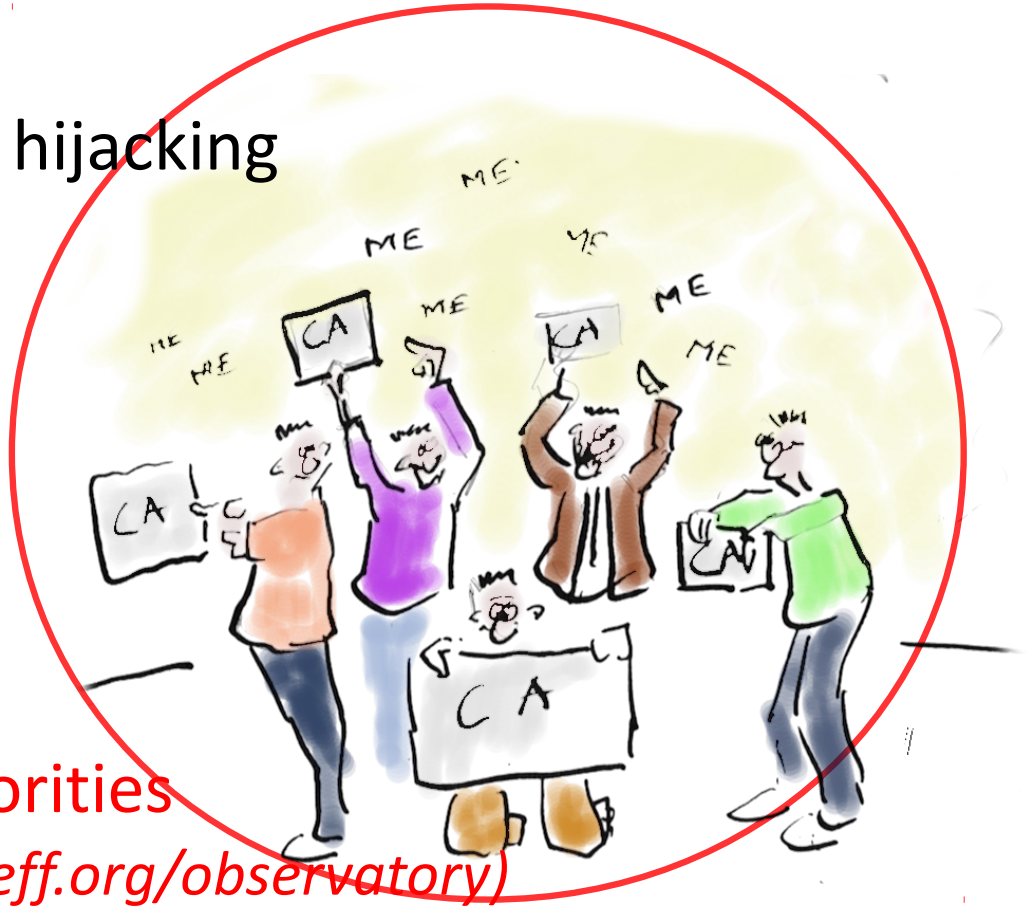
NLNETLABS

TLS – Properties & Limitations (4)

