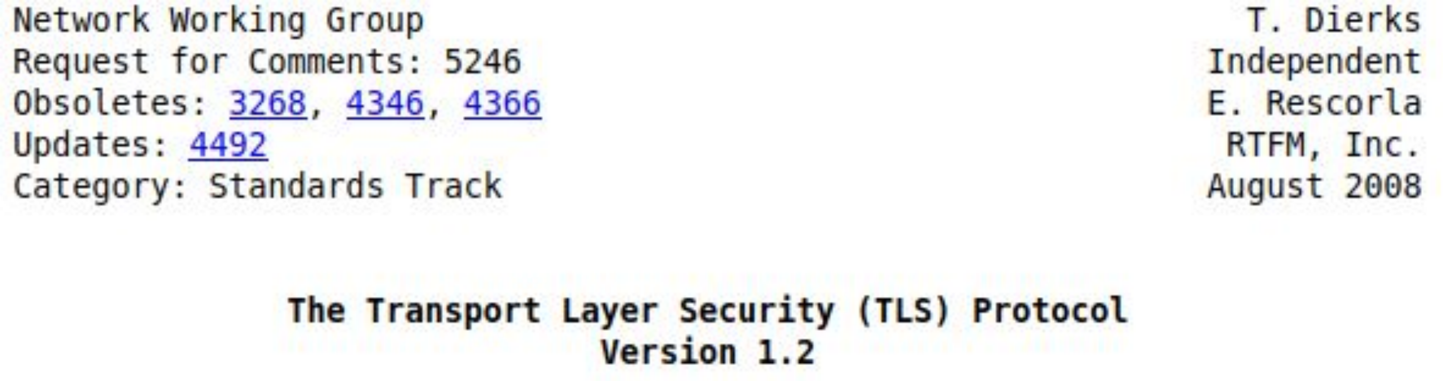
TLSNotary

MPC + ZK to prove web2 data

ethereum
foundation

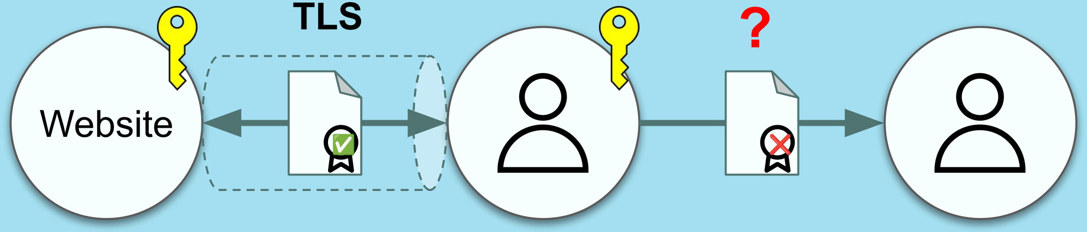
PRIVACY + SCALING EXPLORATIONS

https://



```
Network Working Group                                          T. Dierks
Request for Comments: 5246                                   Independent
Obsoletes: 3268, 4346, 4366                                  E. Rescorla
Updates: 4492                                                 RTFM, Inc.
Category: Standards Track                                    August 2008
```

The Transport Layer Security (TLS) Protocol
Version 1.2


TLS
Website
?

