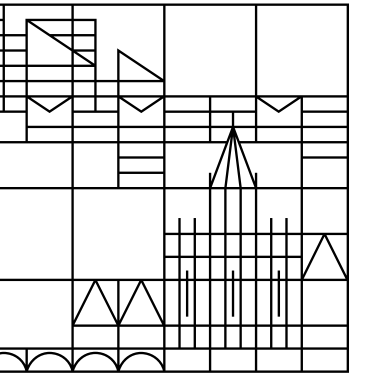


# Boost DNS Privacy, Reliability, and Efficiency with opDNS Safe Query Elimination

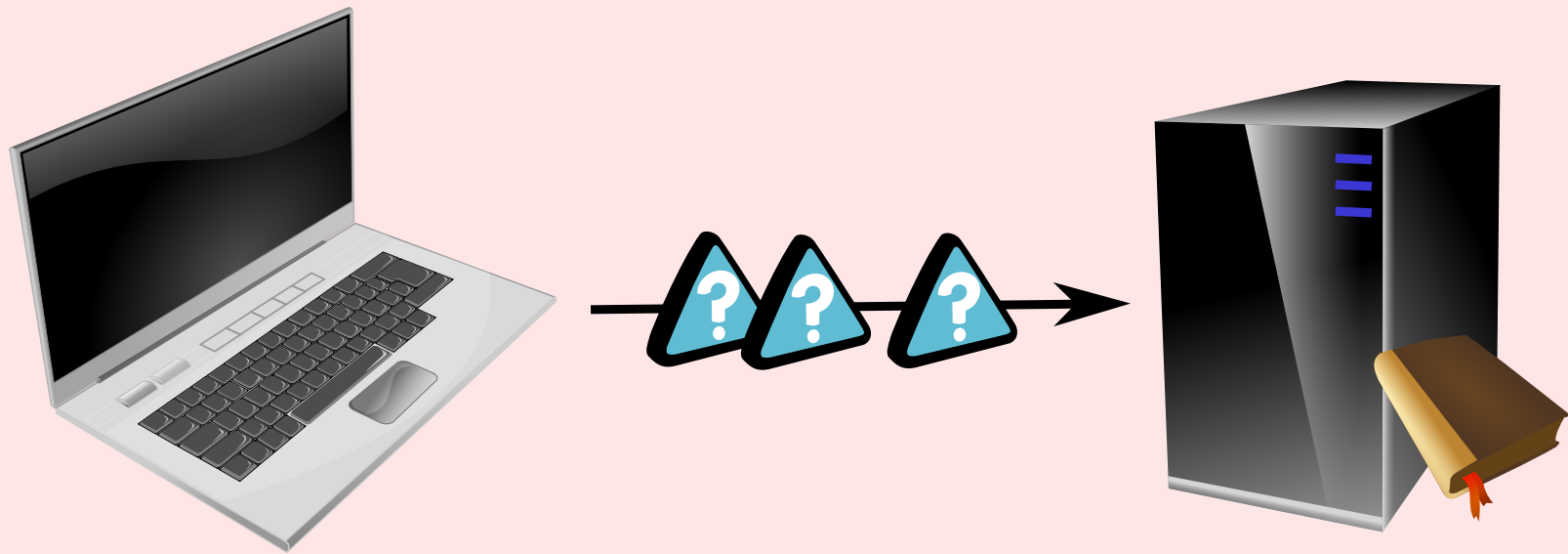


Marcel Waldvogel, Thomas Zink

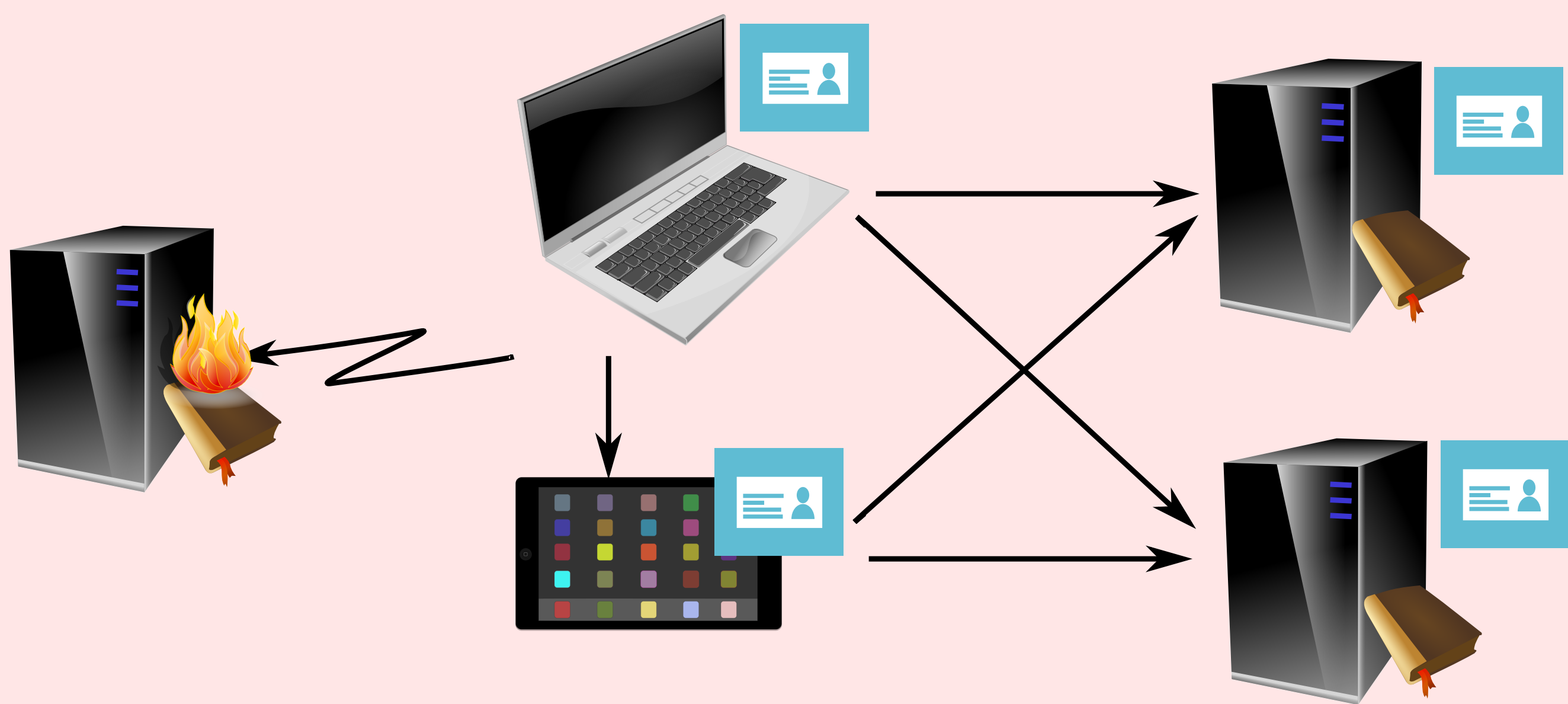
Universität  
Konstanz



## DNS Problems



Before contacting most services the clients send out cleartext DNS queries to DNS servers. The queries are not only revealed to DNS servers but can also easily be observed on the network.

