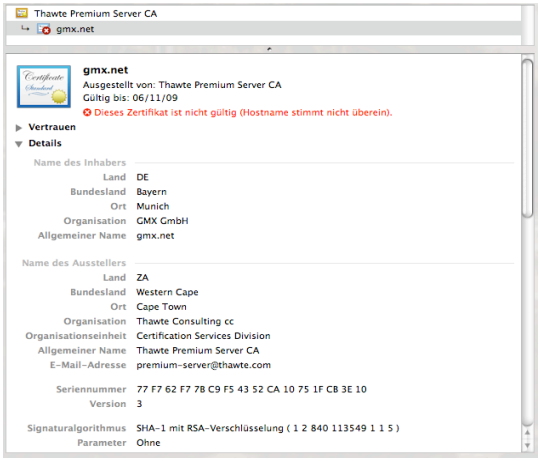
Authentizität im Internet-

Quantencomputersichere Chats

TECHNISCHE UNIVERSITÄT DARMSTADT

Zertifikate

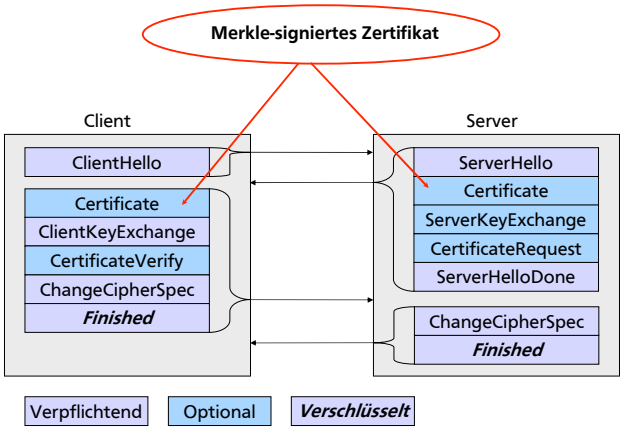
Zertifikate sind eine Art digitaler Personalausweis, mit denen man seine Identität beweisen, sowie Daten signieren kann (z.B. mit dem Merkle-Verfahren). Sie werden von einer sicheren Instanz ausgestellt, und von dieser auch signiert.



TLS Protokoll

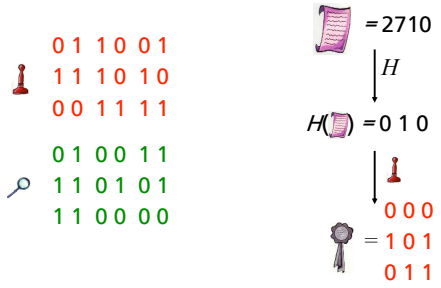
Das Transport Layer Security Protokoll (TLS) wird benutzt um sichere Verbindungen über das Internet aufzubauen.
Es beinhaltet sowohl eine zertifikatsbasierte Authentifizierung, sowie eine Verschlüsselung der Verbindung.

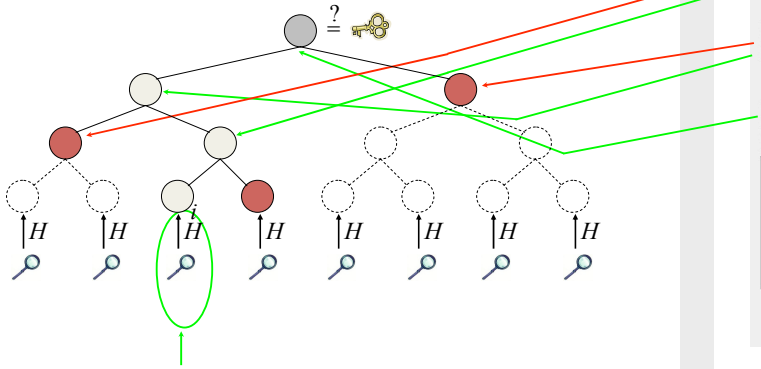
Handshake



Merkle Signaturverfahren

Einmalsignatur



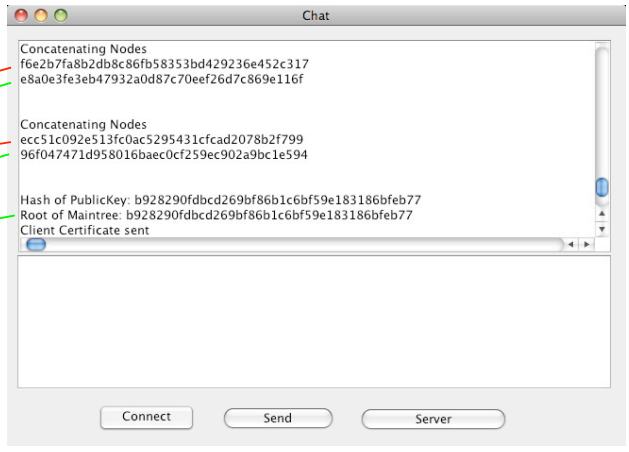


Sichere Authentifizierung bei IM-Chats

Zertifikate bei der Authentifizierung von IM-Chats

Durch das Austauschen von Zertifikaten kann man beim Chatten sicherstellen, dass man es auch wirklich mit der richtigen Person zu tun hat.

Die Nachrichten an sich werden dadurch alleine aber noch nicht für andere unlesbar! Dafür braucht man eine Verschlüsselung!



Prof. Johannes Buchmann, Erik Tews, Erik Dahmen, Elias Most
Fachbereich Informatik, TU Darmstadt
MerkleTLS