Project: TIS	Incident Number/Reference: 033

DESCRIPTION *(data and sequence of actions leading to fault, details of actual and expected response)*

In the Formal Specification S.P1229.41.2 and Formal Design S.P1229.50.1, the intial configuration state is too restrictive. It does not allow anyone to aquire an Auth Certificate so in particular the Security Officer cannot log on to change the configuration data. Futher in the implementation the initial configuration for the audit log should be changed so that re-configuration can be achieved without causing the audit alarm to be raised.

Found in test: UserEntry1

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)*

The Initial configuration should be changed so that use of the system can be made.

See continuation.

Continued YES/~~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.P1229.41.2 (Spec)	1·3		
S.P1229.50.1 (Design)	1·2		
configdata.adb	1·10 → 1·11		

Continued ~~YES~~/NO

Evaluation Continued:

In the **Formal Spec** require that Auth certificates will have a validity period of 2 hours starting from the time of issue. Entry should be permitted at all times. Assuming that durations are measured in 1/10 sec the ~~AlarmSilent, latchUnlock and tokenRemoval durations should all be set to 10 secs.~~ AlarmSilent duration is 1 sec latchUnlock is 15 sec tokenRemovalDuration is 10 sec

This gives the values as follows:

alarmSilentDuration = 10
latchUnlockDuration = 150
tokenRemovalDuraion = 100
authPeriod = PRIVILEGE x{ t: TIME @ t -> t .. t+ 72000 }
entryPeriod = PRIVILEGE x{CLASS x { TIME } }

Change the text introducing the InitConfig to state *The authPeriod and entryPeriod functions are set to enable a securityOfficer to enter the enclave and re-configure the TIS. This configuration will allow Auth Certificates to be generated with a validity of 2 hours from the point of issue (assuming that the unit of time is 1/10sec).*

In the **Formal Design** the intialisation values should be set as follows:

alarmSilentDurationC = 10
latchUnlockDuration = 150
tokenRemovalDuraion = 100
fingerWaitDuration = 100
enclaveClearance = unmarked
minEntryClass = unmarked
maxAuthDuration = 72000
accessPolicy = allHours
systemMaxFar = 1000

The text imidiately preceeding the InitConfigC schema should be changed to be consistent with the new configuration and the Formal Spec text.

In the **Code (configdata.adb** local procedure **SetDefaults**) the default values should be set as follows:

```
LatchUnlockDuration := 150;
MaxAuthPeriod := 72000; - - 2 hours
AccessPolicy := AllHours;
MinPreservedLogSize := 1024 * AuditTypes.SizeAuditElement;
AlarmThresholdSize := 100 * AuditTypes.SizeAuditElement;
SystemMaxFar := 1000;
```

This allows 100 elements to be logged before an audit alarm will be raised.