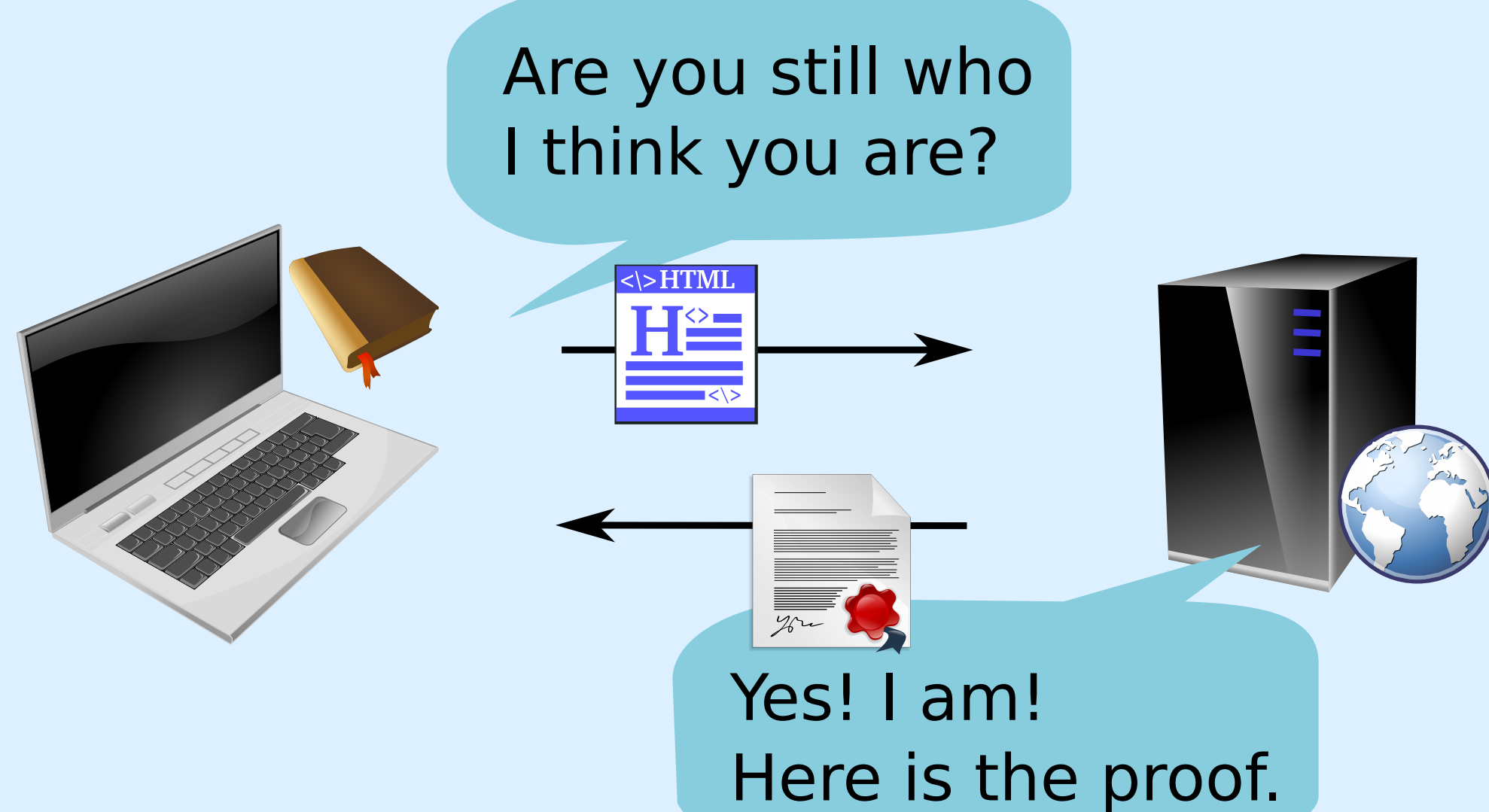


This leads to a number of privacy and reliability problems:

- [privacy] user fingerprinting
- [privacy] user tracking
- [reliability] outages and censorship
- [reliability] DNS malfunctions



