Project: TIS	Incident Number/Reference: 049

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

There are a number of inconsistencies with the Auth Cert generated by TIS.
1. both the validity times (not before and not after) are always the same.
2. the role and privilage are given as the enumeration literal and not the numeric code.
3. the padding field is omitted from the privilage attributes of the certificate.
4. the signature string has a field AlgorithmID where the recognised (by SPRE) field identifier is AlgoRithmID

Found in test: UserEntry1

Supporting documentation attached ~~YES~~/NO   *Continued* ~~YES~~/NO

Found during: ~~Reqs./Sys spec/Security Spec/Proof of Spec/Formal Design/INFORMED Design/~~
(use actual project stages) ~~Proof of Design/Code/Code Proof/Integration/~~Sys test~~/Acceptance (User Manual)~~

Date: 04/09/2003	Signature of Originator:

EVALUATION *(include list of items affected, details of work required, other similar faults, tests to be re-run)*

In **support\certproc.adb** make the following changes.
1. set the Not After fields to the NotAfter time not the NotBefore time.
2. add lookup tables to convert from enumeration type to numeric code for class and role and use these in the privilage.
3. add a pad field in the privilege attributes of the Auth Cert.
In **support\crypto.adb** change the field identifier from AlgorithmID to AlgoRithmID in the construction of signature.

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: 04/09/2003	Signature of Evaluator:

RESPONSE *(detail how incident is to be resolved, identify cause of problem, related faults and change requests)*

Update as described in evaluation.

Continued ~~YES~~/NO

Date: 04/09/2003	Signature of Project Manager:

IMPLEMENTATION *(if applicable)*

Assigned to: janet	Signature of Project Manager:

Item modified	Date/Version	Signature of Checker	Signature of Integrator
certproc.adb	1·8 → 1·9	David Cook	
crypto.adb	1·14 → 1·15	David Cook	
			Continued NO