Methodische Grundlagen des Software Engineering - Übung 13

13 UMLsec und Fragen

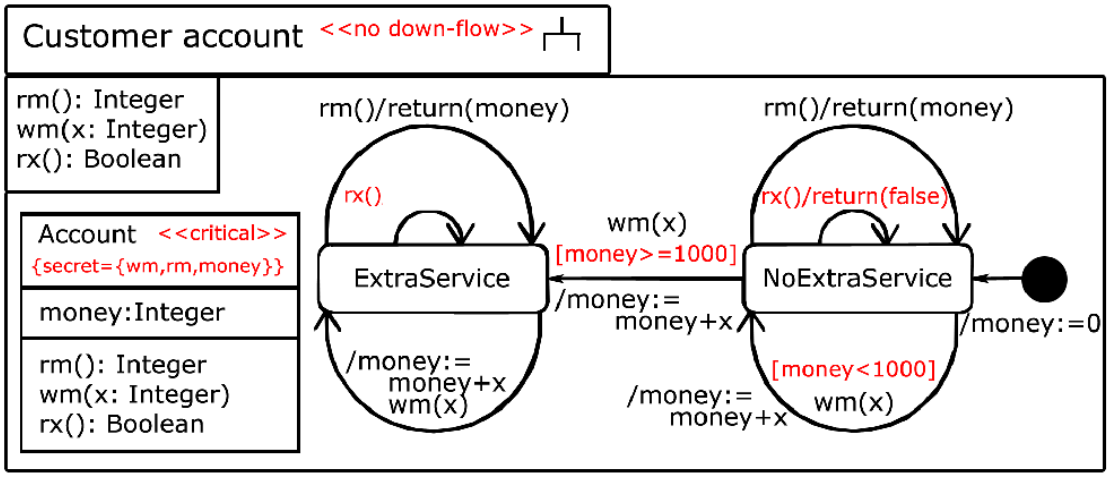
Abgabe der Hausaufgaben am Anfang der jeweiligen Präsenzübung am 12.07.2011 bzw. 13.07.2011.

Keine Präsenzaufgaben für die letzte Übung. Statt dessen können bis Sonntag den 10.07.2011 Fragen per Mail an Stephan.Fassbender@cs.tu-dortmund.de gestellt werden. Diese werden dann in der Übung behandelt.

Hausaufgabe

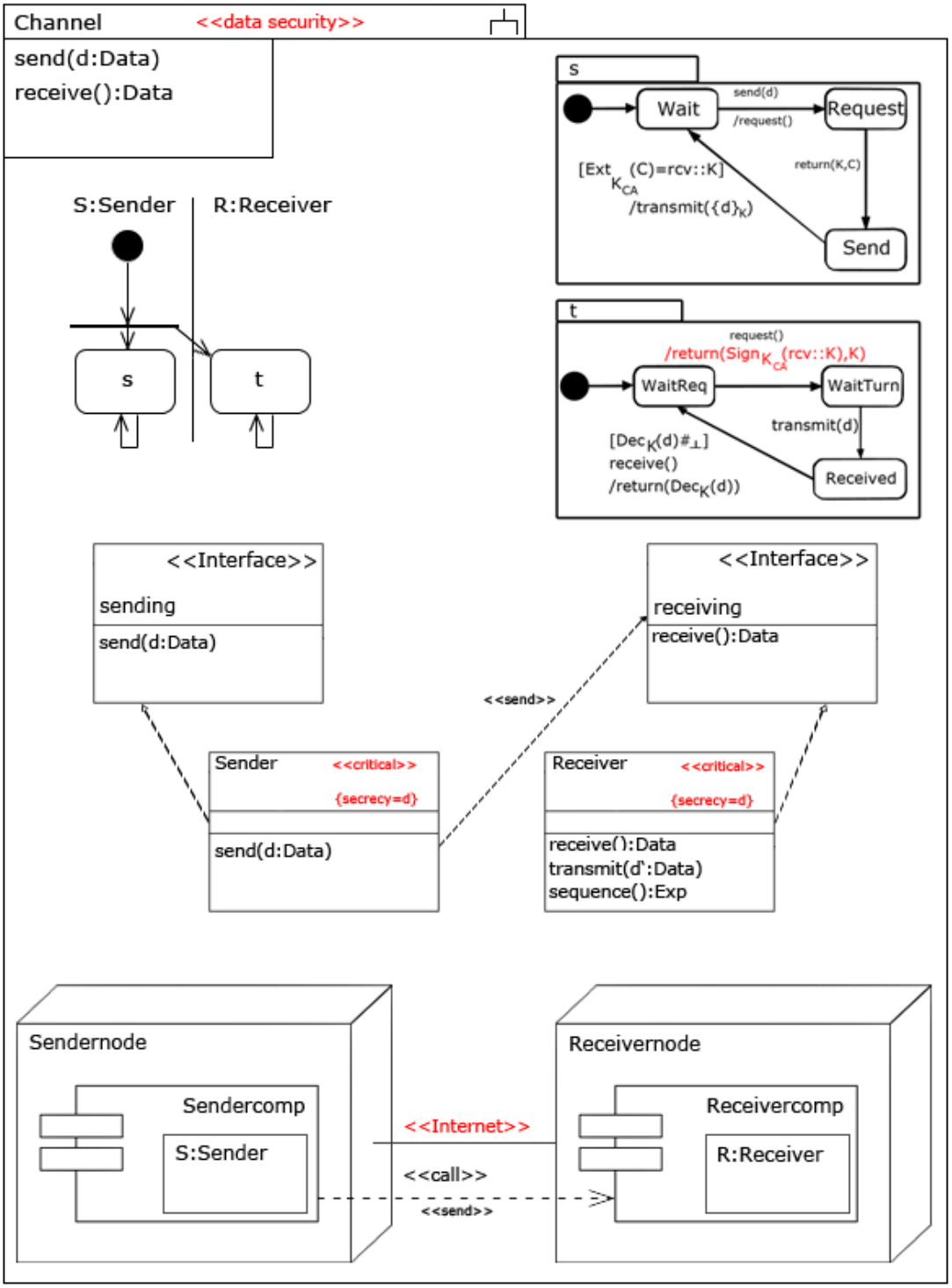
13.1 no down - flow

13.1.1 Im Zustand ExtraService wird auf rx() kein Rückgabewert zurückgegeben. Ist <<no down-flow>> nun erfüllt (mit Begründung)?



1 P

13.2 Protokollanalyse



13.2.1 Zeichne den regulaeren Protokollablauf (d.h. ohne Angriff) des Protokolls

1 P

13.2.2 Angenommen, der Angreifer kommt in Besitz des zum Schluessel $\{K\}_{CA}$ gehörenden vertraulichen Signaturschlüssels der Certification Authority. Wie kann er damit in Besitz des zu übertragenden Geheimnisses d kommen? Zeichne den Angriffsablauf.

3 P