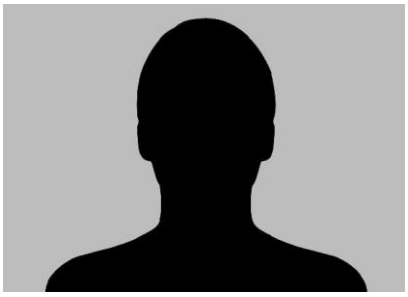
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

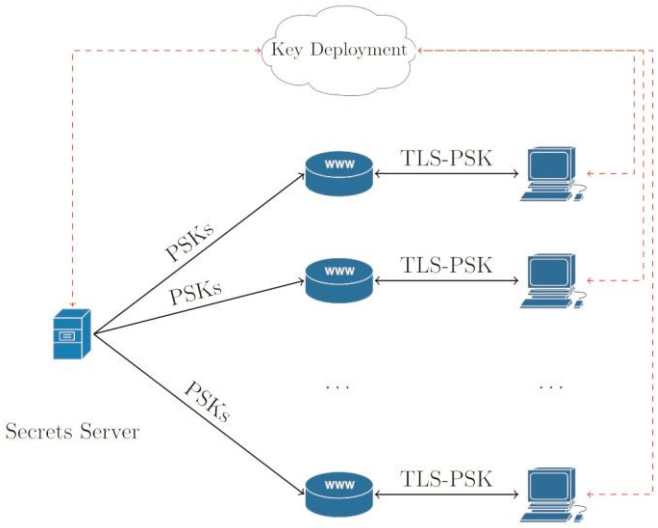
Proof-of-Concept-Implementierung von TLS-PSK

Transport Layer Security (TLS) ist das am weitesten verbreitete Protokoll für sichere und zuverlässige Netzwerkkommunikation. In dieser Arbeit implementiere ich die Preshared Key (PSK)-Erweiterung für das TLS-Protokoll. Sie stellt eine ressourcenschonende Art und Weise dar, TLS-Verbindungen zwischen zwei Parteien, welche im Vorhinein einen gemeinsamen Schlüssel ausgetauscht haben, herzustellen und hat den Vorteil, dass keine Public-Key-Infrastruktur unterhalten werden muss. Des Weiteren schlage ich Methoden vor, um die PSKs in einem TLS-PSK basierenden System zu verwalten und wie TLS-PSK verwendet werden könnte.



Diplomand
Philippe Hürlimann

Dozent
Stephan Neuhaus



Beispielillustration eines Systems, welches TLS-PSK verwenden könnte.