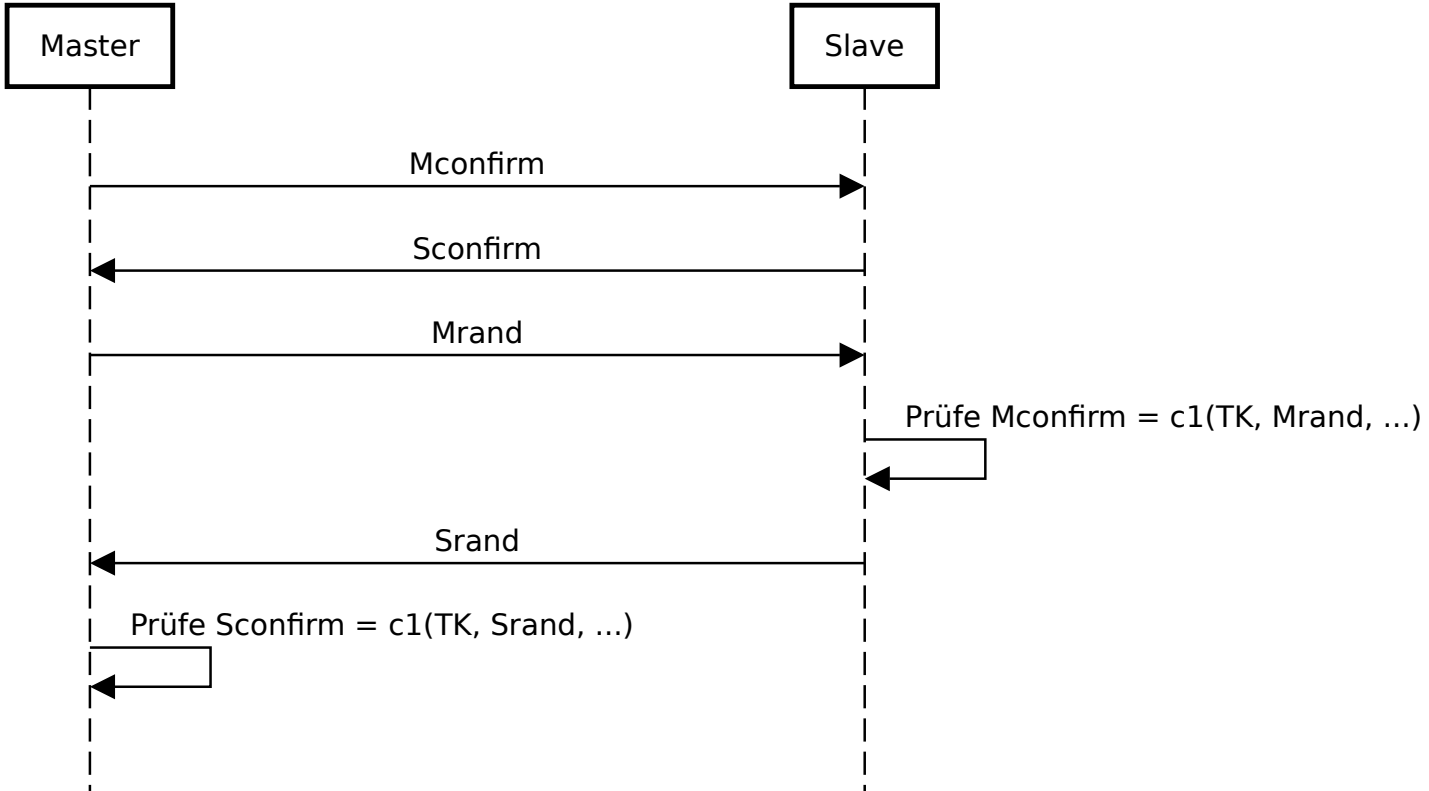
Master
Slave
Mconfirm
Sconfirm
Mrand
Prüfe Mconfirm = c1(TK, Mrand, ...)
Srand
Prüfe Sconfirm = c1(TK, Srand, ...)