Mondex spec: errata and clarifications

Steve King

Version of 19 August 2004
Additions welcome

1 Introduction

Ongoing work on the specification and design of the Mondex electronic purse has been based on the published document [1]. Proof work has revealed a number of typos, confusing points and other small errors. These are listed below in order to help others working on this case study. It should be noted that the published case study differs slightly from the real development:

> As noted above, this case study has been adapted from a larger, real development. In order to produce a case study of a size appropriate for public presentation, much of the real functionality has had to be removed. Some of the structure of the larger specification has remained present in the smaller one, although it might not have been used had the smaller specification been written from scratch. This omitted functionality, whilst important from a business perspective, is peripheral to the central security requirements. [1, p5]

Several of the 'errors' noted below seem to have arisen from this 'sanitisation', and thus are unlikely to have been present in the original specification and design.

2 Details

All references below to sections, page numbers etc refer to [1].

- The index is wildly inaccurate.
- Section 3.3.3 (p19): $AbPurseTransfer$ is defined by

$$AbPurseTransfer \mathrel{\widehat=} AbPurse \setminus_s (\ balance, lost\ )$$

However, *balance* and *lost* are the only two variables in *AbPurse*, so this leaves an empty schema.

- Section 3.3.3 (p20-21): $AbTransferOkayTD$ should include a constraint that $from?$ and $to?$ are in the domain of $abAuthPurse'$. Similarly, $AbTransferLostTD$ should state that $from?$ is in the domain of $abAuthPurse'$.
- Section 3.3.3 (p21): operation $AbTransferLostTD$ constrains the value of $abAuthPurse'\ from?$ by saying that it must be a member of a set. This could equivalently be expressed by saying that it is equal to a μ-expression, as in $AbTransferOkayTD$. (The set has to be a singleton.)
- p32: line 3 of informal text says 'it moves to the *epr* state', while the formal text aboves says $status' = epv$. The formal text is (of course) correct.
- p37: delete the line of informal text above schema $ConWorld$.
- p52: lines 3-4: IFD stands for InterFace Device
- p178, lemma 28.1 (constraint): delete the 2nd sentence of the proof ('From the hypothesis ..').

- p181, lemma 28.6 (logs unchanged): the second hypothesis ($req \rhd ether' = req \rhd ether$) is not required (and so the corresponding informal text can also be deleted). The second half of the proof should also be deleted (final equality on p181 and the lines on p182).

- p207, inference rule B.8 (negation) should contain $false$ in the consequent of the assumption:

Rule

$$\frac{\neg P \vdash false}{\vdash P} \quad negation$$

- p195, Chapter 30: the references in para 3 to 1.4 should all be to 1.2. Also refs to SP6.2 should be deleted (and 'three subgoals' changed to 'two subgoals').

- p63, section 8.2.2. The *AbOp* whose precondition is calculated here is intended to represent an arbitrary abstract operation (other than $AbIgnore$). This *AbOp* should not be confused with the one on p19, which is used in the definition of the abstract operations. (In fact, since there's only one abstract operation other than $AbIgnore$, the *AbOp* on p63 can be replaced with $AbTransfer$.)

References

[1] Susan Stepney, David Cooper, and Jim Woodcock. An electronic purse: Specification, refinement, and proof. Technical monograph PRG-126, Oxford University Computing Laboratory, July 2000.