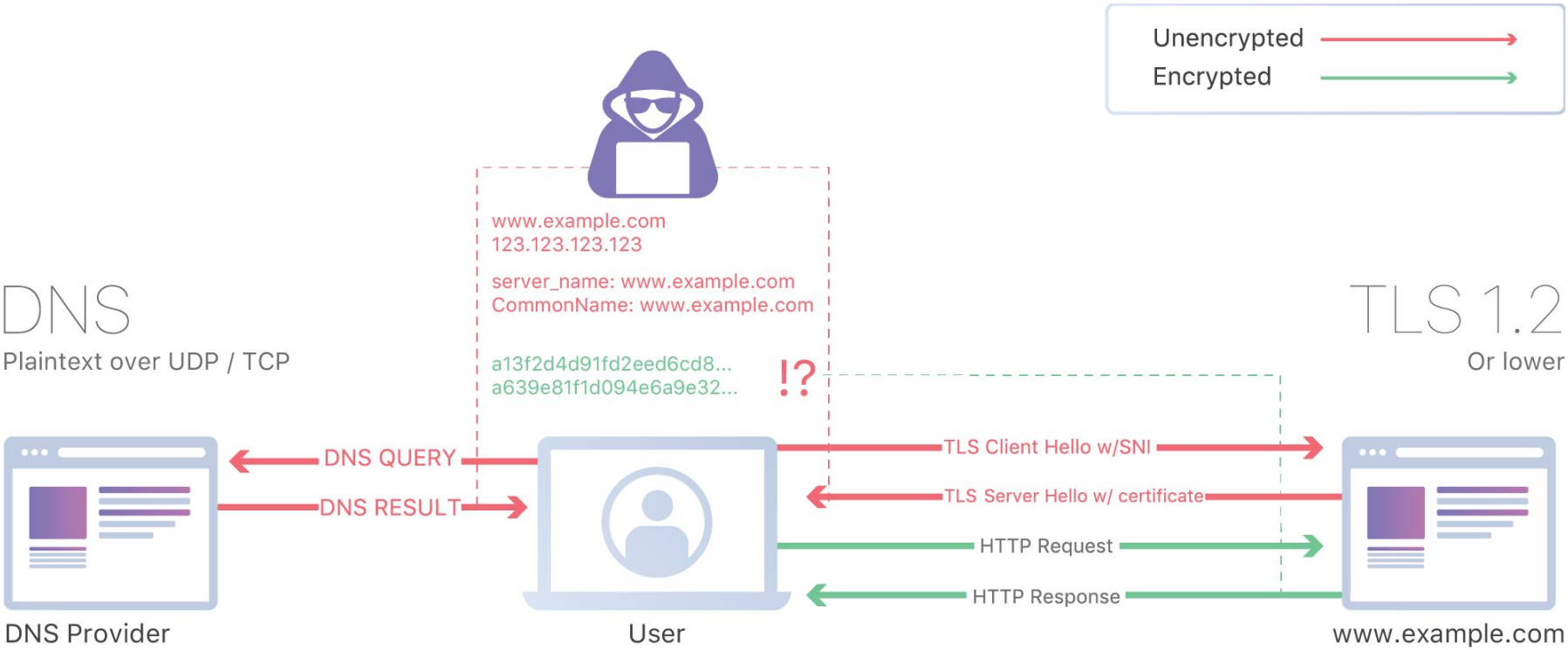
IETF 104 TLSWG

Encrypted SNI

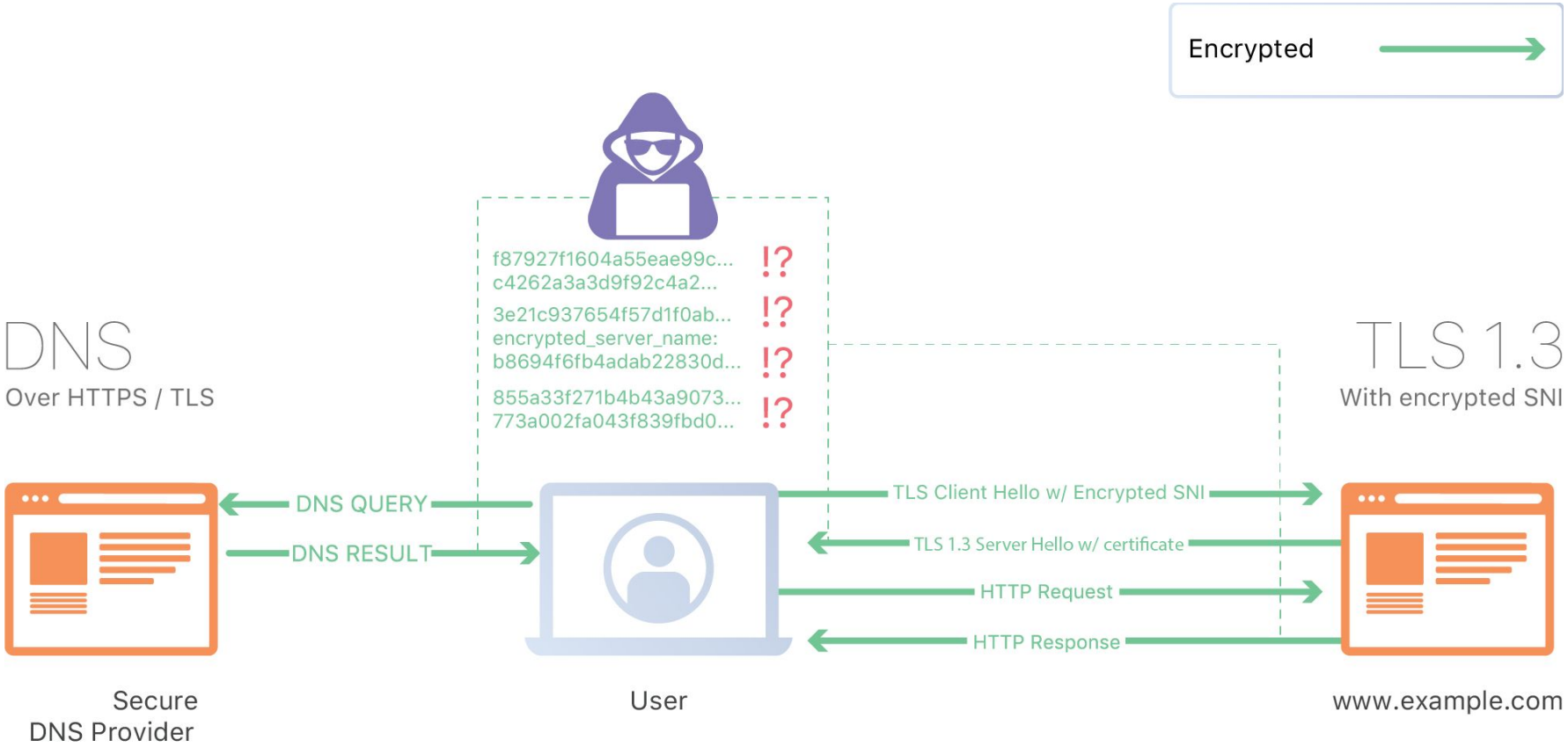
E. Rescorla, K. Oku, N. Sullivan, C. Wood

