Distributed Systems Programming (F21DS1)
Formal Modelling & Verification Assignment

Andrew Ireland

Electronic Purse

1 Introduction

This coursework focuses on a fictitious electronic purse, i.e. a smartcard that is able to store money electronically for use when making purchases at suitably equipped shops. Operationally an electronic purse, what I will henceforth refer to as simply a purse, can be credited with money at a bank or ATM. Making a purchase requires the purse to be inserted into a device called a reader. The reader simply provides the interface between the purse and the bank. Security and robustness are of key importance when designing such a distributed system.

2 Requirements

You are required to focus on the design of the purse from the perspective of how it is used during a purchase. The process of adding credit to a purse is outwith the scope of the coursework.

The key components of the system are i) customers, ii) purses, iii) readers, iv) the bank. Note that while there is a single bank, there may exist multiple customers, purses and readers. Each component should be modelled as a process. Furthermore, your design model should meet the following requirements:

R1: Initiating a purchase requires that a customer engages their purse with a reader. Once engaged, the customer enters an amount to be debited via a keypad on the reader.

R2: Communications between a purse (via the reader) and the bank take the following protocol. Firstly, the purse sends a request to purchase message to the bank. This initial message contains the purses unique id. Secondly, the bank sends an acknowledgement if the id is recognised. Thirdly, on receiving the acknowledgement, the purse sends a request to have an amount of money debited from the account associated with the purse. Finally, if there are sufficient funds in the account then the bank debits the account and then sends a message to the purse acknowledging that the transaction is complete and the the purse can be disengaged. If there is not sufficient funds, then an error message is sent to the purse.

R3: While the bank records the balance associated with each purse, a purse also maintains a copy of its own balance. This means that a purse can reject transactions that are too expensive without having to communicate with the bank. Likewise, the balance on a purse can be checked without communication with the bank.

R4: In terms of robustness, the system must be able to deal with a purse being disengaged from the reader at any point during a transaction. Specifically, the purse should detect such an event, and as a priority synchronise with the bank when next engaged with a reader, i.e. ensure that the purse and bank agree on the balance.

R5: Your design should allow for multiple transactions at the same time, e.g. two purses engaged in transactions simultaneously.

Warning: if you make use of the atomic operator, be sure and justify why. Note that your design will be evaluated in terms of how accurately you have modelled the requirements above.
2.1 The Verification Task
You are required to verify your system design, specifically you should:

R6: verify that your system design is free from deadlocks.
R7: formulate a system assertion and verify its correctness.
R8: using LTL formulate a safety property (i.e. system assertion) and verify its correctness.
R9: using LTL formulate a response property and verify its correctness.

3 Deliverables
Your submission should include the following:

D1: A statement of any assumptions you have made about the requirements.
D2: A diagrammatic presentation of your model which includes all processes and their interconnec-
tions and local state.
D3: The Promela source for your system design.
D4: For each verification effort you should include the property that was verified together with a
transcript of the associated “Verification Output” window.

This assignment should be submitted via the course work box located outside the student office
(1.24) by 12noon on Friday October 21st, 2011. Note that this is an individual project
which means that your submission MUST be your own work.