



TIS
INCIDENT REPORT

S.P1229.6.35
Page 1 of 1

Project: TIS		Incident Number/Reference: 035	
DESCRIPTION (data and sequence of actions leading to fault, details of actual and expected response)			
In the Formal Design (S.P1229.50.1 v1.1) there is no audit entry associated with AdminTokenTimeout causing the Administrator to be automatically logged off. The audit log would be clearer if such an audit element was raised at this point.			
Found in test: AdminLogout1			
Supporting documentation attached		YES/NO	Continued YES/NO
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)			
In the Formal Design introduce an audit element named AdminTokenExpiredElement this is a warning and should be raised within the schema AdminTokenTimeoutC.			
In the code (audittypes.ads) introduce the new enumeration AdminTokenExpired to the type AuditElements. In (enclave.adb) raise the new audit entry when a Admin Token Timeout is detected.			
		Continued	NO
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)			
Update as described in the evaluation.			
		Continued	YES/NO
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.P1229.50.1	1.2		
audittypes.ads	1.7 → 1.8		
enclave.adb	1.10 → 1.11		
		Continued	YES/NO