Anonymous Post-office Protocol (AnonPoP) is a messaging protocol ensuring strong anonymity to senders and recipients, even against powerful adversaries. AnonPoP is practical, scalable and efficient, with reasonable overhead in latency and communication. Furthermore, it is appropriate even for use in mobile devices, with modest, reasonable energy consumption (validated experimentally), and with good security even against MitM adversaries and even for disconnection-intersection attacks.

To provide anonymity and unobservability even against MitM attackers, AnonPoP uses Post-Office Servers, which keep anonymous mailboxes, and Mixes, between the Post-office and senders/ recipients. The Post-Office is aware of the total amount of traffic in the system, but not of traffic patterns of individual senders and recipients. AnonPoP uses efficient cryptographic mechanisms, to ensure anonymity even against a malicious post office, who can also be MitM on all network traffic (and control some mixes).

AnonPop supports many diverse scenarios and applications, with an expressive mailbox authorization policy, including defenses against spam and Denial-of-Service.

Ort: Zentrum Technik und Gesellschaft der TU Berlin, Hardenbergstr. 16-18, 10623 Berlin, Raum HBS 002
Zeit: Donnerstag, der 10. Juli 2014, 16:15 Uhr (s.t.)