## Our Goals



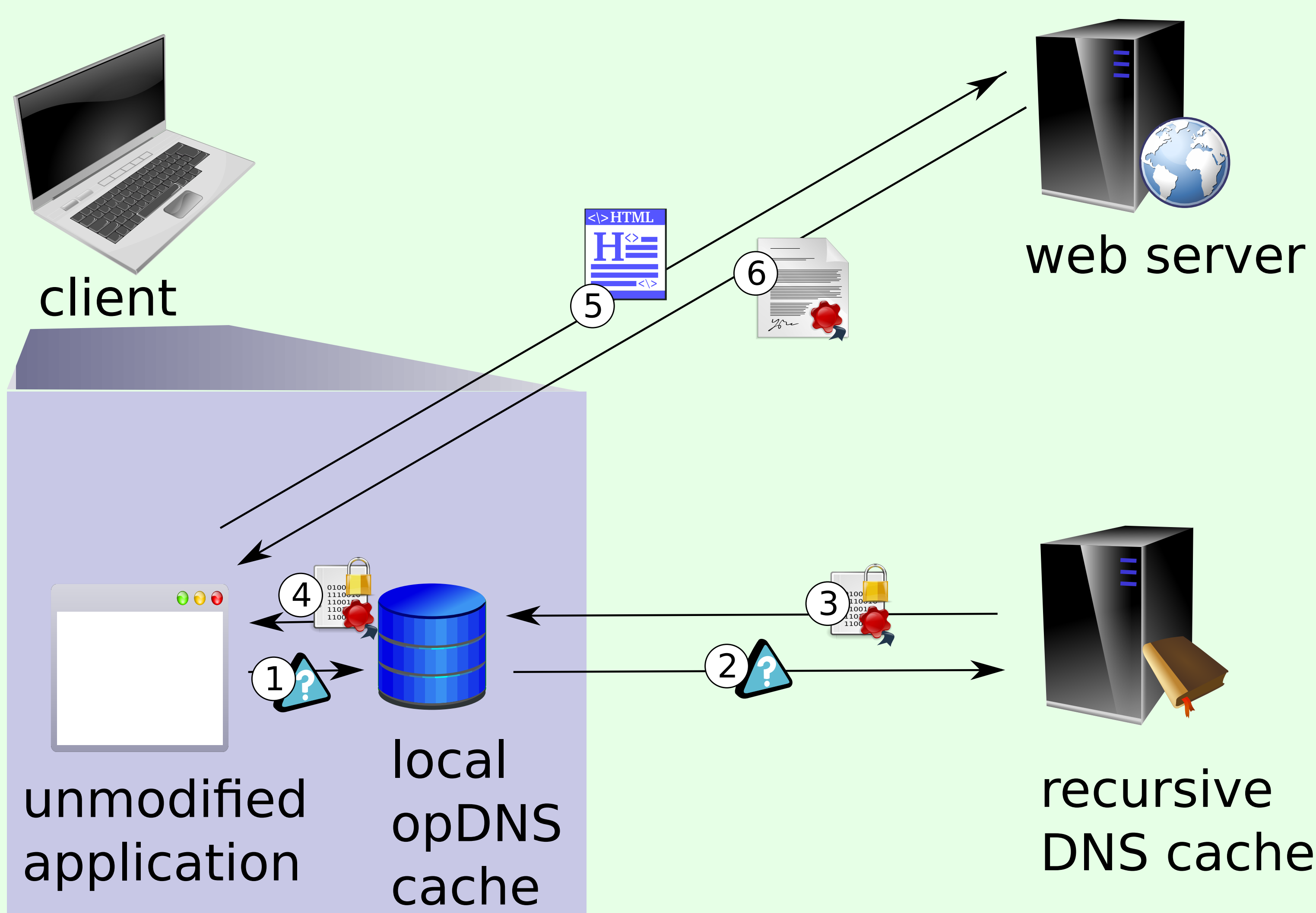
Increase privacy and reliability by

- eliminating unnecessary traffic
- reducing communication to trusted partners

As a side effect, this also boosts efficiency due to reduced network traffic, latency, and computation.



## Our Solution



Opportunistic Persistent DNS (opDNS)

- keeps a local DNS cache
- integrates seamlessly with DANE and DNSSEC to safely retrieve initial records
- caches beyond TTLs for secure services and serves locally cached records
- uses TLS to authenticate services