draft-ietf-tls-esni-03

Overview


Unencrypted
Encrypted
www.example.com
123.123.123.123
server_name: www.example.com
CommonName: www.example.com
a13f2d4d91fd2eed6cd8...
a639e81f1d094e6a9e32...
!?
DNS
Plaintext over UDP / TCP
TLS 1.2
Or lower
DNS QUERY
DNS RESULT
TLS Client Hello w/SNI
TLS Server Hello w/ certificate
HTTP Request
HTTP Response
DNS Provider
User
www.example.com

Overview


Encrypted
f87927f1604a55eae99c...
c4262a3a3d9f92c4a2...
3e21c937654f57d1f0ab...
encrypted_server_name:
b8694f6fb4adab22830d...
855a33f271b4b43a9073...
773a002fa043f839fbd0...
!?
!?
!?
!?
DNS
Over HTTPS / TLS
TLS 1.3
With encrypted SNI
DNS QUERY
DNS RESULT
TLS Client Hello w/ Encrypted SNI
TLS 1.3 Server Hello w/ certificate
HTTP Request
HTTP Response
Secure
DNS Provider
User
www.example.com

Summary of changes in -03

Improve robustness #124

Prohibit cached_info #127

Clarify HRR behavior #128

Multi-CDN “combined records” mandatory extension #136

Use new RRType and remove_esni prefix #144

Pending Changes

Mostly ready to merge:

- GREASE ESNI #125
- Swap version and checksum fields #129

Still WIP:

- Multi-CDN “host pointers” mandatory extension #137

Multi-CDN Case

Overview

- example.com has DNS load balancing of A/AAAA
  - Returns set of A records corresponding to multiple providers
- www.example.com has DNS load balancing via CNAME
  - Returns CNAME that terminates at www.example.com.cdn1.com or www.example.com.cdn2.com randomly

Multi-CDN Case

Failure case

- A/AAAA record request independent of TXT/ESNI record request
- A/AAAA for CDN1, TXT/ESNI for CDN2

CDN1/2 have different ESNI keys, or only CDN1 supports ESNI

Result: Failed connection with no fallback or unnecessary privacy leak

Simple Multi-CDN Solution (PR#136)

- ESNIKeys record can carry an **AddressSet** extension
  - Extensions with the high bit of the type are “mandatory”, i.e., ignore ESNI records with unknown extensions that have this bit set
- This lists addresses that are valid for the requested domain name
- If AddressSet is present, client uses one of those addresses
  - … and ignores A/AAAA records

Tradeoff

Pro

- Rate of A/AAAA and ESNI mismatch is irrelevant

Con

- Requires tight coupling between address assignment and publication and ESNI publication

Generalized Multi-CDN Proposal (PR#137, Simplified)

Main idea: use **AddressPtrs** to determine A/AAAA response validity

- If the AddressPtr net mask filter matches an A/AAAA response, use the address.
- If the AddressPtr canonical name matches the A/AAAA CNAME, use the address.
- Else, resolve the AddressPtr canonical name and use those addresses.

Moving Forward

Are we OK to move forward with the current solution in the draft and continue working on PR#137 as a separate extension draft?

Open Issues and Questions

Adopt Hybrid Public Key Encryption (HPKE), and other KEMs #145

Use ESNI for local discovery, and removing record_digest #138

Remove split mode from the draft #130

Encrypt more than the SNI #40

Per-client ESNI key tracking #146

Reduce padding #134 (related: compress SNI in CH #116)

Third-party SNI sharing #123

Questions?

IETF 104 TLSWG

Encrypted SNI

E. Rescorla, K. Oku, N. Sullivan, C. Wood

draft-ietf-tls-esni-03