Definition of Bachelor Thesis Project

Client-Managed Anonymous Authentication and Authorization for MQTT

ID	KNR1-2-19
Students	
Students	Lukas Läderach Cédric Natanael von Allmen
Advisor	Dr. Reto Koenig
Experts	Dr. Federico Flueckiger
Assignment	Since specification 5.0 MQTT provides the ability of custom authentication methods. The primary goal of this thesis is to implement a state-of-the-art approach to provide authenticity in MQTT sessions using the means of zero-knowledge-proofs. The goal is to completely void session hijacking for the MQTT protocol and providing authenticity without the need for any network-security nor channel-security nor broker-based predefined ACLs. The approach has to extend an existing broker with the ability for anonymous, authentic sessions, without the need of any a priori knowledge at the broker side. As the solution is targeted for applications within the world of IoT, the approach has to embrace client-parties with low energy and data budgets. The solution should be completely agnostic to the application layer at the client side. Furthermore, means for client-managed authorization of authenticated parties shall be introduced and studied.