Project: DRA FRONT END FILTER PROJECT

Title: Proposal for Phase 3

Ref: DS/FMU/FEF/039 *Issue: Revision* : *1.3* *Date:* 5 June 2016

Status: Approved *Type:* Proposal

Keywords:

Author:

Name	*Location*	*Signature*	*Date*
R.D. Arthan	ICL		

Authorisation for Issue:

Name	*Function*	*Signature*	*Date*
R.B. Jones	HAT Manager		

Abstract: A proposal for an extension of Phase 3 of the DRA front end filter project, RSRE 1C/6130, to meet some extensions to the original requirements.

Distribution: HAT FEF File
Simon Wiseman

0 DOCUMENT CONTROL

0.1 Contents List

List of Tables

0.2 Document Cross References

[1] DS/FMU/017. *Secure Database Technical Proposal.* High Assurance Team, ICL Secure Systems, WIN01, 21st January 1992.

[2] DS/FMU/FEF/002. *Errors in the Specifications.* G.M. Prout, ICL Secure Systems, WIN01.

[3] DS/FMU/FEF/036. *Phase II Proof Finale.* R.D. Arthan and G.M. Prout, ICL Secure Systems, WIN01.

[4] *Security Properties of the SWORD secure DBMS Design.* Simon Wiseman, DRA.

0.3 Changes History

Approved issue for DRA.

0.4 Changes Forecast

None.

1 GENERAL

1.1 Scope

DRA have recently identified additional requirements which could be met by extending the scope of phase 3 of the front end filter (FEF) project, RSRE 1C/6130. This document provides a proposal for an extension of Phase 3 to meet these requirements.

1.2 Introduction

In the original proposal for this project, [1], phase 3 comprised solely the production of a final technical report, identified as item 7 in the contract, summarising the achievements of the overall contract.

In recent discussions DRA have identified certain additional requirements which could sensibly be met by ICL in an extension to the scope of phase 3. This document describes a plan of work to meet the extended requirements. The document is structured as follows:

Section 2 — describes the requirements for the extended phase 3.

Section 3 — describes the technical work to be carried out.

Section 4 — describes the timescales for the work and lists the deliverables.

Issue 1.4 Removed dependency on ICL logo font

2 REQUIREMENTS

2.1 Reports

DRA intend to commission a CLEF to report on the potential evaluability of the Front End implementation of SWORD against ITSEC criteria. A report on the overall achievements of the project is therefore required for two different audiences: DRA's MOD sponsors and the CLEF. Since the interests of these two audiences are quite different DRA require two separate final reports as follows:

Managerial Final Report: This is to provide a managerial overview of the achievements of the FEF project and to comment on the cost-effectiveness of the formal methods work.

CLEF Report: This is to provide a technical overview of the formal treatment of the Front End implementation of SWORD and to comment on issues such as the effectiveness of the formal methods work in exposing security-relevant problems with the design and other issues of relevance to evaluation of the SWORD implementation.

2.2 Multi-level Objects

DRA have carried out some research, reported in [4], into extensions of the security policy modelling for SWORD to embrace SSQL queries which are themselves treated as structured multi-level objects. This work endeavours to formulate a non-interference style security policy for systems dealing with such objects and to define a result-labelling property which is intended to capture formally certain intuitions about the desired behaviour of the SWORD implementation. However, as discussed in [4], there are some technical difficulties with the proposed definition of the result-labelling property. DRA would like ICL to give a more formal treatment of the topics discussed in [4] and to investigate how the intuitions behind the result-labelling property may best be formalised.

3 TECHNICAL DESCRIPTION OF WORK

3.1 Reports

Two reports will be prepared as follows.

Managerial Final Report This will provide a managerial overview of the achievements of the FEF project and will comment on the cost-effectiveness of the formal methods work.

CLEF Report This will provide a technical overview of the formal treatment of the Front End implementation of SWORD and will summarise the discussion in the existing documents, [2, 3], of problems discoved during the FEF project. It will also comment upon the relevance of the formal methods work to a development, such as SWORD, which is targetted at an assurance level, such as ITSEC level E3, for which formal methods are not mandated.

3.2 Multi-level Objects

The work on this area will attempt to capture rigorously the intuitions behind the treatment of multi-level objects in [4]. This will proceed as follows.

1. A version of the account in [4] will be formalised. There are some areas, particularly, as regards the structure of objects and the identical object relation where a slightly more abstract treatment might have merits. This will be investigated. The relationship between the multi-level policy and of the single-level non-interference property used in our proof work to date will be investigated.
2. The possibility will be investigated of proving with ProofPower that the result labelling property is consistent with (or even entails) the non-interference property (and is consistent with non-trivial lower bounds on functionality).
3. An investigation will be made into how the phase 2 specifications and proofs might be adapted to the context of the phase 3 formal treatment.

If time permits some attempt will also be made to formulate the over-classification property that mentioned in [4] and to look for any useful general results which hold about the various properties.

4 WORK PLAN

ICL's resource planning for the work plan is based on the supposition that the phase 3 duration will be extended to end of March 1994 and that DRA will authorise the work to begin as soon as possible (and not later than week 1, 1994). It is understood that all technical work shall have been completed by the end of week 10, 1994 at the very latest.

4.1 Outline Work Plan

Table 1 shows a decomposition into subtasks of the work for Phase 3 described in Section 3 above.

Code	Description
WP7a	Prepare Managerial Final Report
WP7b	Prepare CLEF Report
WP7c	Formalise non-interference and result-labelling property for multi-level objects
WP7d	Investigate and report on consistency and other proof opportunities
WP7e	Investigate and report on relationship between phase 2 and phase 3 treatments

Table 1: Tasks in Phase 3

Table 2 shows the major deliverables for Phase 3. Two estimated delivery dates are shown where appropriate. The first is the date (from the start of Phase 3) for a draft for review by DRA-ED, the second is the date for the final version. Note that deliverable D15 is as in the original proposal; all other deliverables are additional to those identified in the original proposal. WP7b is scheduled first to satisfy DRA's request to have the CLEF report early in February.

WP	Code	Description	Draft	Final
WP7a	D15	Managerial Final Report	wk7	wk10
WP7b	D16	CLEF Report	wk4	wk6
WP7c	D17	Formal specification of non-interference and result-labelling property for multi-level objects	wk7	wk10
WP7d	D18	Report on consistency and other proof opportunities	-	wk10
WP7e	D19	Report on relationship between phase 2 and phase 3 treatments	-	wk10

Table 2: Deliverables for Phase 3