Beyond X.509: Evaluating Merkle Tree Certificates against Certificate Transparency

Advisor: **Edona Fasllija**

Motivation

The current PKI ecosystem relies on X.509 certificates with Certificate Transparency (CT) logs to detect CA misissuance. While CT adds auditability, X.509 remains large and complex, and proof sizes grow further with post-quantum signatures. A newer proposal, Merkle Tree Certificates (MTCs), integrates certificates directly into Merkle structures, potentially reducing handshake size, simplifying verification, and offering more efficient transparency. This study aims at comparing the two approaches to evaluate how they can replace or complement the existing model.

Steps

- Study X.509 + CT (RFC 5280, RFC 6962) and the MTC draft; describe how each issues, logs, and verifies certificates.
- Define metrics and compare security, efficiency (size, proof overhead), and deployability (TLS handshake compatibility)

Literature

- D. Benjamin et al.
  Merkle Tree Certificates
  Tech. rep.
  https://datatracker.ietf.org/doc/draft-davidben-tls-merkle-tree-certs/

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

Note: You can select these topics *only* for the ISW course. If you are considering to combine ISW with a bachelor's thesis at ISEC (highly recommended), check the full list of topics:

https://www.isec.tugraz.at/bachelor-thesis

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **WebPKI security**

Advisor Contact

edona.fasllija@tugraz.at