Protects against address hijacking

+ Authentication

+ Privacy



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

- Integrity when service provider ≠ content provider

NLNETLABS

DNS-over-TLS

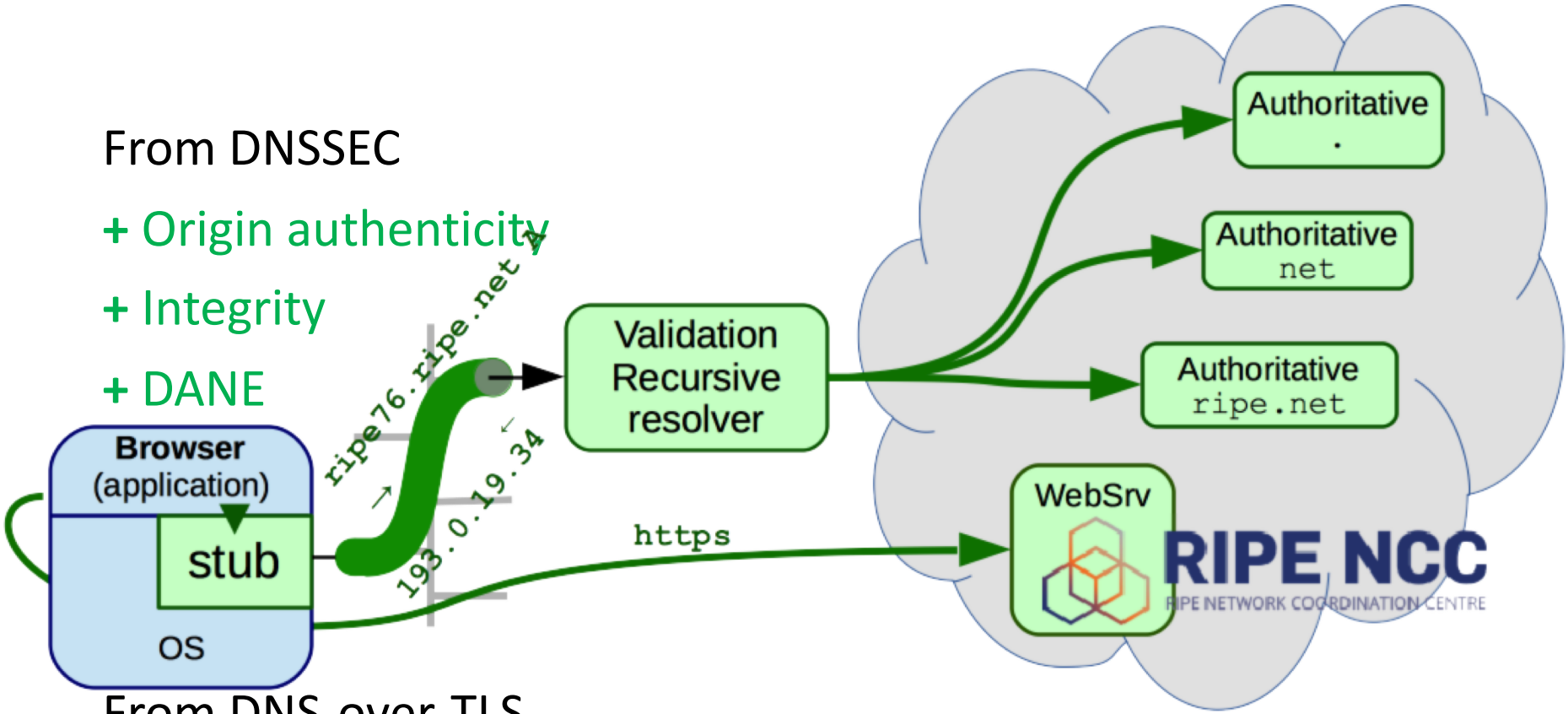
History and motivation

Encryption Everywhere

DNS-over-TLS and DNSSEC

From DNSSEC

+ Origin authenticity
+ Integrity
+ DANE



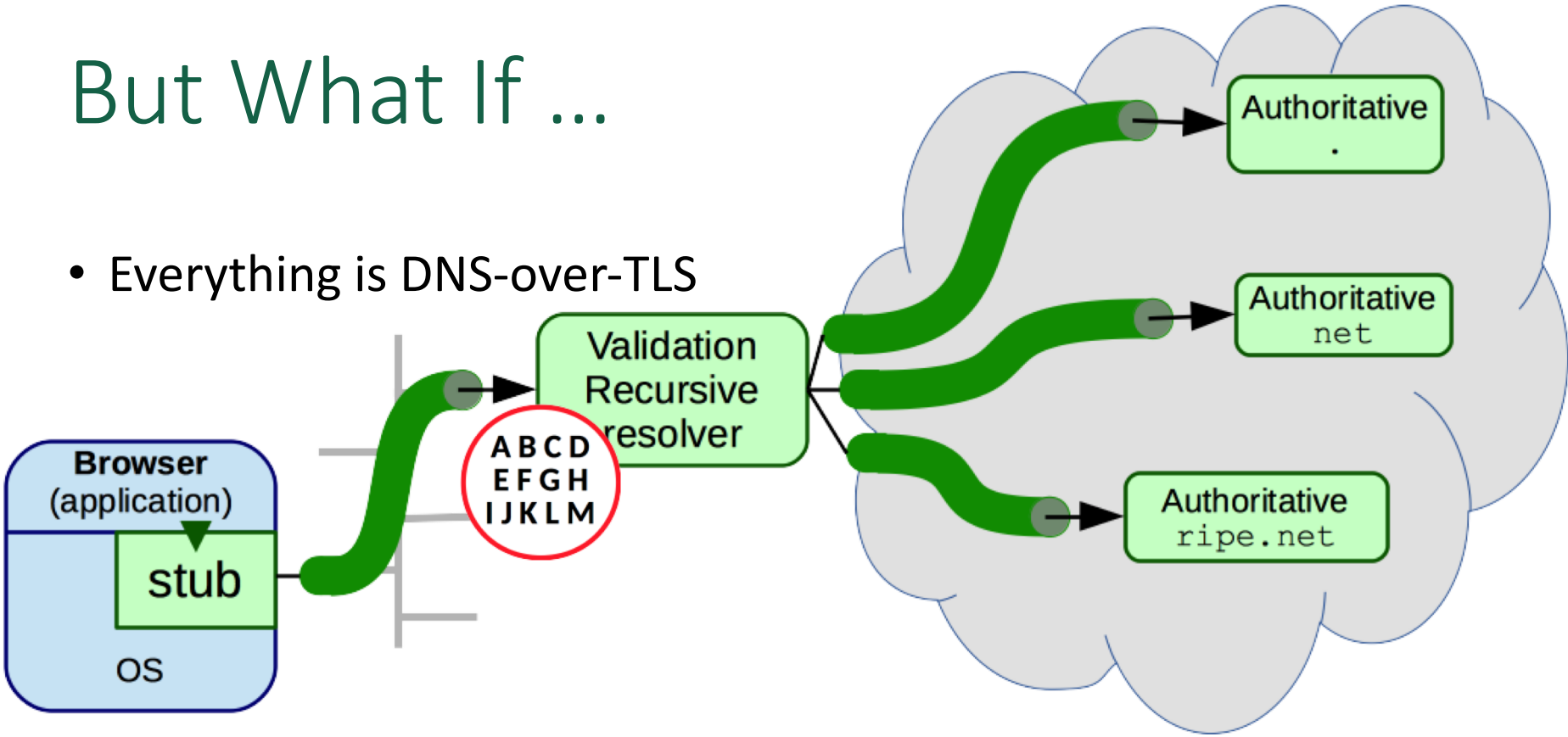
From DNS-over-TLS

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

NLNETLABS

But What If …

- Everything is DNS-over-TLS



- Start with CA store with CAs of the 13 root operators
  - Or the ICANN Root CA/ICANN SSL CA?
- Learn CA of child zone operator when following delegations

Who needs reasons 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 heroes!

- Trust DNS operators chosen to serve the zone
- Trust CAs to authenticate stub → resolver path