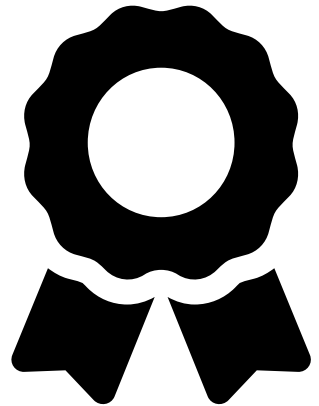


Evaluating CA Predominance Across Regions

Motivation

TLS certificates are essential for the modern web. In recent years, the certificate authority landscape shifted from predominantly commercial entities selling TLS certificates to a consolidation at the non-profit *Let's Encrypt*. This non-profit is US-based and backed by corporate sponsors like Google, Microsoft, AWS and Mozilla. Due to recent geopolitical challenges, focus on reducing foreign critical dependencies is heightening as sanctions and conflicts disrupt trust.

This project intends to analyse how the TLS certificate authority ecosystem is regionally diverse and how these differences change over time. Furthermore, we aim at discovering new insights on what could influence the choice of certificate authority and how these trends are changing. Our team conducts large-scale Internet scans that generate large amounts of data. This includes TLS certificates used by a majority of popular sites which will serve as a basis for this research. Other data sources like CTlogs may be utilized as well.



Your Task

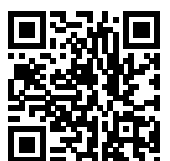
- Familiarize yourself with the web PKI ecosystem
- Familiarize yourself with our TLS scan dataset
- Get comfortable working with ClickHouse for the analyses
- Identify additional data sources needed for the analysis
- Analyse the dataset related to the defined research questions

References

- Rumaisa Habib, Kimberly Ruth, Gautam Akiwate, and Zakir Durumeric. 2025. Formalizing Dependence of Web Infrastructure. In ACM SIGCOMM '25
- <https://news.ycombinator.com/item?id=48453275>
- <https://www.asriran.com/fa/news/1180886>
- <https://nooshdaroo.ir/safe-ecommerce-selling/lets-encrypt-us-sanctions/>

Contact

Tim Betzer betzer@net.cit.tum.de
Christian Dietze diec@net.cit.tum.de
Sebastian Kappes sebastian.kappes@mpi-inf.mpg.de
<https://net.in.tum.de/members/diec/>



Applications will be collected until at least 2026-09-30

