12. Exercise sheet
Hand in solutions until Tuesday, 14 July 2015, 13:00

Exercise 12.1 (Implement). (0+30 points)

(i) Implement the Furguson electronic cash system. Use an authenticated channel for the withdrawal. Make sure that the different parties are logically separated.

Be ready for a demonstration in the tutorial.

(ii) Does this prevent framing Alice? Can the bank prove a double spending, ie. including the fact that it cannot have framed Alice? Prove.