MPC-TLS

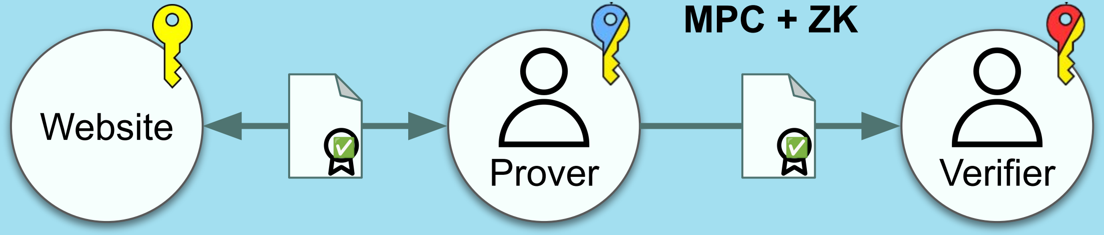
zkTLS

Web
Proof

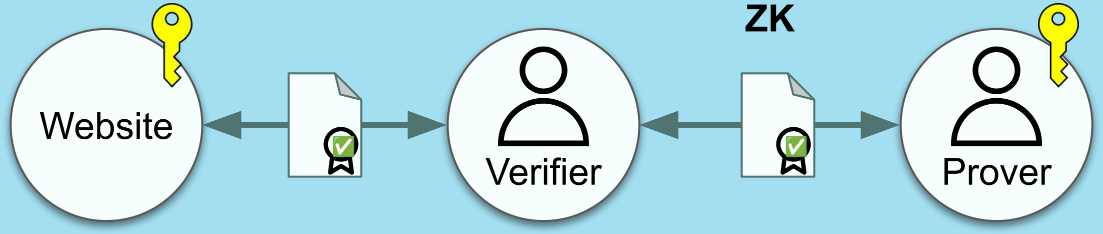
Middlebox

Witness
Proxy

MPC-TLS

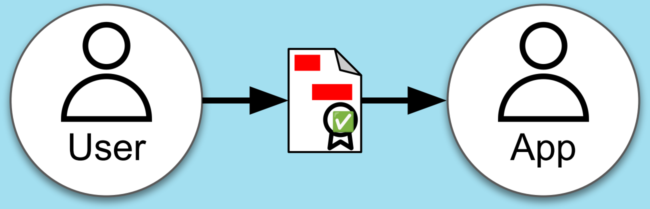


zkTLS (Proxy)



All approaches are **designated-verifier**

Compose with any application.
Trustlessly.
Privately.

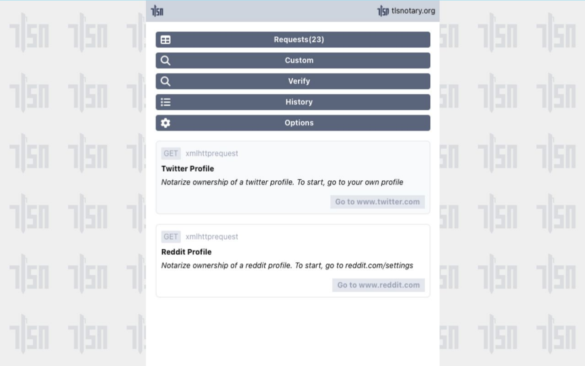


```
--- Request
GET /profile HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
Host: www.example.com
Accept-Language: en-us
Cookie: user_session=[redacted]
Connection: Keep-Alive

--- Response
HTTP/1.1 200 OK
Date: Wed, 14 Jun 2023 16:10:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 03 Jan 2009 19:15:56 GMT
Content-Length: 74
Content-Type: application/json
Connection: Closed

{"username":"sinu","address":"[redacted]","birthday":"[redacted]"}
```

Not in US ✅

18+ ✅

FOSS



GET xmlhttprequest

Twitter Profile

Notarize ownership of a twitter profile. To start, go to your own profile

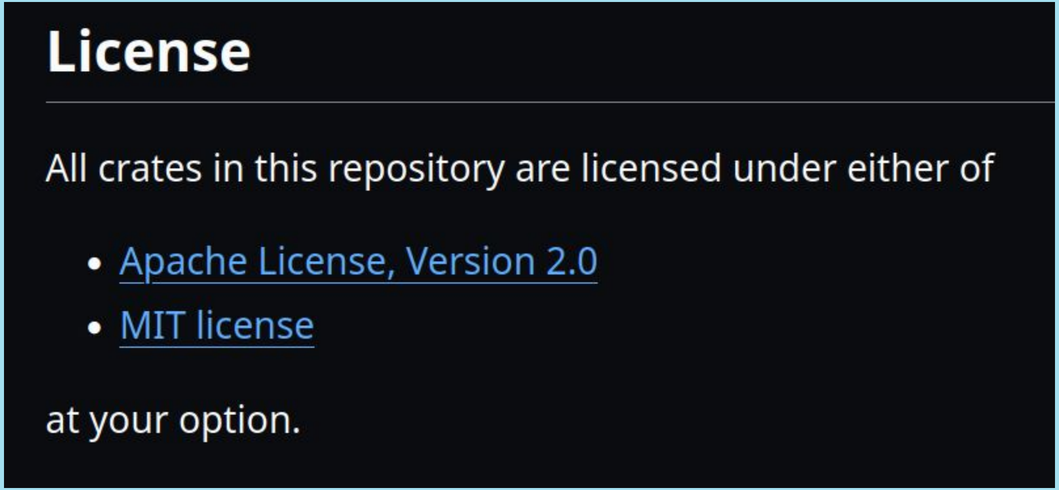
Go to www.twitter.com

GET xmlhttprequest

Reddit Profile

Notarize ownership of a reddit profile. To start, go to reddit.com/settings

Go to www.reddit.com



License

All crates in this repository are licensed under either of

- Apache License, Version 2.0
- MIT license

at your option.

X: @sinu_eth

tlsnotary.org

github.com/tlsnotary/tlsn

Discord Link