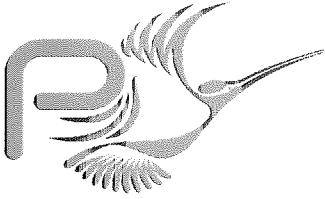


TIS
INCIDENT REPORT

S.P1229.6.36
Page 1 of 3

Project: TIS		Incident Number/Reference: 036	
DESCRIPTION (data and sequence of actions leading to fault, details of actual and expected response)			
<p>In the Formal Specification S.P1229.41.2 and Formal Design S.P1229.50.1 the screen message presented while a user entry operation (long lived) is in progress does not indicate that the administrator cannot perform an action. In particular a logged on administrator is still prompted for an operation request, which will be ignored until the user entry is complete.</p> <p>Found in test: UserEntry6</p> <p>Supporting documentation attached YES/NO Continued YES/NO</p>			
Found during: (use actual project stages)		Reqs /Sys spec/Security Spec/Proof of Spec/Formal Design/INFORMED Design/ Proof of Design/Code/Code Proof/Integration/Sys test/Acceptance	
Date: 13/8/2003		Signature of Originator:	
EVALUATION (Include list of items affected, details of work required, other similar faults, tests to be re-run)			
<p>The screen message should be changed to use the, currently unused, busy message while the system status is anything other than quiescent or waitingRemoveTokenFail.</p> <p>See continuation.</p> <p>Continued YES/NO</p>			
Classification:		Critical/ Major/ Minor / Interfaces / Test / No Fault	
Introduced during: (use actual project stages)		Reqs/Sys spec/Security Spec/Formal Design/INFORMED Design/ Code/Integration/Sys test/Acceptance	
Date: 13/8/2003		Signature of Evaluator:	
RESPONSE (detail how incident is to be resolved, identify cause of problem, related faults and change requests)			
<p>Update as described in the evaluation</p> <p>Continued YES/NO</p>			
Date: 13/8/2003		Signature of Project Manager:	
IMPLEMENTATION (if applicable)			
Assigned to:		Signature of Project Manager:	
Item modified	Date/Version	Signature of Checker	Signature of Integrator
S.P1229.41.2 (Spec)	1.3		
S.P1229.50.1 (Design)	1.2		
S.P1229.50.2 (INFORMED)	1.1		
			Continued YES



Evaluation Continued:

In the **Formal Spec** the UserEntryContext should be changed so that the screen message is set to busy if the current status represents an active user entry state.

To do this we should introduce a new schema *ResetScreenMessage* that defines the appropriate screen message based on the new status and enclave status. Notice that as user entry activities cannot occur concurrently with admin activities we only need concern ourselves with the values when the enclave is quiescent or waitingRemoveAdminTokenFail.

represented equivalently in design

```
ResetScreenMessage
\Delta Internal
\Delta Admin
currentScreen, currentScreen' : Screen

status' \notin { quiescent, waitingRemoveTokenFail } and currentScreen'.screenMsg = busy
or
status' \in { quiescent, waitingRemoveTokenFail } and
(enclaveStatus' = enclaveQuiescent and rolePresent' = nil and currentScreen'.screenMsg = welcomeAdmin
or enclaveStatus' = enclaveQuiescent and rolePresent' /= nil and currentScreen'.screenMsg = requestOp
or enclaveStatus' = waitingRemoveAdminTokenFail and currentScreen'.screenMsg = removeToken
or enclaveStatus' \notin { enclaveQuiescent, waitingRemoveAdminTokenFail }
and currentScreen'.screenMsg = currentScreen.screenMsg)
```

In addition those Admin activities that can occur during the UserEntry (*AdminTokenTimeout* and *AdminTokenTear* as part of *TokenRemovedAdminLogout*) should set the currentScreen'.screenMsg depending on the current status of the UserEntry. This can be achieved by using the above *ResetScreenMessage* schema to update the screen message.

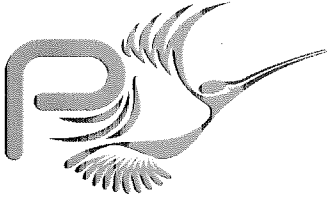
In the **Formal Design** the same changes should be made as for the Specification.

In the **INFORMED Design** a new public operation **ResetScreenMessage** is required in the enclave package – this will set the screen message based on the EnclaveStatus. Also the operation **InProgress** should be added to the public interface of the UserEntry package.

In the **code**

- ✓ **enclave.ads/enclave.adb** add new operation **ResetScreenMessage** and remove the setting of the screen message from the operations that currently implement *AdminTokenTimeout* and *AdminTokenRemovedAdminLogout*.
- ✓ **userentry.ads/adb** make the currently private function **UserEntryInProgress** visible and rename it **InProgress**.
- ✓ **tis.adb** in the operation *Processing* set the screen after calls to *UserEntry.StartEntry*, *UserEntry.Progress* and *Enclave.AdminLogout* this will take the form

```
if UserEntry.UserEntryInProgress then Screen.SetMessage(Screen.Busy);
else Enclave.ResetScreenMessage end if;
```



TIS
INCIDENT REPORT

S.P1229.6.36
Page 3 of 3

IMPLEMENTATION Continued:

Item modified	Date/Version	Signature of Checker	Signature of Integrator
tis.adb	1.15 → 1.16	David Cooper	
enclave.ads	1.11 → 1.12	David Cooper	
enclave.adb	1.12 → 1.13	David Cooper	
userentry.ads	1.10 → 1.11	David Cooper	
userentry.adb	1.12 → 1.13	David Cooper	